

AWS Certified Cloud Practitioner (CPF) Practice Questions – Set 2

1) Multi-AZ deployment is an example of which of the following?

- A. High Availability (**Correct**)
- B. Performance Efficiency
- C. Scale up
- D. Scale out

Correct Options:

High Availability

A system that is available is capable of delivering the designed functionality at a given point in time. Highly available systems are those that can withstand some measure of degradation while still remaining available. On AWS Cloud, you can run instances for an application in a multi-AZ deployment to achieve High Availability.

In Correct Options:

Scale out - The scale out (horizontal scaling) operation refers to an increase in capacity by adding more computers to the system. This is in contrast to a "scale up" operation, which is constrained to running its processes on only one computer; in such systems, the only way to increase performance is to add more resources into one computer in the form of faster (or more) CPUs, memory or storage. Horizontally scalable systems are oftentimes able to outperform vertically scalable systems by enabling parallel execution of workloads and distributing those across many different computers. Auto Scaling Group is an example of Horizontal Scaling on AWS.

Scale up - The scale up (vertical scaling) operation implies adding more resources (like CPU, RAM) to a single node or machine. Example- Resizing an instance of EC2.

Performance Efficiency - Performance Efficiency is the ability to use computing resources efficiently to meet system requirements and to maintain that efficiency as demand changes and technologies evolve.

References:

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

1 2 3 4 5

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

2) Which Amazon Elastic Compute Cloud (Amazon EC2) pricing model is the most cost-effective and flexible with no requirement for a long term resource commitment or upfront payment but still guarantees that instance would not be interrupted?

- A. Dedicated Host
- B. On-demand Instance (**Correct**)
- C. Spot Instance
- D. Reserved Instance (RI)

Correct Options:

On-Demand Instance - An On-Demand Instance is an instance that you use on-demand. You have full control over its lifecycle — you decide when to launch, stop, hibernate, start, reboot, or terminate it. There is no long-term commitment required when you purchase On-Demand Instances. There is no upfront payment and you pay only for the seconds that your On-Demand Instances are running. The price per second for running an On-Demand Instance is fixed. On-demand instances cannot be interrupted.

EC2 Pricing Options Overview: via - <https://aws.amazon.com/ec2/pricing/>

In Correct Options:

Reserved Instance (RI) - Reserved Instance (RI) provides you with significant savings on your Amazon EC2 costs compared to On-Demand Instance pricing. Reserved Instances (RI) are not physical instances, but rather a billing discount applied to the use of On-Demand Instances in your account. You can purchase a Reserved Instance (RI) for a one-year or three-year commitment, with the three-year commitment offering a bigger discount. You will be charged for the entire duration, irrespective of your usage. So this option is not Correct for the given use-case.

Spot Instance - A Spot Instance is an unused EC2 instance that is available for less than the On-Demand price. Because Spot Instances enable you to request unused EC2 instances at steep discounts, you can lower your Amazon EC2 costs significantly. Spot Instances are well-suited for data analysis, batch jobs, background processing, and optional tasks. These can be terminated at short

AWS Certified Cloud Practitioner (CPF) Practice Questions – Set 2

notice, so these are not suitable for critical workloads that need to run at a specific point in time. So this option is not Correct for the given use-case.

Dedicated Host - Amazon EC2 Dedicated Host allows you to use your eligible software licenses from vendors such as Microsoft and Oracle on Amazon EC2 so that you get the flexibility and cost-effectiveness of using your licenses, but with the resiliency, simplicity, and elasticity of AWS. An Amazon EC2 Dedicated Host is a physical server fully dedicated for your use, so you can help address corporate compliance requirement. A Dedicated Host is not cost-efficient compared to an On-Demand instance. So this option is not Correct.

Reference:

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

- 3) What are the fundamental drivers of cost with AWS Cloud ?
- A. Compute, Storage and Inbound Data Transfer
 - B. Compute, Databases and Inbound Data Transfer
 - C. Compute, Storage and Outbound Data Transfer (**Correct**)
 - D. Compute, Databases and Outbound Data Transfer

Correct Options:

Compute, Storage and Outbound Data Transfer

There are three fundamental drivers of cost with AWS: compute, storage, and outbound data transfer. In most cases, there is no charge for inbound data transfer or data transfer between other AWS services within the same region. Outbound data transfer is aggregated across services and then charged at the outbound data transfer rate.

AWS Cloud Pricing Fundamentals: via

- https://d0.awsstatic.com/whitepapers/aws_pricing_overview.pdf

In Correct Options:

Compute, Storage and Inbound Data Transfer

Compute, Databases and Outbound Data Transfer

Compute, Databases and Inbound Data Transfer

These three options contradict the details provided earlier in the , so these options are incorrect.

Reference:

https://d0.awsstatic.com/whitepapers/aws_pricing_overview.pdf

4) A photo sharing web application wants to store thumbnails of user-uploaded images on Amazon Simple Storage Service (Amazon S3). The thumbnails are rarely used but need to be immediately accessible from the web application. The thumbnails can be regenerated easily if they are lost. Which is the most cost-effective way to store these thumbnails on Amazon Simple Storage Service (Amazon S3)?

- A. Use Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) to store the thumbnails (**Correct**)
- B. Use Amazon S3 Standard-Infrequent Access (S3 Standard-IA) to store the thumbnails
- C. Use Amazon S3 Standard to store the thumbnails
- D. Use Amazon S3 Glacier Flexible Retrieval to store the thumbnails

Correct Options:

Use Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) to store the thumbnails

Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) is for data that is accessed less frequently but requires rapid access when needed. Unlike other S3 Storage Classes which store data in a minimum of three Availability Zones (AZs), Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) stores data in a single Availability Zone (AZ) and costs 20% less than Amazon S3 Standard-Infrequent Access (S3 Standard-IA). Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) offers the same high durability, high throughput, and low latency of S3 Standard, with a low per GB storage price and per GB retrieval fee. Although Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) offers less availability than S3 Standard but that's not an issue for the given use-case since the thumbnails can be regenerated easily.

As the thumbnails are rarely used but need to be rapidly accessed when required, so Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) is the best choice for this use-case.

Exam Alert:

Please review this detailed comparison on S3 Storage Classes as you can expect a few questions on this aspect of S3: via
- <https://aws.amazon.com/s3/storage-classes/>

In Correct Options:

Use Amazon S3 Standard-Infrequent Access (S3 Standard-IA) to store the thumbnails - Amazon S3 Standard-Infrequent Access (S3 Standard-IA) storage class is for data that is accessed less frequently but requires rapid access when needed. Amazon S3 Standard-Infrequent Access (S3 Standard-IA) matches the high durability, high throughput, and low latency of S3 Standard, with a low per GB storage price and per GB retrieval fee. Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) costs 20% less than Amazon S3 Standard-Infrequent Access (S3 Standard-IA), so this option is incorrect.

Use Amazon S3 Standard to store the thumbnails - Amazon S3 Standard offers high durability, availability, and performance object storage for frequently accessed data. As described above, Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) is a better fit than Amazon S3 Standard, hence using Amazon S3 standard is ruled out for the given use-case.

Use Amazon S3 Glacier Flexible Retrieval to store the thumbnails - Amazon S3 Glacier Flexible Retrieval is a secure, durable, and low-cost storage class for data archiving. Although Amazon S3 Glacier Flexible Retrieval is cheaper than Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA), however the retrieval time ranges from a minute to hours, so this option is also ruled out for the given use-case.

Reference:

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

5) Which of the following statement is Correct regarding the AWS pricing policy for data transfer charges into or out of an AWS Region?

A. Neither inbound nor outbound data transfer are charged

AWS Certified Cloud Practitioner (CPF) Practice Questions – Set 2

- B. Only inbound data transfer is charged
- C. Only outbound data transfer is charged (**Correct**)
- D. Both inbound data transfer and outbound data transfer are charged

Correct Options:

Only outbound data transfer is charged

One of the main benefits of cloud services is the ability it gives you to optimize costs to match your needs, even as those needs change. AWS services do not have complex dependencies or licensing requirements, so you can get exactly what you need to build innovative, cost-effective solutions using the latest technology.

There are three fundamental drivers of cost with AWS: compute, storage, and outbound data transfer. These characteristics vary somewhat, depending on the AWS product and pricing model you choose. Outbound data to the internet from all AWS regions is billed at region-specific, tiered data transfer rates. Inbound data transfer into all AWS regions from the internet is free.

In Correct Options:

Only inbound data transfer is charged

Both inbound data transfer and outbound data transfer are charged

Neither inbound nor outbound data transfer are charged

These three options contradict the provided above, so these options are incorrect.

Reference:

https://d0.awsstatic.com/whitepapers/aws_pricing_overview.pdf

6) The AWS Well-Architected Framework provides guidance on building cloud based applications using AWS best practices. Which of the following options are the pillars mentioned in the AWS Well-Architected Framework? (Select two)

- A. Reliability (**Correct**)

AWS Certified Cloud Practitioner (CPF) Practice Questions – Set 2

- B. Elasticity
- C. Scalability
- D. Cost Optimization (**Correct**)
- E. Availability

Correct Options:

Reliability

Cost Optimization

The AWS Well-Architected Framework provides guidance on building secure, high-performing, resilient, and efficient infrastructure for cloud based applications. Based on six pillars — operational excellence, security, reliability, performance efficiency, cost optimization and sustainability — the Framework provides a consistent approach for customers and partners to evaluate architectures, and implement designs that will scale over time.

In Correct Options:

Elasticity - Elasticity is the ability to acquire resources as you need them and release resources when you no longer need them. In the cloud, you want to do this automatically.

Availability - A system that is available is capable of delivering the designed functionality at a given point in time. Highly available systems are those that can withstand some measure of degradation while still remaining available.

Scalability - A measurement of a system's ability to grow to accommodate an increase in demand.

These three options are not part of the AWS Well-Architected Framework.

Reference:

https://d1.awsstatic.com/whitepapers/architecture/AWS_Well-Architected_Framework.pdf

- 7) A fleet of Amazon EC2 instances spread across different Availability Zones (AZ) needs to access, edit and share file-based data stored centrally

AWS Certified Cloud Practitioner (CPF) Practice Questions – Set 2

on a system. As a Cloud Practitioner, which AWS service would you recommend for this use-case?

- A. Amazon Simple Storage Service (Amazon S3)
- B. Amazon Elastic Block Store (Amazon EBS)
- C. Amazon Elastic File System (Amazon EFS) (**Correct**)
- D. EC2 Instance Store

Correct Options:

Amazon Elastic File System (Amazon EFS)

Amazon Elastic File System (Amazon EFS) provides a simple, scalable, fully managed, elastic NFS file system. It is built to scale on-demand to petabytes without disrupting applications, growing and shrinking automatically as you add and remove files, eliminating the need to provision and manage capacity to accommodate growth. Amazon EFS is designed to provide massively parallel shared access to thousands of Amazon EC2 instances, enabling your applications to achieve high levels of aggregate throughput and IOPS with consistent low latencies.

How Amazon Elastic File System (Amazon EFS) Works: via
- <https://aws.amazon.com/efs/>

In Correct Options:

Amazon Elastic Block Store (Amazon EBS) - Amazon Elastic Block Store (EBS) is an easy to use, high-performance block storage service designed for use with Amazon Elastic Compute Cloud (EC2) for both throughput and transaction-intensive workloads at any scale. A broad range of workloads, such as relational and non-relational databases, enterprise applications, containerized applications, big data analytics engines, file systems, and media workflows are widely deployed on Amazon EBS. For the Cloud Practitioner exam, you should consider that an EBS volume can only be mounted to one EC2 instance at a time, so this option is not Correct for the given use-case. As a special case, you should note that Amazon EBS Multi-Attach enables you to attach a single Provisioned IOPS SSD (io1 or io2) volume to multiple nitro based instances that are in the same Availability Zone (AZ).

EC2 Instance Store - An instance store provides temporary block-level storage for your EC2 instance. This storage is located on disks that are

physically attached to the host computer. Instance store is ideal for the temporary storage of information that changes frequently, such as buffers, caches, scratch data, and other temporary content, or for data that is replicated across a fleet of instances, such as a load-balanced pool of web servers. Instance storage is temporary, data is lost if instance experiences failure or is terminated. EC2 instance store cannot be used for file sharing between instances.

Amazon Simple Storage Service (Amazon S3) - Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. This means customers of all sizes and industries can use it to store and protect any amount of data for a range of use cases, such as websites, mobile applications, backup and restore, archive, enterprise applications, IoT devices, and big data analytics. As S3 is object-based storage, so it cannot be used for file sharing between instances.

Reference:

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

8) Which characteristic of Cloud Computing imparts the ability to acquire resources as you need and release when you no longer need them?

- A. Reliability
- B. Durability
- C. Resilience
- D. Elasticity (**Correct**)

Correct Options: Elasticity

The ability to acquire resources as you need and release when they are no longer needed is termed as Elasticity of the Cloud. With cloud computing, you don't have to over-provision resources upfront to handle peak levels of business activity in the future. Instead, you provision the number of resources that you need. You can scale these resources up or down instantly to grow and shrink capacity as your business needs change.

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

In Correct Options:

Reliability - Refers to the ability of a system to recover from infrastructure or service disruptions, by dynamically acquiring computing resources to meet demand, and mitigate disruptions.

Durability - Refers to the ability of a system to assure data is stored and data remains consistently on the system as long as it is not changed by legitimate access, i.e. data should not get corrupt or disappear from the cloud because of a system malfunction.

Resiliency - Describes the ability of a system to recover from a failure induced by the load (data or network), attacks, and failures (hardware, software, or network failures).

References:

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

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

9) Which AWS service should be used when you want to run container applications, but want to avoid the operational overhead of scaling, patching, securing, and managing servers?

- A. Amazon Elastic Container Service (Amazon ECS) - EC2 launch type
- B. AWS Lambda
- C. Amazon Elastic Compute Cloud (Amazon EC2)
- D. Amazon Elastic Container Service (Amazon ECS) - Fargate launch type
(Correct)

Correct Options:

Amazon Elastic Container Service (Amazon ECS) - Fargate launch type

AWS Fargate is a serverless compute engine for containers. It works with both Amazon Elastic Container Service (Amazon ECS) and Amazon Elastic Kubernetes Service (Amazon EKS). AWS Fargate makes it easy for you to focus on building your applications. AWS Fargate removes the need to provision and manage servers, lets you specify and pay for resources per application, and improves security through application isolation by design. AWS Fargate

AWS Certified Cloud Practitioner (CPF) Practice Questions – Set 2

allocates the right amount of compute, eliminating the need to choose instances and scale cluster capacity. You only pay for the resources required to run your containers, so there is no over-provisioning and paying for additional servers. AWS Fargate runs each task or pod in its kernel providing the tasks and pods their own isolated compute environment. This enables your application to have workload isolation and improved security by design.

How AWS Fargate Works: via - <https://aws.amazon.com/fargate/>

In Correct Options:

Amazon Elastic Container Service (Amazon ECS) - EC2 launch type -

Amazon Elastic Container Service (Amazon ECS) is a highly scalable, fast, container management service that makes it easy to run, stop, and manage Docker containers and allows you to easily run applications on a managed cluster of Amazon EC2 instances. Unlike AWS Fargate, this is not a fully managed service and you need to manage the underlying servers yourself.

AWS Lambda - AWS Lambda is a compute service that lets you run code without provisioning or managing servers. AWS Lambda executes your code only when needed and scales automatically, from a few requests per day to thousands per second. AWS Lambda does not support running container applications.

Amazon Elastic Compute Cloud (Amazon EC2) - Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud, per-second billing, and access to the underlying OS. It is designed to make web-scale cloud computing easier for developers. Maintenance of the server and its software has to be done by the customer, so this option is ruled out.

Reference:

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

10) A customer has created a VPC and a subnet within AWS Cloud. Which of the following statements is Correct?

- A. A subnet spans all of the Availability Zones (AZ) in the Region whereas an Amazon Virtual Private Cloud (Amazon VPC) spans only one Availability Zone (AZ) in the Region
- B. Both the Amazon Virtual Private Cloud (Amazon VPC) and the subnet span only one Availability Zone (AZ) in the Region

- C. Both the Amazon Virtual Private Cloud (Amazon VPC) and the subnet span all of the Availability Zones (AZ) in the Region
- D. An Amazon Virtual Private Cloud (Amazon VPC) spans all of the Availability Zones (AZ) in the Region whereas a subnet spans only one Availability Zone (AZ) in the Region (**Correct**)

Correct Options:

An Amazon Virtual Private Cloud (Amazon VPC) spans all of the Availability Zones (AZ) in the Region whereas a subnet spans only one Availability Zone (AZ) in the Region

Amazon Virtual Private Cloud (Amazon VPC) is a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including the selection of your IP address range, creation of subnets, and configuration of route tables and network gateways. An Amazon Virtual Private Cloud (Amazon VPC) spans all of the Availability Zones (AZ) in the Region.

A subnet is a range of IP addresses within your Amazon Virtual Private Cloud (Amazon VPC). A subnet spans only one Availability Zone (AZ) in the Region.

Amazon Virtual Private Cloud (Amazon VPC) and Subnet Overview: via - https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Subnets.html

In Correct Options:

Both the Amazon Virtual Private Cloud (Amazon VPC) and the subnet span all of the Availability Zones (AZ) in the Region

Both the Amazon Virtual Private Cloud (Amazon VPC) and the subnet span only one Availability Zone (AZ) in the Region

A subnet spans all of the Availability Zones (AZ) in the Region whereas an Amazon Virtual Private Cloud (Amazon VPC) spans only one Availability Zone (AZ) in the Region

These three options contradict the details provided earlier in the , so these options are incorrect.

Reference:

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

11) Which AWS service helps with global application availability and performance using the AWS global network?

- A. Amazon Route 53
- B. AWS Global Accelerator (**Correct**)
- C. Amazon CloudFront
- D. Elastic Load Balancing (ELB)

Correct Options:

AWS Global Accelerator

AWS Global Accelerator is a service that improves the availability and performance of your applications with local or global users. It provides static IP addresses that act as a fixed entry point to your application endpoints in a single or multiple AWS Regions, such as your Application Load Balancers, Network Load Balancers, or Amazon EC2 instances. AWS Global Accelerator uses the AWS global network to optimize the path from your users to your applications, improving the performance of your traffic by as much as 60%.

AWS Global Accelerator improves performance for a wide range of applications over TCP or UDP by proxying packets at the edge to applications running in one or more AWS Regions. AWS Global Accelerator is a good fit for non-HTTP use cases, such as gaming (UDP), IoT (MQTT), or Voice over IP, as well as for HTTP use cases that specifically require static IP addresses or deterministic, fast regional failover.

How AWS Global Accelerator Works: via - <https://aws.amazon.com/global-accelerator/>

Exam Alert:

Please review the differences between Amazon CloudFront and AWS Global Accelerator: via - <https://aws.amazon.com/global-accelerator/faqs/>

In Correct Options:

Amazon CloudFront - Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a

AWS Certified Cloud Practitioner (CPF) Practice Questions – Set 2

developer-friendly environment. It cannot be used to improve application availability and performance using the AWS global network.

Elastic Load Balancing (ELB) - Elastic Load Balancing (ELB) distributes incoming application or network traffic across multiple targets, such as Amazon EC2 instances, containers, and IP addresses, in multiple Availability Zones. Elastic Load Balancing (ELB) scales your load balancer as traffic to your application changes over time. It can automatically scale to the vast majority of workloads. Elastic Load Balancing (ELB) cannot be used to improve application availability and performance using the AWS global network.

Amazon Route 53 - Amazon Route 53 is a highly available and scalable cloud Domain Name System (DNS) web service. It is designed to give developers and businesses an extremely reliable and cost-effective way to route end users to Internet applications by translating names like `www.example.com` into the numeric IP addresses like `192.0.2.1` that computers use to connect. It cannot be used to improve application availability and performance using the AWS global network.

Reference:

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

12) An organization has a complex IT architecture involving a lot of system dependencies and it wants to track the history of changes to each resource. Which AWS service will help the organization track the history of configuration changes for all the resources?

- A. AWS Config (**Correct**)
- B. AWS Service Catalog
- C. AWS CloudTrail
- D. AWS CloudFormation

Correct Options:

AWS Config

AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. Config continuously monitors and records your AWS resource configurations and allows you to automate the

evaluation of recorded configurations against desired configurations. Think resource-specific history, audit, and compliance; think Config.

With AWS Config, you can do the following: 1. Evaluate your AWS resource configurations for desired settings. 2. Get a snapshot of the current configurations of the supported resources that are associated with your AWS account. 3. Retrieve configurations of one or more resources that exist in your account. 4. Retrieve historical configurations of one or more resources. 5. Receive a notification whenever a resource is created, modified, or deleted. 6. View relationships between resources. For example, you might want to find all resources that use a particular security group.

In Correct Options:

AWS Service Catalog - AWS Service Catalog allows organizations to create and manage catalogs of IT services that are approved for use on AWS. These IT services can include everything from virtual machine images, servers, software, and databases to complete multi-tier application architectures. You cannot use Service Catalog to track changes to each resource on AWS.

AWS CloudFormation - AWS CloudFormation provides a common language to model and provision AWS and third-party application resources in your cloud environment. AWS CloudFormation allows you to use programming languages or a simple text file to model and provision, in an automated and secure manner, all the resources needed for your applications across all Regions and accounts. Think infrastructure as code; think CloudFormation. You cannot use CloudFormation to track changes to each resource on AWS.

AWS CloudTrail - AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. CloudTrail provides the event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command-line tools, and other AWS services. Think account-specific activity and audit; think CloudTrail. You cannot use CloudTrail to track changes to each resource on AWS.

Reference:

<https://docs.aws.amazon.com/config/latest/developerguide/WhatIsConfig.html>

AWS Certified Cloud Practitioner (CPF) Practice Questions – Set 2

13) Which of the following statements are Correct about the AWS root user account? (Select two)

- A. Root user account gets unrestricted permissions when the account is created, but these can be restricted using IAM policies
- B. Root user credentials should only be shared with managers requiring administrative responsibilities to complete their jobs
- C. Root user account password cannot be changed once it is set
- D. Root user access credentials are the email address and password used to create the AWS account (**Correct**)
- E. It is highly recommended to enable Multi-Factor Authentication (MFA) for root user account (**Correct**)

Correct Options:

Root user access credentials are the email address and password used to create the AWS account

It is highly recommended to enable Multi Factor Authentication (MFA) for root user account

The Email address and the password used for signing up for AWS services are the AWS root user account credentials. Root user account, therefore, has full permissions on all AWS resources under that account. Restricting root user account access is not possible. As a best practice, Multi-Factor Authentication (MFA) should be set on the root user account. The root user account password can be changed after account creation. For all employees performing various administrative jobs, create individual user accounts using AWS IAM, and give administrative permissions as needed.

AWS Root User Account Security Best Practices:

via - https://docs.aws.amazon.com/IAM/latest/UserGuide/id_root-user.html

via - <https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#lock-away-credentials>

In Correct Options:

Root user account password cannot be changed once it is set - This is incorrect. Like any other user credentials, the root user password can be changed after creation.

Root user credentials should only be shared with managers requiring administrative responsibilities to complete their jobs - This is a dangerous practice. Root user credentials should only be used only for some limited account-specific activity and root user credentials should be never be shared with anyone.

Root user account gets unrestricted permissions when the account is created, but these can be restricted using IAM policies - Root user account permissions cannot be restricted, whoever has access to these credentials can perform any operation for that AWS account. The root user credentials should be kept safely.

References:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_root-user.html

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

14) Which of the following options can be used to access and manage all AWS services (Select three)?

- A. AWS Systems Manager
- B. AWS Command Line Interface (AWS CLI) (**Correct**)
- C. AWS Software Development Kit (SDK) (**Correct**)
- D. AWS Management Console (**Correct**)
- E. Amazon API Gateway
- F. AWS Secrets Manager

Correct Options:

AWS services can be accessed in three different ways:

AWS Management Console - This is a simple web interface for accessing AWS services.

AWS Command Line Interface (AWS CLI) - You can access AWS services from the command line and automate service management with scripts.

AWS Software Development Kit (SDK) - You can also access via AWS SDK that provides language-specific abstracted APIs for AWS services.

In Correct Options:

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

AWS Secrets Manager - AWS Secrets Manager helps you protect secrets needed to access your applications, services, and IT resources. The service enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle. Users and applications retrieve secrets with a call to AWS Secrets Manager APIs, eliminating the need to hardcode sensitive information in plain text.

Amazon API Gateway - Amazon API Gateway is a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale.

15) A developer has written a simple web application in PHP and he wants to just upload his code to AWS Cloud and have AWS handle the deployment automatically but still wants access to the underlying operating system for further enhancements. As a Cloud Practitioner, which of the following AWS services would you recommend for this use-case?

- A. AWS Elastic Beanstalk (**Correct**)
- B. Amazon Elastic Compute Cloud (Amazon EC2)
- C. AWS CloudFormation
- D. Amazon Elastic Container Service (Amazon ECS)

Correct Options:

AWS Elastic Beanstalk

AWS Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services developed with Java, .NET, PHP, Node.js, Python, Ruby, Go, and Docker on familiar servers such as Apache, Nginx, Passenger, and IIS. Simply upload your code and AWS Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring. At the same time, you retain full control over the AWS resources powering your application and can access the underlying resources at any time. There is no additional charge for AWS Elastic Beanstalk - you pay only for the AWS resources needed to store and run your applications.

Key Benefits of AWS Elastic Beanstalk: via
- <https://aws.amazon.com/elasticbeanstalk/>

In Correct Options:

AWS CloudFormation - AWS CloudFormation allows you to use programming languages or a simple text file (in YAML or JSON format) to model and provision, in an automated and secure manner, all the resources needed for your applications across all Regions and accounts. Think infrastructure as code; think CloudFormation. This is very different from Beanstalk where you just upload your application code and Beanstalk automatically figures out what resources are required to deploy that application. In AWS CloudFormation, you have to explicitly specify which resources you want to provision.

Amazon Elastic Compute Cloud (Amazon EC2) - Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud, per-second billing, and access to the underlying OS. It is designed to make web-scale cloud computing easier for developers. Maintaining the server and its software has to be done by the customer. EC2 cannot handle the application deployment automatically, so this option is not Correct.

Amazon Elastic Container Service (Amazon ECS) - Amazon Elastic Container Service (Amazon ECS) is a highly scalable, fast, container management service that makes it easy to run, stop, and manage Docker containers on a cluster. Amazon Elastic Container Service (Amazon ECS) cannot handle the application deployment automatically, so this option is not Correct.

Reference:

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

16) Which of the following use-cases is NOT supported by Amazon Rekognition?

- A. Quickly resize photos to create thumbnails (**Correct**)
- B. Identify person in a photo
- C. Detect text in a photo
- D. Label objects in a photo

Correct Options:

Quickly resize photos to create thumbnails

You cannot use Amazon Rekognition to resize photos to create thumbnails.

With Amazon Rekognition, you can identify objects, people, text, scenes, and activities in images and videos, as well as detect any inappropriate content. Amazon Rekognition also provides highly accurate facial analysis and facial search capabilities that you can use to detect, analyze, and compare faces for a wide variety of user verification, people counting, and public safety use cases.

Amazon Rekognition Use-Cases:

via - <https://aws.amazon.com/rekognition/>

via - <https://aws.amazon.com/rekognition/>

In Correct Options:

Identify person in a photo

Detect text in a photo

Label objects in a photo

As mentioned in the above, Amazon Rekognition can be used to build solutions for these use-cases.

Reference: <https://aws.amazon.com/rekognition/>

17) Which of the following statements are true about AWS Lambda? (Select two)

- A. AWS Lambda allows you to install databases on the underlying serverless Operating System
- B. AWS Lambda allows you to orchestrate and manage Docker containers to facilitate complex containerized applications on AWS
- C. AWS Lambda lets you run code without provisioning or managing servers (**Correct**)
- D. AWS Lambda provides access to the underlying operating system to control its behavior through code
- E. You pay for the compute time you consume for AWS Lambda (**Correct**)

Correct Options:

AWS Lambda lets you run code without provisioning or managing servers

You pay for the compute time you consume for AWS Lambda

AWS Lambda is a compute service that lets you run code without provisioning or managing servers. AWS Lambda executes your code only when needed and scales automatically, from a few requests per day to thousands per second. You pay for the compute time and the number of requests for your Lambda function - there is no charge when your code is not running. With AWS Lambda, you can run code for virtually any type of application or backend service - all with zero administration. AWS Lambda runs your code on a high-availability compute infrastructure and performs all of the administration of the compute resources, including server and operating system maintenance, capacity provisioning and automatic scaling, code monitoring and logging.

How AWS Lambda Works: via - <https://aws.amazon.com/lambda/>

In Correct Options:

AWS Lambda allows you to install databases on the underlying serverless Operating System - AWS Lambda is a serverless compute service offered by AWS. Since the underlying hardware is only provisioned for the time of compute, it is not possible to install a database.

AWS Certified Cloud Practitioner (CPF) Practice Questions – Set 2

AWS Lambda allows you to orchestrate and manage Docker containers to facilitate complex containerized applications on AWS

- AWS Lambda is a serverless compute service offered by AWS. While AWS Lambda can be used to package and deploy Lambda functions as container images of up to 10 GB in size. But AWS Lambda cannot be used to orchestrate and manage Docker containers. Amazon ECS is better suited for this use-case.

AWS Lambda provides access to the underlying operating system to control its behavior through code

- AWS Lambda is a serverless compute service offered by AWS. It is serverless, so the underlying operating system is not accessible. Amazon Beanstalk or Amazon EC2 services should be used if you need to access the underlying operating system.

Reference:

<https://docs.aws.amazon.com/lambda/latest/dg/welcome.html>

18) A retail company has multiple AWS accounts for each of its departments. Which of the following AWS services can be used to set up consolidated billing and a single payment method for these AWS accounts?

- A. AWS Organizations (**Correct**)
- B. AWS Cost Explorer
- C. AWS Secrets Manager
- D. AWS Budgets

Correct Options:

AWS Organizations

AWS Organizations helps you to centrally manage billing; control access, compliance, and security; and share resources across your AWS accounts. Using AWS Organizations, you can automate account creation, create groups of accounts to reflect your business needs, and apply policies for these groups for governance. You can also simplify billing by setting up a single payment method for all of your AWS accounts. AWS Organizations is available to all AWS customers at no additional charge.

Key Features of AWS Organizations: via
- <https://aws.amazon.com/organizations/>

In Correct Options:

AWS Cost Explorer - AWS Cost Explorer has an easy-to-use interface that lets you visualize, understand, and manage your AWS costs and usage over time. AWS Cost Explorer includes a default report that helps you visualize the costs and usage associated with your top five cost-accruing AWS services, and gives you a detailed breakdown of all services in the table view. The reports let you adjust the time range to view historical data going back up to twelve months to gain an understanding of your cost trends. You cannot use AWS Cost Explorer to set up consolidated billing and a single payment method for multiple AWS accounts.

AWS Budgets - AWS Budgets gives the ability to set custom budgets that alert you when your costs or usage exceed (or are forecasted to exceed) your budgeted amount. You can also use AWS Budgets to set reservation utilization or coverage targets and receive alerts when your utilization drops below the threshold you define. Budgets can be created at the monthly, quarterly, or yearly level, and you can customize the start and end dates. You can further refine your budget to track costs associated with multiple dimensions, such as AWS service, linked account, tag, and others. You cannot use AWS Budgets to set up consolidated billing and a single payment method for multiple AWS accounts.

AWS Secrets Manager - AWS Secrets Manager helps you protect secrets needed to access your applications, services, and IT resources. The service enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle. You cannot use AWS Secrets Manager to set up consolidated billing and a single payment method for multiple AWS accounts.

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

- 19) AWS Compute Optimizer delivers recommendations for which of the following AWS resources? (Select two)
- A. Amazon Elastic Block Store (Amazon EBS), AWS Lambda functions
(Correct)
 - B. Amazon Elastic Compute Cloud (Amazon EC2) instances, Amazon Elastic File System (Amazon EFS)
 - C. AWS Lambda functions, Amazon Simple Storage Service (Amazon S3)
 - D. Amazon Elastic Compute Cloud (Amazon EC2) instances, Amazon EC2 Auto Scaling groups (Correct)

E. Amazon Elastic File System (Amazon EFS), AWS Lambda functions

Correct Options:

Amazon Elastic Compute Cloud (Amazon EC2) instances, Amazon EC2 Auto Scaling groups

Amazon Elastic Block Store (Amazon EBS), AWS Lambda functions

AWS Compute Optimizer helps you identify the optimal AWS resource configurations, such as Amazon EC2 instance types, Amazon EBS volume configurations, and AWS Lambda function memory sizes, using machine learning to analyze historical utilization metrics. AWS Compute Optimizer delivers recommendations for selected types of EC2 instances, EC2 Auto Scaling groups, Amazon EBS volumes, and AWS Lambda functions.

AWS Compute Optimizer calculates an individual performance risk score for each resource dimension of the recommended instance, including CPU, memory, EBS throughput, EBS IOPS, disk throughput, disk throughput, network throughput, and network packets per second (PPS).

AWS Compute Optimizer provides EC2 instance type and size recommendations for EC2 Auto Scaling groups with a fixed group size, meaning desired, minimum, and maximum are all set to the same value and have no scaling policy attached.

AWS Compute Optimizer supports IOPS and throughput recommendations for General Purpose (SSD) (gp3) volumes and IOPS recommendations for Provisioned IOPS (io1 and io2) volumes.

AWS Compute Optimizer helps you optimize two categories of Lambda functions. The first category includes Lambda functions that may be over-provisioned in memory sizes. The second category includes compute-intensive Lambda functions that may benefit from additional CPU power.

In Correct Options:

Amazon Elastic Compute Cloud (Amazon EC2) instances, Amazon Elastic File System (Amazon EFS)

Amazon Elastic File System (Amazon EFS), AWS Lambda functions

AWS Lambda functions, Amazon Simple Storage Service (Amazon S3)

AWS Certified Cloud Practitioner (CPF) Practice Questions – Set 2

AWS Compute Optimizer does not provide optimization recommendations for S3 and EFS, so these options are incorrect.

Reference:

<https://aws.amazon.com/compute-optimizer/faqs/>

- 20) Which of the following statement is Correct for a Security Group and a Network Access Control List (Network ACL)?
- A. Security Group acts as a firewall at the VPC level whereas Network Access Control List (Network ACL) acts as a firewall at the Availability Zone (AZ) level
 - B. Security Group acts as a firewall at the subnet level whereas Network Access Control List (Network ACL) acts as a firewall at the instance level
 - C. Security Group acts as a firewall at the Availability Zone (AZ) level whereas Network Access Control List (Network ACL) acts as a firewall at the VPC level
 - D. Security Group acts as a firewall at the instance level whereas Network Access Control List (Network ACL) acts as a firewall at the subnet level **(Correct)**

Correct Options:

Security Group acts as a firewall at the instance level whereas Network Access Control List (Network ACL) acts as a firewall at the subnet level

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. When you launch an instance in a VPC, you can assign up to five security groups to the instance. Security groups act at the instance level, not the subnet level. A network access control list (network ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets (i.e. it works at subnet level).

Security Group Overview: via

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

Network Access Control List (network NACL) Overview: via

- <https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html>

In Correct Options:

Security Group acts as a firewall at the subnet level whereas Network Access Control List (Network ACL) acts as a firewall at the instance level - As explained above, the security group acts at the instance level and network access control list (network ACL) is at the subnet level.

Security Group acts as a firewall at the VPC level whereas Network Access Control List (Network ACL) acts as a firewall at the Availability Zone (AZ) level - As explained above, the security group acts at the instance level and network access control list (network ACL) is at the subnet level.

Security Group acts as a firewall at the Availability Zone (AZ) level whereas Network Access Control List (Network ACL) acts as a firewall at the VPC level - As explained above, the security group acts at the instance level and network access control list (network ACL) is at the subnet level.

References:

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

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html>

21) Which AWS service can be used to provision resources to run big data workloads on Hadoop clusters?

- A. AWS Step Functions
- B. Amazon EMR (**Correct**)
- C. Amazon Elastic Compute Cloud (Amazon EC2)
- D. AWS Batch

Correct Options:

Amazon EMR

Amazon EMR is the industry-leading cloud big data platform for processing vast amounts of data using open source tools such as Hadoop, Apache Spark, Apache Hive, Apache HBase, Apache Flink, Apache Hudi, and Presto. Amazon EMR can be used to provision resources to run big data workloads on Hadoop clusters.

In Correct Options:

AWS Certified Cloud Practitioner (CPF) Practice Questions – Set 2

AWS Step Functions - AWS Step Functions service lets you coordinate multiple AWS services into serverless workflows. You can design and run workflows that stitch together services such as AWS Lambda, AWS Glue and Amazon SageMaker.

AWS Step Functions Overview: via - <https://aws.amazon.com/step-functions/>

AWS Batch - You can use AWS Batch to plan, schedule and execute your batch computing workloads across the full range of AWS compute services. AWS Batch dynamically provisions the optimal quantity and type of compute resources (e.g., CPU or memory optimized instances) based on the volume and specific resource requirements of the batch jobs submitted. AWS Batch provisions compute resources and optimizes the job distribution based on the volume and resource requirements of the submitted batch jobs.

Please review the common use-cases for AWS Batch: via

- <https://aws.amazon.com/batch/>

Exam Alert:

Understand the difference between AWS Step Functions and AWS Batch. You may get questions to choose one over the other. AWS Batch runs batch computing workloads by provisioning the compute resources. AWS Step Functions does not provision any resources. AWS Step Functions only orchestrates AWS services required for a given workflow. You cannot use AWS Step Functions to plan, schedule and execute your batch computing workloads by provisioning underlying resources.

Amazon Elastic Compute Cloud (Amazon EC2) - Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the AWS cloud. You can use Amazon Elastic Compute Cloud (Amazon EC2) to provision virtual servers on AWS Cloud. You cannot use Amazon Elastic Compute Cloud (Amazon EC2) to plan, schedule and execute your batch computing workloads by provisioning underlying resources.

References:

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

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

<https://aws.amazon.com/step-functions/>

AWS Certified Cloud Practitioner (CPF) Practice Questions – Set 2

- 22) Which tool will help you review your workloads against current AWS best practices for cost optimization, security, and performance improvement and then obtain advice to architect them better?
- A. Amazon Inspector
 - B. Amazon CloudWatch
 - C. AWS Cost Explorer
 - D. AWS Trusted Advisor (**Correct**)

Correct Options:

AWS Trusted Advisor

AWS Trusted Advisor is an online tool that provides you real-time guidance to help you provision your resources following AWS best practices on cost optimization, security, fault tolerance, service limits, and performance improvement. Whether establishing new workflows, developing applications, or as part of ongoing improvement, recommendations provided by Trusted Advisor regularly help keep your solutions provisioned optimally. All AWS customers get access to the seven core Trusted Advisor checks to help increase the security and performance of the AWS environment.

How Trusted Advisor Works: via

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

AWS Trusted Advisor Recommendations: via

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

In Correct Options:

AWS Cost Explorer - AWS Cost Explorer lets you explore your AWS costs and usage at both a high level and at a detailed level of analysis, and empowering you to dive deeper using several filtering dimensions (e.g., AWS Service, Region, Linked Account). Cost Explorer does not offer any recommendations vis-a-vis AWS best practices for cost optimization, security, and performance improvement.

Amazon CloudWatch - Amazon CloudWatch is a monitoring and observability service built for DevOps engineers, developers, site reliability engineers (SREs), and IT managers. CloudWatch provides data and actionable insights to monitor applications, respond to system-wide performance

AWS Certified Cloud Practitioner (CPF) Practice Questions – Set 2

changes, optimize resource utilization, and get a unified view of operational health. This is an excellent service for building Resilient systems. Think resource performance monitoring, events, and alerts; think CloudWatch. CloudWatch does not offer any recommendations vis-a-vis AWS best practices for cost optimization, security, and performance improvement.

Amazon Inspector - Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for exposure, vulnerabilities, and deviations from best practices. Amazon Inspector cannot be used to prevent Distributed Denial-of-Service (DDoS) attack. Inspector does not offer any recommendations vis-a-vis AWS best practices for cost optimization, security, and performance improvement.

Reference:

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

23) Which AWS service can be used to store, manage, and deploy Docker container images?

- A. Amazon Elastic Compute Cloud (Amazon EC2)
- B. Amazon Elastic Container Registry (Amazon ECR) (**Correct**)
- C. Amazon Elastic Container Service (Amazon ECS)
- D. AWS Lambda

Correct Options:

Amazon Elastic Container Registry (Amazon ECR) - Amazon Elastic Container Registry (Amazon ECR) can be used to store, manage, and deploy Docker container images. Amazon Elastic Container Registry (Amazon ECR) eliminates the need to operate your container repositories. You can then pull your docker images from Amazon Elastic Container Registry (Amazon ECR) and run those on Amazon Elastic Container Service (Amazon ECS).

Please see this schematic diagram to understand how Amazon Elastic Container Registry (Amazon ECR) works: via - <https://aws.amazon.com/ecr/>

In Correct Options:

Amazon Elastic Container Service (Amazon ECS) - Amazon Elastic Container Service (Amazon ECS) is a highly scalable, fast, container management service

AWS Certified Cloud Practitioner (CPF) Practice Questions – Set 2

that makes it easy to run, stop, and manage Docker containers on a cluster. You cannot use Amazon Elastic Container Service (Amazon ECS) to store and deploy docker container images.

Please see this schematic diagram to understand how Amazon Elastic Container Service (Amazon ECS) works: via - <https://aws.amazon.com/ecs/>

Amazon Elastic Compute Cloud (Amazon EC2) - Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the AWS cloud. You can use EC2 to provision virtual servers on AWS Cloud. You cannot use EC2 to store and deploy docker container images.

AWS Lambda - AWS Lambda lets you run code without provisioning or managing servers. You pay only for the compute time you consume. You cannot use AWS Lambda to store and deploy docker container images.

References:

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

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

24) Which of the following AWS services allows a database to have flexible schema and supports document data models?

- A. Amazon Relational Database Service (Amazon RDS)
- B. Amazon Aurora
- C. Amazon DynamoDB (**Correct**)
- D. Amazon Redshift

Correct Options:

Amazon DynamoDB

Amazon DynamoDB is a NoSQL database that supports key-value and document data models and enables developers to build modern, serverless applications that can start small and scale globally to support petabytes of data and tens of millions of read and write requests per second.

Amazon DynamoDB supports both key-value and document data models. This enables Amazon DynamoDB to have a flexible schema, so each row can have any number of columns at any point in time. This allows you to easily adapt

the tables as your business requirements change, without having to redefine the table schema as you would in relational databases.

In Correct Options:

Amazon Relational Database Service (Amazon RDS) - Amazon Relational Database Service (Amazon RDS) is an AWS service for relational databases. Schema change on a relational database is not easy and straight-forward as it is on a NoSQL database. Amazon Relational Database Service (Amazon RDS) does not support flexible schema.

Amazon Redshift - Amazon Redshift is a fully-managed petabyte-scale cloud-based data warehouse product designed for large scale data set storage and analysis. Amazon Redshift does not support flexible schema.

Amazon Aurora - Amazon Aurora is an AWS service for relational databases. Schema change on a relational database is not easy and straight-forward as it is on a NoSQL database. Amazon Aurora does not support flexible schema.

Reference:

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

- 25) A company's flagship application runs on a fleet of Amazon Elastic Compute Cloud (Amazon EC2) instances. As per the new policies, the system administrators are looking for the best way to provide secure shell access to Amazon Elastic Compute Cloud (Amazon EC2) instances without opening new ports or using public IP addresses.

Which tool/service will help you achieve this requirement?

- A. Amazon Route 53
- B. Amazon Inspector
- C. AWS Systems Manager Session Manager (**Correct**)
- D. Amazon Elastic Compute Cloud (Amazon EC2) Instance Connect

Correct Options:

AWS Systems Manager Session Manager

AWS Systems Manager Session Manager is a fully-managed service that provides you with an interactive browser-based shell and CLI experience. It

AWS Certified Cloud Practitioner (CPF) Practice Questions – Set 2

helps provide secure and auditable instance management without the need to open inbound ports, maintain bastion hosts, and manage SSH keys. AWS Systems Manager Session Manager helps to enable compliance with corporate policies that require controlled access to instances, increase security and auditability of access to the instances while providing simplicity and cross-platform instance access to end-users.

In Correct Options:

Amazon Elastic Compute Cloud (Amazon EC2) Instance Connect - Amazon Elastic Compute Cloud (Amazon EC2) Instance Connect provides a simple and secure way to connect to your Linux instances using Secure Shell (SSH). With EC2 Instance Connect, you use AWS Identity and Access Management (IAM) policies and principals to control SSH access to your instances, removing the need to share and manage SSH keys. EC2 Instance Connect will need port 22 to be open for traffic. Therefore, not the Correct option here.

Amazon Inspector - Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for exposure, vulnerabilities, and deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity. Amazon Inspector cannot provide secure shell access to EC2 instances.

Amazon Route 53 - Amazon Route 53 is a highly available and scalable cloud Domain Name System (DNS) web service. It is designed to give developers and businesses an extremely reliable and cost-effective way to route end users to Internet applications by translating names like `www.example.com` into the numeric IP addresses like `192.0.2.1` that computers use to connect to each other. Amazon Route 53 cannot provide secure shell access to EC2 instances.

Reference:

<https://aws.amazon.com/systems-manager/faq/>

26) Which Amazon Route 53 routing policy would you use to improve the performance for your customers by routing the requests to the AWS endpoint that provides the fastest experience?

- A. Weighted routing
- B. Latency-based routing (**Correct**)

- C. Failover routing
- D. Simple routing

Correct Options:

Latency-based routing

Amazon Route 53 is a highly available and scalable cloud Domain Name System (DNS) web service. It is designed to give developers and businesses an extremely reliable and cost-effective way to route end users to Internet applications by translating names like `www.example.com` into the numeric IP addresses like `192.0.2.1` that computers use to connect to each other.

If your application is hosted in multiple AWS Regions, you can use latency-based routing policy to improve the performance for your users by serving their requests from the AWS Region that provides the lowest latency. To use latency-based routing, you create latency records for your resources in multiple AWS Regions. When Amazon Route 53 receives a DNS query for your domain or subdomain (`example.com` or `acme.example.com`), it determines which AWS Regions you've created latency records for, determines which region gives the user the lowest latency, and then selects a latency record for that region. Amazon Route 53 responds with the value from the selected record, such as the IP address for a web server.

Amazon Route 53 Routing Policy Overview: via
- <https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html>

In Correct Options:

Failover routing - This routing policy is used when you want to configure active-passive failover.

Weighted routing - This routing policy is used to route traffic to multiple resources in proportions that you specify.

Simple routing - With simple routing, you typically route traffic to a single resource, for example, to a web server for your website.

Reference:

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html>

AWS Certified Cloud Practitioner (CPF) Practice Questions – Set 2

- 27) An e-commerce company wants to assess its applications deployed on Amazon Elastic Compute Cloud (Amazon EC2) instances for vulnerabilities and deviations from AWS best practices. Which AWS service can be used to facilitate this?
- A. AWS Trusted Advisor
 - B. AWS CloudHSM
 - C. AWS Secrets Manager
 - D. Amazon Inspector (**Correct**)

Correct Options:

Amazon Inspector

Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for exposure, vulnerabilities, and deviations from best practices.

Overview of Amazon Inspector: via - <https://aws.amazon.com/inspector/>

In Correct Options:

AWS Secrets Manager - AWS Secrets Manager helps you protect secrets needed to access your applications, services, and IT resources. The service enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle. Users and applications retrieve secrets with a call to Secrets Manager APIs, eliminating the need to hardcode sensitive information in plain text. Secrets Manager cannot be used for security assessment of applications deployed on AWS.

AWS CloudHSM - AWS CloudHSM is a cloud-based hardware security module (HSM) that enables you to easily generate and use your encryption keys on the AWS Cloud. With CloudHSM, you can manage your encryption keys using FIPS 140-2 Level 3 validated HSMs. It is a fully-managed service that automates time-consuming administrative tasks for you, such as hardware provisioning, software patching, high-availability, and backups. CloudHSM cannot be used for the security assessment of applications deployed on AWS.

AWS Trusted Advisor - AWS Trusted Advisor is an online tool that provides you real-time guidance to help you provision your resources following AWS

AWS Certified Cloud Practitioner (CPF) Practice Questions – Set 2

best practices on cost optimization, security, fault tolerance, service limits, and performance improvement. Whether establishing new workflows, developing applications, or as part of ongoing improvement, recommendations provided by Trusted Advisor regularly help keep your solutions provisioned optimally. Trusted Advisor cannot be used for assessing vulnerabilities for applications deployed on AWS.

Reference:

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

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

- A. AWS Identity and Access Management (AWS IAM) (**Correct**)
- B. Amazon Simple Storage Service (Amazon S3)
- C. Amazon CloudFront (**Correct**)
- D. Amazon Relational Database Service (Amazon RDS)
- E. Amazon Elastic Compute Cloud (Amazon EC2)

Correct Options:

AWS Identity and Access Management (AWS IAM)

Amazon CloudFront

Most of the services that AWS offers are Region specific. But few services, by definition, need to be in a global scope because of the underlying service they offer. AWS Identity and Access Management (AWS IAM), Amazon CloudFront, Amazon Route 53 and AWS Web Application Firewall (AWS WAF) are some of the global services.

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

Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally

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

In Correct Options:

Amazon Relational Database Service (Amazon RDS) - Amazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and scale a relational database in the cloud. This is a regional service.

Amazon Elastic Compute Cloud (Amazon EC2) - Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud. It comes under Infrastructure as a Service (IaaS) type of Cloud Computing. This is a regional service.

Exam Alert:

Amazon Simple Storage Service (Amazon S3) - Amazon Simple Storage Service (Amazon S3) is a unique service in the sense that it follows a global namespace but the buckets are regional. You specify an AWS Region when you create your Amazon S3 bucket. This is a regional service.

References:

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

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

- 29) A gaming company is looking at a technology/service that can deliver a consistent low-latency gameplay to ensure a great user experience for end-users in various locations.

Which AWS technology/service will provide the necessary low-latency access to the end-users?

- A. AWS Wavelength
- B. AWS Edge Locations
- C. AWS Direct Connect
- D. AWS Local Zones (**Correct**)

Correct Options:

AWS Local Zones

AWS Certified Cloud Practitioner (CPF) Practice Questions – Set 2

AWS Local Zones allow you to use select AWS services, like compute and storage services, closer to more end-users, providing them very low latency access to the applications running locally. AWS Local Zones are also connected to the parent region via Amazon's redundant and very high bandwidth private network, giving applications running in AWS Local Zones fast, secure, and seamless access to the rest of AWS services.

You should use AWS Local Zones to deploy workloads closer to your end-users for low-latency requirements. AWS Local Zones have their connection to the internet and support AWS Direct Connect, so resources created in the Local Zone can serve local end-users with very low-latency communications.

Various AWS services such as Amazon Elastic Compute Cloud (EC2), Amazon Virtual Private Cloud (VPC), Amazon Elastic Block Store (EBS), Amazon FSx, Amazon Elastic Load Balancing, Amazon EMR, Amazon ElastiCache, and Amazon Relational Database Service (RDS) are available locally in the AWS Local Zones. You can also use services that orchestrate or work with local services such as Amazon EC2 Auto Scaling, Amazon EKS clusters, Amazon ECS clusters, Amazon EC2 Systems Manager, Amazon CloudWatch, AWS CloudTrail, and AWS CloudFormation. AWS Local Zones also provide a high-bandwidth, secure connection to the AWS Region, allowing you to seamlessly connect to the full range of services in the AWS Region through the same APIs and toolsets.

In Correct Options:

AWS Edge Locations - An AWS Edge location is a site that CloudFront uses to cache copies of the content for faster delivery to users at any location.

AWS Wavelength - AWS Wavelength extends the AWS cloud to a global network of 5G edge locations to enable developers to innovate and build a whole new class of applications that require ultra-low latency. Wavelength Zones provide a high-bandwidth, secure connection to the parent AWS Region, allowing developers to seamlessly connect to the full range of services in the AWS Region through the same APIs and toolsets.

AWS Direct Connect - AWS Direct Connect is a cloud service that links your network directly to AWS, bypassing the internet to deliver more consistent, lower-latency performance. When creating a new connection, you can choose a hosted connection provided by an AWS Direct Connect Delivery Partner, or choose a dedicated connection from AWS—and deploy at over 100 AWS Direct Connect locations around the world. AWS Direct Connect provides consistently high bandwidth, low-latency access and it is generally used

AWS Certified Cloud Practitioner (CPF) Practice Questions – Set 2

between on-premises data centers and AWS network. Direct Connect is overkill for the given requirement.

Reference:

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

30) Which AWS service enables users to find, buy, and immediately start using software solutions in their AWS environment?

- A. AWS Config
- B. AWS Marketplace (**Correct**)
- C. AWS Systems Manager
- D. AWS OpsWorks

Correct Options:

AWS Marketplace

AWS Marketplace is a digital catalog with thousands of software listings from independent software vendors that make it easy to find, test, buy, and deploy software that runs on AWS. AWS Marketplace includes thousands of software listings from popular categories such as security, networking, storage, machine learning, IoT, business intelligence, database, and DevOps. You can use AWS Marketplace as a buyer (subscriber) or as a seller (provider), or both. Anyone with an AWS account can use AWS Marketplace as a consumer and can register to become a seller.

In Correct Options:

AWS Config - AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. Think resource-specific history, audit, and compliance; think Config.

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

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

Reference:

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

31) A company is using a message broker service on its on-premises application and wants to move this messaging functionality to AWS Cloud. Which of the following AWS services is the right choice to move the existing functionality easily?

- A. Amazon Kinesis Data Streams
- B. Amazon MQ (**Correct**)
- C. Amazon Simple Queue Service (Amazon SQS)
- D. Amazon Simple Notification Service (Amazon SNS)

Correct Options:

Amazon MQ

Amazon MQ is a managed message broker service for Apache ActiveMQ and RabbitMQ that makes it easy to set up and operate message brokers on AWS. Amazon MQ reduces your operational responsibilities by managing the provisioning, setup, and maintenance of message brokers for you. Because Amazon MQ connects to your current applications with industry-standard APIs and protocols, you can easily migrate to AWS without having to rewrite code.

If you're using messaging with existing applications, and want to move the messaging functionality to the cloud quickly and easily, AWS recommends you consider Amazon MQ. It supports industry-standard APIs and protocols so you can switch from any standards-based message broker to Amazon MQ without rewriting the messaging code in your applications. If you are building brand

AWS Certified Cloud Practitioner (CPF) Practice Questions – Set 2

new applications in the cloud, AWS recommends you consider Amazon SQS and Amazon SNS.

How Amazon MQ works: via - <https://aws.amazon.com/amazon-mq/>

In Correct Options:

Amazon Simple Queue Service (Amazon SQS) - Amazon Simple Queue Service (Amazon SQS) offers a reliable, highly scalable hosted queue for storing messages as they travel between computers. Amazon SQS lets you easily move data between distributed application components and helps you build applications in which messages are processed independently (with message-level ack/fail semantics), such as automated workflows.

Amazon Simple Notification Service (Amazon SNS) - Amazon Simple Notification Service (Amazon SNS) is a fully managed messaging service for both application-to-application (A2A) and application-to-person (A2P) communication. The A2A pub/sub functionality provides topics for high-throughput, push-based, many-to-many messaging between distributed systems, microservices, and event-driven serverless applications. Amazon SNS allows applications to send time-critical messages to multiple subscribers through a “push” mechanism, which implies that the receiving applications have to be present and running to receive the messages.

Amazon Kinesis Data Streams - Amazon Kinesis Data Streams enables you to build custom applications that process or analyze streaming data for specialized needs. You can continuously add various types of data such as clickstreams, application logs, and social media to an Amazon Kinesis data stream from hundreds of thousands of sources. Within seconds, the data will be available for your Amazon Kinesis Applications to read and process from the stream.

Reference:

<https://aws.amazon.com/amazon-mq/faqs/>

32) As per the AWS Shared Responsibility Model, which of the following is a responsibility of the customer from a security and compliance point of view?

- A. Availability Zone (AZ) infrastructure management
- B. Configuration management for AWS global infrastructure

- C. Patching/fixing flaws within the AWS infrastructure
- D. Managing patches of the guest operating system on Amazon Elastic Compute Cloud (Amazon EC2) (**Correct**)

Correct Options:

Managing patches of the guest operating system on Amazon Elastic Compute Cloud (Amazon EC2)

Security and Compliance is a shared responsibility between AWS and the customer. This shared model can help relieve the customer's operational burden as AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates.

As per the AWS shared responsibility model, the customer is responsible for security "in" the cloud. Customers that deploy an Amazon EC2 instance are responsible for the management of the guest operating system (including updates and security patches), any application software or utilities installed by the customer on the instances, and the configuration of the AWS-provided firewall (called a security group) on each instance.

Exam Alert:

Please review the Shared Responsibility Model in detail as you can expect multiple questions on the shared responsibility model in the exam: via - <https://aws.amazon.com/compliance/shared-responsibility-model/>

In Correct Options:

Configuration management for AWS global infrastructure

Availability Zone (AZ) infrastructure management

Patching/fixing flaws within the AWS infrastructure

AWS is responsible for "Security of the Cloud". AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services. Hence, all of the above options - Configuration management for AWS global infrastructure, Availability Zone (AZ) infrastructure management, and patching/fixing flaws within the AWS infrastructure are responsibilities of AWS.

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

- 33) Which AWS service publishes up-to-the-minute information on the general status and availability of all AWS services in all the Regions of AWS Cloud?
- A. AWS Health Dashboard – Your account health
 - B. AWS Health Dashboard - service health (**Correct**)
 - C. AWS CloudFormation
 - D. Amazon CloudWatch

Correct Options: AWS Health Dashboard - service health

AWS Health Dashboard - service health is the single place to learn about the availability and operations of AWS services. You can view the overall status of AWS services, and you can sign in to view personalized communications about your particular AWS account or organization.

You can check on this page <https://health.aws.amazon.com/health/status> to get current status information.

In Correct Options:

AWS CloudFormation - AWS CloudFormation allows you to use programming languages or a simple text file to model and provision, in an automated and secure manner, all the resources needed for your applications across all Regions and accounts. Think infrastructure as code; think CloudFormation. CloudFormation does not provide the general status of AWS services availability for all Regions.

AWS Health Dashboard – Your account health - AWS Health Dashboard – Your account health provides alerts and remediation guidance when AWS is experiencing events that may impact you.

Exam Alert:

While the AWS Health Dashboard - service health displays the general status of AWS services; the AWS Health Dashboard – Your account health gives you a personalized view of the performance and availability of the AWS services underlying your AWS resources.

Amazon CloudWatch - Amazon CloudWatch is a monitoring and observability service built for DevOps engineers, developers, site reliability

AWS Certified Cloud Practitioner (CPF) Practice Questions – Set 2

engineers (SREs), and IT managers. CloudWatch provides data and actionable insights to monitor applications, respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health. This is an excellent service for building Resilient systems. Think resource performance monitoring, events, and alerts; think CloudWatch. CloudWatch does not provide the general status of AWS services availability for all Regions.

Reference:

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

34) Which of the following solutions can you use to connect your on-premises network with AWS Cloud (Select two)?

- A. Amazon Virtual Private Cloud (Amazon VPC)
- B. Amazon Route 53
- C. AWS Direct Connect (**Correct**)
- D. AWS Virtual Private Network (VPN) (**Correct**)
- E. Internet Gateway

Correct Options:

AWS Direct Connect - AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect, you can establish private connectivity between AWS and your datacenter, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.

How AWS Direct Connect Works: via
- <https://aws.amazon.com/directconnect/>

AWS Virtual Private Network (VPN) - AWS Virtual Private Network (VPN) solutions establish secure connections between on-premises networks, remote offices, client devices, and the AWS global network. AWS VPN is comprised of two services: AWS Site-to-Site VPN and AWS Client VPN. Together, they deliver a highly-available, managed, and elastic cloud VPN solution to protect your network traffic.

How AWS Client VPN Works: via - <https://aws.amazon.com/vpn/>

How AWS Site-to-Site VPN Works: via - <https://aws.amazon.com/vpn/>

In Correct Options:

Amazon Virtual Private Cloud (Amazon VPC) - 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 the selection of your IP address range, creation of subnets, and configuration of route tables and network gateways. You cannot use Amazon VPC to connect your on-premises network with AWS Cloud.

Internet Gateway - An Internet Gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the internet. Therefore, it imposes no availability risks or bandwidth constraints on your network traffic. You cannot use an Internet Gateway to interconnect your on-premises network with AWS Cloud, hence this option is incorrect.

Amazon Route 53 - Amazon Route 53 is a highly available and scalable cloud Domain Name System (DNS) web service. It is designed to give developers and businesses an extremely reliable and cost-effective way to route end users to Internet applications by translating names like `www.example.com` into the numeric IP addresses like `192.0.2.1` that computers use to connect. You cannot use Amazon Route 53 to connect your on-premises network with AWS Cloud.

References:

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

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

- 35) The engineering team at an IT company wants to monitor the CPU utilization for its fleet of Amazon Elastic Compute Cloud (Amazon EC2) instances and send an email to the administrator if the utilization exceeds 80%. As a Cloud Practitioner, which AWS services would you recommend to build this solution? (Select two)

- A. Amazon CloudWatch (**Correct**)
- B. AWS Lambda

AWS Certified Cloud Practitioner (CPF) Practice Questions – Set 2

- C. Amazon Simple Queue Service (SQS)
- D. Amazon Simple Notification Service (SNS) (**Correct**)
- E. AWS CloudTrail

Correct Options:

Amazon CloudWatch - Amazon CloudWatch is a monitoring and observability service built for DevOps engineers, developers, site reliability engineers (SREs), and IT managers. CloudWatch provides data and actionable insights to monitor applications, respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health. You can create a CloudWatch alarm that sends an email message using Amazon SNS when the alarm changes state from OK to ALARM. The alarm changes to the ALARM state when the average CPU use of an EC2 instance exceeds a specified threshold for consecutive specified periods.

Amazon Simple Notification Service (SNS) - Amazon Simple Notification Service (SNS) is a highly available, durable, secure, fully managed pub/sub messaging service that enables you to decouple microservices, distributed systems, and serverless applications.

How SNS Works: via - <https://aws.amazon.com/sns/>

In Correct Options:

AWS CloudTrail - AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. Think account-specific activity and audit; think CloudTrail. CloudTrail cannot be used to monitor CPU utilization for EC2 instances or send emails.

AWS Lambda - AWS Lambda lets you run code without provisioning or managing servers. You pay only for the compute time you consume. Lambda cannot be used to monitor CPU utilization for EC2 instances or send emails.

Amazon Simple Queue Service (SQS) - Amazon Simple Queue Service (SQS) is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SQS offers two types of message queues - Standard queues vs FIFO queues. SQS cannot be used to monitor CPU utilization for EC2 instances or send emails.

AWS Certified Cloud Practitioner (CPF) Practice Questions – Set 2

References:

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

https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/US_AlarmAtThresholdEC2.html

36) Due to regulatory and compliance reasons, an organization is supposed to use a hardware device for any data encryption operations in the cloud. Which AWS service can be used to meet this compliance requirement?

- A. AWS CloudHSM (**Correct**)
- B. AWS Secrets Manager
- C. AWS Trusted Advisor
- D. AWS Key Management Service (AWS KMS)

Correct Options:

AWS CloudHSM

AWS CloudHSM is a cloud-based Hardware Security Module (HSM) that enables you to easily generate and use your encryption keys on the AWS Cloud. With CloudHSM, you can manage your encryption keys using FIPS 140-2 Level 3 validated HSMs. It is a fully-managed service that automates time-consuming administrative tasks for you, such as hardware provisioning, software patching, high-availability, and backups.

Please review this detailed description for CloudHSM: via - <https://aws.amazon.com/cloudhsm/>

In Correct Options:

AWS Key Management Service (AWS KMS) - AWS Key Management Service (AWS KMS) makes it easy for you to create and manage cryptographic keys and control their use across a wide range of AWS services and in your applications. It is a secure and resilient service that uses hardware security modules that have been validated under FIPS 140-2, or are in the process of being validated, to protect your keys. It cannot be used as a Hardware Security Module for data encryption operations in AWS Cloud.

AWS Secrets Manager - AWS Secrets Manager helps you protect secrets needed to access your applications, services, and IT resources. The service

enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle. Users and applications retrieve secrets with a call to Secrets Manager APIs, eliminating the need to hardcode sensitive information in plain text. Secrets Manager cannot be used as a Hardware Security Module for data encryption operations in AWS Cloud.

AWS Trusted Advisor - AWS Trusted Advisor is an online tool that provides you real-time guidance to help you provision your resources following AWS best practices on cost optimization, security, fault tolerance, service limits, and performance improvement. Whether establishing new workflows, developing applications, or as part of ongoing improvement, recommendations provided by Trusted Advisor regularly help keep your solutions provisioned optimally.

Reference:

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

37) A social media company wants to protect its web application from common web exploits such as SQL injection and cross-site scripting. Which of the following AWS services can be used to address this use-case?

- A. Amazon GuardDuty
- B. AWS CloudWatch
- C. AWS Web Application Firewall (AWS WAF) (**Correct**)
- D. Amazon Inspector

Correct Options:

AWS Web Application Firewall (AWS WAF)

AWS Web Application Firewall (AWS WAF) is a web application firewall that helps protect your web applications or APIs against common web exploits that may affect availability, compromise security, or consume excessive resources. AWS Web Application Firewall (AWS WAF) gives you control over how traffic reaches your applications by enabling you to create security rules that block common attack patterns such as SQL injection or cross-site scripting. You can also use rate-based rules to mitigate the Web layer DDoS attack.

How AWS Web Application Firewall (AWS WAF) Works: via

- <https://aws.amazon.com/waf/>

An SQL injection attack works by exploiting any one of the known SQL vulnerabilities that allow the SQL server to run malicious code. For example, if a SQL server is vulnerable to an injection attack, it may be possible for an attacker to go to a website's search box and type in code that would force the site's SQL server to dump all of its stored usernames and passwords for the site.

Similar to an SQL injection attack, a cross-site scripting attack also involves injecting malicious code into a website, but in this case, the website itself is not being attacked. Instead, the malicious code the attacker has injected only runs in the user's browser when they visit the attacked website, and it goes after the visitor directly, not the website.

In Correct Options:

Amazon GuardDuty

Amazon GuardDuty is a threat detection service that monitors malicious activity and unauthorized behavior to protect your AWS account. Amazon GuardDuty analyzes billions of events across your AWS accounts from AWS CloudTrail (AWS user and API activity in your accounts), Amazon VPC Flow Logs (network traffic data), and DNS Logs (name query patterns). Amazon GuardDuty cannot be used to protect from web exploits such as SQL injection and cross-site scripting.

How Amazon GuardDuty Works: via - <https://aws.amazon.com/guardduty/>

Amazon Inspector - Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for exposure, vulnerabilities, and deviations from best practices. Amazon Inspector cannot be used to protect from web exploits such as SQL injection and cross-site scripting.

Amazon CloudWatch - Amazon CloudWatch is a monitoring and observability service built for DevOps engineers, developers, site reliability engineers (SREs), and IT managers. CloudWatch provides data and actionable insights to monitor applications, respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health. This is an excellent service for building Resilient systems. Think resource performance monitoring, events, and alerts; think CloudWatch. CloudWatch cannot be used to protect from web exploits such as SQL injection and cross-site scripting.

Reference:

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

38) Which of the following is Correct about AWS Developer Support plan?

- A. Allows one contact to open unlimited cases (**Correct**)
- B. Allows unlimited contacts to open unlimited cases
- C. Allows unlimited contacts to open a limited number of cases per month
- D. Allows one contact to open a limited number of cases per month

Correct Options:

Allows one contact to open unlimited cases

AWS Developer Support plan allows one primary contact to open unlimited cases.

In Correct Options:

Allows one contact to open a limited number of cases per month - As mentioned earlier, the AWS Developer Support plan allows one primary contact to open unlimited cases. So this option is incorrect.

Allows unlimited contacts to open unlimited cases - This is true for AWS Business Support, AWS Enterprise On-Ramp Support and AWS Enterprise Support plans. So this is incorrect for AWS Developer Support plan.

Allows unlimited contacts to open a limited number of cases per month - This is a made-up option and has been added as a distractor.

Reference:

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

39) Which of the following are examples of Horizontal Scalability (aka Elasticity)? (Select two)

- A. Modify an EC2 instance type from t2.nano to u-12tb1.metal
- B. Read Replicas in Amazon Relational Database Service (Amazon RDS) (**Correct**)

- C. Modify a Database instance to higher CPU and RAM
- D. Add a bigger CPU to a computer
- E. Elastic Load Balancing (ELB) (**Correct**)

Correct Options:

A "horizontally scalable" system is one that can increase capacity by adding more computers to the system. This is in contrast to a "vertically scalable" system, which is constrained to running its processes on only one computer; in such systems, the only way to increase performance is to add more resources into one computer in the form of faster (or more) CPUs, memory or storage. Horizontally scalable systems are oftentimes able to outperform vertically scalable systems by enabling parallel execution of workloads and distributing those across many different computers.

Elastic Load Balancing (ELB)

Elastic Load Balancing (ELB) automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, IP addresses, and Lambda functions. It can handle the varying load of your application traffic in a single Availability Zone (AZ) or across multiple Availability Zones (AZ). This falls under Horizontal Scaling.

Read Replicas in Amazon Relational Database Service (Amazon RDS)

Amazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and scale a relational database in the cloud. Read replicas allow you to create read-only copies that are synchronized with your master database. You can also place your read replica in a different AWS Region closer to your users for better performance. Read replicas are an example of horizontal scaling of resources.

In Correct Options:

Add a bigger CPU to a computer - As explained above, this comes under vertical scaling since the bigger resource is being added to a single computer or node.

Modify an EC2 instance type from t2.nano to u-12tb1.metal - Enhancing the type of a single Amazon EC2 system is also an example of vertical scaling since the extra capacity is being added to a single instance.

Modify a Database instance to higher CPU and RAM - This is also an example of vertical scaling since the focus is on increasing the capacity of a single machine or instance.

Reference:

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

40) A data analytics company stores its data on Amazon Simple Storage Service (Amazon S3) and wants to do SQL based analysis on this data with minimum effort. As a Cloud Practitioner, which of the following AWS services will you suggest for this use case?

- A. Amazon DynamoDB
- B. Amazon Aurora
- C. Amazon Redshift
- D. Amazon Athena (**Correct**)

Correct Options:

Amazon Athena

Amazon Athena is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL. Amazon Athena is serverless, so there is no infrastructure to manage, and you pay only for the queries that you run.

Key features of Amazon Athena: via - <https://aws.amazon.com/athena/>

To use Amazon Athena, simply point to your data in Amazon Simple Storage Service (Amazon S3), define the schema, and start querying using standard SQL. Most results are delivered within seconds. With Amazon Athena, there's no need for complex ETL jobs to prepare your data for analysis. This makes it easy for anyone with SQL skills to quickly analyze large-scale datasets.

In Correct Options:

Amazon Aurora - Amazon Aurora is a MySQL and PostgreSQL-compatible relational database built for the cloud, that combines the performance and

availability of traditional enterprise databases with the simplicity and cost-effectiveness of open source databases. You cannot use Amazon Aurora for SQL analysis on S3 based data.

Amazon Redshift - Amazon Redshift is the most popular and fastest cloud data warehouse. Though analytics can be run on Redshift, in the current use case, old data is residing on S3, and Athena is the right choice since analytics can be run directly while data is sitting on S3. You cannot use Amazon Redshift for SQL analysis on S3 based data.

Amazon DynamoDB - Amazon DynamoDB is a key-value and document database that delivers single-digit millisecond performance at any scale. It's a fully managed, multi-Region, multi-master, durable database with built-in security, backup and restore, and in-memory caching for internet-scale applications. You cannot use Amazon DynamoDB for SQL analysis on S3 based data.

Reference:

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

41) Which AWS compute service provides the EASIEST way to access resizable compute capacity in the cloud with support for per-second billing and access to the underlying OS?

- A. Amazon Elastic Compute Cloud (Amazon EC2) (**Correct**)
- B. Amazon Elastic Container Service (Amazon ECS)
- C. AWS Lambda
- D. Amazon Lightsail

Correct Options:

Amazon Elastic Compute Cloud (Amazon EC2)

Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud with support for per-second billing. It is the easiest way to provision servers on AWS Cloud and access the underlying OS. Amazon EC2 reduces the time required to obtain and boot new server instances to minutes, allowing you to quickly scale capacity, both up and down, as your computing requirements change.

AWS Certified Cloud Practitioner (CPF) Practice Questions – Set 2

Amazon Elastic Compute Cloud (Amazon EC2) Overview: via
- <https://aws.amazon.com/ec2/>

In Correct Options:

Amazon Elastic Container Service (Amazon ECS) - Amazon Elastic Container Service (Amazon ECS) is a highly scalable, high-performance container management service that supports Docker containers and allows you to easily run applications on a managed cluster of Amazon EC2 instances. Technically, you can access the underlying EC2 instances, but the set up is more complex than just using the EC2 service directly, so this option is ruled out.

How Amazon Elastic Container Service (Amazon ECS) Works: via
- <https://aws.amazon.com/ecs/>

AWS Lambda - AWS Lambda lets you run code without provisioning or managing servers. You pay only for the compute time you consume. AWS Lambda is serverless, so you don't get access to the underlying OS.

Amazon Lightsail - Amazon Lightsail is an easy-to-use cloud platform that offers you everything needed to build an application or website, plus a cost-effective, monthly plan. Amazon Lightsail offers several preconfigured, one-click-to-launch operating systems, development stacks, and web applications, including Linux, Windows OS, and WordPress. Amazon Lightsail comes with monthly payment plans and does not support per second billing, so this option is ruled out.

Reference:

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

42) Which of the following is the Correct statement regarding the AWS Storage services?

- A. Amazon Simple Storage Service (Amazon S3) is object based storage, Amazon Elastic Block Store (Amazon EBS) is file based storage and Amazon Elastic File System (Amazon EFS) is block based storage
- B. Amazon Simple Storage Service (Amazon S3) is object based storage, Amazon Elastic Block Store (Amazon EBS) is block based storage and Amazon Elastic File System (Amazon EFS) is file based storage
(Correct)

AWS Certified Cloud Practitioner (CPF) Practice Questions – Set 2

- C. Amazon Simple Storage Service (Amazon S3) is block based storage, Amazon Elastic Block Store (Amazon EBS) is object based storage and Amazon Elastic File System (Amazon EFS) is file based storage
- D. Amazon Simple Storage Service (Amazon S3) is file based storage, Amazon Elastic Block Store (Amazon EBS) is block based storage and Amazon Elastic File System (Amazon EFS) is object based storage

Correct Options:

Amazon Simple Storage Service (Amazon S3) is object based storage, Amazon Elastic Block Store (Amazon EBS) is block based storage and Amazon Elastic File System (Amazon EFS) is file based storage

Amazon Elastic File System (Amazon EFS) provides a simple, scalable, fully managed, elastic NFS file system.

Amazon Elastic Block Store (Amazon EBS) is an easy to use, high-performance block storage service designed for use with Amazon Elastic Compute Cloud (Amazon EC2) for both throughput and transaction-intensive workloads at any scale.

Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance.

In Correct Options:

Amazon Simple Storage Service (Amazon S3) is block based storage, Amazon Elastic Block Store (Amazon EBS) is object based storage and Amazon Elastic File System (Amazon EFS) is file based storage

Amazon Simple Storage Service (Amazon S3) is object based storage, Amazon Elastic Block Store (Amazon EBS) is file based storage and Amazon Elastic File System (Amazon EFS) is block based storage

Amazon Simple Storage Service (Amazon S3) is file based storage, Amazon Elastic Block Store (Amazon EBS) is block based storage and Amazon Elastic File System (Amazon EFS) is object based storage

These three options contradict the details provided earlier in the , so these options are incorrect.

References:

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

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

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

43) Access Key ID and Secret Access Key are tied to which of the following AWS Identity and Access Management (AWS IAM) entities?

- A. IAM Role
- B. IAM User (**Correct**)
- C. IAM User Group
- D. IAM Policy

Correct Options: IAM User

Access keys are long-term credentials for an IAM user or the AWS account root user. You can use access keys to sign programmatic requests to the AWS CLI or AWS API (directly or using the AWS SDK). Access keys consist of two parts: an access key ID (for example, AKIAIOSFODNN7EXAMPLE) and a secret access key (for example, wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY). As a user name and password, you must use both the access key ID and secret access key together to authenticate your requests. Access Keys are secret, just like a password. You should never share them.

In Correct Options:

IAM Role - An IAM role is similar to an IAM user, in that it is an AWS identity with permission policies that determine what the identity can and cannot do in AWS. However, instead of being uniquely associated with one person, a role is intended to be assumable by anyone who needs it.

IAM User Group - An IAM User Group is a collection of IAM users. Groups let you specify permissions for multiple users, which can make it easier to manage the permissions for those users.

IAM Policy - You manage access in AWS by creating policies and attaching them to IAM identities (users, groups of users, or roles) or AWS resources. A policy is an object in AWS that, when associated with an identity or resource, defines their permissions.

Access keys are not tied to the IAM role, IAM group, or AWS policy. So all three options are incorrect.

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

- 44) A startup is looking for 24x7 phone based technical support for its AWS account. Which of the following is the MOST cost-effective AWS support plan for this use-case?
- A. AWS Business Support (**Correct**)
 - B. AWS Enterprise Support
 - C. AWS Enterprise On-Ramp Support
 - D. AWS Developer Support

Correct Options:

AWS offers four different support plans to cater to each of its customers - AWS Developer Support, AWS Business Support, AWS Enterprise On-Ramp Support and AWS Enterprise Support plans. A basic support plan is included for all AWS customers.

AWS Business Support - You should use the AWS Business Support plan if you have production workloads on AWS and want 24x7 phone, email and chat access to technical support and architectural guidance in the context of your specific use-cases. AWS Business Support plan is the MOST cost-effective option for the given use-case.

Exam Alert:

Please review the differences between the AWS Developer Support, AWS Business Support, AWS Enterprise On-Ramp Support and AWS Enterprise Support plans as you can expect at least a couple of questions on the exam:

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

In Correct Options:

AWS Enterprise On-Ramp Support - You should use the AWS Enterprise On-Ramp Support plan if you have production/business critical workloads in AWS and want 24x7 access to technical support and need expert guidance to grow and optimize in the Cloud. AWS Enterprise On-Ramp Support plan provides 24x7 phone, email and chat access to technical support however it's costlier than the AWS Business Support plan.

AWS Developer Support - You should use the AWS Developer Support plan if you are testing or doing early development on AWS and want the ability to get email based technical support during business hours as well as general architectural guidance as you build and test. This plan does not support 24x7 phone based technical support.

AWS Enterprise Support - You should use the AWS Enterprise Support plan to provide customers with concierge-like service where the main focus is helping the customer achieve their outcomes and find success in the cloud. With AWS Enterprise Support plan, you get 24x7 technical support from high-quality engineers, tools and technology to automatically manage the health of your environment, consultative architectural guidance delivered in the context of your applications and use-cases, and a designated Technical Account Manager (TAM) to coordinate access to proactive/preventative programs and AWS subject matter experts. AWS Enterprise Support plan provides 24x7 phone, email and chat access to technical support however it's costlier than the AWS Business Support plan.

Reference:

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

- 45) Which AWS support plan provides access to a designated Technical Account Manager (TAM)?
- A. AWS Business Support
 - B. AWS Developer Support
 - C. AWS Enterprise Support (**Correct**)
 - D. AWS Enterprise On-Ramp Support

Correct Options:

AWS Enterprise Support

AWS offers four different support plans to cater to each of its customers - AWS Developer Support, AWS Business Support, AWS Enterprise On-Ramp Support and AWS Enterprise Support plans. A basic support plan is included for all AWS customers.

AWS Enterprise Support provides customers with concierge-like service where the main focus is helping the customer achieve their outcomes and find

AWS Certified Cloud Practitioner (CPF) Practice Questions – Set 2

success in the cloud. With AWS Enterprise Support, you get 24x7 technical support from high-quality engineers, tools and technology to automatically manage the health of your environment, consultative architectural guidance delivered in the context of your applications and use-cases, and a designated Technical Account Manager (TAM) to coordinate access to proactive/preventative programs and AWS subject matter experts.

Exam Alert:

Please review the differences between the AWS Developer Support, AWS Business Support, AWS Enterprise On-Ramp Support and AWS Enterprise Support plans as you can expect at least a couple of questions on the exam:

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

In Correct Options:

AWS Developer Support - You should use the AWS Developer Support plan if you are testing or doing early development on AWS and want the ability to get technical support during business hours as well as general architectural guidance as you build and test.

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

AWS Enterprise On-Ramp Support - You should use the AWS Enterprise On-Ramp Support plan if you have production/business critical workloads in AWS and want 24x7 access to technical support and need expert guidance to grow and optimize in the Cloud. With this plan, you get access to a pool of Technical Account Managers to provide proactive guidance, and coordinate access to programs and AWS experts.

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

- 46) An organization deploys its IT infrastructure in a combination of its on-premises data center along with AWS Cloud. How would you categorize this deployment model?
- A. Private deployment
 - B. Cloud deployment
 - C. Hybrid deployment (**Correct**)

D. Mixed deployment

Correct Options:

Hybrid deployment

A hybrid deployment is a way to connect your on-premises infrastructure to the cloud. The most common method of hybrid deployment is between the cloud and existing on-premises infrastructure to extend an organization's infrastructure into the cloud while connecting cloud resources to internal systems.

Overview of Cloud Computing Deployment Models: via
- <https://aws.amazon.com/types-of-cloud-computing/>

In Correct Options:

Cloud deployment - For this type of deployment, a cloud-based application is fully deployed in the cloud, and all parts of the application run in the cloud. Applications in the cloud have either been created in the cloud or have been migrated from an existing infrastructure to take advantage of the benefits of cloud computing.

Private deployment - For this deployment model, resources are deployed on-premises using virtualization technologies. On-premises deployment does not provide many of the benefits of cloud computing but is sometimes sought for its ability to provide dedicated resources.

Mixed deployment - This is a made-up option and has been added as a distractor.

References:

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

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

- 47) What is the primary benefit of deploying an Amazon RDS Multi-AZ database with one standby?
- A. Amazon RDS Multi-AZ protects the database from a regional failure
 - B. Amazon RDS Multi-AZ improves database performance for read-heavy workloads

- C. Amazon RDS Multi-AZ enhances database availability (Correct)
- D. Amazon RDS Multi-AZ reduces database usage costs

Correct Options:

Amazon RDS Multi-AZ enhances database availability

Amazon RDS Multi-AZ deployments provide enhanced availability and durability for Amazon Relational Database Service (Amazon RDS) instances, making them a natural fit for production database workloads. When you provision an Amazon RDS Multi-AZ Instance with one standby, Amazon RDS automatically creates a primary DB Instance and synchronously replicates the data to a standby instance in a different Availability Zone (AZ).

In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete.

How Amazon RDS Multi-AZ Works: via

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

Exam Alert:

Please review the differences between Multi-AZ, Multi-Region and Read Replica deployments for RDS: via

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

In Correct Options:

Amazon RDS Multi-AZ improves database performance for read-heavy workloads

- Amazon RDS Multi-AZ with one standby does not allow read operations from the standby. Read Replicas allow you to create read-only copies that are synchronized with your master database. Read Replicas are used for improved read performance. Therefore, this option is incorrect.

Amazon RDS Multi-AZ protects the database from a regional failure

- You need to use RDS in Multi-Region deployment configuration to protect from a regional failure. Amazon RDS Multi-AZ cannot protect from a regional failure.

Amazon RDS Multi-AZ reduces database usage costs

- Amazon RDS Multi-AZ increases the database costs compared to the standard deployment. So this option is incorrect.

Reference:

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

48) As per the AWS Shared Responsibility Model, which of the following is a responsibility of AWS from a security and compliance point of view?

- A. Edge Location Management (**Correct**)
- B. Server-side Encryption (SSE)
- C. Identity and Access Management
- D. Customer Data

Correct Options:

Edge Location Management

Security and Compliance is a shared responsibility between AWS and the customer. The AWS Shared Responsibility Model can help relieve the customer's operational burden as AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates.

AWS is responsible for security "of" the cloud. This covers their global infrastructure elements including Regions, Availability Zones (AZ), and Edge Locations.

In Correct Options:

Customer Data

Identity and Access Management

Server-side Encryption (SSE)

The customer is responsible for security "in" the cloud. Customers are responsible for managing their data including encryption options and using Identity and Access Management tools for implementing appropriate access control policies as per their organization requirements. For abstracted services, such as Amazon S3 and Amazon DynamoDB, AWS operates the infrastructure layer, the operating system, and platforms, and customers access the endpoints to store and retrieve data. Therefore, these three options fall under

the responsibility of the customer according to the AWS shared responsibility model.

Exam Alert:

Please review the AWS Shared Responsibility Model in detail as you can expect multiple questions on this topic in the exam: via

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

Reference:

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

49) Which of the following AWS services are always free to use (Select two)?

- A. AWS Auto Scaling (**Correct**)
- B. Amazon DynamoDB
- C. AWS Identity and Access Management (AWS IAM) (**Correct**)
- D. Amazon Simple Storage Service (Amazon S3)
- E. Amazon Elastic Compute Cloud (Amazon EC2)

Correct Options:

AWS Identity and Access Management (AWS IAM) - AWS Identity and Access Management (AWS IAM) enables you to manage access to AWS services and resources securely. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources. IAM is a feature of your AWS account offered at no additional charge.

AWS Auto Scaling - AWS Auto Scaling monitors your applications and automatically adjusts the capacity to maintain steady, predictable performance at the lowest possible cost. Using AWS Auto Scaling, it's easy to setup application scaling for multiple resources across multiple services in minutes. AWS Auto Scaling is available at no additional charge. You pay only for the AWS resources needed to run your applications and Amazon CloudWatch monitoring fees.

In Correct Options:

Amazon Elastic Compute Cloud (Amazon EC2) - Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud. It is designed to make web-scale cloud computing easier for developers. This is not a free service. You pay for what you use or depending on the plan you choose.

Amazon Simple Storage Service (Amazon S3) - Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. S3 service is not free and you pay to depend on the storage class you choose for your data.

Amazon DynamoDB - Amazon DynamoDB is a key-value and document database that delivers single-digit millisecond performance at any scale. It's a fully managed, multi-Region, multi-master, durable database with built-in security, backup and restore, and in-memory caching for internet-scale applications. DynamoDB is not free and you are charged for reading, writing, and storing data in your DynamoDB tables, along with any optional features you choose to enable.

References:

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

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

- 50) Which AWS technology/service helps you to scale your resources to match supply with demand while still keeping your cloud solution cost-effective?
- A. AWS CloudFormation
 - B. AWS OpsWorks
 - C. AWS Cost Explorer
 - D. AWS Auto Scaling (Correct)

Correct Options: AWS Auto Scaling

AWS Auto Scaling monitors applications and automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost. Using AWS Auto Scaling, it's easy to setup application scaling for multiple resources across multiple services in minutes. The service provides a simple, powerful user interface that lets you build scaling plans for resources including Amazon EC2 instances and Spot Fleets, Amazon ECS tasks, Amazon DynamoDB tables and indexes, and Amazon Aurora Replicas. AWS Auto Scaling makes scaling

simple with recommendations that allow you to optimize performance, costs, or balance between them.

How AWS Auto Scaling Works: via - <https://aws.amazon.com/autoscaling/>

In Correct Options:

AWS Cost Explorer - AWS Cost Explorer lets you explore your AWS costs and usage at both a high level and at a detailed level of analysis, and empowering you to dive deeper using many filtering dimensions (e.g., AWS Service, Region, Linked Account). It's a handy tool to keep track of costs of AWS resources, but auto-scaling is not part of its feature set.

AWS OpsWorks - 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. OpsWorks cannot auto-scale resources.

AWS CloudFormation - AWS CloudFormation allows you to use programming languages or a simple text file to model and provision, in an automated and secure manner, all the resources needed for your applications across all Regions and accounts. Think infrastructure as code; think CloudFormation. CloudFormation cannot auto-scale resources.

References:

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

<https://aws.amazon.com/aws-cost-management/aws-cost-explorer/>

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

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

51) An online gaming company wants to block users from certain geographies from accessing its content. Which AWS service can be used to accomplish this task?

A. Security group

AWS Certified Cloud Practitioner (CPF) Practice Questions – Set 2

- B. Amazon CloudWatch
- C. AWS Web Application Firewall (AWS WAF) (**Correct**)
- D. AWS Shield

Correct Options:

AWS Web Application Firewall (AWS WAF)

AWS Web Application Firewall (AWS WAF) is a web application firewall that helps protect web applications from attacks by allowing you to configure rules that allow, block, or monitor (count) web requests based on conditions that you define. These conditions include IP addresses, HTTP headers, HTTP body, URI strings, SQL injection, and cross-site scripting. You can use the IP address based match rule to block specific geographies. The accuracy of the IP Address to country lookup database varies by Region. Based on recent tests, AWS mentions that the overall accuracy for the IP address to country mapping is 99.8%.

How AWS Web Application Firewall (AWS WAF) Works: via
- <https://aws.amazon.com/waf/>

In Correct Options:

Amazon CloudWatch - Amazon CloudWatch is a monitoring and observability service built for DevOps engineers, developers, site reliability engineers (SREs), and IT managers. Amazon CloudWatch provides data and actionable insights to monitor applications, respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health. This is an excellent service for building Resilient systems. Think resource performance monitoring, events, and alerts; think CloudWatch. Amazon CloudWatch cannot be used to block users from certain geographies.

AWS Shield - AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS. AWS Shield provides always-on detection and automatic inline mitigations that minimize application downtime and latency, so there is no need to engage AWS Support to benefit from DDoS protection. AWS Shield cannot be used to block users from certain geographies.

Security group - A security group acts as a virtual firewall for your EC2 instances to control incoming and outgoing traffic. Inbound rules control the incoming traffic to your instance, and outbound rules control the outgoing

AWS Certified Cloud Practitioner (CPF) Practice Questions – Set 2

traffic from your instance. Security groups only have "allow" rules. You cannot use the security groups to block users from certain geographies.

Reference:

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

- 52) Which of the following AWS services are part of the AWS Foundation services for the Reliability pillar of the Well-Architected Framework in AWS Cloud? (Select two)
- A. AWS CloudFormation
 - B. AWS CloudTrail
 - C. Amazon CloudWatch
 - D. Service Quotas (**Correct**)
 - E. AWS Trusted Advisor (**Correct**)

Correct Options:

AWS Trusted Advisor

Service Quotas

Foundations are part of the Reliability pillar of the AWS Well-Architected Framework. AWS states that before architecting any system, foundational requirements that influence reliability should be in place. The services that are part of foundations are: Amazon VPC, AWS Trusted Advisor, AWS Service Quotas (formerly called AWS Service Limits).

AWS Trusted Advisor is an online tool that provides you real-time guidance to help you provision your resources following AWS best practices on cost optimization, security, fault tolerance, service limits, and performance improvement. Whether establishing new workflows, developing applications, or as part of ongoing improvement, recommendations provided by Trusted Advisor regularly help keep your solutions provisioned optimally.

Service Quotas enables you to view and manage your quotas for AWS services from a central location. Quotas, also referred to as limits in AWS, are the maximum values for the resources, actions, and items in your AWS account.

AWS Certified Cloud Practitioner (CPF) Practice Questions – Set 2

Each AWS service defines its quotas and establishes default values for those quotas.

In Correct Options:

AWS CloudTrail - AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. CloudTrail provides the event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command-line tools, and other AWS services. Think account-specific activity and audit; think CloudTrail.

AWS CloudFormation - AWS CloudFormation provides a common language to model and provision AWS and third-party application resources in your cloud environment. AWS CloudFormation allows you to use programming languages or a simple text file to model and provision, in an automated and secure manner, all the resources needed for your applications across all Regions and accounts. Think infrastructure as code; think CloudFormation.

Amazon CloudWatch - Amazon CloudWatch is a monitoring and observability service built for DevOps engineers, developers, site reliability engineers (SREs), and IT managers. CloudWatch provides data and actionable insights to monitor applications, respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health. This is an excellent service for building Resilient systems. Think resource performance monitoring, events, and alerts; think CloudWatch.

Reference:

<https://wa.aws.amazon.com/wat.pillar.reliability.en.html>

53) Which AWS service would you use to send alerts when the costs for your AWS account exceed your budgeted amount?

- A. AWS Pricing Calculator
- B. AWS Budgets (**Correct**)
- C. AWS Cost Explorer
- D. AWS Organizations

Correct Options:

AWS Budgets

AWS Budgets gives the ability to set custom budgets that alert you when your costs or usage exceed (or are forecasted to exceed) your budgeted amount. You can also use AWS Budgets to set reservation utilization or coverage targets and receive alerts when your utilization drops below the threshold you define. Budgets can be created at the monthly, quarterly, or yearly level, and you can customize the start and end dates. You can further refine your budget to track costs associated with multiple dimensions, such as AWS service, linked account, tag, and others. Budget alerts can be sent via email and/or Amazon Simple Notification Service (Amazon SNS) topic.

AWS Budgets Overview: via - <https://aws.amazon.com/aws-cost-management/aws-budgets/>

Exam Alert:

It is useful to note the difference between CloudWatch Billing vs AWS Budgets:

CloudWatch Billing Alarms: Sends an alarm when the actual cost exceeds a certain threshold.

AWS Budgets: Sends an alarm when the actual cost exceeds the budgeted amount or even when the cost forecast exceeds the budgeted amount.

In Correct Options:

AWS Cost Explorer - AWS Cost Explorer has an easy-to-use interface that lets you visualize, understand, and manage your AWS costs and usage over time. AWS Cost Explorer includes a default report that helps you visualize the costs and usage associated with your top five cost-accruing AWS services, and gives you a detailed breakdown on all services in the table view. The reports let you adjust the time range to view historical data going back up to twelve months to gain an understanding of your cost trends.

AWS Cost Explorer Reports: via - <https://aws.amazon.com/aws-cost-management/aws-cost-explorer/>

Exam Alert:

Watch out for questions on AWS Cost Explorer vs AWS Budgets. AWS Budgets can alert you when your costs exceed your budgeted amount. Cost Explorer helps you visualize and manage your AWS costs and usage over time.

AWS Organizations - AWS Organizations helps you centrally govern your environment as you grow and scale your workloads on AWS. Whether you are a growing startup or a large enterprise, Organizations helps you to centrally manage billing; control access, compliance, and security; and share resources across your AWS accounts.

AWS Pricing Calculator - AWS Pricing Calculator lets you explore AWS services and create an estimate for the cost of your use cases on AWS. You can model your solutions before building them, explore the price points and calculations behind your estimate, and find the available instance types and contract terms that meet your needs. This enables you to make informed decisions about using AWS. You can plan your AWS costs and usage or price out setting up a new set of instances and services. AWS Pricing Calculator can be accessed at <https://calculator.aws/#/>.

Reference:

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

- 54) An IT company wants to run a log backup process every Monday at 2 AM. The usual runtime of the process is 5 minutes. As a Cloud Practitioner, which AWS services would you recommend to build a serverless solution for this use-case? (Select two)
- A. AWS Systems Manager
 - B. AWS Lambda (**Correct**)
 - C. AWS Step Function
 - D. Amazon Elastic Compute Cloud (Amazon EC2)
 - E. Amazon CloudWatch (**Correct**)

Correct Options:

Amazon CloudWatch - Amazon CloudWatch is a monitoring and observability service built for DevOps engineers, developers, site reliability engineers (SREs), and IT managers. CloudWatch provides data and actionable insights to monitor applications, respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health.

AWS Lambda - AWS Lambda lets you run code without provisioning or managing servers. You pay only for the compute time you consume. The

lambda has a maximum execution time of 15 minutes, so it can be used to run this log backup process.

To build the solution for the given use-case, you can create a CloudWatch Events rule that triggers on a schedule via a cron expression. You can then set the Lambda as the target for this rule.

In Correct Options:

AWS Systems Manager - AWS Systems Manager gives you visibility and control of your infrastructure on AWS. Systems Manager provides a unified user interface so you can view operational data from multiple AWS services and allows you to automate operational tasks across your AWS resources. With Systems Manager, you can group resources, like Amazon EC2 instances, Amazon S3 buckets, or Amazon RDS instances, by application, view operational data for monitoring and troubleshooting, and take action on your groups of resources. Secrets Manager cannot be used to run a process on a schedule.

Amazon Elastic Compute Cloud (Amazon EC2) - Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud with support for per-second billing. It is the easiest way to provision servers on AWS Cloud and access the underlying OS. As the company wants a serverless solution, so this option is ruled out.

AWS Step Function - AWS Step Function lets you coordinate multiple AWS services into serverless workflows. You can design and run workflows that stitch together services such as AWS Lambda, AWS Glue and Amazon SageMaker. Step Function cannot be used to run a process on a schedule.

Reference:

<https://wa.aws.amazon.com/wat.concepts.wa-concepts.en.html>

55) Which policy describes prohibited uses of the web services offered by Amazon Web Services?

- A. AWS Applicable Use Policy
- B. AWS Fair Use Policy
- C. AWS Acceptable Use Policy (**Correct**)
- D. AWS Trusted Advisor

Correct Options:

AWS Acceptable Use Policy

The Acceptable Use Policy describes prohibited uses of the web services offered by Amazon Web Services, Inc. and its affiliates (the "Services") and the website located at <http://aws.amazon.com> (the "AWS Site"). This policy is present at <https://aws.amazon.com/aup/> and is updated on a need basis by AWS.

In Correct Options:

AWS Trusted Advisor - AWS Trusted Advisor is an online tool that provides you real-time guidance to help you provision your resources following AWS best practices on cost optimization, security, fault tolerance, service limits, and performance improvement. Whether establishing new workflows, developing applications, or as part of ongoing improvement, recommendations provided by Trusted Advisor regularly help keep your solutions provisioned optimally. Trusted Advisor does not describe prohibited uses of the web services offered by Amazon Web Services.

AWS Fair Use Policy - This is a made-up option and has been added as a distractor.

AWS Applicable Use Policy - This is a made-up option and has been added as a distractor.

Reference:

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

56) According to the AWS Shared Responsibility Model, which of the following are responsibilities of the customer for Amazon RDS?

- A. Managing the underlying server hardware on which Amazon Relational Database Service (Amazon RDS) runs
- B. Applying patches to the underlying OS
- C. Applying patches to the Amazon Relational Database Service (Amazon RDS) database
- D. Database encryption (**Correct**)

Correct Options:

Security and Compliance is a shared responsibility between AWS and the customer. This shared model can help relieve the customer's operational burden as AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates.

Database encryption - Under the AWS Shared Responsibility Model, customers are responsible for managing their data, including data encryption.

AWS Shared Responsibility Model Overview: via

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

In Correct Options:

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

Amazon Relational Database Service (Amazon RDS) is a managed service that makes it easy to set up, operate, and scale a relational database in the cloud.

Managing the underlying server hardware on which Amazon Relational Database Service (Amazon RDS) runs - Since Amazon Relational Database Service (Amazon RDS) is a managed service, the underlying infrastructure is the responsibility of AWS.

Applying patches to the Amazon Relational Database Service (Amazon RDS) database - Since Amazon Relational Database Service (Amazon RDS) is a managed service, the underlying infrastructure is the responsibility of AWS.

Applying patches to the underlying OS - Since Amazon Relational Database Service (Amazon RDS) is a managed service, the underlying infrastructure is the responsibility of AWS.

Reference:

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

57) Which of the following AWS services comes under the Software as a Service (SaaS) Cloud Computing Type?

A. Amazon Rekognition (**Correct**)

AWS Certified Cloud Practitioner (CPF) Practice Questions – Set 2

- B. AWS Elastic Beanstalk
- C. Elastic Load Balancing (ELB)
- D. Amazon Elastic Compute Cloud (Amazon EC2)

Correct Options: Amazon Rekognition

Cloud Computing can be broadly divided into three types - Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS).

IaaS contains the basic building blocks for cloud IT. It typically provides access to networking features, computers (virtual or on dedicated hardware), and data storage space. IaaS gives the highest level of flexibility and management control over IT resources. Examples - Amazon EC2 (on AWS), GCP, Azure, Rackspace, Digital Ocean, Linode.

PaaS removes the need to manage underlying infrastructure (usually hardware and operating systems) and allows you to focus on the deployment and management of your applications. You don't need to worry about resource procurement, capacity planning, software maintenance, patching, or any of the other undifferentiated heavy lifting involved in running your application. Examples - Elastic Beanstalk (on AWS), Heroku, Google App Engine (GCP), Windows Azure (Microsoft).

SaaS provides you with a complete product that is run and managed by the service provider. With a SaaS offering, you don't have to think about how the service is maintained or how the underlying infrastructure is managed. You only need to think about how you will use that particular software. Examples - Amazon Rekognition, Google Apps (Gmail), Dropbox, Zoom.

Overview of Cloud Computing Types: via - <https://aws.amazon.com/types-of-cloud-computing/>

You can use Amazon Rekognition to add image and video analysis to your applications using proven, highly scalable, deep learning technology that requires no machine learning expertise. With Amazon Rekognition, you can identify objects, people, text, scenes, and activities in images and videos as well as detect any inappropriate content. Rekognition is an example of Software as a Service (SaaS) model.

In Correct Options:

AWS Certified Cloud Practitioner (CPF) Practice Questions – Set 2

Amazon Elastic Compute Cloud (Amazon EC2) - Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud. Hence, it comes under Infrastructure as a Service (IaaS) type of Cloud Computing.

AWS Elastic Beanstalk - AWS Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services. You simply upload your code and Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring. Per the definitions above, Elastic Beanstalk falls under the Platform as a Service (PaaS) type.

Elastic Load Balancing (ELB) - Elastic Load Balancing (ELB) automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, IP addresses, and Lambda functions. It can handle the varying load of your application traffic in a single Availability Zone (AZ) or across multiple Availability Zones (AZ). This has been added as a distractor.

References:

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

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

58) What foundational capability under the operations perspective is part of the AWS Cloud Adoption Framework (AWS CAF)?

- A. Application portfolio management
- B. Performance and capacity management (**Correct**)
- C. Vulnerability management
- D. Platform engineering

Correct Options:

Performance and capacity management

The AWS Cloud Adoption Framework (AWS CAF) leverages AWS experience and best practices to help you digitally transform and accelerate your business outcomes through innovative use of AWS. Use the AWS CAF to identify and prioritize transformation opportunities, evaluate and improve your cloud readiness, and iteratively evolve your transformation roadmap.

AWS Certified Cloud Practitioner (CPF) Practice Questions – Set 2

AWS CAF groups its capabilities in six perspectives: Business, People, Governance, Platform, Security, and Operations. Each perspective comprises a set of capabilities that functionally related stakeholders own or manage in your cloud transformation journey.

Operations perspective helps ensure that your cloud services are delivered at a level that meets the needs of your business. Performance and capacity management under the Operations perspective is part of the AWS Cloud Adoption Framework (AWS CAF)

AWS Cloud Adoption Framework (AWS CAF) - Foundational capabilities: via - <https://docs.aws.amazon.com/whitepapers/latest/overview-aws-cloud-adoption-framework/foundational-capabilities.html>

In Correct Options:

Vulnerability management - Vulnerability management is a foundational capability under the Security perspective for the AWS Cloud Adoption Framework (AWS CAF).

Platform engineering - Platform engineering is a foundational capability under the Platform perspective for the AWS Cloud Adoption Framework (AWS CAF).

Application portfolio management - Application Portfolio Management is a foundational capability under the Governance perspective for the AWS Cloud Adoption Framework (AWS CAF).

Reference:

<https://docs.aws.amazon.com/whitepapers/latest/overview-aws-cloud-adoption-framework/foundational-capabilities.html>

59) An organization is planning to move its infrastructure from the on-premises datacenter to AWS Cloud. As a Cloud Practitioner, which options would you recommend so that the organization can identify the right AWS services to build solutions on AWS Cloud (Select two)?

- A. Amazon CloudWatch
- B. AWS Partner Network (APN) (**Correct**)
- C. AWS Service Catalog (**Correct**)

AWS Certified Cloud Practitioner (CPF) Practice Questions – Set 2

- D. AWS Organizations
- E. AWS CloudTrail

Correct Options:

AWS Service Catalog - AWS Service Catalog allows organizations to create and manage catalogs of IT services that are approved for use on AWS. These IT services can include everything from virtual machine images, servers, software, and databases to complete multi-tier application architectures.

AWS Partner Network (APN) - Organizations can take help from the AWS Partner Network (APN) to identify the right AWS services to build solutions on AWS Cloud. AWS Partner Network (APN) is the global partner program for technology and consulting businesses that leverage Amazon Web Services to build solutions and services for customers.

In Correct Options:

AWS Organizations - AWS Organizations helps you centrally govern your environment as you grow and scale your workloads on AWS. AWS Organizations help you to centrally manage billing; control access, compliance, and security; and share resources across your AWS accounts. AWS Organizations cannot help in identifying the right AWS services to build solutions on AWS Cloud.

Amazon CloudWatch - Amazon CloudWatch is a monitoring and observability service built for DevOps engineers, developers, site reliability engineers (SREs), and IT managers. CloudWatch provides data and actionable insights to monitor your applications, respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health. Think resource performance monitoring, events, and alerts; think CloudWatch. CloudWatch cannot help in identifying the right AWS services to build solutions on AWS Cloud.

AWS CloudTrail - AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. Think account-specific activity and audit; think CloudTrail. CloudTrail cannot help in identifying the right AWS services to build solutions on AWS Cloud.

References:

1 4 8 5 1 7 0

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

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

60) Which of the following AWS services is essential for implementing security of resources in AWS Cloud?

- A. AWS Identity and Access Management (IAM) (**Correct**)
- B. AWS Web Application Firewall (AWS WAF)
- C. AWS Shield
- D. Amazon CloudWatch

Correct Options:

AWS Identity and Access Management (IAM)

AWS Identity and Access Management (IAM) enables you to manage access to AWS services and resources securely. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources. IAM enables security best practices by allowing you to grant unique security credentials to users and groups to specify which AWS service APIs and resources they can access. These features make IAM an important service for the overall security of AWS resources in your account. IAM is secure by default; users have no access to AWS resources until permissions are explicitly granted.

In Correct Options:

Amazon CloudWatch - Amazon CloudWatch is a monitoring and observability service built for DevOps engineers, developers, site reliability engineers (SREs), and IT managers. CloudWatch provides data and actionable insights to monitor applications, respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health. This is an excellent service for building Resilient systems. Think resource performance monitoring, events, and alerts; think CloudWatch.

AWS Shield - AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS. AWS Shield provides always-on detection and automatic inline mitigations that minimize application downtime and latency, so there is no need to engage AWS

AWS Certified Cloud Practitioner (CPF) Practice Questions – Set 2

Support to benefit from DDoS protection. AWS Shield cannot be used to handle resource-specific security on AWS.

AWS Web Application Firewall (AWS WAF) - By using AWS Web Application Firewall (AWS WAF), you can configure web access control lists (Web ACLs) on your CloudFront distributions or Application Load Balancers to filter and block requests based on request signatures. Besides, by using AWS WAF's rate-based rules, you can automatically block the IP addresses of bad actors when requests matching a rule exceed a threshold that you define. AWS WAF cannot be used to handle resource-specific security on AWS.

Reference:

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

- 61) Which service gives a personalized view of the status of the AWS services that are part of your Cloud architecture so that you can quickly assess the impact on your business when AWS service(s) are experiencing issues?
- A. AWS Health - Service Health Dashboard
 - B. Amazon Inspector
 - C. AWS Health - Your Account Health Dashboard (**Correct**)
 - D. Amazon CloudWatch

Correct Options:

AWS Health - Your Account Health Dashboard

AWS Health - Your Account Health Dashboard provides alerts and remediation guidance when AWS is experiencing events that may impact you.

With AWS Health - Your Account Health Dashboard, alerts are triggered by changes in the health of your AWS resources, giving you event visibility, and guidance to help quickly diagnose and resolve issues.

You can check on this page <https://phd.aws.amazon.com/phd/home> to get current status information.

In Correct Options:

Amazon Inspector - Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications

AWS Certified Cloud Practitioner (CPF) Practice Questions – Set 2

deployed on AWS. Amazon Inspector automatically assesses applications for exposure, vulnerabilities, and deviations from best practices. Amazon Inspector cannot be used to prevent Distributed Denial-of-Service (DDoS) attack. It cannot provide the status of your AWS resources.

Amazon CloudWatch - Amazon CloudWatch is a monitoring and observability service built for DevOps engineers, developers, site reliability engineers (SREs), and IT managers. CloudWatch provides data and actionable insights to monitor applications, respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health. This is an excellent service for building Resilient systems. Think resource performance monitoring, events, and alerts; think CloudWatch. It cannot provide the status of your AWS resources.

AWS Health - Service Health Dashboard - The AWS Health - Service Health Dashboard is the single place to learn about the availability and operations of AWS services. You can view the overall status of AWS services, and you can sign in to view personalized communications about your particular AWS account or organization.

You can check on this page <https://health.aws.amazon.com/health/status> to get current status information.

Exam Alert:

While the AWS Health - Service Health Dashboard displays the general status of AWS services; the AWS Health - Your Account Health Dashboard gives you a personalized view of the performance and availability of the AWS services underlying your AWS resources.

Reference:

<https://docs.aws.amazon.com/health/latest/ug/what-is-aws-health.html>

- 62) A company wants a fully managed, flexible, and scalable file storage system, with low latency access, for its Windows-based applications. Which AWS service is the right choice for the company?
- A. Amazon Elastic File System (Amazon EFS)
 - B. Amazon Elastic Block Storage (Amazon EBS)
 - C. Amazon FSx for Lustre

D. Amazon FSx for Windows File Server (**Correct**)

Correct Options: Amazon FSx for Windows File Server

Amazon FSx for Windows File Server provides fully managed, highly reliable, and scalable file storage that is accessible over the industry-standard Service Message Block (SMB) protocol. It is built on Windows Server, delivering a wide range of administrative features such as user quotas, end-user file restore, and Microsoft Active Directory (AD) integration.

To support a wide spectrum of workloads, Amazon FSx provides high levels of throughput, IOPS and consistent sub-millisecond latencies. Amazon FSx is accessible from Windows, Linux, and macOS compute instances and devices.

For Windows-based applications, Amazon FSx provides fully managed Windows file servers with features and performance optimized for "lift-and-shift" business-critical application workloads including home directories (user shares), media workflows, and ERP applications. It is accessible from Windows and Linux instances via the SMB protocol.

In Correct Options:

Amazon Elastic File System (Amazon EFS) - Amazon Elastic File System (Amazon EFS) is a cloud-native fully managed file system that provides simple, scalable, elastic file storage accessible from Linux instances via the NFS protocol.

Amazon FSx pour Lustre - For compute-intensive and fast processing workloads, like high-performance computing (HPC), machine learning, EDA, and media processing, Amazon FSx for Lustre, provides a file system that's optimized for performance, with input and output stored on Amazon S3. Amazon FSx for Lustre is only compatible with Linux.

Amazon Elastic Block Storage (Amazon EBS) - Amazon EBS is an easy-to-use, high-performance, block-storage service designed for use with Amazon EC2 instances. It is a block-storage service and not a file storage service.

Reference:

<https://aws.amazon.com/fsx/windows/>

- 63) Which of the following AWS services can be used to prevent Distributed Denial-of-Service (DDoS) attack? (Select three)

AWS Certified Cloud Practitioner (CPF) Practice Questions – Set 2

- A. AWS Trusted Advisor
- B. AWS Shield (**Correct**)
- C. AWS Web Application Firewall (AWS WAF) (**Correct**)
- D. AWS CloudHSM
- E. Amazon CloudFront with Amazon Route 53 (**Correct**)
- F. Amazon Inspector

Correct Options:

AWS Shield - AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS. AWS Shield provides always-on detection and automatic inline mitigations that minimize application downtime and latency, so there is no need to engage AWS Support to benefit from DDoS protection.

AWS Web Application Firewall (AWS WAF) - By using AWS Web Application Firewall (AWS WAF), you can configure web access control lists (Web ACLs) on your Amazon CloudFront distributions or Application Load Balancers to filter and block requests based on request signatures. Besides, by using the AWS Web Application Firewall (AWS WAF) rate-based rules, you can automatically block the IP addresses of bad actors when requests matching a rule exceed a threshold that you define.

Amazon CloudFront with Amazon Route 53 - AWS hosts Amazon CloudFront and Amazon Route 53 services on a distributed network of proxy servers in data centers throughout the world called edge locations. Using the global Amazon network of edge locations for application delivery and DNS service plays an important part in building a comprehensive defense against DDoS attacks for your dynamic web applications.

How AWS Shield, AWS Web Application Firewall (AWS WAF), and Amazon CloudFront with Amazon Route 53 help mitigate DDoS attacks: via
- <https://aws.amazon.com/blogs/security/how-to-protect-dynamic-web-applications-against-ddos-attacks-by-using-amazon-cloudfront-and-amazon-route-53/>

In Correct Options:

AWS CloudHSM - AWS CloudHSM is a cloud-based hardware security module (HSM) that enables you to easily generate and use your encryption

AWS Certified Cloud Practitioner (CPF) Practice Questions – Set 2

keys on the AWS Cloud. With CloudHSM, you can manage your encryption keys using FIPS 140-2 Level 3 validated HSMs. It is a fully-managed service that automates time-consuming administrative tasks for you, such as hardware provisioning, software patching, high-availability, and backups. CloudHSM cannot be used to prevent Distributed Denial-of-Service (DDoS) attack.

AWS Trusted Advisor - AWS Trusted Advisor is an online tool that provides you real-time guidance to help you provision your resources following AWS best practices on cost optimization, security, fault tolerance, service limits and performance improvement. Whether establishing new workflows, developing applications, or as part of ongoing improvement, recommendations provided by Trusted Advisor regularly help keep your solutions provisioned optimally. Trusted Advisor cannot be used to prevent Distributed Denial-of-Service (DDoS) attack.

Amazon Inspector - Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for exposure, vulnerabilities, and deviations from best practices. Amazon Inspector cannot be used to prevent Distributed Denial-of-Service (DDoS) attack.

References:

<https://docs.aws.amazon.com/waf/latest/developerguide/ddos-overview.html>

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

https://d1.awsstatic.com/whitepapers/Security/DDoS_White_Paper.pdf

<https://aws.amazon.com/blogs/security/how-to-protect-dynamic-web-applications-against-ddos-attacks-by-using-amazon-cloudfront-and-amazon-route-53/>

64) What are the different gateway types supported by AWS Storage Gateway service?

- A. Tape Gateway, Object Gateway and Volume Gateway
- B. Tape Gateway, File Gateway and Volume Gateway (**Correct**)
- C. Object Gateway, File Gateway and Block Gateway
- D. Tape Gateway, File Gateway and Block Gateway

Correct Options:

Tape Gateway, File Gateway and Volume Gateway

AWS Storage Gateway is a hybrid cloud storage service that connects your existing on-premises environments with the AWS Cloud. Customers use Storage Gateway to simplify storage management and reduce costs for key hybrid cloud storage use cases. These include moving tape backups to the cloud, reducing on-premises storage with cloud-backed file shares, providing low latency access to data in AWS for on-premises applications, as well as various migration, archiving, processing, and disaster recovery use cases.

AWS Storage Gateway service provides three different types of gateways – Tape Gateway, File Gateway, and Volume Gateway – that seamlessly connect on-premises applications to cloud storage, caching data locally for low-latency access.

Gateway Storage Types Overview: via
- <https://aws.amazon.com/storagegateway/features/>

In Correct Options:

Object Gateway, File Gateway and Block Gateway

Tape Gateway, Object Gateway and Volume Gateway

Tape Gateway, File Gateway and Block Gateway

Block Gateway and Object Gateway are made-up options, so these three options are incorrect.

Reference:

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

65) Which of the following statements is INCORRECT about AWS Auto Scaling?

- A. You can automatically deploy AWS Shield when a DDoS attack is detected (**Correct**)
- B. You can scale out and add more Amazon Elastic Compute Cloud (Amazon EC2) instances to match an increase in demand as well as scale in and remove Amazon Elastic Compute Cloud (Amazon EC2) instances to match a reduced demand
- C. You can automatically remove unhealthy instances

D. You can automatically register new instances to a load balancer

Correct Options:

You can automatically deploy AWS Shield when a DDoS attack is detected

AWS Auto Scaling is helpful during a DDoS attack, as it can scale out resources fast. But, it cannot automatically deploy AWS Shield service onto its group of resources.

In Correct Options:

AWS Auto Scaling monitors your applications and automatically adjusts the capacity to maintain steady, predictable performance at the lowest possible cost. Using AWS Auto Scaling, it's easy to setup application scaling for multiple resources across multiple services in minutes. The service provides a simple, powerful user interface that lets you build scaling plans for resources including Amazon EC2 instances and Spot Fleets, Amazon ECS tasks, Amazon DynamoDB tables and indexes, and Amazon Aurora Replicas.

You can scale out and add more Amazon Elastic Compute Cloud (Amazon EC2) instances to match an increase in demand as well as scale in and remove Amazon Elastic Compute Cloud (Amazon EC2) instances to match a reduced demand - As explained above, it can scale out resources on-demand as well as scale in resources to match reduced demand.

You can automatically remove unhealthy instances - Based on health checks, Auto Scaling can remove unhealthy instances.

You can automatically register new instances to a load balancer - During a scale out process, Auto scaling can spin up new instances and register them with the load balancer, also part of the Scaling group.

Reference:

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