Practice Test 2

Question 1:
A startup is looking for 24x7 phone based technical support for his AWS account. Which of the following is the MOST cost-effective AWS support plan for this use-case?

Explanation
Correct option:

AWS offers three different support plans to cater to each of its customers - Developer, Business, and Enterprise Support plans.

A basic support plan is included for all AWS customers.

Business - AWS recommends Business Support 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. Enterprise Support plan also provides 24x7 phone, email and chat access to technical support however it's much costlier than Business Support plan. Developer plan does not provide 24x7 phone based technical support. Therefore Business Support plan is the correct option for the given use-case.

Exam Alert:

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

	Developer	Business	Enterprise
	Recommended if you are experimenting or testing in AWS.	*Recommended if you have production workloads in AWS.*	*Recommended if you have business and/or mission critical workloads in AWS.*
AWS Trusted Advisor Best Practice Checks	7 Core checks	Full set of checks	Full set of checks
Enhanced Technical Support	Business hours** email access to Cloud Support Associates Unlimited cases / 1 primary contact	24x7 phone, email, and chat access to Cloud Support Engineers Unlimited cases / unlimited contacts (IAM supported)	24x7 phone, email, and chat access to Cloud Support Engineers Unlimited cases / unlimited contacts (IAM supported)
Case Severity / Response Times*	General guidance: < 24 business hours** System impaired: < 12 business hours**	General guidance: < 24 hours System impaired: < 12 hours Production system impaired: < 4 hours Production system down: < 1 hour	General guidance: < 24 hours System impaired: < 12 hours Production system impaired: < 4 hours Production system down: < 1 hour Business-critical system down: < 15 minutes
Architectural Guidance	General	Contextual to your use-cases	Consultative review and guidance based on your applications
Programmatic Case Management		AWS Support API	AWS Support API
Third-Party Software Support		Interoperability & configuration guidance and troubleshooting	Interoperability & configuration guidance and troubleshooting

	Developer	Business	Enterprise
Proactive Programs		Access to Infrastructure Event Management for additional fee.	Infrastructure Event Management Well-Architected Reviews Operations Reviews Technical Account Manager (TAM) coordinates access to programs and other AWS experts as needed.
Technical Account Management			Designated Technical Account Manager (TAM) to proactively monitor your environment and assist with optimization.
Training			Access to online self-paced labs
Account Assistance			Concierge Support Team
Pricing	Greater of $29 / month*** - or - 3% of monthly AWS usage See pricing detail and example.	Greater of $100 / month*** - or - 10% of monthly AWS usage for the first $0–$10K 7% of monthly AWS usage from $10K–$80K 5% of monthly AWS usage from $80K–$250K 3% of monthly AWS usage over $250K See pricing detail and example.	Greater of $15,000 - or - 10% of monthly AWS usage for the first $0–$150K 7% of monthly AWS usage from $150K–$500K 5% of monthly AWS usage from $500K–$1M 3% of monthly AWS usage over $1M See pricing detail and example.

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

Incorrect options:

Basic - The basic plan only provides access to the following:

Customer Service & Communities - 24x7 access to customer service, documentation, whitepapers, and support forums. AWS Trusted Advisor - Access to the 7 core Trusted Advisor checks and guidance to provision your resources following best practices to increase performance and improve security. AWS Personal Health Dashboard - A personalized view of the health of AWS services, and alerts when your resources are impacted.

Developer - AWS recommends Developer Support 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.

Enterprise - AWS Enterprise Support provides customers with concierge-like service where the main focus is helping the customer achieve their outcomes and find success in the cloud. With 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. Enterprise Support plan provides 24x7 phone, email and chat access to technical support however it's much costlier than Business Support plan.

Reference:

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

Question 2:

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)

Explanation
Correct options:

AWS Trusted Advisor

AWS Identity and Access Management (IAM)

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: AWS IAM, Amazon VPC, AWS Trusted Advisor, AWS Service Quotas (earlier known as 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.

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.

Incorrect 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

Question 3:

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

-
- **Explanation**

Correct option:

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.

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

AWS WAF - By using 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/

Question 4:

Which AWS service enables users to find, buy, and immediately start using software solutions in their AWS environment?
Explanation
Correct option:

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.

Incorrect 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

Question 5:
Which design principle of the AWS Well-Architected Framework can answer the question- "Who did what"?
Explanation
Correct option:

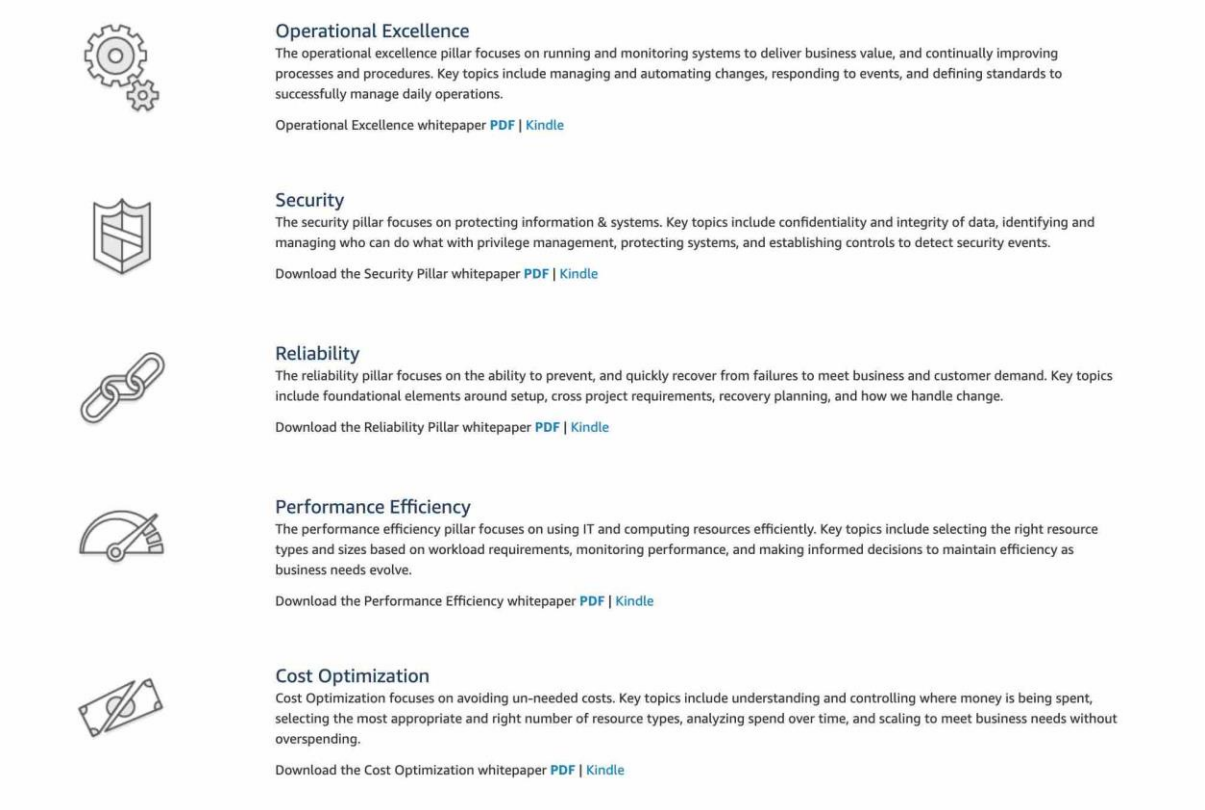
Security

"Who did what" is nothing but traceability of action by any user on the system. It tells us which user performed what action on the system. Traceability is part of the Security design principle of AWS Cloud. So this is the correct option.

The Well-Architected Framework has been developed to help cloud architects build secure, high-performing, resilient, and efficient infrastructure for their applications. Based on five pillars — operational excellence, security, reliability, performance

efficiency, and cost optimization — the Framework provides a consistent approach for customers and partners to evaluate architectures, and implement designs that will scale over time.

Overview of the five pillars of the Well-Architected Framework:



via - https://aws.amazon.com/architecture/well-architected/

Incorrect options:

Reliability - This design principle includes the ability of a system to recover from infrastructure or service disruptions, dynamically acquire computing resources to meet demand (keep the systems available, plan for failure). The Reliability pillar cannot help with traceability of action by any user on the system.

Operational Excellence - This design principle includes the ability to run and monitor systems to deliver business value (monitor systems and proactively take actions). Operational Excellence pillar cannot help with traceability of action by any user on the system.

Performance Efficiency - This design principle includes the ability to use computing resources efficiently and maintain efficiency as demand changes. Performance Efficiency pillar cannot help with traceability of action by any user on the system.

Reference:

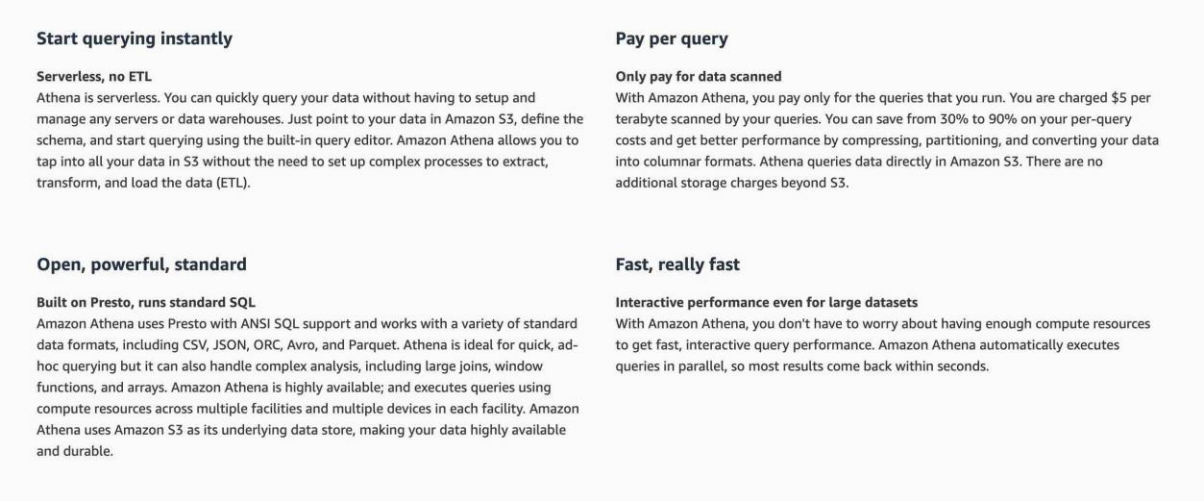
https://aws.amazon.com/blogs/apn/the-5-pillars-of-the-aws-well-architected-framework/

Question 6:
A data analytics company has some data stored on 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?
Explanation
Correct option:

Amazon Athena

Amazon Athena is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL. 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:



Start querying instantly

Serverless, no ETL
Athena is serverless. You can quickly query your data without having to setup and manage any servers or data warehouses. Just point to your data in Amazon S3, define the schema, and start querying using the built-in query editor. Amazon Athena allows you to tap into all your data in S3 without the need to set up complex processes to extract, transform, and load the data (ETL).

Pay per query

Only pay for data scanned
With Amazon Athena, you pay only for the queries that you run. You are charged $5 per terabyte scanned by your queries. You can save from 30% to 90% on your per-query costs and get better performance by compressing, partitioning, and converting your data into columnar formats. Athena queries data directly in Amazon S3. There are no additional storage charges beyond S3.

Open, powerful, standard

Built on Presto, runs standard SQL
Amazon Athena uses Presto with ANSI SQL support and works with a variety of standard data formats, including CSV, JSON, ORC, Avro, and Parquet. Athena is ideal for quick, ad-hoc querying but it can also handle complex analysis, including large joins, window functions, and arrays. Amazon Athena is highly available; and executes queries using compute resources across multiple facilities and multiple devices in each facility. Amazon Athena uses Amazon S3 as its underlying data store, making your data highly available and durable.

Fast, really fast

Interactive performance even for large datasets
With Amazon Athena, you don't have to worry about having enough compute resources to get fast, interactive query performance. Amazon Athena automatically executes queries in parallel, so most results come back within seconds.

via - https://aws.amazon.com/athena/

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

Incorrect 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 Aurora for SQL analysis on S3 based data.

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 Redshift for SQL analysis on S3 based data.

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 DynamoDB for SQL analysis on S3 based data.

Reference:

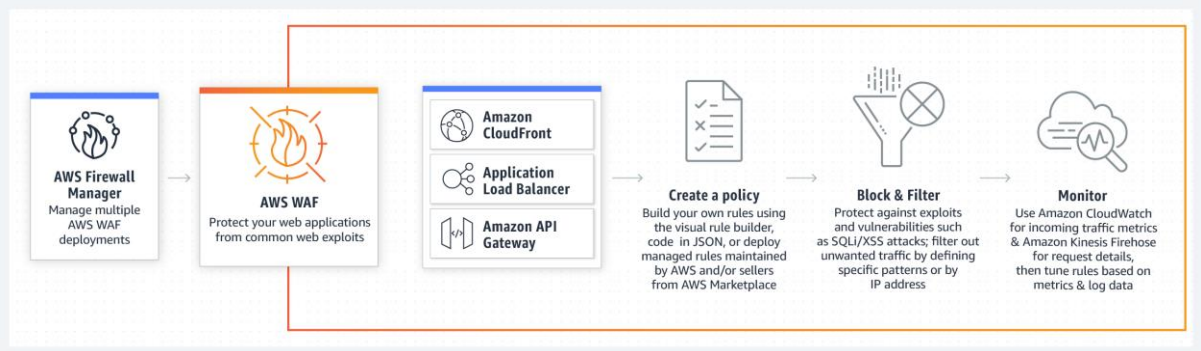
https://aws.amazon.com/athena/

Question 7:
An online gaming company wants to block users from certain geographies from accessing its content. Which AWS services can be used to accomplish this task? (Select two)
Explanation
Correct options:

AWS WAF

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 WAF
Works:



via - https://aws.amazon.com/waf/

Route 53

Route 53 is Amazon's Domain Name System (DNS) web service. You can use Route 53 geolocation routing policy to block certain geographies. When you use

geolocation routing, you can localize your content and present some or all of your website in the language of your users. You can also use geolocation routing to restrict the distribution of content to only the locations in which you have distribution rights.

Incorrect options:

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 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.

AWS Protect - This is no such thing as AWS Protect and it has been added as a distractor.

References:

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

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

Question 8:

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?

-
- **Explanation**

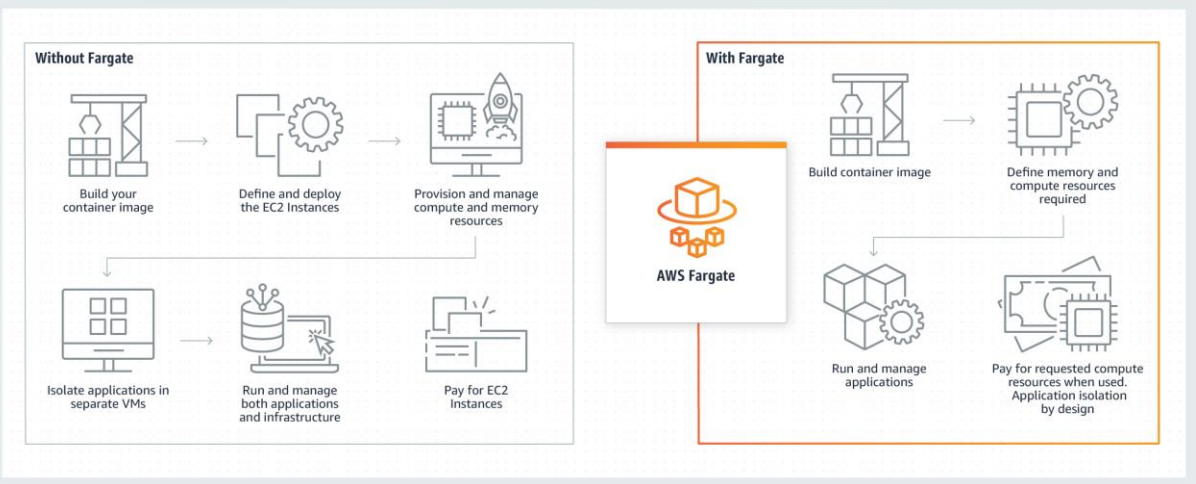
Correct option:

AWS Fargate

AWS Fargate is a serverless compute engine for containers. It works with both Amazon Elastic Container Service (ECS) and Amazon Elastic Kubernetes Service (EKS). Fargate makes it easy for you to focus on building your applications. 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. Fargate 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. 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 Fargate
Works:



via - https://aws.amazon.com/fargate/

Incorrect options:

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. Unlike 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. 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/

Question 9:

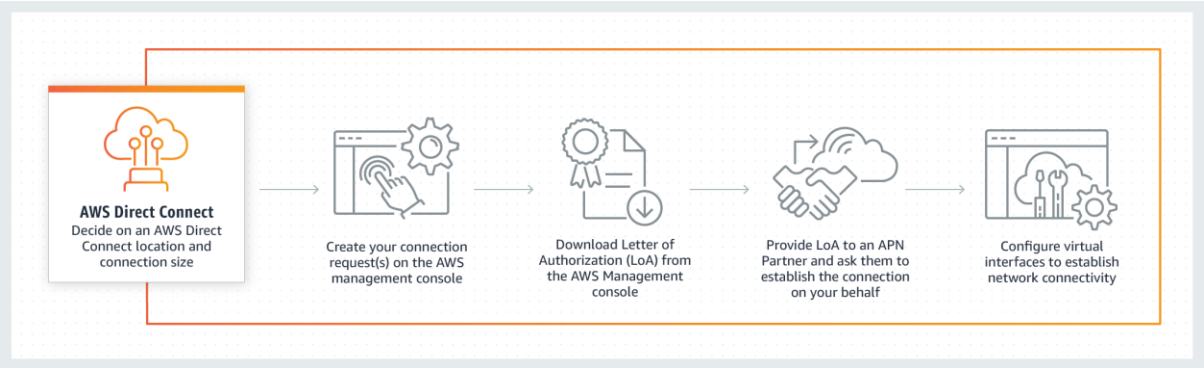
Which of the following solutions can you use to connect your on-premises network with AWS Cloud (Select two).

- ☑
- **Explanation**

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.

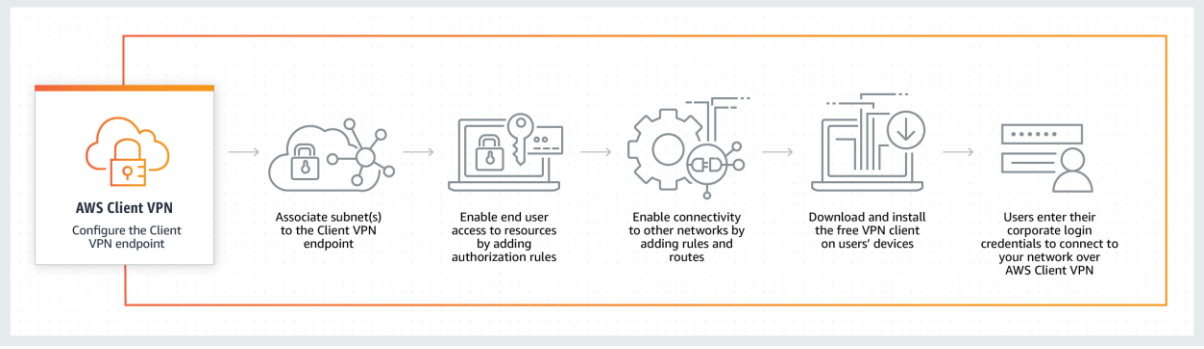
How AWS Direct Connect Works:



via - https://aws.amazon.com/directconnect/

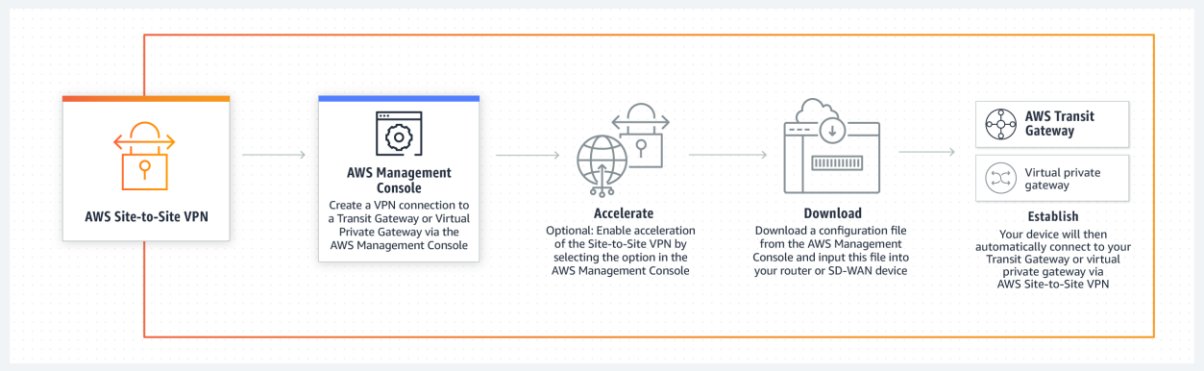
AWS VPN - AWS Virtual Private Network (VPN) solutions establish secure connections between on-premises networks, remote offices, client devices, and the AWS global network. AWS VPN is comprised of two services: AWS Site-to-Site VPN and AWS Client VPN. Together, they deliver a highly-available, managed,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

Incorrect options:

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/

Question 10:
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?

-
- **Explanation**

Correct option:

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.

Incorrect 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

Question 11:

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

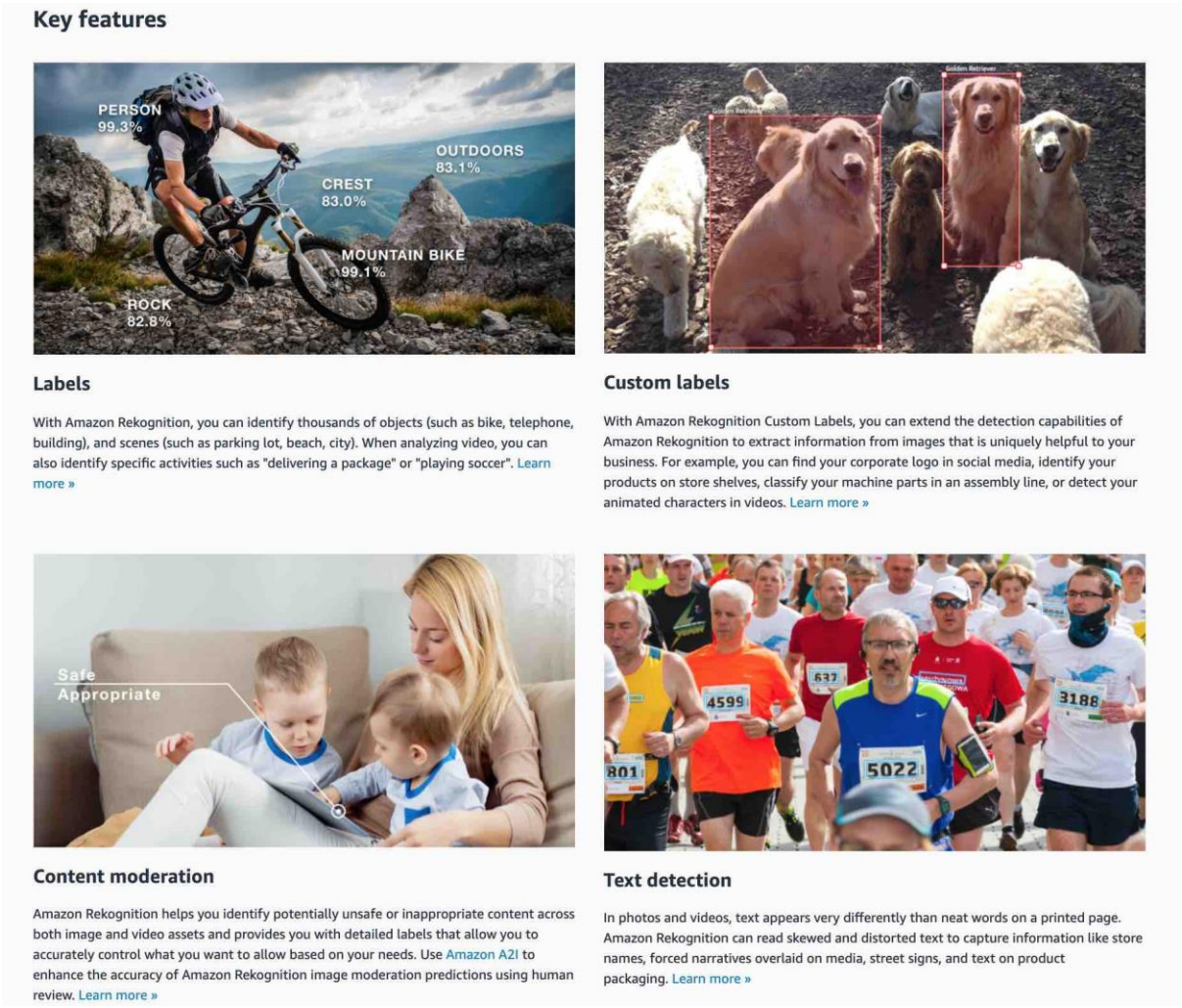
-

Explanation
Correct options:

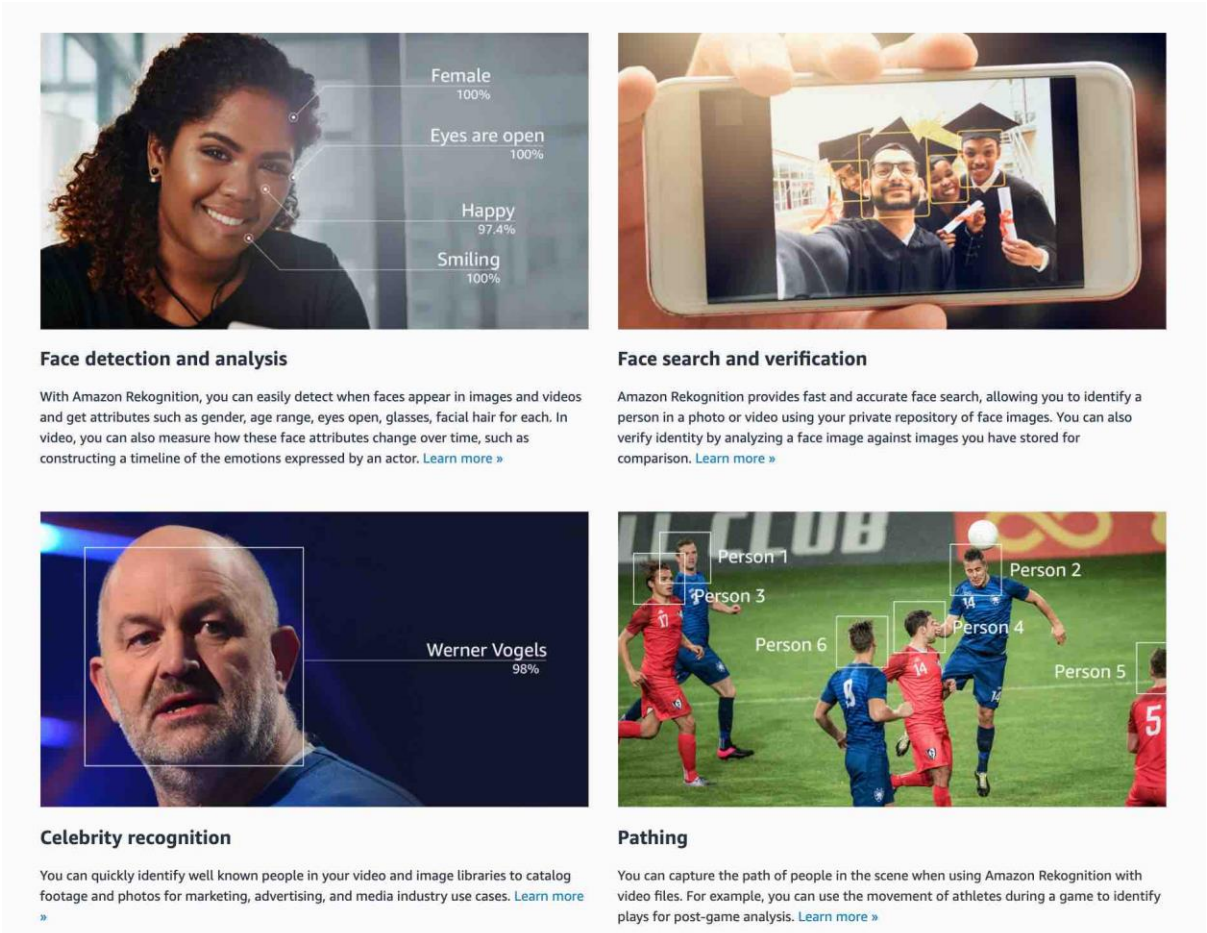
Quickly resize photos to create thumbnails - You cannot use Rekognition to resize photos to create thumbnails.

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/

Incorrect options:

Identify person in a photo

Detect text in a photo

Label objects in a photo

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

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

Question 12:

Which of the following is correct about AWS "Developer" Support plan?

-
- **Explanation**

Correct option:

Allows one contact to open unlimited cases

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

Incorrect 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 supported by AWS "Business" and "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/

Question 13:
What is the primary benefit of deploying an RDS database in a Multi-AZ configuration?

-
- **Explanation**

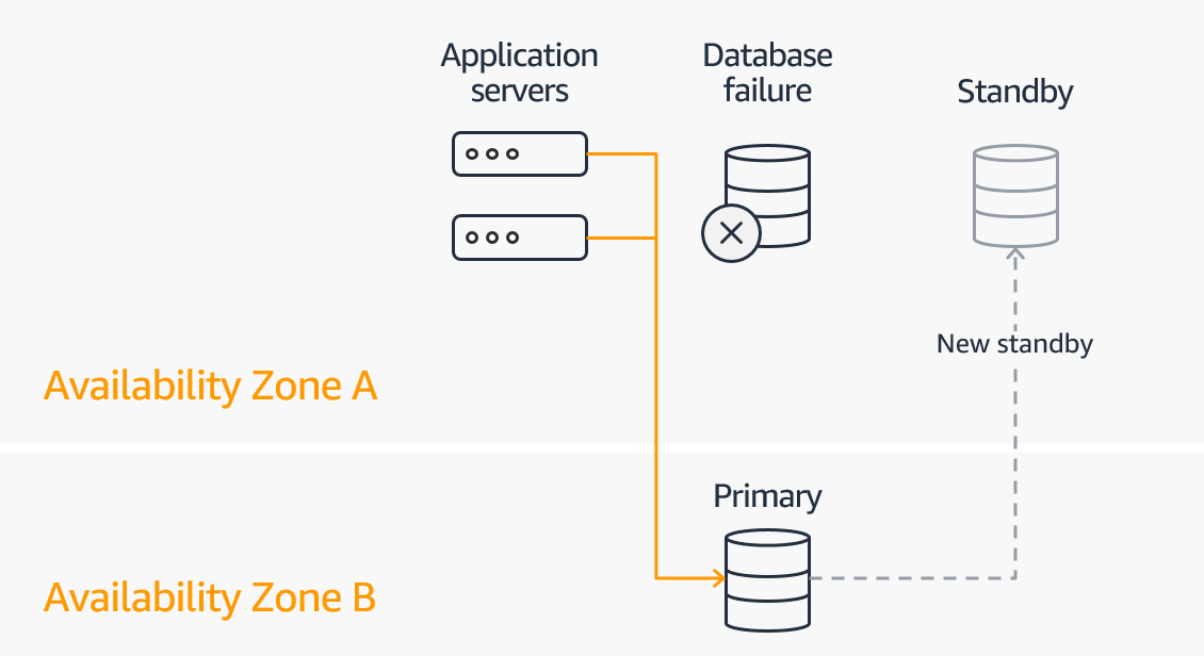
Correct option:

Multi-AZ enhances database availability

Amazon RDS Multi-AZ deployments provide enhanced availability and durability for RDS database (DB) instances, making them a natural fit for production database workloads. When you provision a Multi-AZ DB Instance, 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 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:

Read replicas, Multi-AZ deployments, and multi-region deployments

Amazon RDS read replicas complement Multi-AZ deployments. While both features maintain a second copy of your data, there are differences between the two:

Multi-AZ deployments	Multi-Region deployments	Read replicas
Main purpose is high availability	Main purpose is disaster recovery and local performance	Main purpose is scalability
Non-Aurora: synchronous replication; Aurora: asynchronous replication	Asynchronous replication	Asynchronous replication
Non-Aurora: only the primary instance is active; Aurora: all instances are active	All regions are accessible and can be used for reads	All read replicas are accessible and can be used for readscaling
Non-Aurora: automated backups are taken from standby; Aurora: automated backups are taken from shared storage layer	Automated backups can be taken in each region	No backups configured by default
Always span at least two Availability Zones within a single region	Each region can have a Multi-AZ deployment	Can be within an Availability Zone, Cross-AZ, or Cross-Region
Non-Aurora: database engine version upgrades happen on primary; Aurora: all instances are updated together	Non-Aurora: database engine version upgrade is independent in each region; Aurora: all instances are updated together	Non-Aurora: database engine version upgrade is independent from source instance; Aurora: all instances are updated together
Automatic failover to standby (non-Aurora) or read replica (Aurora) when a problem is detected	Aurora allows promotion of a secondary region to be the master	Can be manually promoted to a standalone database instance (non-Aurora) or to be the primary instance (Aurora)

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

Incorrect options:

Multi-AZ improves database performance for read-heavy workloads - 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.

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. Multi-AZ cannot protect from a regional failure.

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

Reference:

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

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

- ☐
- **Explanation**

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

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

Incorrect 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.

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.

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.

Question 15:
The engineering team at an IT company wants to monitor the CPU utilization for its fleet of 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)

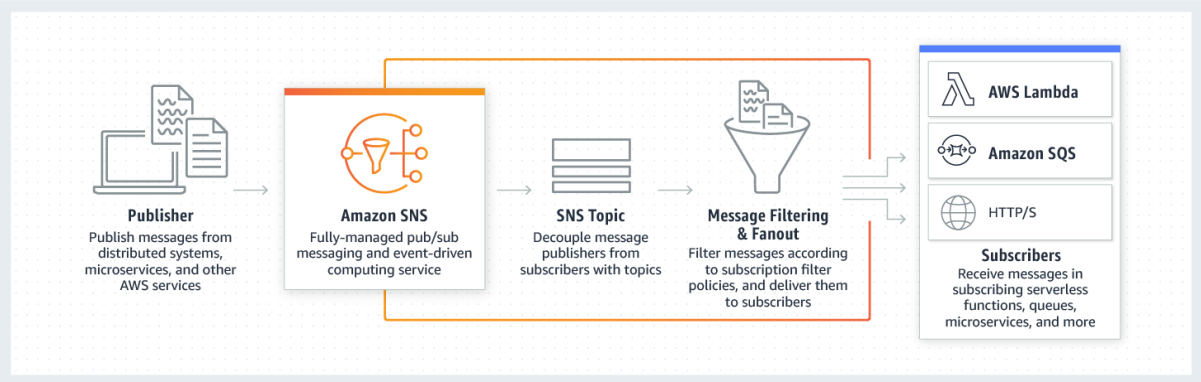
- ☑
- **Explanation**

Correct options:

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 an 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.

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/

Incorrect options:

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.

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.

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.

References:

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

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

Question 16:
Multi AZ (Availability Zone) deployment is an example of which of the following?

- High

Explanation

Correct option:

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 across multi AZ to achieve High Availability.

Incorrect options:

Horizontal Scaling - 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. Auto Scaling Group is an example of Horizontal Scaling on AWS.

Vertical Scaling - Vertical Scaling is adding more resources (like CPU, RAM) to a single node or machine. Example- Resizing an instance of EC2.

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

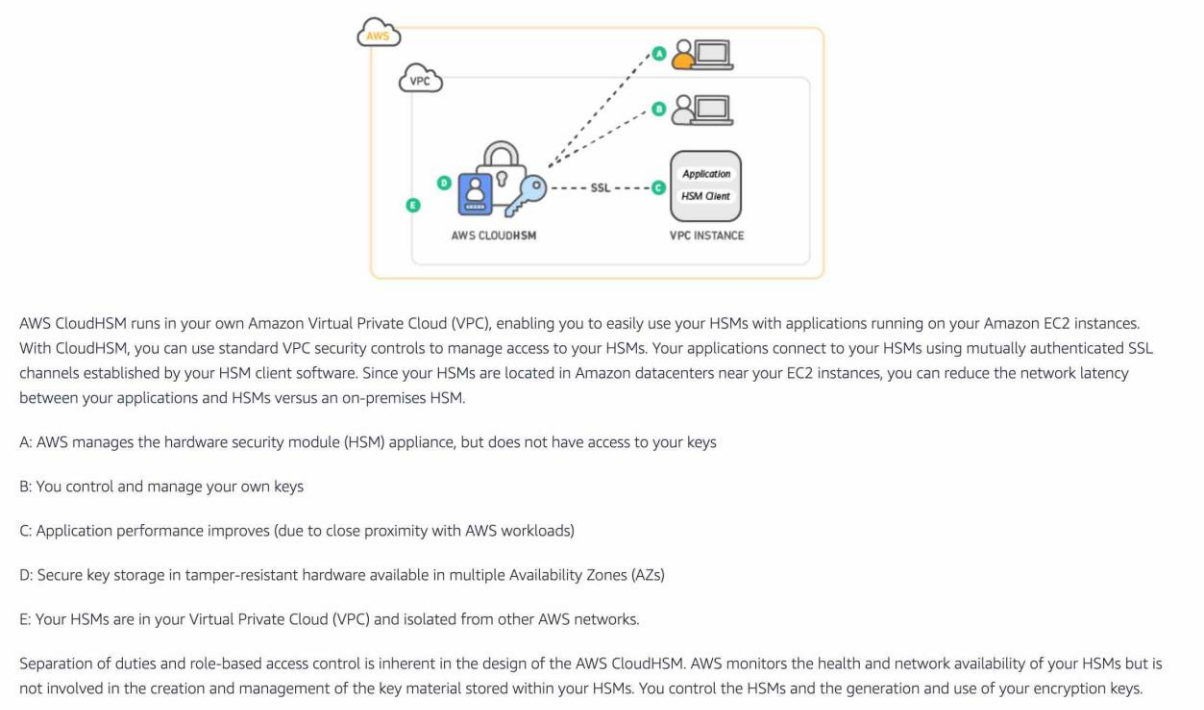
https://wa.aws.amazon.com/wat.concept.horizontal-scaling.en.html

Question 17: Correct
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?
Explanation
Correct option:

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 of how CloudHSM
works:



AWS CloudHSM runs in your own Amazon Virtual Private Cloud (VPC), enabling you to easily use your HSMs with applications running on your Amazon EC2 instances. With CloudHSM, you can use standard VPC security controls to manage access to your HSMs. Your applications connect to your HSMs using mutually authenticated SSL channels established by your HSM client software. Since your HSMs are located in Amazon datacenters near your EC2 instances, you can reduce the network latency between your applications and HSMs versus an on-premises HSM.

A: AWS manages the hardware security module (HSM) appliance, but does not have access to your keys

B: You control and manage your own keys

C: Application performance improves (due to close proximity with AWS workloads)

D: Secure key storage in tamper-resistant hardware available in multiple Availability Zones (AZs)

E: Your HSMs are in your Virtual Private Cloud (VPC) and isolated from other AWS networks.

Separation of duties and role-based access control is inherent in the design of the AWS CloudHSM. AWS monitors the health and network availability of your HSMs but is not involved in the creation and management of the key material stored within your HSMs. You control the HSMs and the generation and use of your encryption keys.

via - https://aws.amazon.com/cloudhsm/

Incorrect options:

AWS Key Management Service (KMS) - AWS Key Management Service (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. AWS KMS 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. KMS 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/

Question 18:

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

- ☑
- **Explanation**

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

Incorrect options:

AWS Organizations - AWS Organizations helps you centrally govern your environment as you grow and scale your workloads on 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:

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

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

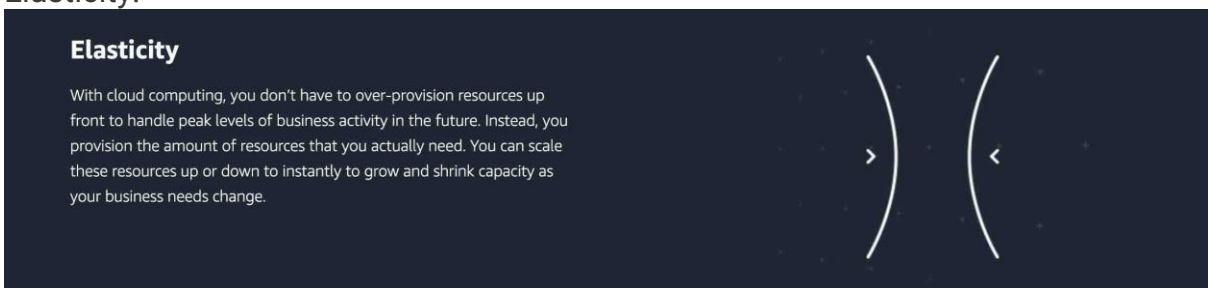
Question 19:
Which characteristic of Cloud Computing imparts the ability to acquire resources as you need and release when you no longer need them?

-
- **Explanation**

Correct option: **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/

Incorrect 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.

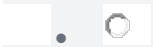
Resiliency - Describes the ability of a system to recover from a failure induced by the load (data or network), attacks, and failures (hardware, software, or network failures).

References:

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

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

Question 20: Correct
Which AWS service helps you define your infrastructure as code?



Explanation
Correct option:

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. You can use AWS CloudFormation's sample templates or create your templates to describe the AWS resources, and any associated dependencies or runtime parameters, required to run your application.

Incorrect 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 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 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.

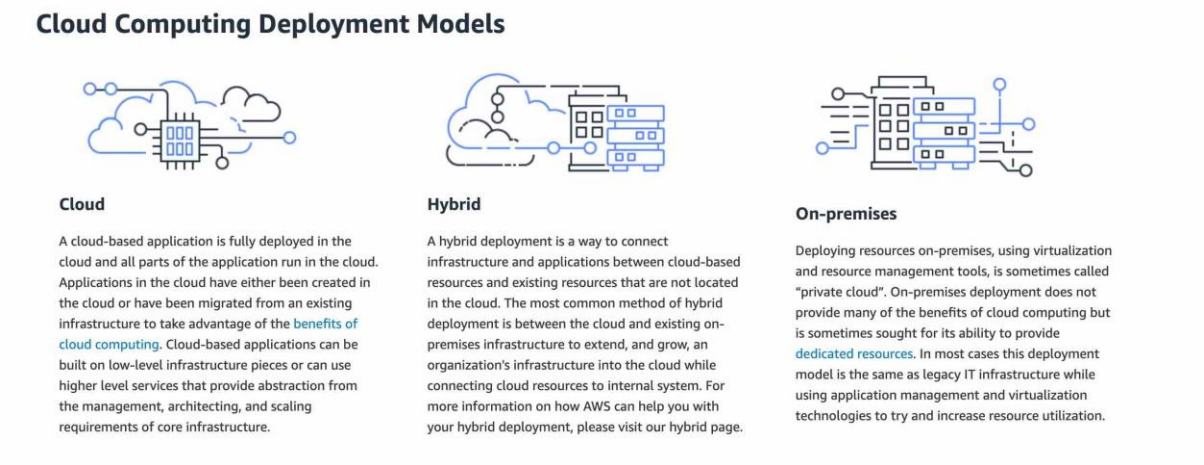
Reference: https://aws.amazon.com/cloudformation/

Question 21:

Due to regulatory and compliance reasons, an organization has deployed its entire IT infrastructure on its on-premises data center. How would you classify this deployment model?
Explanation
Correct option:

Private - 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 to meet compliance and regulatory guidelines.

Overview of Cloud Computing Deployment Models:



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

Incorrect options:

Cloud - 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.

Hybrid - 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.

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

Reference:

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

Question 22:

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

-
- **Explanation**

Correct options: **Elastic Load Balancing**

Read Replicas in Amazon RDS

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 - Elastic Load Balancing 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 or across multiple Availability Zones. This falls under Horizontal Scaling.

"Read Replicas in 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.

Incorrect 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

Question 23:

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?

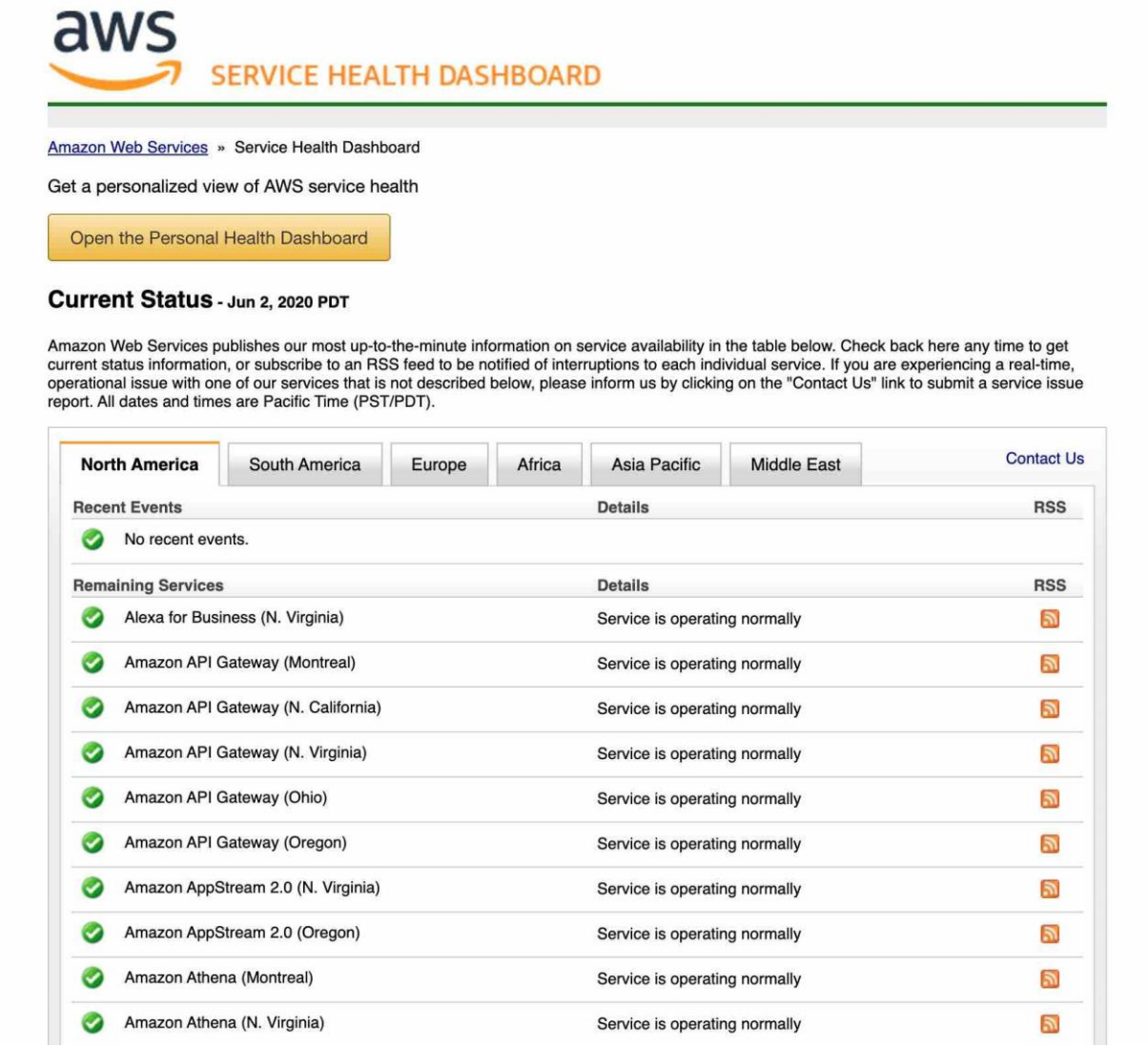
-
- **Explanation**

Correct option: **AWS Service Health Dashboard**

AWS Service Health Dashboard publishes most up-to-the-minute information on the status and availability of all AWS services in tabular form for all Regions that AWS is

present in. You can check on this page https://status.aws.amazon.com/ to get current status information.

AWS Service Health Dashboard
Overview:



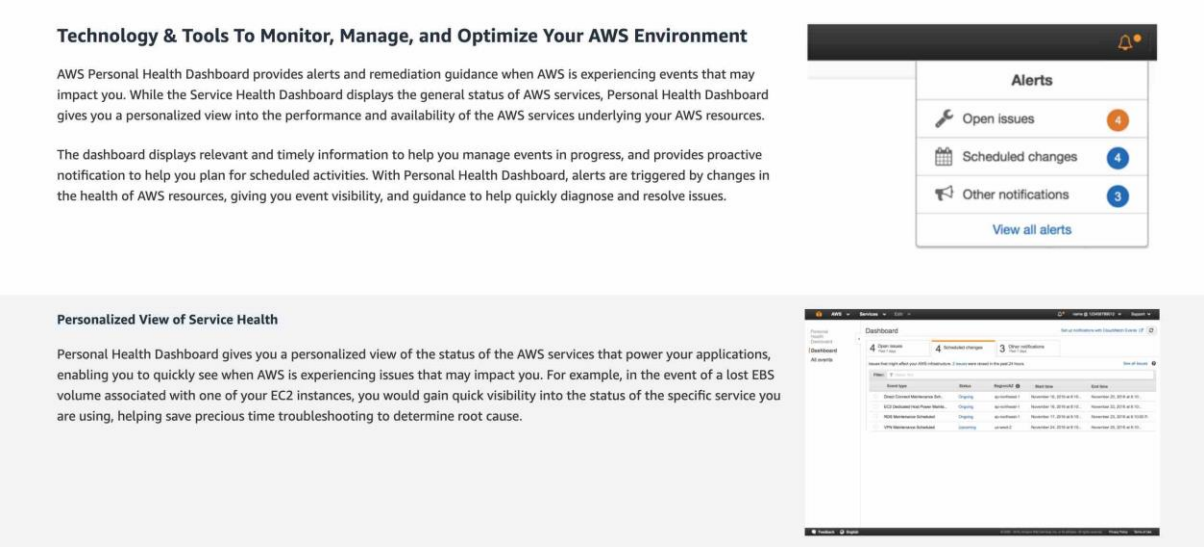
via - https://status.aws.amazon.com/

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

AWS Personal Health Dashboard
Overview:



via - https://status.aws.amazon.com/

Exam Alert:

While the Service Health Dashboard displays the general status of AWS services, Personal Health Dashboard 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 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/

Question 24:

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?

-
- **Explanation**

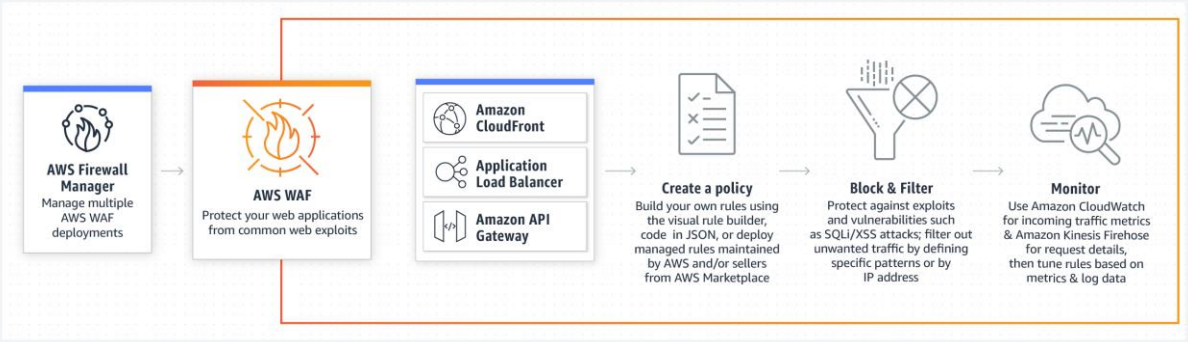
Correct option:

AWS Web Application Firewall (WAF)

AWS WAF is a web application firewall that helps protect your web applications or APIs against common web exploits that may affect availability, compromise security,

or consume excessive resources. AWS WAF gives you control over how traffic reaches your applications by enabling you to create security rules that block common attack patterns such as SQL injection or cross-site scripting. You can also use rate-based rules to mitigate the Web layer DDoS attack.

How 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.

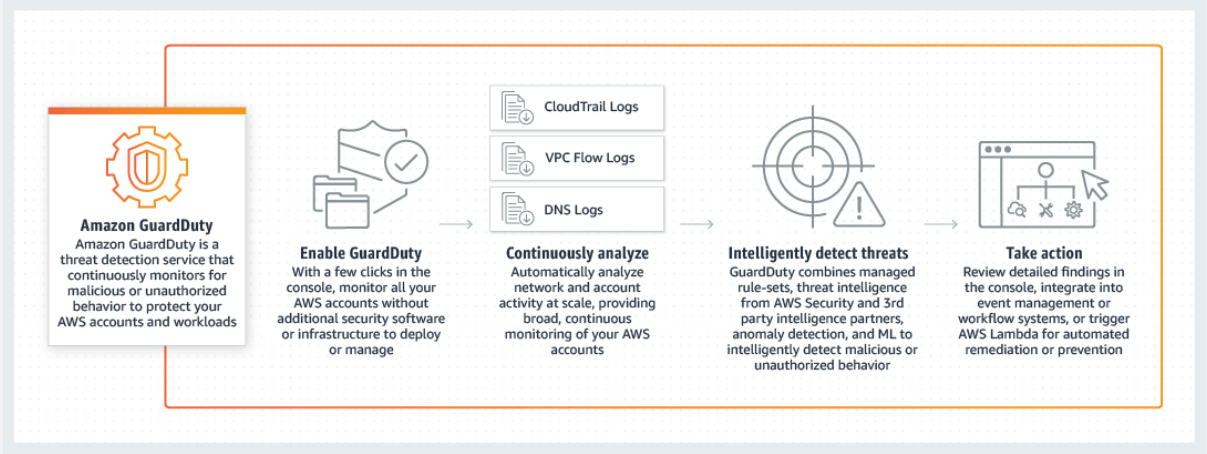
Similar to an SQL injection attack, a cross-site scripting attack also involves injecting malicious code into a website, but in this case, the website itself is not being attacked. Instead, the malicious code the attacker has injected only runs in the user's browser when they visit the attacked website,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

Incorrect options:

Amazon GuardDuty

GuardDuty is a threat detection service that monitors malicious activity and unauthorized behavior to protect your AWS account. 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). GuardDuty cannot be used to protect from web exploits such as SQL injection and cross-site scripting.

How 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/

Question 25:

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

-
- **Explanation**

Correct option: **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).

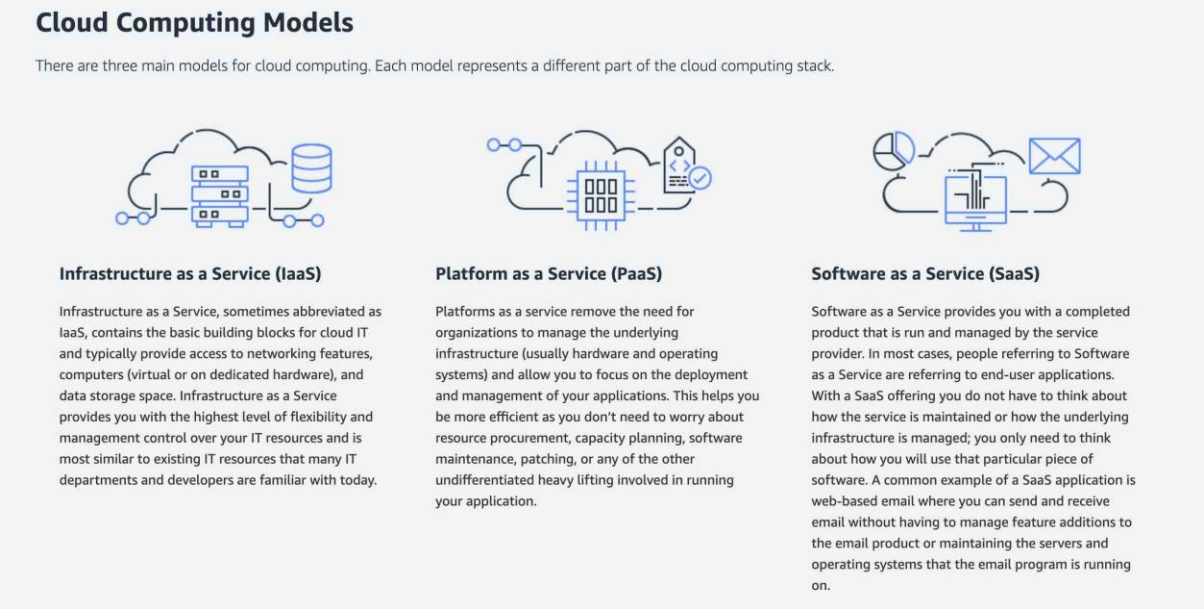
IaaS contains the basic building blocks for cloud IT. It typically provides access to networking features, computers (virtual or on dedicated hardware), and data storage space. IaaS gives the highest level of flexibility and management control over IT

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 model.

Incorrect options:

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 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 type.

Elastic Load Balancing - Elastic Load Balancing 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 or across multiple Availability Zones. This has been added as a distractor.

References:

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

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

Question 26:
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?

- 
- **Explanation**

Correct option:

Amazon Elastic Compute Cloud (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.

Amazon EC2
Overview:

Amazon EC2 presents a true virtual computing environment, allowing you to use web service interfaces to launch instances with a variety of operating systems, load them with your custom application environment, manage your network's access permissions, and run your image using as many or few systems as you desire.

To use Amazon EC2, you simply:

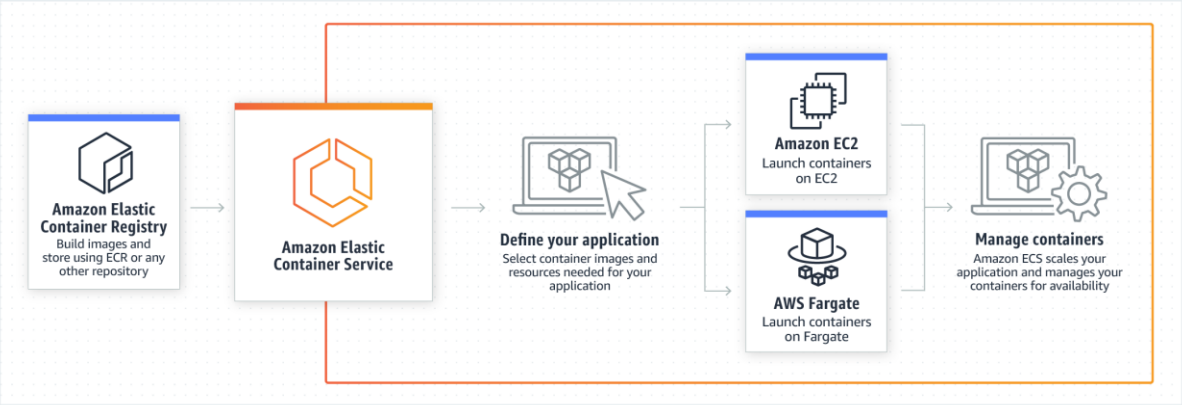
- Select a pre-configured, templated Amazon Machine Image (AMI) to get up and running immediately. Or create an AMI containing your applications, libraries, data, and associated configuration settings.
- Configure security and network access on your Amazon EC2 instance.
- Choose which instance type(s) you want, then start, terminate, and monitor as many instances of your AMI as needed, using the web service APIs or the variety of management tools provided.
- Determine whether you want to run in multiple locations, utilize static IP endpoints, or attach persistent block storage to your instances.
- Pay only for the resources that you actually consume, like instance-hours or data transfer.

via - https://aws.amazon.com/ec2/

Incorrect options:

Amazon Elastic Container Service (ECS) - Amazon Elastic Container Service (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 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 - 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. Lightsail offers several preconfigured, one-click-to-launch operating systems, development stacks, and web applications, including Linux, Windows OS, and

WordPress. Lightsail comes with monthly payment plans and does not support per second billing, so this option is ruled out.

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

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

Question 27:
Which AWS service would you use to send alerts when the costs for your AWS account exceed your budgeted amount?

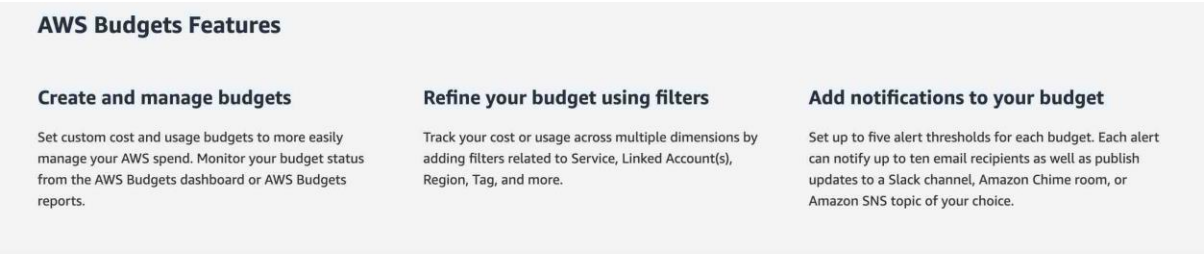
-
- **Explanation**

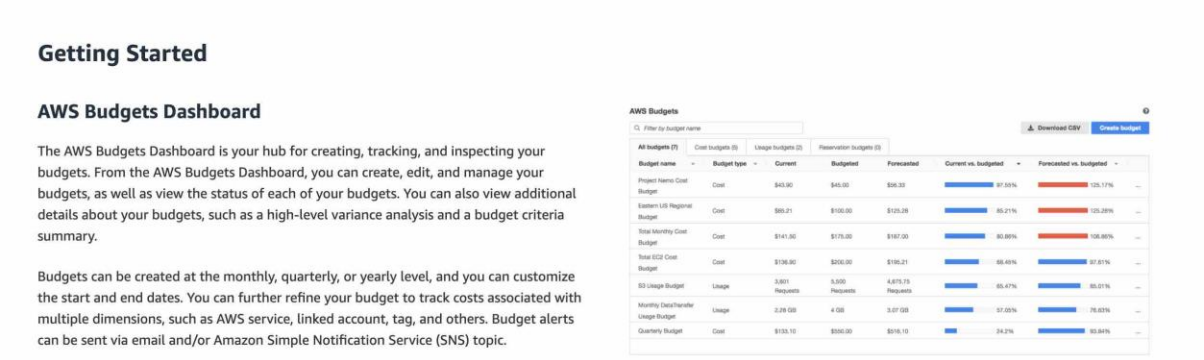
Correct option:

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 (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 Budgets:

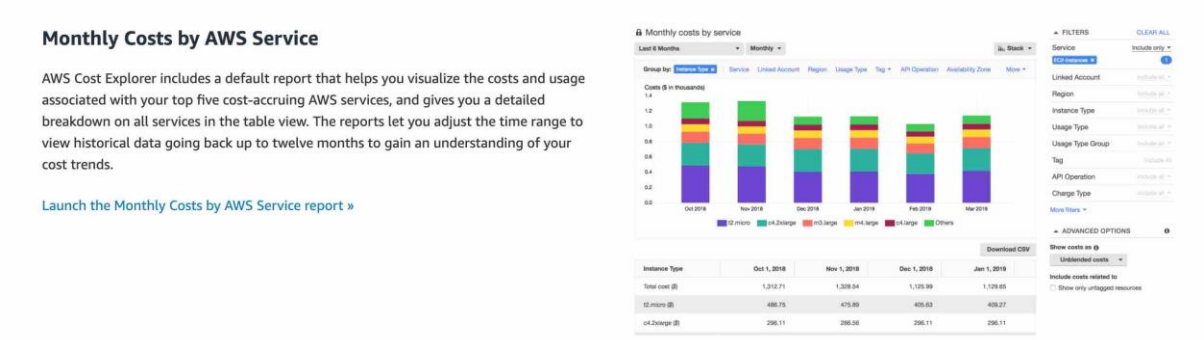
CloudWatch Billing Alarms: Sends an alarm when the actual cost exceeds a certain threshold.

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

Incorrect 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 Total Cost of Ownership (TCO) Calculator - AWS helps reduce Total Cost of Ownership (TCO) by reducing the need to invest in large capital expenditures and providing a pay-as-you-go model that empowers to invest in the capacity you need and use it only when the business requires it. TCO calculator helps to compare the cost of your applications in an on-premises or traditional hosting environment to AWS. Once you describe your on-premises or hosting environment configuration, it

produces a detailed cost comparison with AWS. TCO calculator can be used from https://awstcocalculator.com/.

Reference:

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

Question 28:

A fleet of Amazon EC2 instances spread across different Availability Zones needs to access, edit and share file-based data stored centrally on a system. As a Cloud Practitioner, which AWS service would you recommend for this use-case?

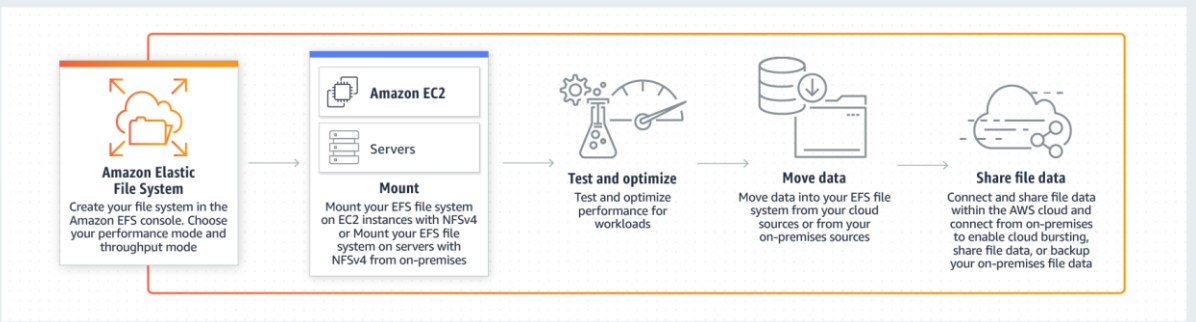
-
- **Explanation**

Correct option:

Elastic File System (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 EFS Works:



via - https://aws.amazon.com/efs/

Incorrect options:

Elastic Block Store (EBS) Volume - 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. An

EBS can only be mounted to one EC2 instance at a time, so this option is not correct for the given use-case.

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 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/

Question 29:

Which of the following statements are correct about the AWS account root user (Select two)

-
- **Explanation**

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 account root user credentials. Root account, therefore, has full permissions on all AWS resources under that account. Restricting root account access is not possible. As a best practice, Multi-Factor Authentication (MFA) should be set on the root account. The root 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 Account Security Best Practices:

The AWS Account Root User

PDF | Kindle | RSS

When you first create an Amazon Web Services (AWS) account, you begin with a single sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account *root user* and is accessed by signing in with the email address and password that you used to create the account.

> **Important**
>
> We strongly recommend that you do not use the root user for your everyday tasks, even the administrative ones. Instead, adhere to the best practice of using the root user only to create your first IAM user. Then securely lock away the root user credentials and use them to perform only a few account and service management tasks. To view the tasks that require you to sign in as the root user, see AWS Tasks That Require Root User. For a tutorial on how to set up an administrator for daily use, see Creating Your First IAM Admin User and Group.

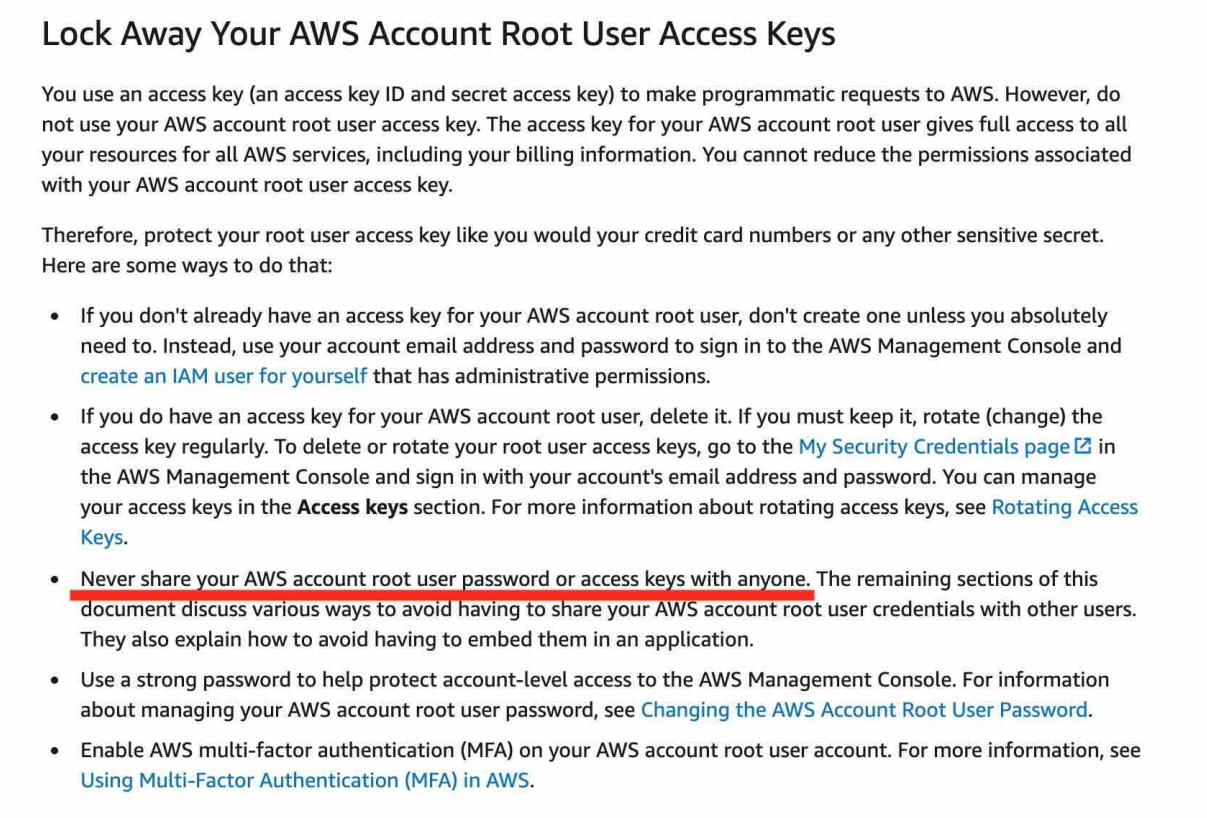
You can create, rotate, disable, or delete access keys (access key IDs and secret access keys) for your AWS account root user. You can also change your root user password. Anyone who has root user credentials for your AWS account has unrestricted access to all the resources in your account, including billing information.

When you create access keys, you create the access key ID and secret access key as a set. During access key creation, AWS gives you one opportunity to view and download the secret access key part of the access key. If you don't download it or if you lose it, you can delete the access key and then create a new one. You can create root user access keys with the IAM console, AWS CLI, or AWS API.

A newly created access key has the status of *active*, which means that you can use the access key for CLI and API calls. You are limited to two access keys for each IAM user, which is useful when you want to rotate the access keys. You can also assign up to two access keys to the root user. When you disable an access key, you can't use it for API calls, and inactive keys do count toward your limit. You can create or delete an access key any time. However, when you delete an access key, it's gone forever and can't be retrieved.

You can change the email address and password on the Security Credentials page. You can also choose **Forgot password?** on the AWS sign-in page to reset your password.

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



Lock Away Your AWS Account Root User Access Keys

You use an access key (an access key ID and secret access key) to make programmatic requests to AWS. However, do not use your AWS account root user access key. The access key for your AWS account root user gives full access to all your resources for all AWS services, including your billing information. You cannot reduce the permissions associated with your AWS account root user access key.

Therefore, protect your root user access key like you would your credit card numbers or any other sensitive secret. Here are some ways to do that:

- If you don't already have an access key for your AWS account root user, don't create one unless you absolutely need to. Instead, use your account email address and password to sign in to the AWS Management Console and create an IAM user for yourself that has administrative permissions.
- If you do have an access key for your AWS account root user, delete it. If you must keep it, rotate (change) the access key regularly. To delete or rotate your root user access keys, go to the My Security Credentials page in the AWS Management Console and sign in with your account's email address and password. You can manage your access keys in the **Access keys** section. For more information about rotating access keys, see Rotating Access Keys.
- Never share your AWS account root user password or access keys with anyone. The remaining sections of this document discuss various ways to avoid having to share your AWS account root user credentials with other users. They also explain how to avoid having to embed them in an application.
- Use a strong password to help protect account-level access to the AWS Management Console. For information about managing your AWS account root user password, see Changing the AWS Account Root User Password.
- Enable AWS multi-factor authentication (MFA) on your AWS account root user account. For more information, see Using Multi-Factor Authentication (MFA) in AWS.

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

Incorrect options:

Root user account password cannot be changed once it is set - This is incorrect. Like any other user credentials, the root 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 credentials should be never be shared with anyone.

Root account gets unrestricted permissions when the account is created, but these can be restricted using IAM policies - Root 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

Question 30:

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)

-
- **Explanation**

Correct option:

Reliability

Cost Optimization

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

Incorrect 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

Question 31: Correct

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

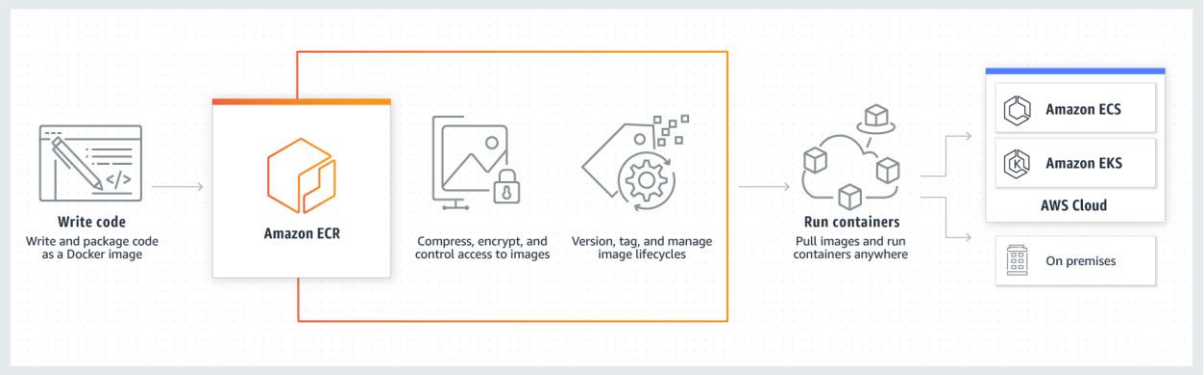
-
- **Explanation**

Correct option:

Amazon Elastic Container Registry (ECR) - Amazon Elastic Container Registry (ECR) can be used to store, manage, and deploy Docker container images. Amazon ECR

eliminates the need to operate your container repositories. You can then pull your docker images from ECR and run those on Amazon Elastic Container Service (ECS).

Please see this schematic diagram to understand how ECR works:

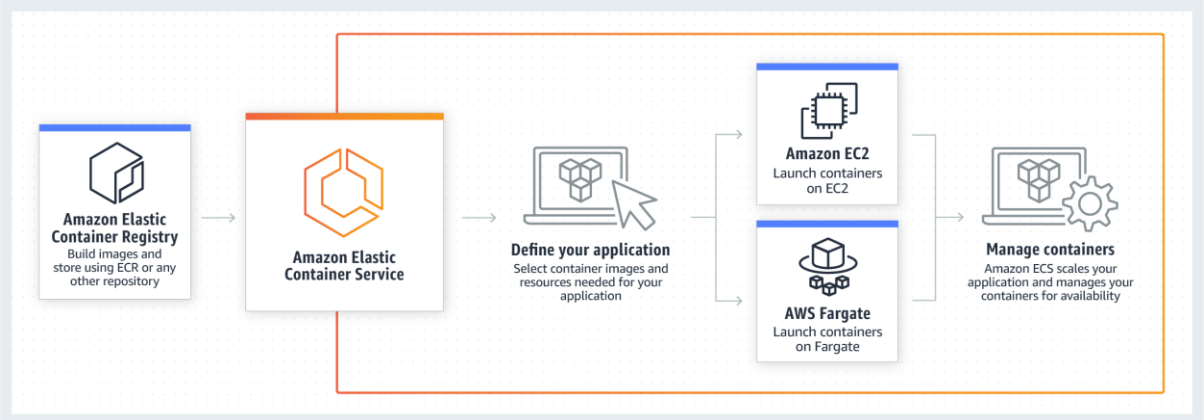


via - https://aws.amazon.com/ecr/

Incorrect options:

Amazon Elastic Container Service (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. You cannot use ECS to store and deploy docker container images.

Please see this schematic diagram to understand how ECS works:



via - https://aws.amazon.com/ecs/

Amazon EC2 - 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.

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

References:

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

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

Question 32:

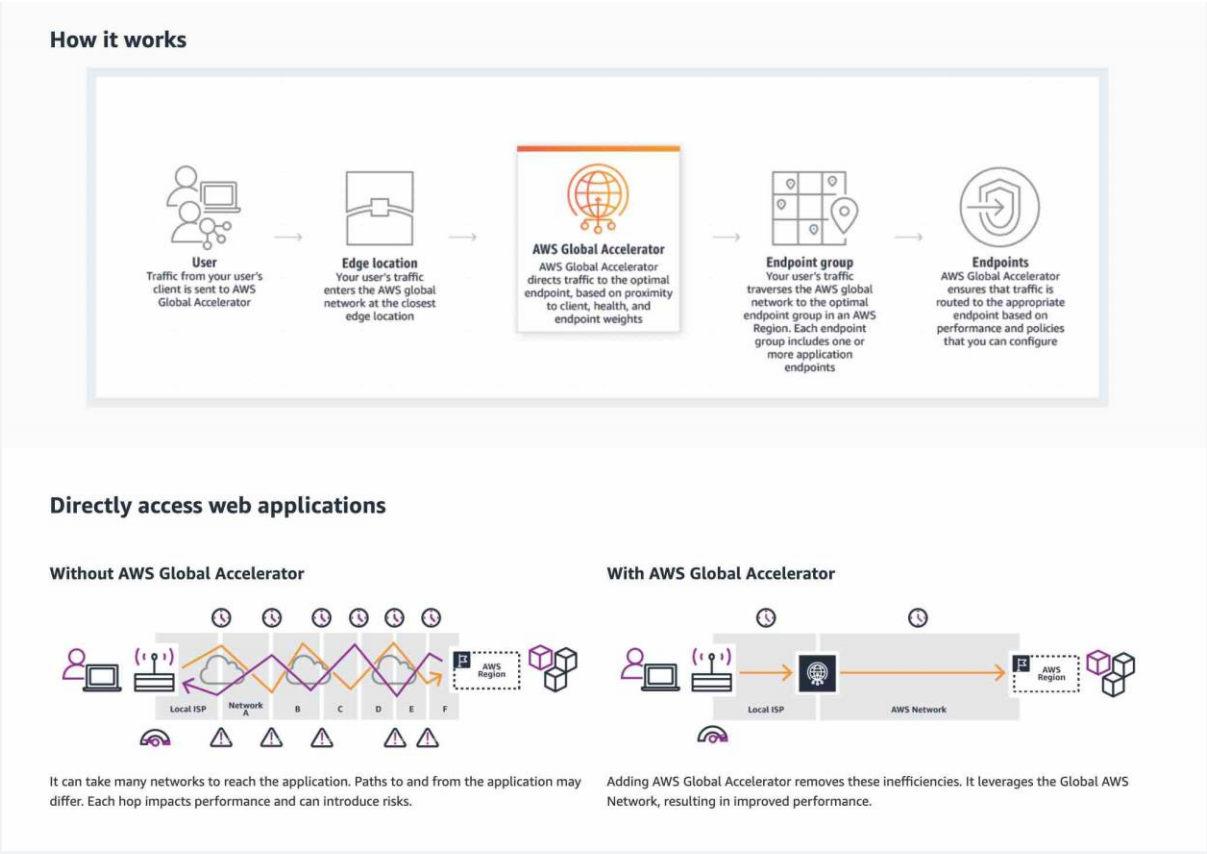
Which AWS service helps with global application availability and performance using the AWS global network?
Explanation
Correct option:

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%.

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. 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 Global Accelerator
Works:



via - https://aws.amazon.com/global-accelerator/

Exam Alert:

Please review the differences between CloudFront and Global Accelerator:

Q: How is AWS Global Accelerator different from Amazon CloudFront?

A: AWS Global Accelerator and Amazon CloudFront are separate services that use the AWS global network and its edge locations around the world. CloudFront improves performance for both cacheable content (such as images and videos) and dynamic content (such as API acceleration and dynamic site delivery). 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. 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. Both services integrate with AWS Shield for DDoS protection.

via - https://aws.amazon.com/global-accelerator/faqs/

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

Elastic Load Balancer - Elastic Load Balancer 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 scales your load balancer as traffic to your application changes over time. It can automatically scale to the vast majority of workloads. Elastic Load Balancer 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. Route 53 cannot be used to improve application availability and performance using the AWS global network.

Reference:

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

Question 33:
What are the fundamental drivers of cost with AWS Cloud?

Explanation
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:

Understand the fundamentals of pricing

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.

In most cases, there is no charge for inbound data transfer or for data transfer between other AWS services within the same region. There are some exceptions, so be sure to verify data transfer rates before beginning. Outbound data transfer is aggregated across services and then charged at the outbound data transfer rate. This charge appears on the monthly statement as AWS Data Transfer Out. The more data you transfer, the less you pay per GB. For compute resources, you pay hourly from the time you launch a resource until the time you terminate it, unless you have made a reservation for which the cost is agreed upon beforehand. For data storage and transfer, you typically pay per GB.

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

Incorrect options:

"Compute, Storage and Inbound Data Transfer"

"Compute, Databases and Outbound Data Transfer"

"Compute, Storage and Outbound Data Transfer"

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

Reference:

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

Question 34:

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)

- Step

Explanation

Correct option:

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.

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.

Incorrect options:

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.

EC2 Instance - 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.

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

Question 35:

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 Practioner, which of the following AWS services would you recommend for this use-case?

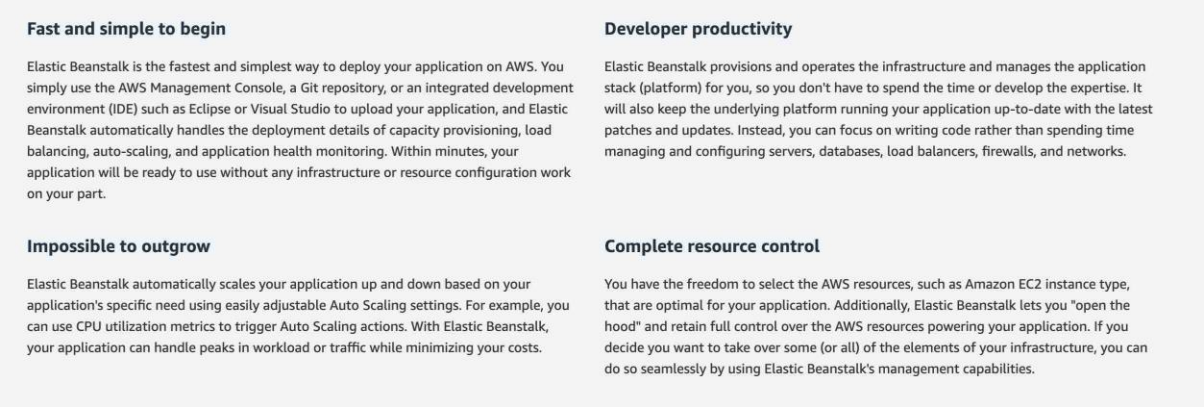
-
- **Explanation**

Correct option:

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 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 Elastic Beanstalk - you pay only for the AWS resources needed to store and run your applications.

Key Benefits of Elastic
Beanstalk:



via - https://aws.amazon.com/elasticbeanstalk/

Incorrect 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 CloudFormation, you have to explicitly specify which resources you want to provision.

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.

AWS Elastic Container Service (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. ECS cannot handle the application deployment automatically, so this option is not correct.

Reference:

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

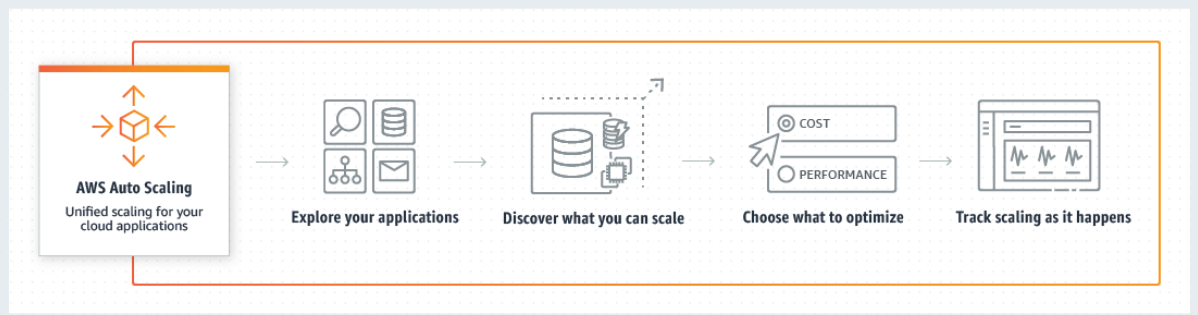
Question 36:
Which AWS technology/service helps you to scale your resources to match supply with demand while still keeping your cloud solution cost-effective?

-
- **Explanation**

Correct option: **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 Auto Scaling Works:



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

Incorrect 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/

Question 37:

Which AWS service can be used to review the compliance and governance-related documents on AWS?
Explanation
Correct option:

Artifact

AWS Artifact is your central resource for compliance-related information on AWS Cloud. It provides on-demand access to AWS' security and compliance reports and select online agreements. Reports available in AWS Artifact include the Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, and certifications from accreditation bodies across geographies. Agreements available in AWS Artifact also include the Business Associate Addendum (BAA) and the Nondisclosure Agreement (NDA).

Incorrect options:

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 review the compliance and governance-related documents on 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. Service Catalog cannot be used to review the compliance and governance-related documents on 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 to review the compliance and governance-related documents on AWS.

Reference:

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

Question 38:
Which policy describes prohibited uses of the web services offered by Amazon Web Services?

- 
- **Explanation**

Correct option:

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.

Incorrect 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/

Question 39:
Which of the following AWS services allows a database to have flexible schema and supports document data models?

Explanation

Correct option:

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. DynamoDB supports both key-value and document data models. This enables 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.

Incorrect options:

Amazon RDS for PostgreSQL - Amazon RDS for PostgreSQL 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. RDS for PostgreSQL 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. Aurora does not support flexible schema.

Reference:

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

Question 40:
Which AWS service can be used to provision resources to run big data workloads on Hadoop clusters?

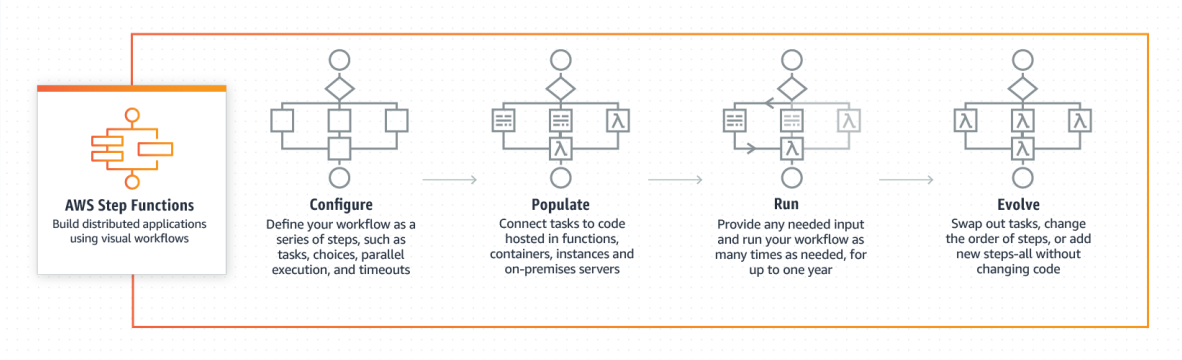
Explanation
Correct option:

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.

Incorrect options:

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.

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:

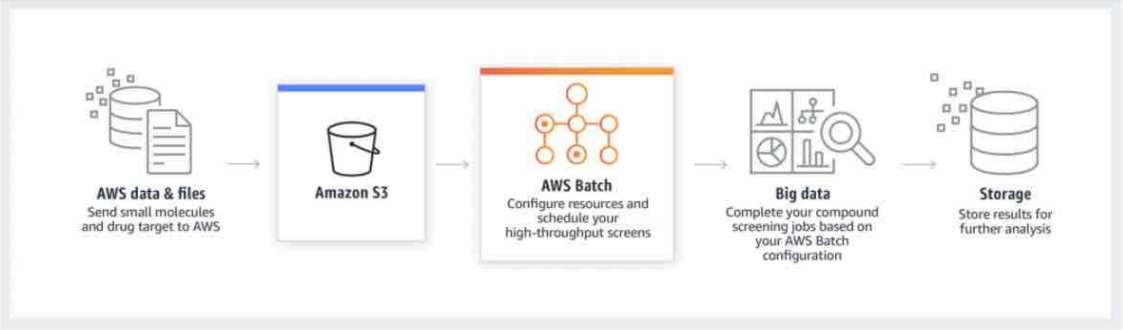
Use cases

Financial services: Post-trade analytics

Automate the analysis of the day's transaction costs, execution reporting, and market performance.

Life sciences: Drug screening for biopharma

Rapidly search libraries of small molecules for drug discovery.



Digital media: Visual effects rendering

Automate content rendering workloads and reduce the need for human intervention due to execution dependencies or resource scheduling.

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 Function does not provision any resources. Step Function only orchestrates AWS services required for a given workflow. You cannot use Step Functions to plan, schedule and execute your batch computing workloads by provisioning underlying resources.

Amazon EC2 - 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 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/

Question 41:
What are the different gateway types supported by AWS Storage Gateway service?

-
- **Explanation**

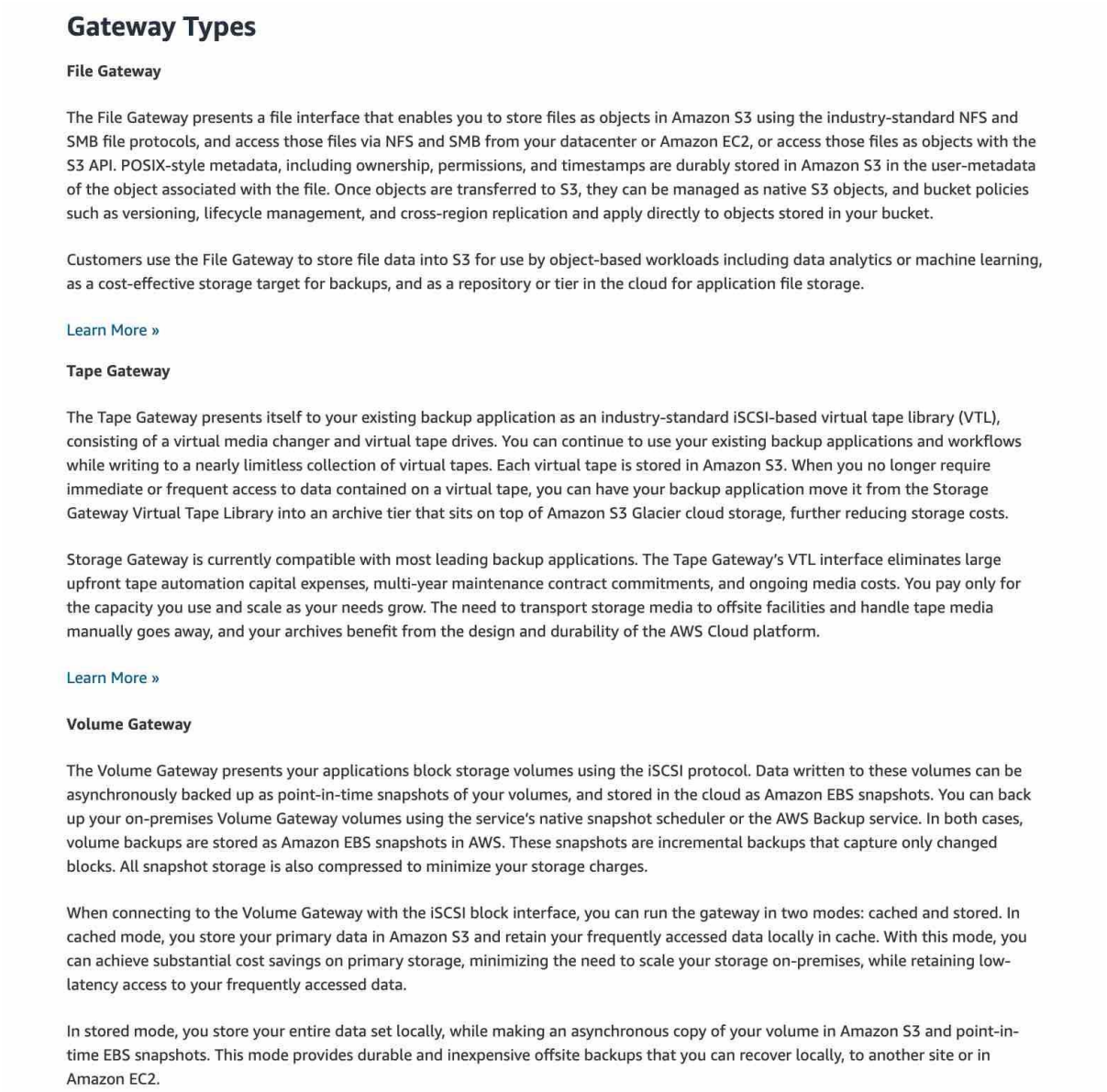
Correct option:

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:



Gateway Types

File Gateway

The File Gateway presents a file interface that enables you to store files as objects in Amazon S3 using the industry-standard NFS and SMB file protocols, and access those files via NFS and SMB from your datacenter or Amazon EC2, or access those files as objects with the S3 API. POSIX-style metadata, including ownership, permissions, and timestamps are durably stored in Amazon S3 in the user-metadata of the object associated with the file. Once objects are transferred to S3, they can be managed as native S3 objects, and bucket policies such as versioning, lifecycle management, and cross-region replication and apply directly to objects stored in your bucket.

Customers use the File Gateway to store file data into S3 for use by object-based workloads including data analytics or machine learning, as a cost-effective storage target for backups, and as a repository or tier in the cloud for application file storage.

Learn More »

Tape Gateway

The Tape Gateway presents itself to your existing backup application as an industry-standard iSCSI-based virtual tape library (VTL), consisting of a virtual media changer and virtual tape drives. You can continue to use your existing backup applications and workflows while writing to a nearly limitless collection of virtual tapes. Each virtual tape is stored in Amazon S3. When you no longer require immediate or frequent access to data contained on a virtual tape, you can have your backup application move it from the Storage Gateway Virtual Tape Library into an archive tier that sits on top of Amazon S3 Glacier cloud storage, further reducing storage costs.

Storage Gateway is currently compatible with most leading backup applications. The Tape Gateway's VTL interface eliminates large upfront tape automation capital expenses, multi-year maintenance contract commitments, and ongoing media costs. You pay only for the capacity you use and scale as your needs grow. The need to transport storage media to offsite facilities and handle tape media manually goes away, and your archives benefit from the design and durability of the AWS Cloud platform.

Learn More »

Volume Gateway

The Volume Gateway presents your applications block storage volumes using the iSCSI protocol. Data written to these volumes can be asynchronously backed up as point-in-time snapshots of your volumes, and stored in the cloud as Amazon EBS snapshots. You can back up your on-premises Volume Gateway volumes using the service's native snapshot scheduler or the AWS Backup service. In both cases, volume backups are stored as Amazon EBS snapshots in AWS. These snapshots are incremental backups that capture only changed blocks. All snapshot storage is also compressed to minimize your storage charges.

When connecting to the Volume Gateway with the iSCSI block interface, you can run the gateway in two modes: cached and stored. In cached mode, you store your primary data in Amazon S3 and retain your frequently accessed data locally in cache. With this mode, you can achieve substantial cost savings on primary storage, minimizing the need to scale your storage on-premises, while retaining low-latency access to your frequently accessed data.

In stored mode, you store your entire data set locally, while making an asynchronous copy of your volume in Amazon S3 and point-in-time EBS snapshots. This mode provides durable and inexpensive offsite backups that you can recover locally, to another site or in Amazon EC2.

via - https://aws.amazon.com/storagegateway/features/

Incorrect 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/

Question 42:
A log archival application deployed on Amazon EC2 instances runs every Monday between 3 AM and 5 AM. Can you suggest a cost-effective EC2 instance purchasing option for this use-case?

Explanation

Correct option:

Scheduled Reserved Instances

Scheduled Reserved Instances (Scheduled Instances) enable you to purchase capacity reservations that recur on a daily, weekly, or monthly basis, with a specified start time and duration, for a one-year term. Scheduled Instances are a good choice for workloads that do not run continuously, but do run on a regular schedule. For example, you can use Scheduled Instances for an application that runs during business hours or for batch processing that runs at the end of the week. You pay for the time that the instances are scheduled, even if you do not use them.

Incorrect options:

On-Demand Instances - 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. 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 would be costlier than Scheduled Reserved instances, so this option is ruled out.

Reserved Instances - Reserved Instances provide you with significant savings on your Amazon EC2 costs compared to On-Demand Instance pricing. Reserved Instances 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 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 running weekly workloads.

Spot Instances - 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 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.

Reference:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-scheduled-instances.html

Question 43:
Which of the following statements is INCORRECT about AWS Auto Scaling?

Explanation
Correct option:

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.

Incorrect 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 EC2 instances to match an increase in demand as well as scale in and remove 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:

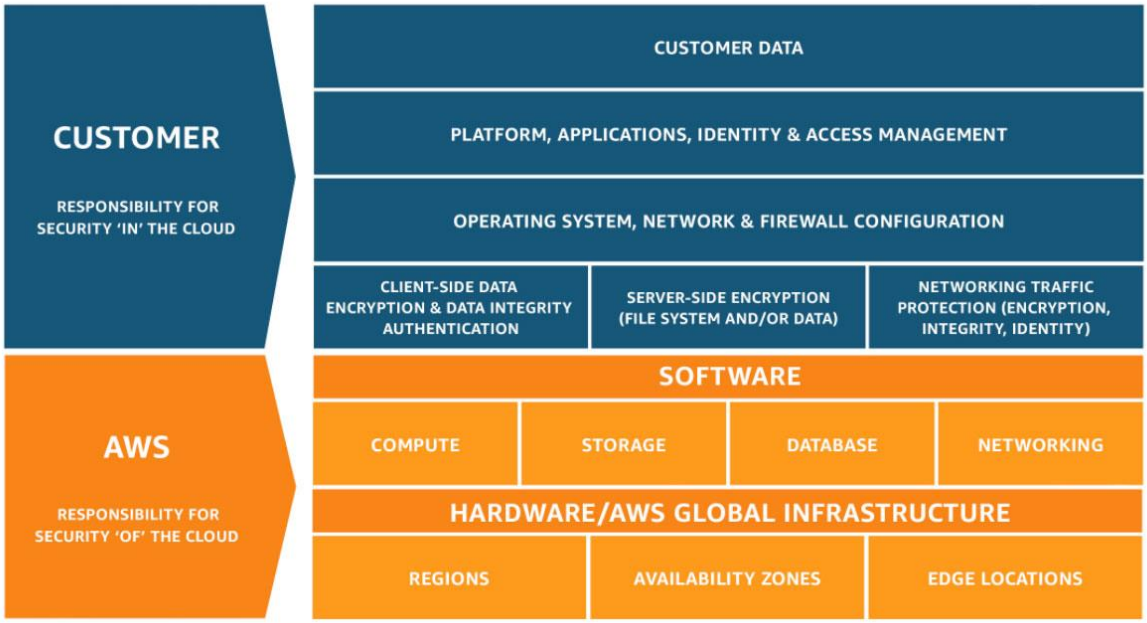
https://aws.amazon.com/autoscaling/

Question 44:
According to the AWS Shared Responsibility Model, which of the following are responsibilities of the customer for Amazon RDS?
Explanation
Correct option:

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 shared model, customers are responsible for managing their data, including data encryption.

Shared Responsibility Model
Overview:



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

Incorrect 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 RDS runs - Since RDS is a managed service, the underlying infrastructure is the responsibility of AWS.

Applying patches to the RDS database - Since RDS is a managed service, the underlying infrastructure is the responsibility of AWS.

Applying patches to the underlying OS - Since RDS is a managed service, the underlying infrastructure is the responsibility of AWS.

Reference:

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

Question 45:

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

- ☐

Explanation
Correct options:

AWS Identity and Access Management (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 IAM, Amazon CloudFront, Route 53 and WAF are some of the global services.

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.

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.

Incorrect 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 type of Cloud Computing. This is a regional service.

Exam Alert:

Amazon S3 - 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/

Question 46:

Which AWS 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?

- **Explanation**

Correct option:

Latency routing policy

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 those computers use to connect to each other.

If your application is hosted in multiple AWS Regions, you can use latency 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 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. Route 53 responds with the value from the selected record, such as the IP address for a web server.

Route 53 Routing Policy
Overview:

Choosing a routing policy

PDF | Kindle | RSS

When you create a record, you choose a routing policy, which determines how Amazon Route 53 responds to queries:

- **Simple routing policy** – Use for a single resource that performs a given function for your domain, for example, a web server that serves content for the example.com website.
- **Failover routing policy** – Use when you want to configure active-passive failover.
- **Geolocation routing policy** – Use when you want to route traffic based on the location of your users.
- **Geoproximity routing policy** – Use when you want to route traffic based on the location of your resources and, optionally, shift traffic from resources in one location to resources in another.
- **Latency routing policy** – Use when you have resources in multiple AWS Regions and you want to route traffic to the region that provides the best latency.
- **Multivalue answer routing policy** – Use when you want Route 53 to respond to DNS queries with up to eight healthy records selected at random.
- **Weighted routing policy** – Use to route traffic to multiple resources in proportions that you specify.

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

Incorrect options:

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

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

Simple routing policy - 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

Question 47:
Access Key ID and Secret Access Key are tied to which of the following AWS Identity and Access Management entities?

- **Explanation**

Correct option: **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.

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

AWS 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

Question 48: Correct
A customer has created a VPC and a subnet within AWS Cloud. Which of the following statements is correct?
Explanation
Correct option:

A VPC spans all of the Availability Zones in the Region whereas a subnet spans only one Availability Zone 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. A VPC spans all of the Availability Zones in the Region.

A subnet is a range of IP addresses within your VPC. A subnet spans only one Availability Zone in the Region.

VPC and Subnet
Overview:

The following diagram shows a new VPC with an IPv4 CIDR block.

The main route table has the following routes.

Destination	Target
10.0.0.0/16	local

A VPC spans all of the Availability Zones in the Region. After creating a VPC, you can add one or more subnets in each Availability Zone. You can optionally add subnets in a Local Zone, which is an AWS infrastructure deployment that places compute, storage, database, and other select services closer to your end users. A Local Zone enables your end users to run applications that require single-digit millisecond latencies. For information about the Regions that support Local Zones, see Available Regions in the *Amazon EC2 User Guide for Linux Instances*. When you create a subnet, you specify the CIDR block for the subnet, which is a subset of the VPC CIDR block. Each subnet must reside entirely within one Availability Zone and cannot span zones. Availability Zones are distinct locations that are engineered to be isolated from failures in other Availability Zones. By launching instances in separate Availability Zones, you can protect your applications from the failure of a single location. We assign a unique ID to each subnet.

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

Incorrect options:

Both the VPC and the subnet span all of the Availability Zones in the Region

Both the VPC and the subnet span only one Availability Zone in the Region

A subnet spans all of the Availability Zones in the Region whereas a VPC spans only one Availability Zone in the Region

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

Reference:

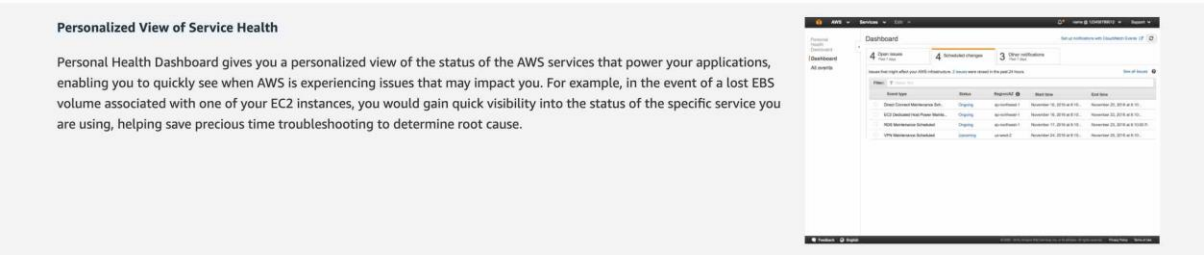
https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Subnets.html

Question 49:
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?

Explanation
Correct option: **AWS Personal Health Dashboard**

AWS Personal Health Dashboard provides alerts and remediation guidance when AWS is experiencing events that may impact you. With Personal 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.

AWS Personal Health Dashboard
Overview:



via - https://status.aws.amazon.com/

Incorrect options:

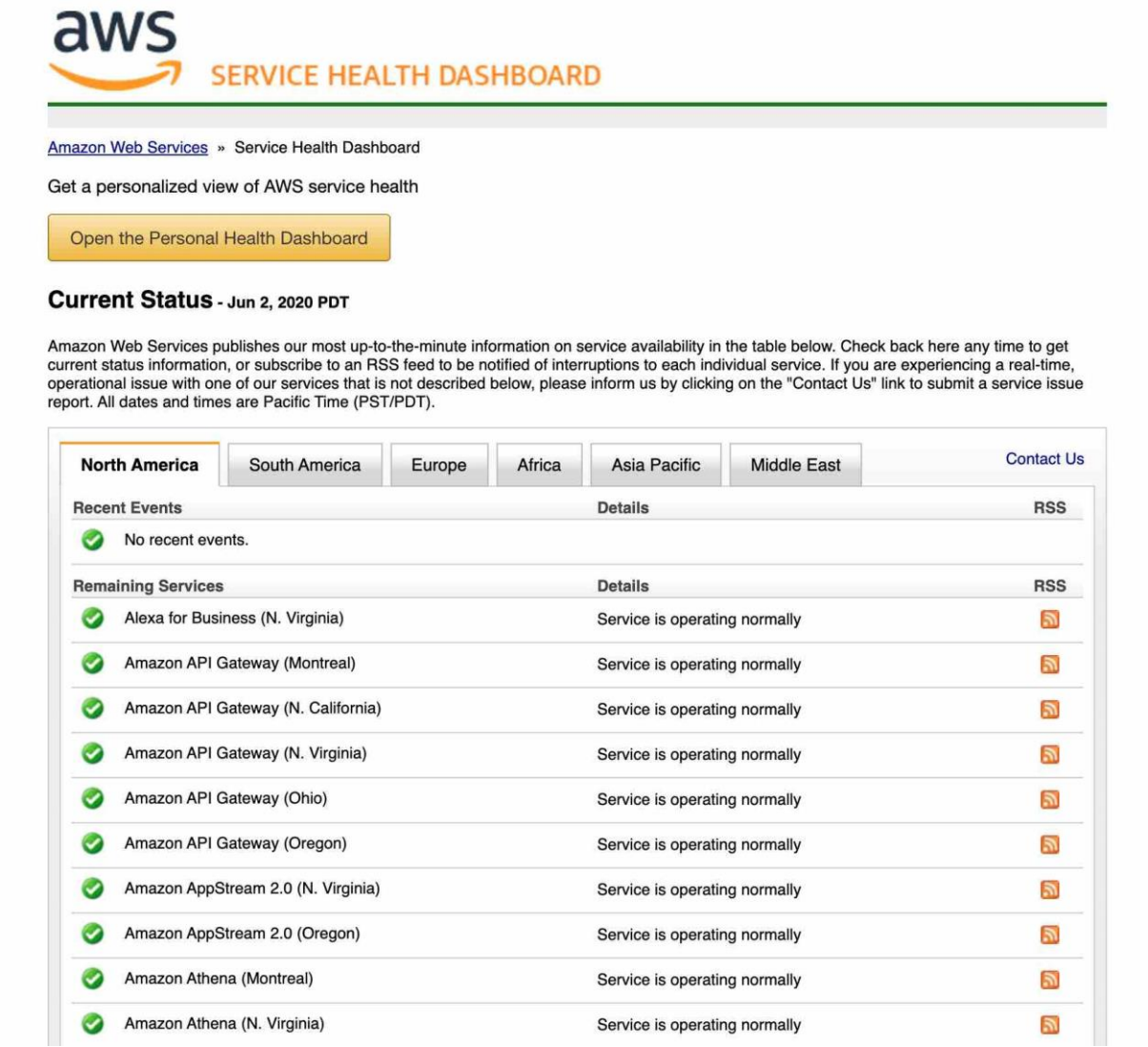
Amazon Inspector - Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for exposure, vulnerabilities, and deviations from best practices. Amazon Inspector cannot 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 Service Health Dashboard - AWS Service Health Dashboard publishes most up-to-the-minute information on the status and availability of all AWS services in tabular form for all Regions that AWS is present in. You can check on this page (https://status.aws.amazon.com/) any time to get current status information or subscribe to an RSS feed to be notified of interruptions to each service.

AWS Service Health Dashboard
Overview:



via - https://status.aws.amazon.com/

Exam Alert:

While the Service Health Dashboard displays the general status of AWS services, Personal Health Dashboard gives you a personalized view of the performance and availability of the AWS services underlying your AWS resources.

Reference:

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

Question 50:
Which of the following statement is correct for a Security Group and a Network Access Control List?

Explanation
Correct option:

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

Security group basics

The following are the basic characteristics of security groups for your VPC:

- There are quotas on the number of security groups that you can create per VPC, the number of rules that you can add to each security group, and the number of security groups that you can associate with a network interface. For more information, see Amazon VPC quotas.
- You can specify allow rules, but not deny rules.
- You can specify separate rules for inbound and outbound traffic.
- When you create a security group, it has no inbound rules. Therefore, no inbound traffic originating from another host to your instance is allowed until you add inbound rules to the security group.
- By default, a security group includes an outbound rule that allows all outbound traffic. You can remove the rule and add outbound rules that allow specific outbound traffic only. If your security group has no outbound rules, no outbound traffic originating from your instance is allowed.
- Security groups are stateful — if you send a request from your instance, the response traffic for that request is allowed to flow in regardless of inbound security group rules. Responses to allowed inbound traffic are allowed to flow out, regardless of outbound rules.

  Note

  Some types of traffic are tracked differently from other types. For more information, see Connection tracking in the *Amazon EC2 User Guide for Linux Instances*.

- Instances associated with a security group can't talk to each other unless you add rules allowing the traffic (exception: the default security group has these rules by default).
- Security groups are associated with network interfaces. After you launch an instance, you can change the security groups that are associated with the instance, which changes the security groups associated with the primary network interface (eth0). You can also specify or change the security groups associated with any other network interface. By default, when you create a network interface, it's associated with the default security group for the VPC, unless you specify a different security group. For more information about network interfaces, see Elastic network interfaces.
- When you create a security group, you must provide it with a name and a description. The following rules apply:
  - Names and descriptions can be up to 255 characters in length.
  - Names and descriptions are limited to the following characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*.
  - A security group name cannot start with `sg-` as these indicate a default security group.
  - A security group name must be unique within the VPC.
- A security group can only be used in the VPC that you specify when you create the security group.

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

Network Access Control List (NACL)
Overview:

Network ACL basics

The following are the basic things that you need to know about network ACLs:

- Your VPC automatically comes with a modifiable default network ACL. By default, it allows all inbound and outbound IPv4 traffic and, if applicable, IPv6 traffic.
- You can create a custom network ACL and associate it with a subnet. By default, each custom network ACL denies all inbound and outbound traffic until you add rules.
- Each subnet in your VPC must be associated with a network ACL. If you don't explicitly associate a subnet with a network ACL, the subnet is automatically associated with the default network ACL.
- You can associate a network ACL with multiple subnets. However, a subnet can be associated with only one network ACL at a time. When you associate a network ACL with a subnet, the previous association is removed.
- A network ACL contains a numbered list of rules. We evaluate the rules in order, starting with the lowest numbered rule, to determine whether traffic is allowed in or out of any subnet associated with the network ACL. The highest number that you can use for a rule is 32766. We recommend that you start by creating rules in increments (for example, increments of 10 or 100) so that you can insert new rules where you need to later on.
- A network ACL has separate inbound and outbound rules, and each rule can either allow or deny traffic.
- Network ACLs are stateless, which means that responses to allowed inbound traffic are subject to the rules for outbound traffic (and vice versa).

There are quotas (limits) for the number of network ACLs per VPC, and the number of rules per network ACL. For more information, see Amazon VPC quotas.

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

Incorrect options:

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

Security Group acts as a firewall at the VPC level whereas Network Access Control List acts as a firewall at the AZ level - As explained above, the security group acts at the instance level and ACL is at the subnet level.

Security Group acts as a firewall at the AZ level whereas Network Access Control List acts as a firewall at the VPC level - As explained above, the security group acts at the instance level and 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

Question 51:
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?

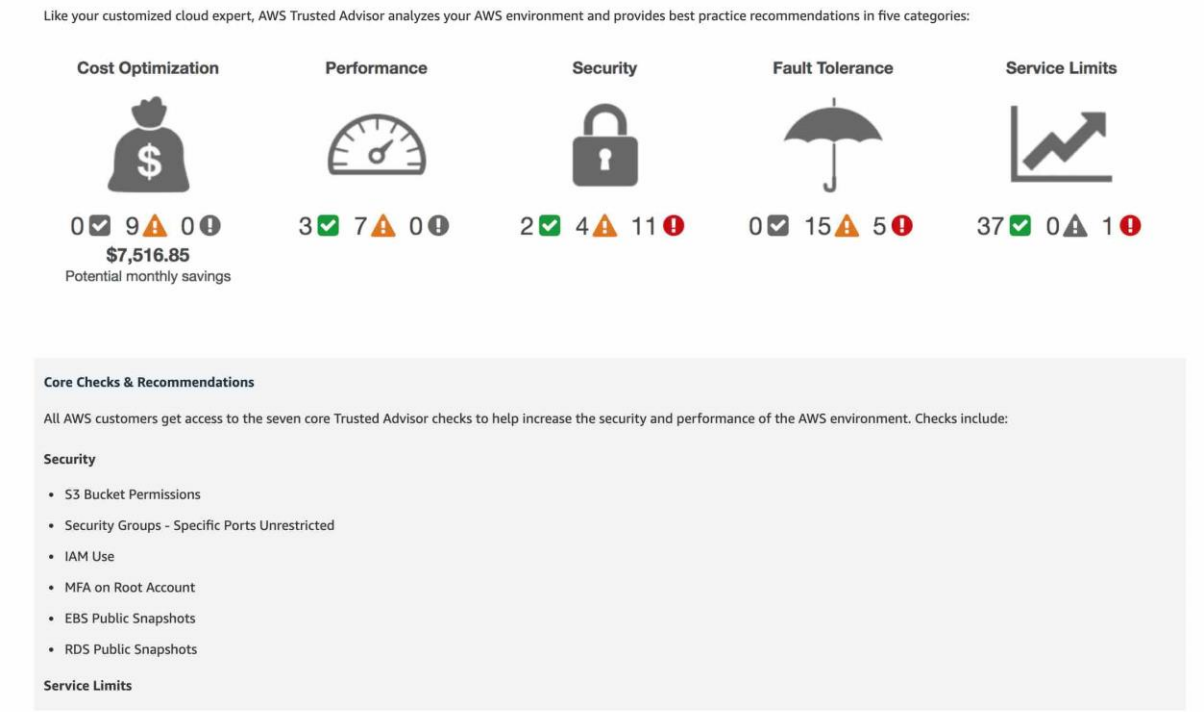
Explanation
Correct option: **AWS Trusted Advisor**

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/

Incorrect 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.

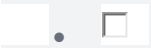
Amazon CloudWatch - Amazon CloudWatch is a monitoring and observability service built for DevOps engineers, developers, site reliability engineers (SREs), and IT managers. CloudWatch provides data and actionable insights to monitor applications, respond to system-wide performance changes, optimize resource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

Question 52:
Which of the following AWS services are always free to use (Select two)?



Explanation
Correct options:

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 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.

Incorrect options:

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.

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.

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/

Question 53:

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?

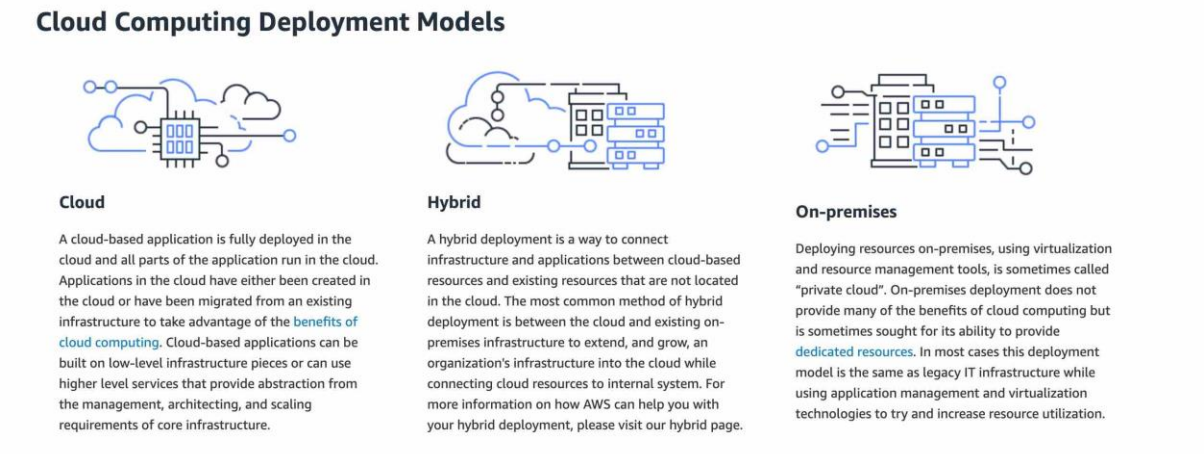
-

Explanation
Correct option:

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/

Incorrect 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/

Question 54:
An e-commerce company wants to assess its applications for vulnerabilities and deviations from AWS best practices. Which AWS service can be used to facilitate this?

Explanation
Correct option:

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/

Incorrect 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 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 security assessment of applications deployed on AWS.

Reference:

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

Question 55:
A photo sharing web application wants to store thumbnails of user-uploaded images on 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 S3?

Explanation
Correct option:

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

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

	S3 Standard	S3 Intelligent-Tiering*	S3 Standard-IA	S3 One Zone-IA†	S3 Glacier	S3 Glacier Deep Archive
Designed for durability	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)
Designed for availability	99.99%	99.9%	99.9%	99.5%	99.99%	99.99%
Availability SLA	99.9%	99%	99%	99%	99.9%	99.9%
Availability Zones	≥3	≥3	≥3	1	≥3	≥3
Minimum capacity charge per object	N/A	N/A	128KB	128KB	40KB	40KB
Minimum storage duration charge	N/A	30 days	30 days	30 days	90 days	180 days
Retrieval fee	N/A	N/A	per GB retrieved	per GB retrieved	per GB retrieved	per GB retrieved
First byte latency	milliseconds	milliseconds	milliseconds	milliseconds	select minutes or hours	select hours
Storage type	Object	Object	Object	Object	Object	Object
Lifecycle transitions	Yes	Yes	Yes	Yes	Yes	Yes

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

Incorrect options:

Use S3 Standard Infrequent Access (Standard-IA) to store the thumbnails - S3 Standard-IA storage class is for data that is accessed less frequently but requires rapid access when needed. 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. S3 One Zone-IA costs 20% less than S3 Standard-IA, so this option is incorrect.

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

Use S3 Glacier to store the thumbnails - S3 Glacier is a secure, durable, and low-cost storage class for data archiving. Although Glacier is cheaper than 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/

Question 56:
As per the AWS shared responsibility model, which of the following is a responsibility of AWS from a security and compliance point of view?

Explanation
Correct option:

Edge Location Management

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.

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

Incorrect options:

Customer Data

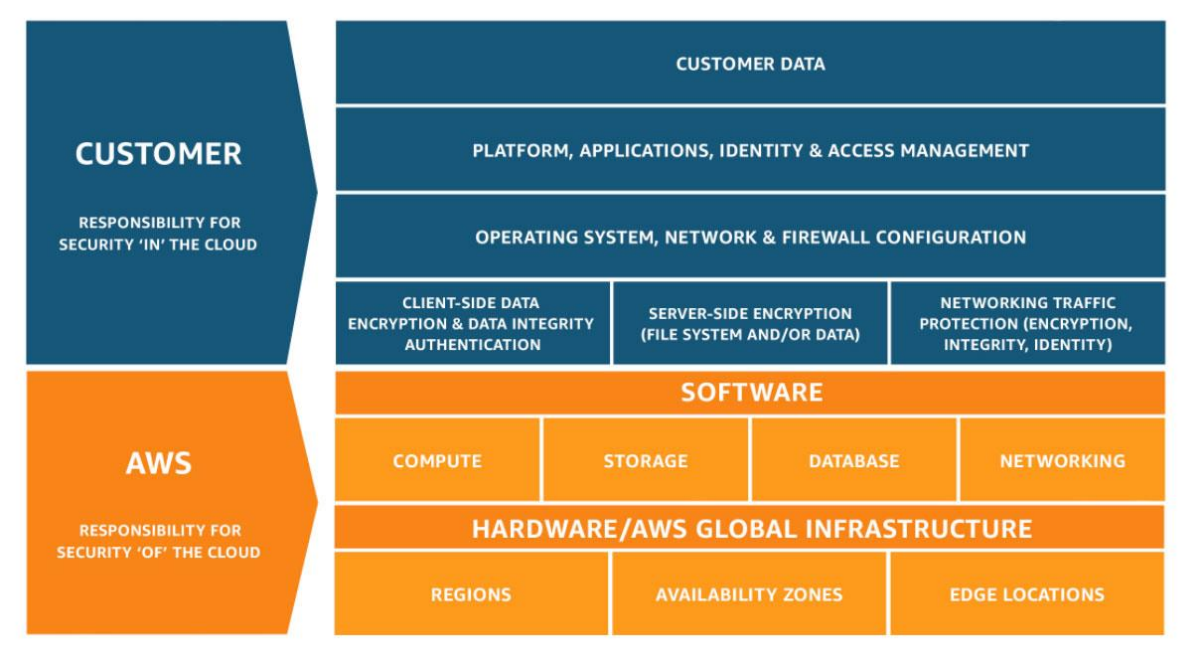
Identity and Access Management

Server-side Encryption

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 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/

Reference:

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

Question 57:

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?

Explanation
Correct option:

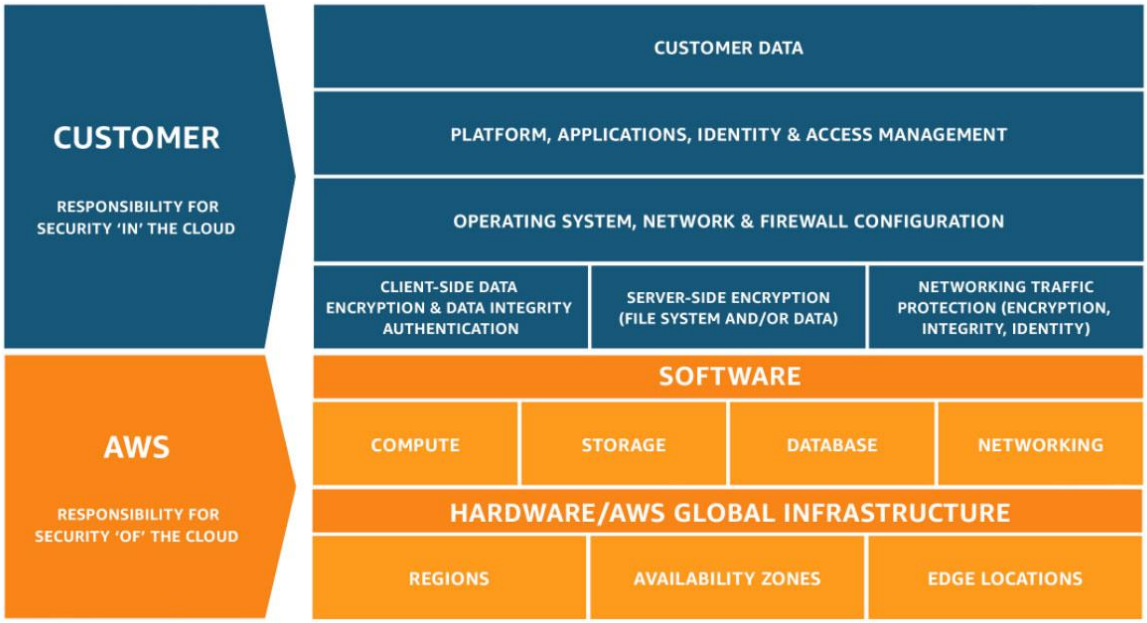
Managing patches of the guest operating system on Amazon EC2

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/

Incorrect options:

Configuration management for AWS global infrastructure

Availability Zone 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 infrastructure management, and patching/fixing flaws within the AWS infrastructure are responsibilities of AWS.

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

Question 58:
A multi-national company wants to migrate its IT infrastructure to AWS Cloud and is looking for a concierge support team as well as a response time of around an hour in case the systems go down. As a Cloud Practitioner, which of the following support plans would you recommend to the company?

Explanation
Correct option:

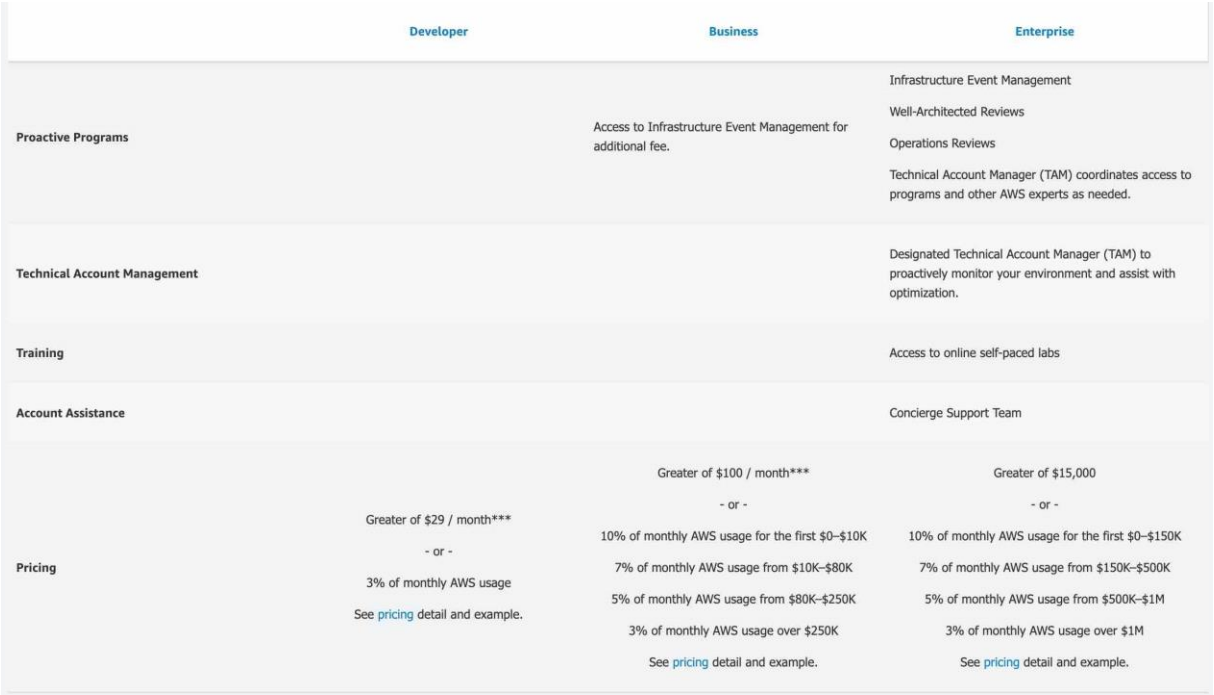
Enterprise

The Concierge Support Team is only available for the Enterprise Support plan. The Concierge Team are AWS billing and account experts that specialize in working with enterprise accounts. They will quickly and efficiently assist you with your billing and account inquiries. Enterprise Support plan provides a response time of fewer than 15 minutes for business-critical systems and provides a response time of less than an hour for production systems related outage. So this is the correct option.

Exam Alert:

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

	Developer	Business	Enterprise
	Recommended if you are experimenting or testing in AWS.	*Recommended if you have production workloads in AWS.*	*Recommended if you have business and/or mission critical workloads in AWS.*
AWS Trusted Advisor Best Practice Checks	7 Core checks	Full set of checks	Full set of checks
Enhanced Technical Support	Business hours** email access to Cloud Support Associates Unlimited cases / 1 primary contact	24x7 phone, email, and chat access to Cloud Support Engineers Unlimited cases / unlimited contacts (IAM supported)	24x7 phone, email, and chat access to Cloud Support Engineers Unlimited cases / unlimited contacts (IAM supported)
Case Severity / Response Times*	General guidance: < 24 business hours** System impaired: < 12 business hours**	General guidance: < 24 hours System impaired: < 12 hours Production system impaired: < 4 hours Production system down: < 1 hour	General guidance: < 24 hours System impaired: < 12 hours Production system impaired: < 4 hours Production system down: < 1 hour Business-critical system down: < 15 minutes
Architectural Guidance	General	Contextual to your use-cases	Consultative review and guidance based on your applications
Programmatic Case Management		AWS Support API	AWS Support API
Third-Party Software Support		Interoperability & configuration guidance and troubleshooting	Interoperability & configuration guidance and troubleshooting



	Developer	Business	Enterprise
Proactive Programs		Access to Infrastructure Event Management for additional fee.	Infrastructure Event Management Well-Architected Reviews Operations Reviews Technical Account Manager (TAM) coordinates access to programs and other AWS experts as needed.
Technical Account Management			Designated Technical Account Manager (TAM) to proactively monitor your environment and assist with optimization.
Training			Access to online self-paced labs
Account Assistance			Concierge Support Team
Pricing	Greater of $29 / month*** - or - 3% of monthly AWS usage See pricing detail and example.	Greater of $100 / month*** - or - 10% of monthly AWS usage for the first $0–$10K 7% of monthly AWS usage from $10K–$80K 5% of monthly AWS usage from $80K–$250K 3% of monthly AWS usage over $250K See pricing detail and example.	Greater of $15,000 - or - 10% of monthly AWS usage for the first $0–$150K 7% of monthly AWS usage from $150K–$500K 5% of monthly AWS usage from $500K–$1M 3% of monthly AWS usage over $1M See pricing detail and example.

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

Incorrect options:

Developer - Concierge Support Team is only available for Enterprise Support plan so this option is incorrect.

Business - Concierge Support Team is only available for Enterprise Support plan so this option is incorrect.

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

Reference:

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

Question 59:
Which of the following statement is correct regarding the AWS pricing policy for data transfer charges?
Explanation
Correct option:

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.

Incorrect options:

Only inbound data transfer is charged - There is no charge for inbound data transfer or data transfer between other AWS services within the same Region.

Both inbound data transfer and outbound data transfer are charged - This is an incorrect statement.

Data transfer between AWS services within the same region is charged - Per AWS pricing, data transfer between AWS services within the same region is not charged.

Reference:

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

Question 60:
Which of the following AWS services can be used to prevent Distributed Denial-of-Service (DDoS) attack? (Select three)

- ☑

Explanation
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 WAF - By using 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.

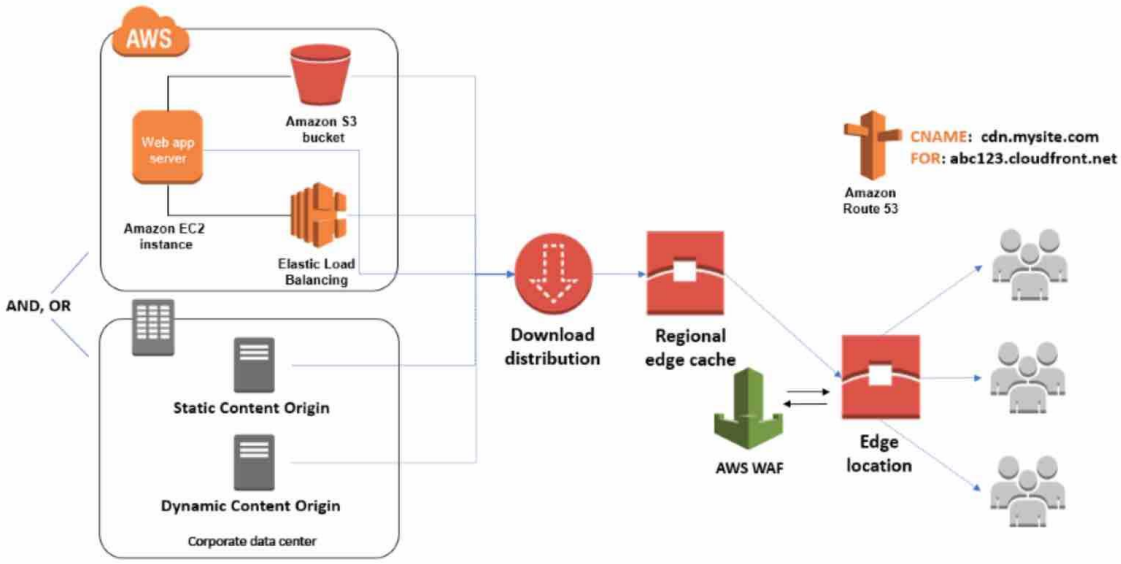
Amazon CloudFront with Route 53 - AWS hosts CloudFront and Route 53 services on a distributed network of proxy servers in data centers throughout the world called edge locations. Using the global Amazon network of edge locations for application delivery and DNS service plays an important part in building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

How AWS Shield, WAF, and CloudFront with Route 53 help mitigate DDoS attacks:

How AWS Shield, CloudFront, and Route 53 work to help protect against DDoS attacks

To help keep your dynamic web applications available when they are under DDoS attack, the steps in this post enable AWS Shield Standard by configuring your applications behind CloudFront and Route 53. AWS Shield Standard protects your resources from common, frequently occurring network and transport layer DDoS attacks. Attack traffic can be geographically isolated and absorbed using the capacity in edge locations close to the source. Additionally, you can configure geographical restrictions to help block attacks originating from specific countries.

The request-routing technology in CloudFront connects each client to the nearest edge location, as determined by continuously updated latency measurements. HTTP and HTTPS requests sent to CloudFront can be monitored, and access to your application resources can be controlled at edge locations using AWS WAF. Based on conditions that you specify in AWS WAF, such as the IP addresses that requests originate from or the values of query strings, traffic can be allowed, blocked, or allowed and counted for further investigation or remediation. The following diagram shows how static and dynamic web application content can originate from endpoint resources within AWS or your corporate data center. For more details, see How CloudFront Delivers Content and How CloudFront Works with Regional Edge Caches.



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

Incorrect 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. 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/

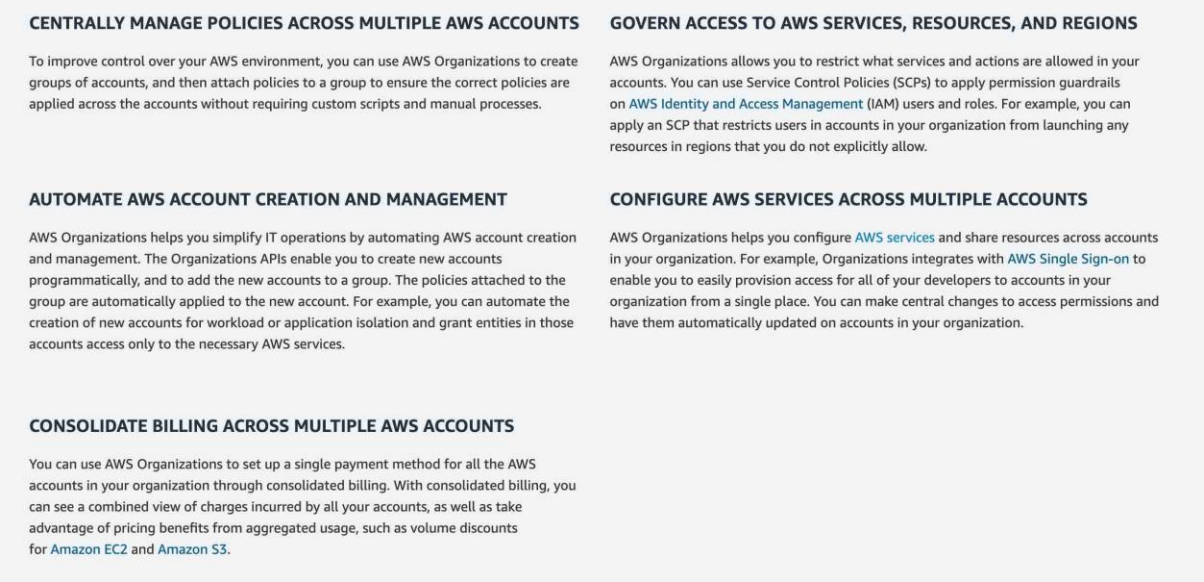
Question 61:
A retail company has multiple AWS accounts for each of its departments. Which of the following AWS services can be used to set up consolidated billing and a single payment method for these AWS accounts?

Explanation
Correct option:

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/

Incorrect 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 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 Secrets Manager to set up consolidated billing and a single payment method for multiple AWS accounts.

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

Question 62:
Which AWS support plan provides access to a Technical Account Manager (TAM)?

Explanation
Correct option:

"Enterprise"

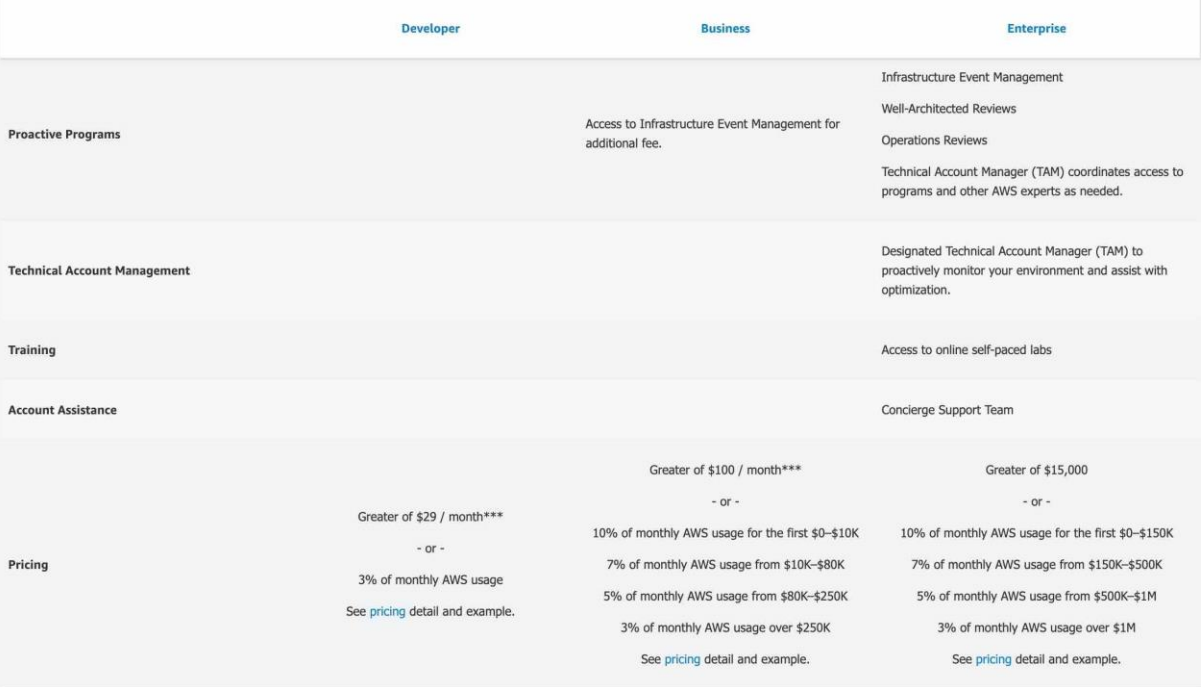
AWS offers three different support plans to cater to each of its customers - Developer, Business, and Enterprise Support plans. A basic support plan is included for all AWS customers.

AWS Enterprise Support provides customers with concierge-like service where the main focus is helping the customer achieve their outcomes and find success in the cloud. With 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 Developer, Business, and Enterprise support plans as you can expect at least a couple of questions on the exam:

	Developer	Business	Enterprise
	Recommended if you are experimenting or testing in AWS.	*Recommended if you have production workloads in AWS.*	*Recommended if you have business and/or mission critical workloads in AWS.*
AWS Trusted Advisor Best Practice Checks	7 Core checks	Full set of checks	Full set of checks
Enhanced Technical Support	Business hours** email access to Cloud Support Associates Unlimited cases / 1 primary contact	24x7 phone, email, and chat access to Cloud Support Engineers Unlimited cases / unlimited contacts (IAM supported)	24x7 phone, email, and chat access to Cloud Support Engineers Unlimited cases / unlimited contacts (IAM supported)
Case Severity / Response Times*	General guidance: < 24 business hours** System impaired: < 12 business hours**	General guidance: < 24 hours System impaired: < 12 hours Production system impaired: < 4 hours Production system down: < 1 hour	General guidance: < 24 hours System impaired: < 12 hours Production system impaired: < 4 hours Production system down: < 1 hour Business-critical system down: < 15 minutes
Architectural Guidance	General	Contextual to your use-cases	Consultative review and guidance based on your applications
Programmatic Case Management		AWS Support API	AWS Support API
Third-Party Software Support		Interoperability & configuration guidance and troubleshooting	Interoperability & configuration guidance and troubleshooting



	Developer	Business	Enterprise
Proactive Programs		Access to Infrastructure Event Management for additional fee.	Infrastructure Event Management Well-Architected Reviews Operations Reviews Technical Account Manager (TAM) coordinates access to programs and other AWS experts as needed.
Technical Account Management			Designated Technical Account Manager (TAM) to proactively monitor your environment and assist with optimization.
Training			Access to online self-paced labs
Account Assistance			Concierge Support Team
Pricing	Greater of $29 / month*** - or - 3% of monthly AWS usage See pricing detail and example.	Greater of $100 / month*** - or - 10% of monthly AWS usage for the first $0–$10K 7% of monthly AWS usage from $10K–$80K 5% of monthly AWS usage from $80K–$250K 3% of monthly AWS usage over $250K See pricing detail and example.	Greater of $15,000 - or - 10% of monthly AWS usage for the first $0–$150K 7% of monthly AWS usage from $150K–$500K 5% of monthly AWS usage from $500K–$1M 3% of monthly AWS usage over $1M See pricing detail and example.

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

Incorrect options:

"Developer" - AWS recommends Developer Support 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.

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

"Business & Enterprise" - This is an invalid option and has been added as a distractor. An Enterprise plan will include all the facilities offered by Developer and Business Support plans already.

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

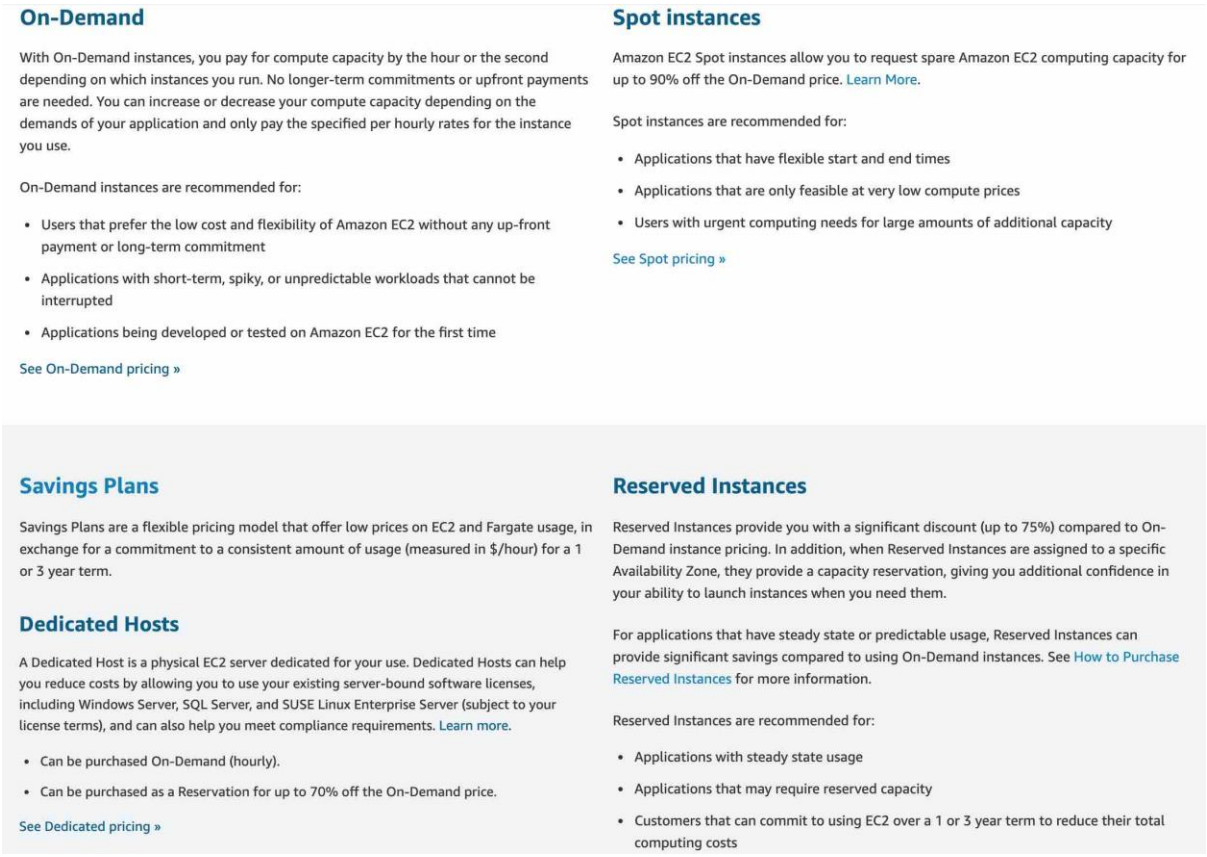
Question 63:
Which AWS EC2 pricing model is the most cost-effective and flexible with no requirement for a long term resource commitment or upfront payment but still guarantees that instance would not be interrupted?

Explanation
Correct option:

On-Demand Instances - 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:



On-Demand

With On-Demand instances, you pay for compute capacity by the hour or the second depending on which instances you run. No longer-term commitments or upfront payments are needed. You can increase or decrease your compute capacity depending on the demands of your application and only pay the specified per hourly rates for the instance you use.

On-Demand instances are recommended for:

- Users that prefer the low cost and flexibility of Amazon EC2 without any up-front payment or long-term commitment
- Applications with short-term, spiky, or unpredictable workloads that cannot be interrupted
- Applications being developed or tested on Amazon EC2 for the first time

See On-Demand pricing »

Spot instances

Amazon EC2 Spot instances allow you to request spare Amazon EC2 computing capacity for up to 90% off the On-Demand price. Learn More.

Spot instances are recommended for:

- Applications that have flexible start and end times
- Applications that are only feasible at very low compute prices
- Users with urgent computing needs for large amounts of additional capacity

See Spot pricing »

Savings Plans

Savings Plans are a flexible pricing model that offer low prices on EC2 and Fargate usage, in exchange for a commitment to a consistent amount of usage (measured in $/hour) for a 1 or 3 year term.

Dedicated Hosts

A Dedicated Host is a physical EC2 server dedicated for your use. Dedicated Hosts can help you reduce costs by allowing you to use your existing server-bound software licenses, including Windows Server, SQL Server, and SUSE Linux Enterprise Server (subject to your license terms), and can also help you meet compliance requirements. Learn more.

- Can be purchased On-Demand (hourly).
- Can be purchased as a Reservation for up to 70% off the On-Demand price.

See Dedicated pricing »

Reserved Instances

Reserved Instances provide you with a significant discount (up to 75%) compared to On-Demand instance pricing. In addition, when Reserved Instances are assigned to a specific Availability Zone, they provide a capacity reservation, giving you additional confidence in your ability to launch instances when you need them.

For applications that have steady state or predictable usage, Reserved Instances can provide significant savings compared to using On-Demand instances. See How to Purchase Reserved Instances for more information.

Reserved Instances are recommended for:

- Applications with steady state usage
- Applications that may require reserved capacity
- Customers that can commit to using EC2 over a 1 or 3 year term to reduce their total computing costs

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

Incorrect options:

Reserved Instances - Reserved Instances provide you with significant savings on your Amazon EC2 costs compared to On-Demand Instance pricing. Reserved Instances 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 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 running weekly workloads. So this option is not correct for the given use-case.

Spot Instances - 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 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 Hosts - Amazon EC2 Dedicated Hosts allow 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. They're not cost-efficient compared to On-Demand instances. So this option is not correct.

Reference:

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

Question 64:
Which of the following is the correct statement regarding the AWS Storage services?

Explanation
Correct option:

S3 is object based storage, EBS is block based storage and 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 (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.

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

Incorrect options:

S3 is block based storage, EBS is object based storage and EFS is file based storage

S3 is object based storage, EBS is file based storage and EFS is block based storage

S3 is file based storage, EBS is block based storage and EFS is object based storage

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

References:

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

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

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

Question 65:
Which of the following statements are true about AWS Lambda? (Select two)

- ☑

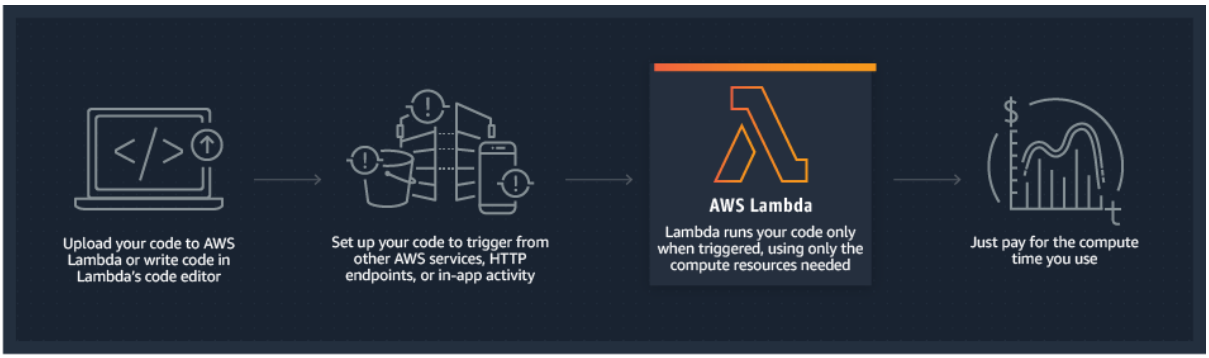
Explanation
Correct options:

AWS Lambda lets you run code without provisioning or managing servers

You pay only for the compute time you consume

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 only for the compute time you consume - 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 Lambda
Works:



via - https://aws.amazon.com/lambda/

Incorrect options:

Allows you to install databases on the underlying serverless Operating System - 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.

Allows you to easily run, scale, and secure Docker container applications on 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 run Docker container applications, though it can serve as backend for applications.

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