

Question 1:

Which of the following criteria are used to charge for Elastic Block Store (EBS) volumes?
(Select TWO)

-

Explanation

Correct option:

Provisioned IOPS

Volume Type

Amazon Elastic Block Store (Amazon EBS) provides persistent block storage volumes for use with Amazon EC2 instances in the AWS Cloud. Each Amazon EBS volume is automatically replicated within its Availability Zone to protect you from component failure, offering high availability and durability. Amazon EBS volumes offer the consistent and low-latency performance needed to run your workloads. With Amazon EBS, you can scale your usage up or down within minutes—all while paying a low price for only what you provision.

The fundamental charges for EBS volumes are: the volume type (based on performance), the storage volume in GB per month provisioned, the number of IOPS provisioned per month, the storage consumed by snapshots, and outbound data transfer.

Incorrect options:

Data transfer IN - Data transfer-in is always free, including for EBS volumes.

The EC2 instance type the EBS volume is attached to - The EC2 instance type the EBS volume is attached to does not influence the EBS volume pricing.

Data type - The type of data stored on EBS volumes does not influence the price.

Reference:

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

Question 2: **Correct**

Which of the following options are the benefits of using AWS Elastic Load Balancing (ELB)? (Select TWO)

Explanation

Correct option:

High availability

Fault tolerance

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

Elastic Load Balancing offers three types of load balancers that all feature the high availability, automatic scaling, and robust security necessary to make your applications fault-tolerant: Application Load Balancer (best suited for HTTP and HTTPS traffic), Network Load Balancer (best suited for TCP traffic), and Classic Load Balancer.

Incorrect options:

Agility - Agility refers to new IT resources being only a click away, which means that you reduce the time to make those resources available to your developers from weeks to just minutes. AWS Elastic Load Balancing does not help with agility.

Less costly - AWS Elastic Load Balancing does not help with reducing costs.

Storage - AWS Elastic Load Balancing does not offer storage benefits. It is not a storage-related service.

Reference:

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

Question 3: **Correct**

A developer would like to automate operations on his on-premises environment using Chef and Puppet. Which AWS service can help with this task?

Explanation

Correct option:

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.

Incorrect options:

AWS CloudFormation - AWS CloudFormation gives developers and systems administrators an easy way to create and manage a collection of related AWS resources, provisioning and updating them in an orderly and predictable fashion. It does not use Chef and Puppet and is more focused on what and how AWS resources are procured.

AWS CodeDeploy - AWS CodeDeploy is a service that automates code deployments to any instance, including EC2 instances and instances running on premises. It does not use Chef and Puppet, and does not deal with infrastructure configuration and orchestration.

AWS Batch - AWS Batch enables developers, scientists, and engineers to easily and efficiently run hundreds of thousands of batch computing jobs on AWS. It is not used to automate operations on his on-premises environment using Chef and Puppet.

Reference:

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

Question 4:

A company would like to reserve EC2 compute capacity for three years to reduce costs. The company also plans to increase their workloads during this period. As a Cloud Practitioner, which EC2 Reserved Instance type would you recommend?



Explanation

Correct option:

Convertible Reserved Instances

Purchase Convertible Reserved Instances if you need additional flexibility, such as the ability to use different instance families, operating systems, or tenancies over the Reserved Instance term. Convertible Reserved Instances provide you with a significant discount (up to 54%) compared to On-Demand Instances and can be purchased for a 1-year or 3-year term.

Convertible Reserved Instances can be useful when workloads are likely to change. In this case, a Convertible Reserved Instance enables you to adapt as needs evolve while still obtaining discounts and capacity reservations.

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:

Standard Reserved Instances - Standard Reserved Instances provide you with a significant discount (up to 72%) compared to On-Demand Instance pricing, and can be purchased for a 1-year or 3-year term. Standard Reserved Instances do not offer as much flexibility as Convertible Reserved Instances (such as not being able to change the instance family type), and therefore are not best-suited for this use case.

Review the differences between Standard Reserved Instances and Convertible Reserved Instances: <https://docs.aws.amazon.com/whitepapers/latest/cost-optimization-reservation-models/standard-vs.-convertible-offering-classes.html>

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. In this use case, the company would like to purchase EC2 compute capacity for 3 years, thus Scheduled Reserved Instances are not suited.

Adaptable Reserved Instances - Adaptable Reserved Instances are not a valid type of reserved instances. It is a distractor.

Reference:

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

Question 5: **Correct**

A start-up would like to quickly deploy a popular technology on AWS. As a Cloud Practitioner, which AWS tool would you use for this task?



Explanation

Correct option:

AWS Quick Starts references

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

Each Quick Start includes AWS CloudFormation templates that automate the deployment and a guide that discusses the architecture and provides step-by-step deployment instructions.

Incorrect options:

AWS Forums - AWS Forums is an AWS community platform where people can help each other. It is not used to deploy technologies on AWS.

AWS CodeDeploy - AWS CodeDeploy is a service that automates code deployments to any instance, including EC2 instances and instances running on-premises. It is not suited to rapidly deploy popular technologies on AWS ready to use immediately.

AWS Whitepapers - AWS Whitepapers are technical content authored by AWS and the AWS community to expand your knowledge of the cloud. They include technical whitepapers, technical guides, reference material, and reference architectures diagrams. You can find useful content for your deployment, but it is not a service that will deploy technologies.

Reference:

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

Question 6:

A company would like to separate cost for AWS services by the department for cost allocation. Which of the following actions can assist with this task?



Explanation

Correct option:

Create tags for each department

You can assign metadata to your AWS resources in the form of tags. Each tag is a label consisting of a user-defined key and value. Tags can help you manage, identify, organize, search for, and filter resources. You can create tags to categorize resources by purpose, owner, environment, or other criteria.

Typically, you use business tags such as cost center/business unit, customer, or project to associate AWS costs with traditional cost-allocation dimensions. But a cost allocation report can include any tag. This lets you associate costs with technical or security dimensions, such as specific applications, environments, or compliance programs.

Example of tagging for cost

Total Cost	user:Owner	user:Stack	user:Cost Center	user:Application
0.95	DbAdmin	Test	80432	Widget2
0.01	DbAdmin	Test	80432	Widget2
3.84	DbAdmin	Prod	80432	Widget2
6.00	DbAdmin	Test	78925	Widget1
234.63	SysEng	Prod	78925	Widget1
0.73	DbAdmin	Test	78925	Widget1
0.00	DbAdmin	Prod	80432	Portal
2.47	DbAdmin	Prod	78925	Portal

optimization: via

- https://docs.aws.amazon.com/general/latest/gr/aws_tagging.html

Incorrect options:

Create different accounts for different departments - Users can belong to several departments. Therefore, having different accounts for different departments would imply some users having several accounts. This is contrary to the security best practice: one physical user = one account.

Create one account for each department and share this account - Sharing accounts is not a security best practice, and is not recommended.

Create different VPCs for different departments - Creating different VPCs will not help with separating costs.

Reference:

https://docs.aws.amazon.com/general/latest/gr/aws_tagging.html

Question 7:

Which AWS database is an easily scalable relational database?



Explanation

Correct option:

Amazon RDS

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

You can highly scale your database's compute and storage resources with only a few mouse clicks or an API call, often with no downtime. Many Amazon RDS engine types allow you to launch one or more Read Replicas to offload read traffic from your primary database instance.

Incorrect options:

Amazon ElastiCache - Amazon ElastiCache is a web service that makes it easy to deploy, operate, and scale an in-memory cache in the cloud. It is an in-memory cache, and uses key/value store.

Amazon S3 - Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. It is not a relational database.

Amazon DynamoDB - DynamoDB is a fast and flexible nonrelational database service for any scale. 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. It is not a relational database.

Reference:

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

Question 8:

According to the Well-Architected Framework, which of the following action is recommended in the Security pillar?



Explanation

Correct option:

Use AWS KMS to encrypt data

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

Encrypting data is part of the design principle "Protect data in transit and at rest": Classify your data into sensitivity levels and use mechanisms, such as encryption, tokenization, and access control where appropriate.

AWS Key Management Service (AWS KMS) makes it easy for you to create and control keys used for encryption. It is a key service of the Security pillar.

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

The AWS Well-Architected Framework is based on five pillars — Operational Excellence, Security, Reliability, Performance Efficiency, and Cost Optimization.

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



Operational Excellence

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

[Operational Excellence whitepaper PDF | Kindle](#)



Security

The security pillar focuses on protecting information & systems. Key topics include confidentiality and integrity of data, identifying and managing who can do what with privilege management, protecting systems, and establishing controls to detect security events.

[Download the Security Pillar whitepaper PDF | Kindle](#)



Reliability

The reliability pillar focuses on the ability to prevent, and quickly recover from failures to meet business and customer demand. Key topics include foundational elements around setup, cross project requirements, recovery planning, and how we handle change.

[Download the Reliability Pillar whitepaper PDF | Kindle](#)



Performance Efficiency

The performance efficiency pillar focuses on using IT and computing resources efficiently. Key topics include selecting the right resource types and sizes based on workload requirements, monitoring performance, and making informed decisions to maintain efficiency as business needs evolve.

[Download the Performance Efficiency whitepaper PDF | Kindle](#)



Cost Optimization

Cost Optimization focuses on avoiding un-needed costs. Key topics include understanding and controlling where money is being spent, selecting the most appropriate and right number of resource types, analyzing spend over time, and scaling to meet business needs without overspending.

[Download the Cost Optimization whitepaper PDF | Kindle](#)

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

Incorrect options:

Use AWS Cost Explorer to view and track your usage in detail - AWS Cost Explorer has an easy-to-use interface that lets you visualize, understand, and manage your AWS costs and usage over time. Using Cost Explorer to view and track your usage in detail relates more to the Cost Optimization pillar.

Use Amazon CloudWatch to measure overall efficiency - Amazon CloudWatch is a monitoring and management service built for developers, system operators, site reliability engineers (SRE), and IT managers. Using Amazon CloudWatch to measure overall efficiency relates more to the Reliability pillar.

Use AWS CloudFormation to automate security best practices - AWS CloudFormation provides a common language for you to model and provision AWS and third-party application resources in your cloud environment. It is not used to automate security best practices. If you want to automate security best practices, you should use Amazon Inspector.

Reference:

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

Question 9:

A streaming application delivers content around the world. Which AWS service can improve performance for users?

Explanation

Correct option:

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 is integrated with AWS – both physical locations that are directly connected to the AWS global infrastructure, as well as other AWS services.

Incorrect options:

AWS Lambda - AWS Lambda lets you run code without provisioning or managing servers. It does not improve application performance.

AWS Auto Scaling - Amazon EC2 Auto Scaling helps you maintain application availability and allows you to automatically add or remove EC2 instances according to conditions you define. It does not improve application performance.

AWS Trusted Advisor - AWS Trusted Advisor is an online resource to help you reduce cost, increase performance, and improve security by optimizing your AWS environment. Trusted Advisor provides real-time guidance to help you provision your resources following AWS best practices. It does not improve application performance.

Reference:

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

Question 10:

Adding more CPU/RAM to an Amazon EC2 instance represents which of the following?



Loose coupling

Explanation

Correct option:

Vertical scaling

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.

Incorrect options:

Horizontal scaling - A "horizontally scalable" system is one that can increase capacity by adding more computers to the system.

Managing increasing volumes of data - Traditional data storage and analytics tools can no longer provide the agility and flexibility required to deliver relevant business insights. That's why many organizations are shifting to a data lake architecture. A data lake is an architectural

approach that allows you to store massive amounts of data in a central location so that it's readily available to be categorized, processed, analyzed, and consumed by diverse groups within your organization.

Loose coupling - As application complexity increases, a desirable attribute of an IT system is that it can be broken into smaller, loosely coupled components. This means that IT systems should be designed in a way that reduces interdependencies—a change or a failure in one component should not cascade to other components.

Reference:

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

Question 11:

Which AWS service allows you to quickly and easily add user sign-up, sign-in, and access control to web and mobile applications?

Explanation

Correct option:

Amazon Cognito

Amazon Cognito lets you add user sign-up, sign-in, and access control to your web and mobile apps quickly and easily. With Amazon Cognito, you also have the option to authenticate users through social identity providers such as Facebook, Twitter, or Amazon, with SAML identity solutions, or by using your own identity system.

Incorrect options:

AWS Identity and Access Management (IAM) - AWS Identity and Access Management (IAM) enables you to securely control access to AWS services and resources for your users. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources. It does not provide user sign-up, sign-in, and access control to web and mobile applications.

AWS Single Sign-On (SSO) - AWS Single Sign-On (SSO) is a cloud SSO service that makes it easy to centrally manage SSO access to multiple AWS accounts and business applications. With just a few clicks, you can enable a highly available SSO service without the upfront investment and on-going maintenance costs of operating your own SSO infrastructure. With AWS SSO, you can easily manage SSO access and user permissions to all of your accounts in AWS Organizations centrally. It does not provide user sign-up, sign-in, and access control to web and mobile applications.

AWS Organizations - AWS Organizations offers policy-based management for multiple AWS accounts. With Organizations, you can create groups of accounts, automate account creation, apply and manage policies for those groups. Organizations enables you to centrally manage policies across multiple accounts, without requiring custom scripts and manual processes. It does not provide user sign-up, sign-in, and access control to web and mobile applications.

Reference:

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

Question 12:

A multinational company has just moved its infrastructure to AWS Cloud and has employees traveling to different offices around the world. How should the company set the AWS accounts?



Explanation

Correct option:

There is nothing to do, IAM is a global service

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 global service. Users created within IAM can access their accounts all around the world, and deploy resources in every region.

Incorrect options:

Create an IAM user for each user in each region - IAM users can access their accounts in different regions.

Create 'global' permissions so users can access resources from all around the world - IAM is a global service. You can use it globally without implementing anything.

As employees travel, they can use other employees' accounts - You should never share IAM users.

Reference:

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

Question 13:

An organization would like to copy data across different Availability Zones (AZs) using EBS snapshots. Where are EBS snapshots stored in the AWS Cloud?



Explanation

Correct option:

Amazon S3

You can create a point-in-time snapshot of an EBS volume and use it as a baseline for new volumes or data backup. If you make periodic snapshots of a volume, the snapshots are incremental—the new snapshot saves only the blocks that have changed since your last snapshot.

You can back up the data on your Amazon EBS volumes to Amazon S3 by taking point-in-time snapshots.

Incorrect options:

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 computing easier for developers. EBS snapshots cannot be stored on Amazon EC2.

Amazon RDS - Amazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and scale a relational database in the cloud. EBS snapshots cannot be stored on Amazon RDS.

Amazon EFS - Amazon Elastic File System (Amazon EFS) provides a simple, scalable, elastic file system for Linux-based workloads for use with AWS Cloud services and on-premises resources. EBS snapshots cannot be stored on Amazon EFS.

Reference:

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

Question 14:

A Cloud Practitioner would like to deploy identical resources across all regions and accounts using templates while estimating costs. Which AWS service can assist with this task?



Explanation

Correct option:

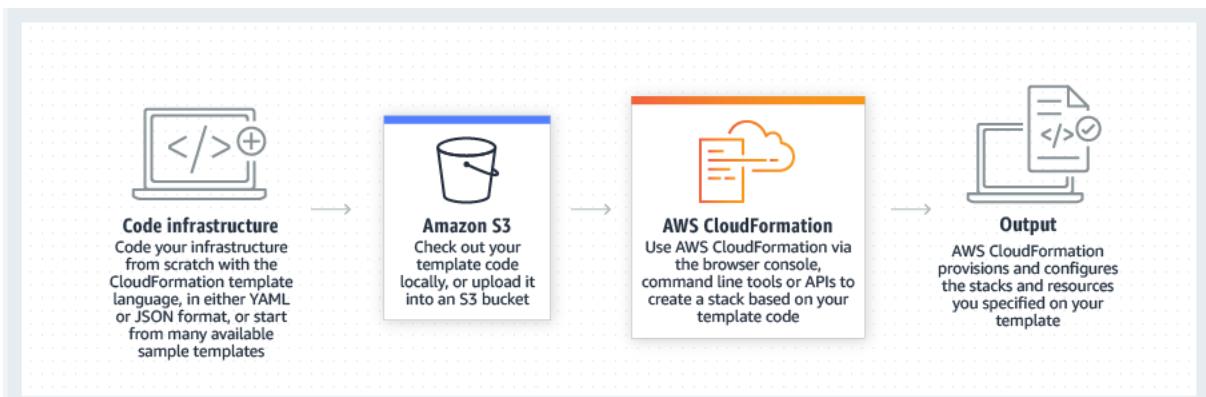
AWS CloudFormation

AWS CloudFormation gives developers and systems administrators an easy way to create and manage a collection of related AWS resources, provisioning and updating them in an orderly and predictable fashion.

You can use the AWS CloudFormation sample templates or create your own templates to describe your AWS resources, and any associated dependencies or runtime parameters, required to run your application. This provides a single source of truth for all your resources and helps you to standardize infrastructure components used across your organization, enabling configuration compliance and faster troubleshooting.

CloudFormation templates allow you to estimate the cost of your resources.

How AWS CloudFormation works:



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

Incorrect options:

AWS Directory Service - AWS Directory Service for Microsoft Active Directory, also known as AWS Managed Microsoft AD, enables your directory-aware workloads and AWS resources to use managed Active Directory in the AWS Cloud. It is not used to deploy resources.

Amazon LightSail - Amazon Lightsail is designed to be the easiest way to launch and manage a virtual private server with AWS. It is not best suited when deploying more complex resources, while CloudFormation can.

AWS CodeDeploy - AWS CodeDeploy is a service that automates code deployments to any instance, including EC2 instances and instances running on-premises. Unlike CloudFormation, it does not deal with infrastructure configuration and orchestration.

Reference:

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

Question 15:

A research lab needs to be notified in case of a configuration change for security and compliance reasons. Which AWS service can assist with this task?

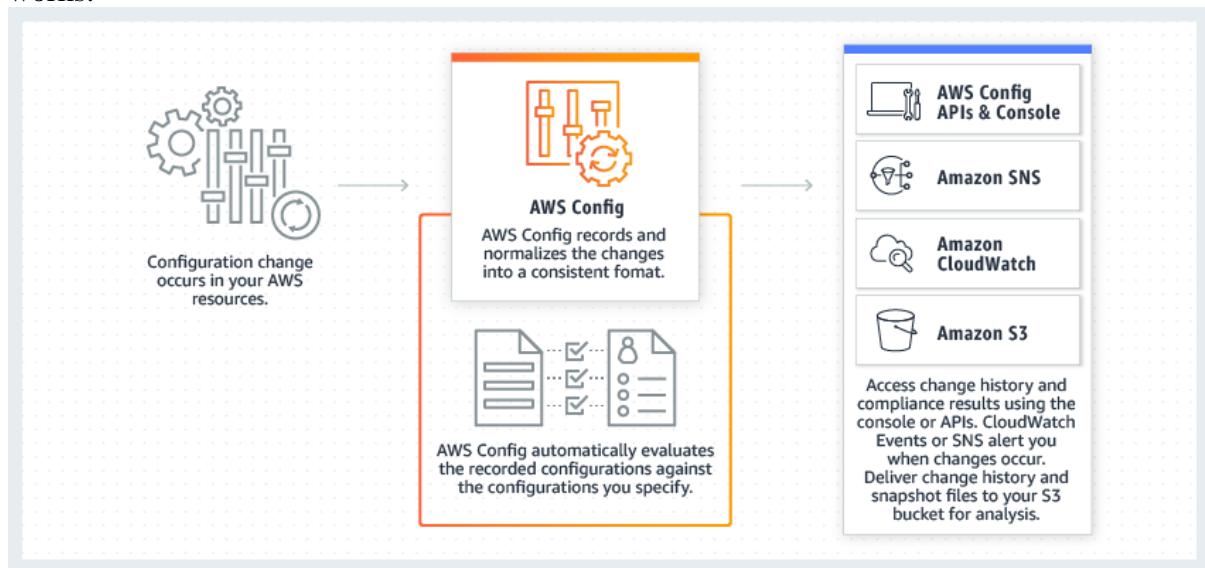
- **Explanation**

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. With Config, you can review changes in configurations and relationships between AWS resources, dive into detailed resource configuration histories, and determine your overall compliance against the configurations specified in your internal guidelines. This enables you to simplify compliance auditing, security analysis, change management, and operational troubleshooting.

How AWS Config works:



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

Incorrect options:

Amazon Inspector - Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on your Amazon EC2 instances. Amazon Inspector automatically assesses applications for exposure, vulnerabilities, and deviations from best practices. It cannot notify configuration changes.

AWS Trusted Advisor - AWS Trusted Advisor is an online resource to help you reduce cost, increase performance, and improve security by optimizing your AWS environment. Trusted Advisor provides real-time guidance to help you provision your resources following AWS best practices. It cannot notify configuration changes.

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. It cannot notify configuration changes.

Reference:

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

Question 16:

An engineering team is new to the AWS Cloud and it would like to launch a dev/test environment with low monthly pricing. Which AWS service can address this use-case?

-
-
-
-

Explanation

Correct option:

Amazon Lightsail

Amazon Lightsail is designed to be the easiest way to launch and manage a virtual private server with AWS. Lightsail plans include everything you need to jumpstart your project – a virtual machine, SSD- based storage, data transfer, DNS management, and a static IP address – for a low, predictable price. It is not used to run batch jobs.

It is great for people with little cloud experience to launch quickly a popular IT solution ready to use immediately.

Incorrect options:

AWS CloudFormation - AWS CloudFormation gives developers and systems administrators an easy way to create and manage a collection of related AWS resources, provisioning and updating them in an orderly and predictable fashion. Using CloudFormation requires experience as resources are deployed within a VPC.

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 computing easier for developers. Deploying a dev/test environment with Amazon EC2 requires experience as instances are deployed within a VPC.

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

Reference:

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

Question 17:

According to the Shared Responsibility Model, in which of the following is both the responsibility of AWS and the customer?

- **Explanation**

Correct option:

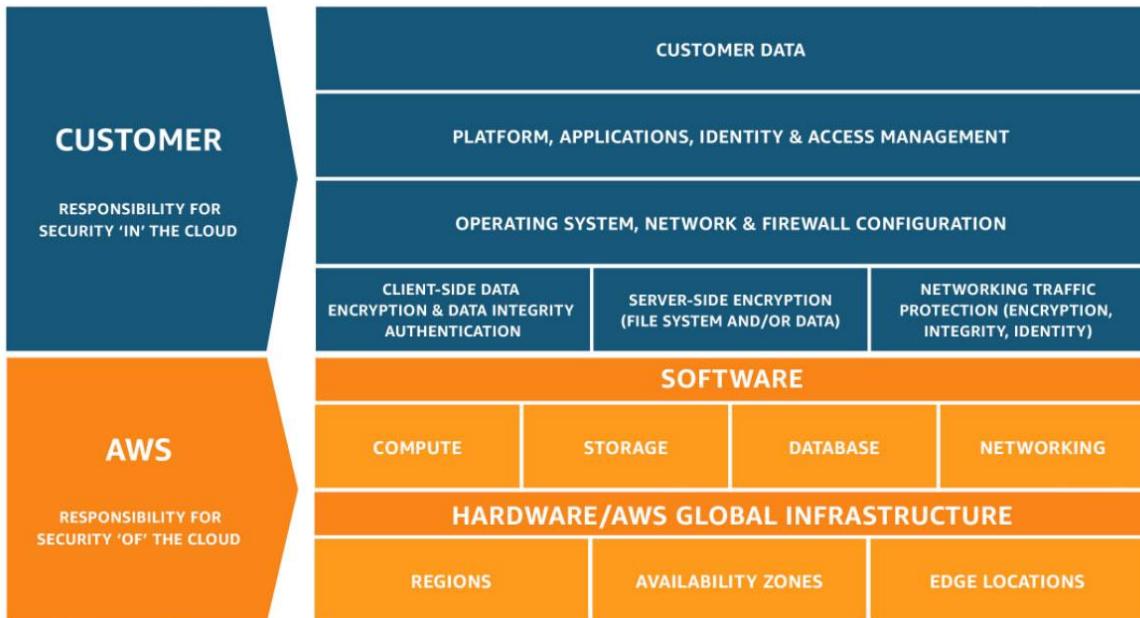
Configuration management

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

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

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:

Customer data

Operating system (OS) configuration

The customers are responsible for "Security IN the cloud". It includes customer data, as well as the guest operating system configuration.

OS configuration as a whole is a shared responsibility, but be careful: the host OS configuration is the responsibility of AWS, and the guest OS configuration is the responsibility of the customer.

Disposal of disk drives

AWS is responsible for "Security OF the cloud". It includes the infrastructure, which is composed of the hardware, software, networking, and facilities that run AWS Cloud services. It includes the disposal and the replacement of disk drives.

Reference:

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

Question 18:

A start-up would like to monitor its cost on the AWS Cloud and would like to choose an optimal Savings Plan. As a Cloud Practitioner, which AWS service would you use?



Explanation

Correct option:

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, etc.) AWS Cost Explorer also gives you access to a set of default reports to help you get started, while also allowing you to create custom reports from scratch.

Customers can receive Savings Plan recommendations at the member (linked) account level in addition to the existing AWS organization-level recommendations in AWS Cost Explorer.

Incorrect options:

AWS Cost and Usage Reports - The AWS Cost & Usage Report is a single location for accessing comprehensive information about your AWS costs and usage. It does not provide Savings Plan recommendations.

AWS Pricing Calculator - AWS Pricing Calculator lets you explore AWS services, and create an estimate for the cost of your use cases on AWS. It does not provide Savings Plan recommendations.

AWS Budgets - AWS Budgets gives you the ability to set custom budgets that alert you when your costs or usage exceed (or are forecasted to exceed) your budgeted amount. You can also use AWS Budgets to set RI utilization or coverage targets and receive alerts when your utilization drops below the threshold you define. It does not provide Savings Plan recommendations.

Exam Alert:

Please review the differences between "AWS Cost and Usage Reports" and "AWS Cost Explorer". Think of "AWS Cost and Usage Reports" as a cost management tool providing the most detailed cost and usage data for your AWS account. It can provide reports that break down your costs by the hour into your S3 bucket. On the other hand, "AWS Cost Explorer" is more of a high-level cost management tool that helps you visualize the costs and usage associated with your AWS account.

"AWS Cost Explorer" vs "AWS Cost and Usage Reports":

Monthly Costs by AWS Service

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.

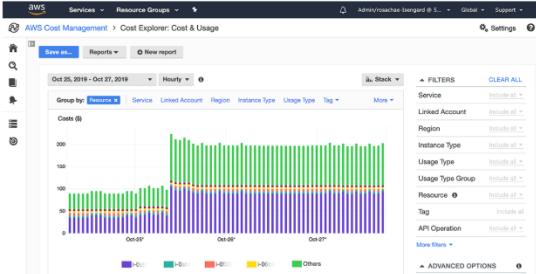
[Launch the Monthly Costs by AWS Service report »](#)



Hourly and Resource Level Granularity

AWS Cost Explorer helps you visualize, understand, and manage your AWS costs and usage over a daily or monthly granularity. The solution also lets you dive deeper using granular filtering and grouping dimensions such as Usage Type and Tags. You can also access your data with further granularity by enabling hourly and resource level granularity.

[Get started using Hourly and Resource Level Granularity »](#)



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

!AWS Cost and Usage Reports<https://media.datacumulus.com/aws-clf-pt/assets/pt5-q46-i2.jpg>) via - <https://aws.amazon.com/aws-cost-management/aws-cost-and-usage-reporting/>

References:

<https://aws.amazon.com/about-aws/whats-new/2020/03/aws-cost-explorer-now-offers-savings-plans-recommendations-for-member-linked-accounts/>

<https://docs.aws.amazon.com/cur/latest/userguide/what-is-cur.html>

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

<https://aws.amazon.com/aws-cost-management/aws-cost-and-usage-reporting/>

Question 19:

According to the Shared Responsibility Model, which of the following are responsibilities of AWS? (Select TWO)



Explanation

Correct option:

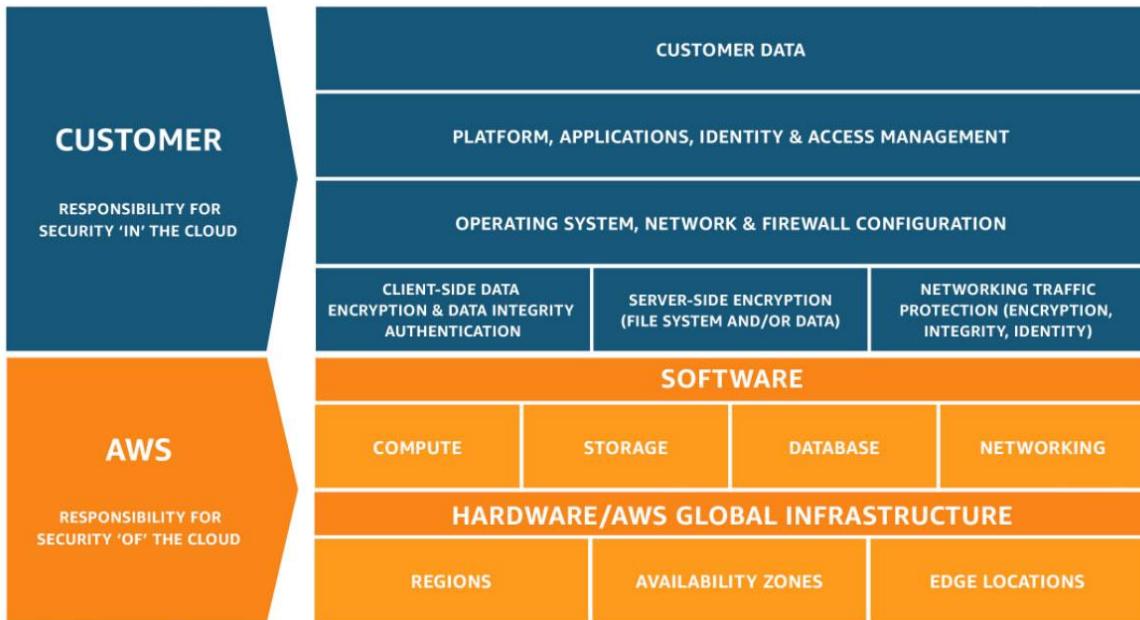
Data center security

Network operability

AWS responsibility “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.

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:

Installing security patches of the guest operating system (OS) - The customers are responsible for patching their guest OS.

Please review the IT controls under the Shared Responsibility Model:

Inherited Controls – Controls which a customer fully inherits from AWS.

- Physical and Environmental controls

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

- Patch Management – AWS is responsible for patching and fixing flaws within the infrastructure, but customers are responsible for patching their guest OS and applications.
- Configuration Management – AWS maintains the configuration of its infrastructure devices, but a customer is responsible for configuring their own guest operating systems, databases, and applications.
- Awareness & Training – AWS trains AWS employees, but a customer must train their own employees.

Customer Specific – Controls which are solely the responsibility of the customer based on the application they are deploying within AWS services. Examples include:

- Service and Communications Protection or Zone Security which may require a customer to route or zone data within specific security environments.

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

Encrypting application data - The customers are responsible for encrypting application data.

Configuring IAM Roles - The customers are responsible for configuring IAM Roles.

Reference:

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

Question 20:

According to the Shared Responsibility Model, which of the following is a responsibility of the customer?



Explanation

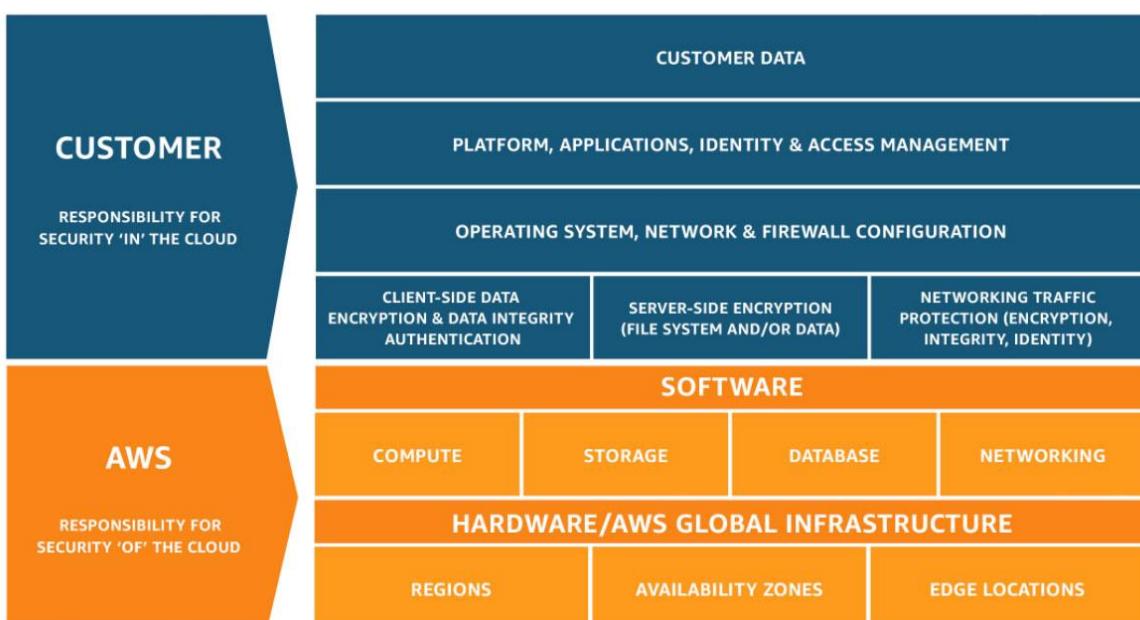
Correct option:

Firewall & networking configuration in EC2

The customers are responsible for "Security IN the cloud". It includes the configuration of the operating system, network & firewall of applications.

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:

Managing DynamoDB - DynamoDB is a fully managed service. AWS operates the infrastructure layer, the operating system, and platforms, and customers access the endpoints to store and retrieve data.

Protecting hardware infrastructure

Edge locations security

AWS is responsible for "Security OF the cloud". It includes the infrastructure, which is composed of the hardware, software, networking, and facilities that run AWS Cloud services.

Reference:

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

Question 21:

Which of the following statements is INCORRECT regarding EBS Volumes?

Explanation

Correct option:

EBS Volumes can be bound to several Availability Zones (AZs)

An Amazon EBS volume is a durable, block-level storage device that you can attach to your instances. After you attach a volume to an instance, you can use it as you would use a physical hard drive.

When using EBS Volumes, the volume and the instance must be in the same Availability Zone.

Incorrect options:

EBS Volumes can be mounted to one instance at a time - At the Certified Cloud Practitioner level, EBS Volumes can be mounted to one instance at a time. It is also possible that an EBS Volume is not mounted to an instance.

EBS Volumes are bound to a specific Availability Zone (AZ) - As mentioned, when using EBS Volumes, the volume and the instance must be in the same Availability Zone.

EBS Volumes can persist data after their termination - Unlike EC2 instance store, an EBS volume is off-instance storage that can persist independently from the life of an instance.

Reference:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volumes.html>

Question 22:

A company would like to create a private, high bandwidth network connection between its on-premises data centers and AWS Cloud. As a Cloud Practitioner, which of the following options would you recommend?

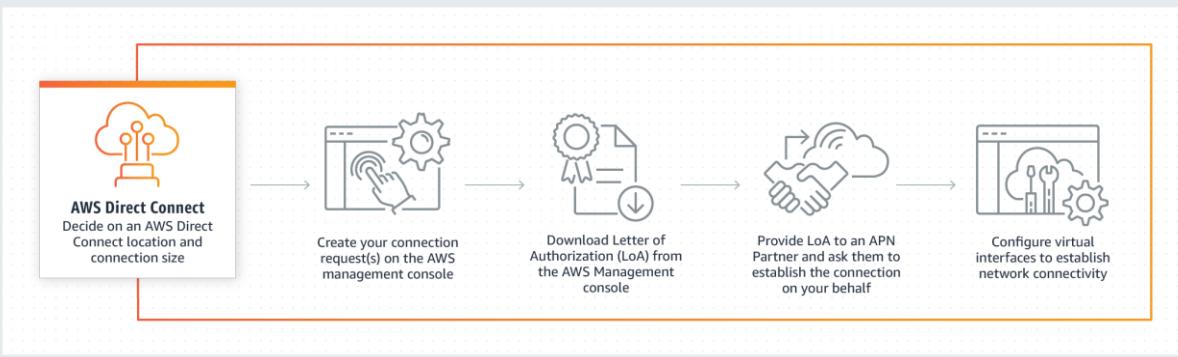
- **Explanation**

Correct option:

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/>

Incorrect options:

Site-to-Site VPN - By default, instances that you launch into an Amazon VPC can't communicate with your own (remote) network. You can enable access to your remote network from your VPC by creating an AWS Site-to-Site VPN (Site-to-Site VPN) connection, and configuring routing to pass traffic through the connection. It uses the public internet and is therefore not suited for this use case.

VPC Endpoints - A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by AWS PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. It does not connect your on-premises data centers and AWS Cloud.

VPC Peering - A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. It is used to connect VPCs together, and not on-premises data centers and AWS Cloud.

Reference:

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

Question 23:

Which of the following are advantages of using the AWS Cloud? (Select TWO)

- Explanation**

Correct option:

Increase speed and agility

Stop guessing about capacity

Exam Alert:

Please check out the following six advantages of Cloud Computing. You would certainly be asked questions on the advantages of Cloud Computing compared to a traditional on-premises setup:

Six Advantages of Cloud Computing

[PDF](#) | [RSS](#)

- **Trade capital expense for variable expense** – Instead of having to invest heavily in data centers and servers before you know how you're going to use them, you can pay only when you consume computing resources, and pay only for how much you consume.
- **Benefit from massive economies of scale** – By using cloud computing, you can achieve a lower variable cost than you can get on your own. Because usage from hundreds of thousands of customers is aggregated in the cloud, providers such as AWS can achieve higher economies of scale, which translates into lower pay-as-you-go prices.
- **Stop guessing capacity** – Eliminate guessing on your infrastructure capacity needs. When you make a capacity decision prior to deploying an application, you often end up either sitting on expensive idle resources or dealing with limited capacity. With cloud computing, these problems go away. You can access as much or as little capacity as you need, and scale up and down as required with only a few minutes' notice.
- **Increase speed and agility** – In a cloud computing environment, new IT resources are only a click away, which means that you reduce the time to make those resources available to your developers from weeks to just minutes. This results in a dramatic increase in agility for the organization, since the cost and time it takes to experiment and develop is significantly lower.
- **Stop spending money running and maintaining data centers** – Focus on projects that differentiate your business, not the infrastructure. Cloud computing lets you focus on your own customers, rather than on the heavy lifting of racking, stacking, and powering servers.
- **Go global in minutes** – Easily deploy your application in multiple regions around the world with just a few clicks. This means you can provide lower latency and a better experience for your customers at minimal cost.

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

Incorrect options:

Limited scaling - Scaling is not limited in the cloud. You can access as much or as little capacity as you need, and scale up and down as required with only a few minutes' notice.

AWS is responsible for security in the cloud - AWS is responsible for security OF the cloud, which means AWS is responsible for protecting the infrastructure that runs all the services offered in the AWS Cloud.

Trade operational expense for capital expense - In the cloud, you trade capital expense (CAPEX) for the operational expense (OPEX). Instead of having to invest heavily in data centers and servers before you know how you're going to use them, you can pay only when you consume computing resources, and pay only for how much you consume.

Reference:

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

Question 24:

Which of the following options is NOT a feature of Amazon Inspector?



Explanation

Correct option:

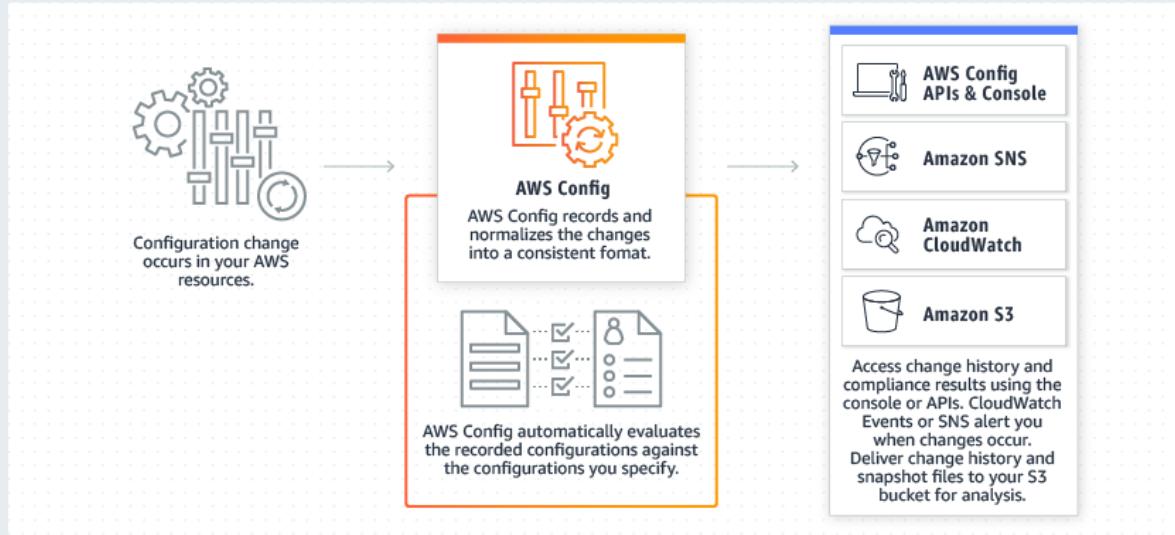
Track configuration changes

Tracking configuration changes is a feature of 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.

How AWS Config works:



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

Incorrect options:

Automate security assessments

Analyze against unintended network accessibility

Inspect running operating systems (OS) against known vulnerabilities

These options are all features of 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 security assessments help you check for unintended network accessibility of your Amazon EC2 instances and for vulnerabilities on those EC2 instances.

Amazon Inspector also offers predefined software called an agent that you can optionally install in the operating system of the EC2 instances that you want to assess. The agent monitors the behavior of the EC2 instances, including network, file system, and process activity. It also collects a wide set of behavior and configuration data (telemetry).

References:

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

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

Question 25:

A company would like to define a set of rules to manage objects cost-effectively between storage classes. As a Cloud Practitioner, which Amazon S3 feature would you use?

-

Explanation

Correct option:

S3 Lifecycle management

To manage your objects so that they are stored cost-effectively throughout their lifecycle, configure their Amazon S3 Lifecycle. An S3 Lifecycle configuration is a set of rules that define actions that Amazon S3 applies to a group of objects. There are two types of actions: Transition actions (define when objects transition to another storage class) and expiration actions (define when objects expire. Amazon S3 deletes expired objects on your behalf).

In this particular use-case, you would use a transition action.

Incorrect options:

S3 Transfer Acceleration - Amazon S3 Transfer Acceleration enables fast, easy, and secure transfers of files over long distances between your client and an S3 bucket. It is not used to move objects between storage classes.

S3 Bucket policies - A bucket policy is a resource-based AWS Identity and Access Management (IAM) policy. You add a bucket policy to a bucket to grant other AWS accounts or IAM users access permissions for the bucket and the objects in it. Object permissions apply only to the objects that the bucket owner creates. It is not used to move objects between storage classes.

S3 Cross-Region Replication (CRR) - Replication enables automatic, asynchronous copying of objects across Amazon S3 buckets. Cross-Region replication (CRR) is used to copy objects across Amazon S3 buckets in different AWS Regions. It is not used to move objects between storage classes.

References:

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

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

Question 26:

Which AWS tool can provide best practice recommendations for performance, service limits, and cost optimization?

-

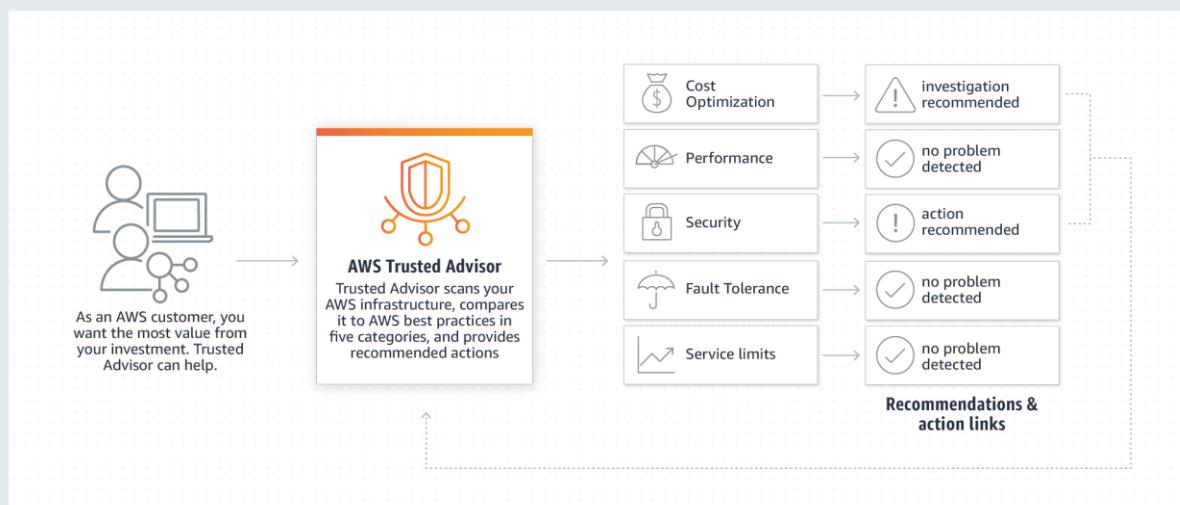
Explanation

Correct option:

AWS Trusted Advisor

AWS Trusted Advisor is an online resource to help you reduce cost, increase performance, and improve security by optimizing your AWS environment. Trusted Advisor provides real-time guidance to help you provision your resources following AWS best practices.

How AWS Trusted Advisor works:



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

Incorrect options:

Amazon Inspector - Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on your Amazon EC2 instances. Amazon Inspector automatically assesses applications for exposure, vulnerabilities, and deviations from best practices. Nevertheless, it does not provide best practice recommendations.

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. It does not provide best practice recommendations.

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 best practice recommendations.

Reference:

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

Question 27:

A growing start-up has trouble identifying and protecting sensitive data at scale. Which AWS fully managed service can assist with this task?

Explanation

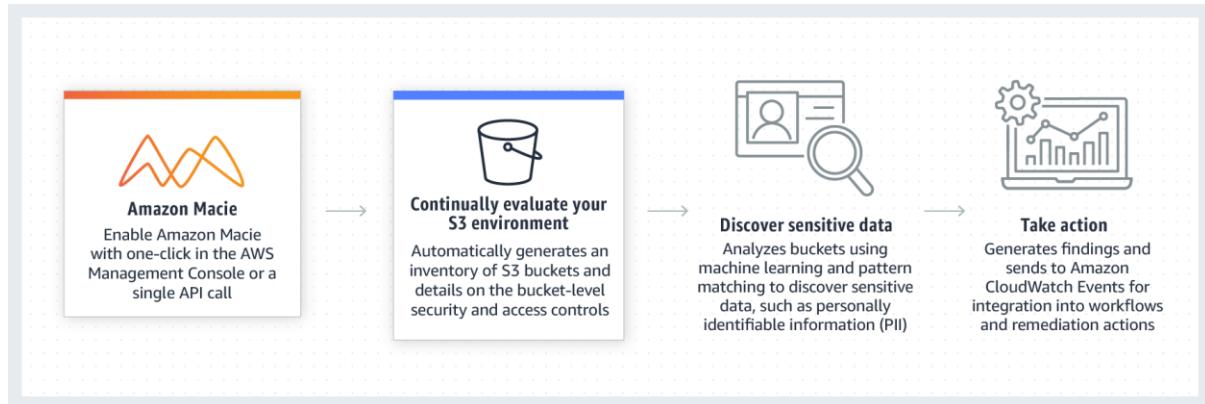
Correct option:

Amazon Macie

Amazon Macie is a fully managed data security and data privacy service that uses machine learning and pattern matching to discover and protect your sensitive data in AWS.

Amazon Macie uses machine learning and pattern matching to cost-efficiently discover sensitive data at scale. Macie automatically detects a large and growing list of sensitive data types, including personally identifiable information (PII) such as names, addresses, and credit card numbers. It also gives you constant visibility of the data security and data privacy of your data stored in Amazon S3.

How Amazon Macie works:



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

Incorrect options:

AWS Artifact - AWS Artifact is your go-to, central resource for compliance-related information that matters to you. It provides on-demand access to AWS' security and compliance reports and select online agreements. It is not used to discover and protect sensitive data in AWS.

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. It is not used to discover and protect sensitive data in AWS.

AWS KMS - AWS Key Management Service (KMS) makes it easy for you to create and manage keys and control the use of encryption across a wide range of AWS services and in your applications. It is not used to discover and protect sensitive data in AWS.

Reference:

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

Question 28:

Which types of monitoring can be provided by Amazon CloudWatch? (Select TWO)

Explanation

Correct option:

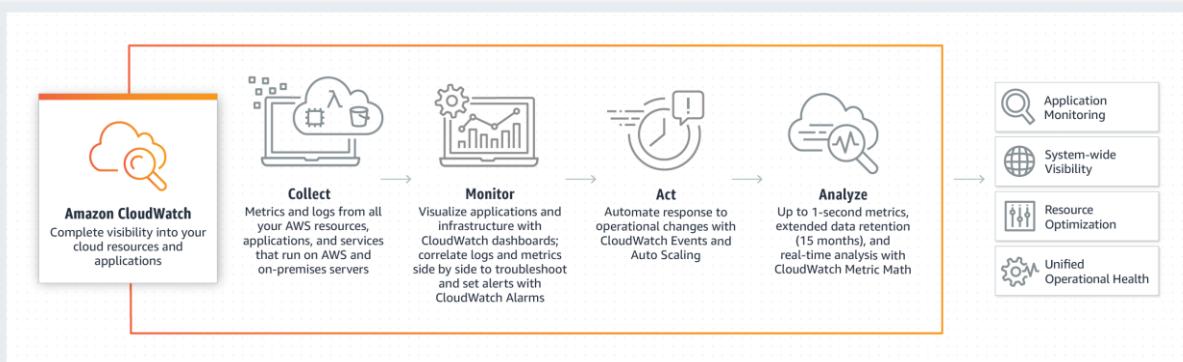
Application performance

Resource utilization

Amazon CloudWatch is a monitoring service for AWS cloud resources and the applications you run on AWS. You can use Amazon CloudWatch to collect and track metrics, collect and monitor log files, and set alarms. Amazon CloudWatch can monitor AWS resources such as Amazon EC2 instances, Amazon DynamoDB tables, and Amazon RDS DB instances, as well as custom metrics generated by your applications and services, and any log files your applications generate.

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

How Amazon CloudWatch works:



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

Incorrect options:

API access - Recording API calls is a feature of CloudTrail, not CloudWatch.

Performance and availability of AWS services - The Personal Health Dashboard gives you a personalized view into the performance and availability of the AWS services underlying your AWS resources, not CloudWatch.

Account management - Identity and Access Management (IAM) is usually used to manage accounts, not CloudWatch.

References:

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

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

Question 29:

A company using a hybrid cloud would like to store secondary backup copies of on-premises data for disaster recovery purposes. Which S3 Storage Class would you use?



Explanation

Correct option:

S3 One Zone - Infrequent Access

S3 One Zone-IA is for data that is accessed less frequently but requires rapid access when needed. Unlike other S3 Storage Classes which store data in a minimum of three Availability Zones (AZs), S3 One Zone-IA stores data in a single AZ and costs 20% less than S3 Standard-IA. S3 One Zone-IA is ideal for customers who want a lower-cost option for infrequently accessed data but do not require the availability and resilience of S3 Standard or S3 Standard-IA. It's a good choice for **storing secondary backup copies of** on-premises data or easily re-creatable data. You can also use it as cost-effective storage for data that is replicated from another AWS Region using S3 Cross-Region Replication.

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)					
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:

S3 Glacier - S3 Glacier is a secure, durable, and low-cost storage class for data archiving. You can reliably store any amount of data at costs that are competitive with or cheaper than on-premises solutions. It is not used for secondary backup copies but for archiving data.

S3 Standard - General Purposes - S3 Standard offers high durability, availability, and performance object storage for frequently accessed data. Because it delivers low latency and high throughput, S3 Standard is appropriate for a wide variety of use cases, including cloud applications, dynamic websites, content distribution, mobile and gaming applications, and big data analytics. However, it is not used to store secondary backup copies of on-premises data as data store in S3 Standard - General Purposes is for frequently accessed data.

S3 Standard - Infrequent Access - S3 Standard-IA is for data that is accessed less frequently, but requires rapid access when needed. S3 Standard-IA offers the high durability, high throughput, and low latency of S3 Standard, with a low per GB storage price and per GB retrieval fee. This combination of low cost and high performance makes S3 Standard-IA ideal for long-term storage, backups, and as a data store for disaster recovery files. It can be used for backups, but it is more expensive than S3 One Zone - Infrequent Access. Hence, S3 One Zone - Infrequent Access is a better option for secondary backup copies.

Reference:

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

Question 30:

Which AWS service can inspect CloudFront distributions running on any HTTP web-server?



Explanation

Correct option:

AWS WAF

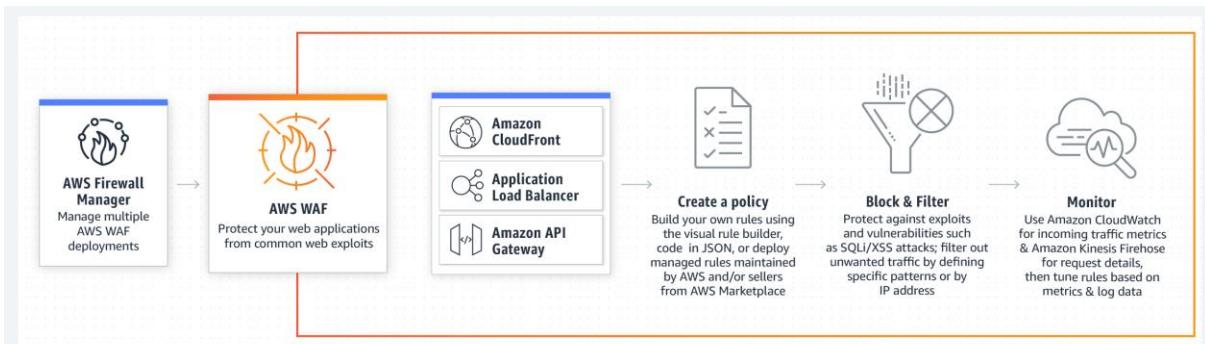
AWS WAF is a web application firewall that helps protect web applications from attacks by allowing you to configure rules that allow, block, or monitor (count) web requests based on conditions that you define. These conditions include IP addresses, HTTP headers, HTTP body, URI strings, SQL injection and cross-site scripting.

AWS WAF is a web application firewall that lets you monitor the HTTP and HTTPS requests that are forwarded to CloudFront, and lets you control access to your content.

When you use AWS WAF on Amazon CloudFront, your rules run in all AWS Edge Locations, located around the world close to your end-users. This means security doesn't come at the expense of performance. Blocked requests are stopped before they reach your web servers.

How AWS WAF

works:



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

Incorrect options:

AWS GuardDuty - Amazon GuardDuty is a threat detection service that continuously monitors for malicious or unauthorized behavior to help you protect your AWS accounts and workloads. It does not inspect CloudFront distributions.

AWS Shield - AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards web applications running on AWS. It does not inspect CloudFront distributions.

AWS Elastic Load Balancer - Elastic Load Balancing (ELB) automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, and IP addresses. It does not inspect CloudFront distributions.

Reference:

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

Question 31:

Which of the following AWS Support plans is the MOST cost-effective when getting enhanced technical support by Cloud Support Engineers?

-

Correct option:

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**. You get full access to AWS Trusted Advisor Best Practice Checks. It is also the cheapest support plan to provide enhanced technical support by Cloud Support Engineers.

AWS Business Support Plan

Offerings:

We recommend Business Support if you have production workloads on AWS and want 24x7 access to technical support and architectural guidance in the context of your specific use-cases. In addition to what is available with Basic Support, Business Support provides:

AWS Trusted Advisor - Access to the full set of Trusted Advisor checks and guidance to provision your resources following best practices to help reduce costs, increase performance and fault tolerance, and improve security.

AWS Personal Health Dashboard - A personalized view of the health of AWS services, and alerts when your resources are impacted. Also includes the Health API for integration with your existing management systems.

Enhanced Technical Support – 24x7 access to Cloud Support Engineers via phone, chat, and email. You can have an unlimited number of contacts that can open an unlimited amount of cases. Response times are as follows:

- General Guidance - < 24 hours
- System Impaired - < 12 hours
- Production System Impaired - < 4 hours
- Production System Down - < 1 hour

Architecture Support – Contextual guidance on how services fit together to meet your specific use-case, workload, or application.

AWS Support API - Programmatic access to AWS Support Center features to create, manage, and close your support cases, and operationally manage your Trusted Advisor check requests and status.

Third-Party Software Support - Guidance, configuration, and troubleshooting of AWS interoperability with many common operating systems, platforms, and application stack components.

Access to Proactive Support Programs – Ability to purchase [Infrastructure Event Management](#) for an additional fee. This provides Architecture and scaling guidance, and real-time operational support during the preparation and execution of planned events, product launches, and migrations.

Pricing:

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

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
	<i>Recommended if you are experimenting or testing in AWS.</i>	<i>Recommended if you have production workloads in AWS.</i>	<i>Recommended if you have business and/or mission critical workloads in AWS.</i>
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 \$100 / 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. It provides enhanced technical support, but by Cloud Support Associates.

Basic - A basic support plan is included for all AWS customers. It does not provide enhanced 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. It provides enhanced technical support by Cloud Support Engineers, but is more expensive than the Business support plan.

References:

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

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

Question 32:

Which of the following databases allows you to store data structured in key-value format?



Explanation

Correct option:

Amazon DynamoDB

Amazon DynamoDB is a key-value and document database that delivers single-digit millisecond performance at any scale. It's a fully managed, multi-Region, multi-master, durable database with built-in security, backup and restore, and in-memory caching for internet-scale applications.

Incorrect options:

AWS Glue - AWS Glue is a fully managed extract, transform, and load (ETL) service that makes it easy for customers to prepare and load their data for analytics. AWS Glue job is meant to be used for batch ETL data processing.

Amazon RDS - Amazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and scale a relational database in the cloud. Data is not stored in a key-value format.

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. EMR provisions EC2 instances to manage its workload. It is not a database.

Reference:

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

Question 33:

Which of the following AWS services can be used to generate, use, and manage encryption keys on the AWS Cloud?

Explanation

Correct option:

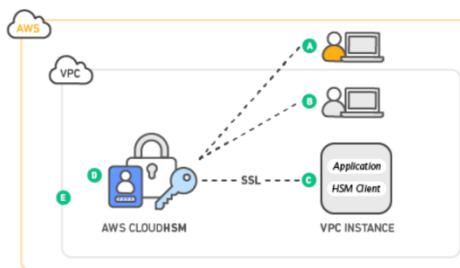
AWS CloudHSM

The AWS CloudHSM service helps you meet corporate, contractual, and regulatory compliance requirements for data security by using a dedicated Hardware Security Module (HSM) instances within the AWS cloud.

CloudHSM allows you to securely generate, store, and manage cryptographic keys used for data encryption in a way that keys are accessible only by you.

How AWS CloudHSM works:

How it 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:

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. It cannot be used to generate, use, and manage encryption keys.

AWS GuardDuty - Amazon GuardDuty is a threat detection service that continuously monitors for malicious or unauthorized behavior to help you protect your AWS accounts and workloads. It cannot be used to generate, use, and manage encryption keys.

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. It is integrated with AWS CloudHSM to generate, use, and manage encryption keys.

Reference:

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

Question 34:

Which of the following services are provided by Amazon Route 53? (Select TWO)

-

Explanation

Correct option:

Domain registration

Health checks and monitoring

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

Amazon Route 53 offers domain name registration services, where you can search for and register available domain names or transfer in existing domain names to be managed by Route 53.

Amazon Route 53 can monitor the health and performance of your application as well as your web servers and other resources.

Incorrect options:

IP routing - Despite its name, Amazon Route 53 does not offer IP routing. However, it can route traffic based on multiple criteria, such as endpoint health, geographic location, and latency, using routing policies.

Load balancing - It is a feature of Elastic Load Balancing (ELB) and not Amazon Route 53. 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.

Transfer acceleration - Transfer acceleration is a feature of Amazon S3. Amazon S3 Transfer Acceleration can speed up content transfers to and from Amazon S3 by as much as 50-500% for long-distance transfer of larger objects.

Reference:

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

Question 35:

A data science team would like to build Machine Learning models for its projects. Which AWS service can it use?



Explanation

Correct option:

Amazon SageMaker - Amazon SageMaker is a fully-managed platform that enables developers and data scientists to quickly and easily build, train, and deploy machine learning models at any scale. Amazon SageMaker removes all the barriers that typically slow down developers who want to use machine learning.

Incorrect options:

Amazon Polly - You can use Amazon Polly to turn text into lifelike speech thereby allowing you to create applications that talk. Polly's Text-to-Speech (TTS) service uses advanced deep learning technologies to synthesize natural sounding human speech.

Amazon Comprehend - Amazon Comprehend is a natural language processing (NLP) service that uses machine learning to find meaning and insights in text. Natural Language Processing (NLP) is a way for computers to analyze, understand, and derive meaning from textual information in a smart and useful way. By utilizing NLP, you can extract important phrases, sentiment, syntax, key entities such as brand, date, location, person, etc., and the language of the text.

Amazon Connect -

Reference:

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

Question 36:

Which AWS service can be used to send, store, and receive messages between software components at any volume to decouple application tiers?

Explanation

Correct option:

Amazon SQS

Amazon Simple Queue Service (Amazon SQS) is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SQS eliminates the complexity and overhead associated with managing and

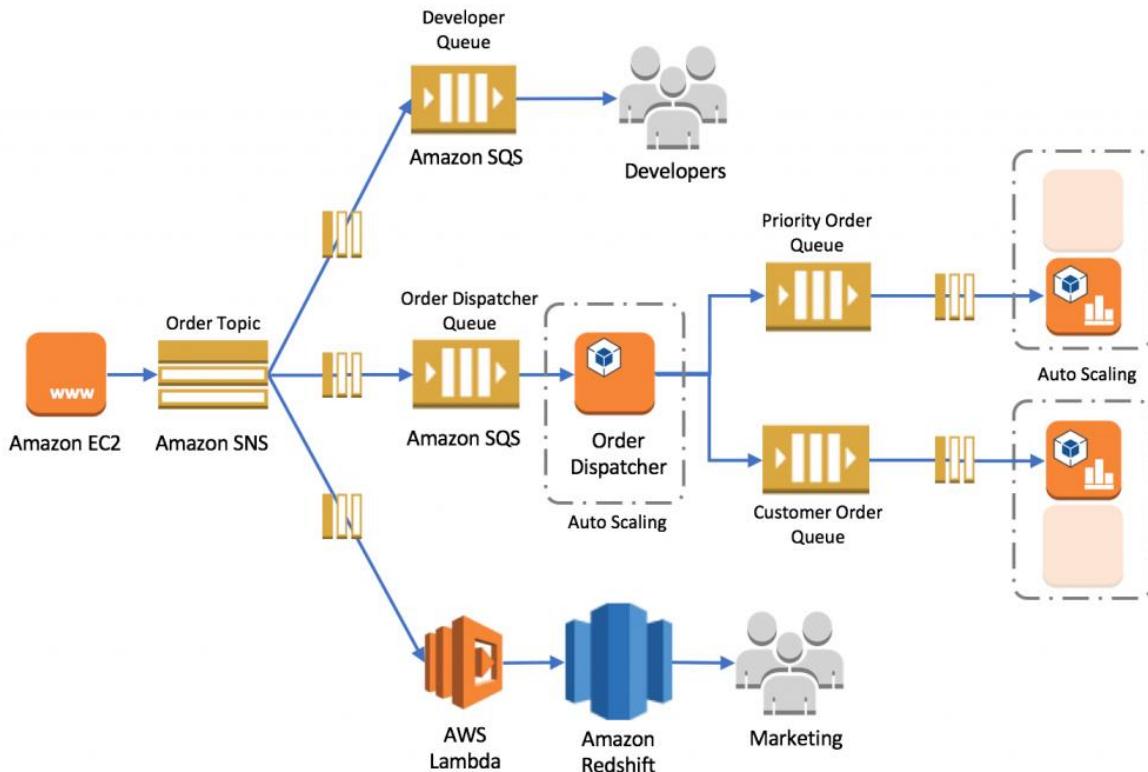
operating message-oriented middleware, and empowers developers to focus on differentiating work.

Using SQS, you can send, store, and receive messages between software components at any volume, without losing messages or requiring other services to be available.

Incorrect options:

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

Please review this reference architecture for building a decoupled order processing system using SNS and SQS:



via - <https://aws.amazon.com/blogs/compute/building-loosely-coupled-scalable-applications-with-amazon-sqs-and-amazon-sns/>

AWS Elastic Beanstalk - AWS Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services. You can simply upload your code, and AWS Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, and auto-scaling to application health monitoring. It is not used to send, store, and receive message between software components.

AWS Organizations - AWS Organizations offers policy-based management for multiple AWS accounts. With Organizations, you can create groups of accounts, automate account creation, apply and manage policies for those groups. Organizations enables you to centrally

manage policies across multiple accounts, without requiring custom scripts and manual processes. It is not used to send, store, and receive message between software components.

Reference:

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

Question 37:

Which AWS service can be used to subscribe to an RSS feed to be notified of services' interruptions?

-  **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 offers the possibility to subscribe to an RSS feed to be notified of interruptions to each service.

AWS Service Health Dashboard

Overview:



[Amazon Web Services](#) » Service Health Dashboard

Get a personalized view of AWS service health

[Open the Personal Health Dashboard](#)

Current Status - Jun 2, 2020 PDT

Amazon Web Services publishes our most up-to-the-minute information on service availability in the table below. Check back here any time to get current status information, or subscribe to an RSS feed to be notified of interruptions to each individual service. If you are experiencing a real-time, operational issue with one of our services that is not described below, please inform us by clicking on the "Contact Us" link to submit a service issue report. All dates and times are Pacific Time (PST/PDT).

North America	South America	Europe	Africa	Asia Pacific	Middle East	Contact Us
Recent Events				Details		RSS
No recent events.						
Remaining Services				Details		RSS
Alexa for Business (N. Virginia)				Service is operating normally		
Amazon API Gateway (Montreal)				Service is operating normally		
Amazon API Gateway (N. California)				Service is operating normally		
Amazon API Gateway (N. Virginia)				Service is operating normally		
Amazon API Gateway (Ohio)				Service is operating normally		
Amazon API Gateway (Oregon)				Service is operating normally		
Amazon AppStream 2.0 (N. Virginia)				Service is operating normally		
Amazon AppStream 2.0 (Oregon)				Service is operating normally		
Amazon Athena (Montreal)				Service is operating normally		
Amazon Athena (N. Virginia)				Service is operating normally		

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

Incorrect options:

Amazon SNS - Amazon Simple Notification Service (Amazon SNS) is a highly available, durable, secure, fully managed pub/sub messaging service that enables you to decouple microservices, distributed systems, and serverless applications. It can be used to deliver notifications, but it does not provide current services' status.

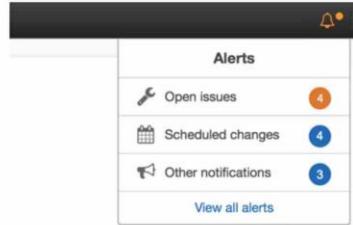
AWS Personal Health Dashboard - AWS Personal Health Dashboard provides alerts and remediation guidance when AWS is experiencing events that may impact you. It does not provide current services' status, and does not offer the possibility to be notified in case of services' interruptions.

AWS Personal Health Dashboard Overview:

Technology & Tools To Monitor, Manage, and Optimize Your AWS Environment

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

The dashboard displays relevant and timely information to help you manage events in progress, and provides proactive notification to help you plan for scheduled activities. With Personal Health Dashboard, alerts are triggered by changes in the health of AWS resources, giving you event visibility, and guidance to help quickly diagnose and resolve issues.



Personalized View of Service Health

Personal Health Dashboard gives you a personalized view of the status of the AWS services that power your applications, enabling you to quickly see when AWS is experiencing issues that may impact you. For example, in the event of a lost EBS volume associated with one of your EC2 instances, you would gain quick visibility into the status of the specific service you are using, helping save precious time troubleshooting to determine root cause.

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.

AWS Lambda - AWS Lambda lets you run code without provisioning or managing servers. It does not provide current services' status.

Reference:

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

Question 38:

A company would like to move its infrastructure to AWS Cloud. Which of the following should be included in the Total Cost of Ownership (TCO) estimate? (Select TWO)

- Application

Explanation

Correct option:

Server administration

Power/Cooling

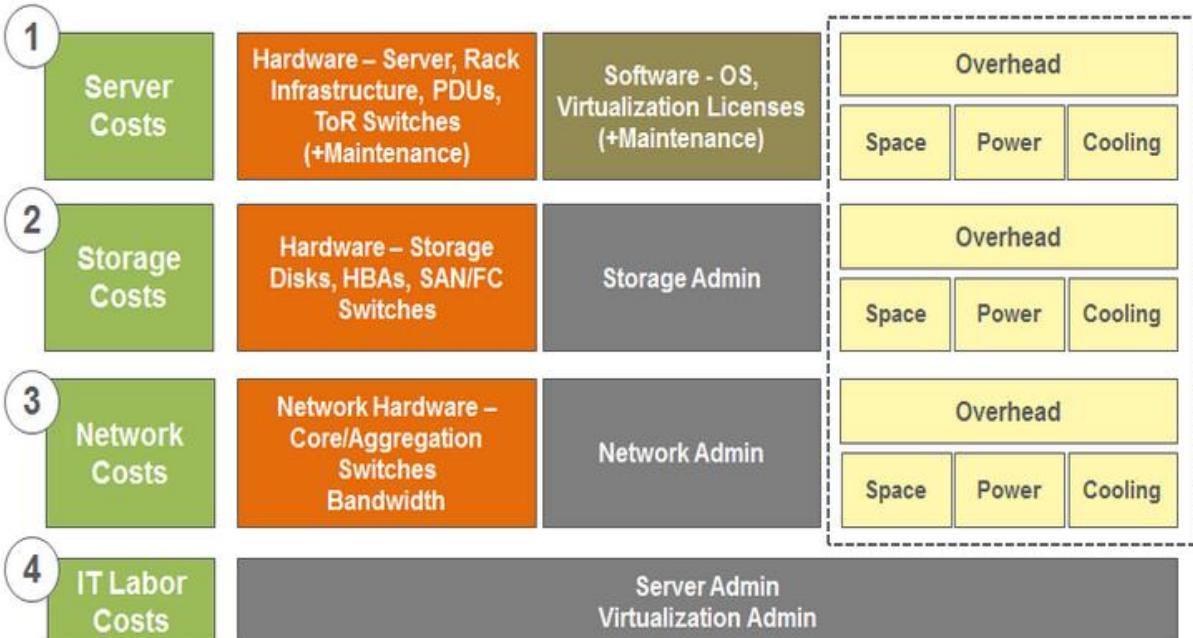
TCO calculator helps to compare the cost of your applications in an on-premises or traditional hosting environment to AWS. AWS helps reduce Total Cost of Ownership (TCO) by reducing the need to invest in large capital expenditures and providing a pay-as-you-go model that empowers to invest in the capacity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

TCO calculator compares the cost of your applications in an on-premises or traditional hosting environment to AWS: server, storage, network, IT labor. Therefore, you need to include every element relevant to these points of comparison.

Server administration is included in the IT labor costs.

Power/Cooling are included in the server, storage and network cost.

Points of comparison of on-premises and AWS:



via - <https://aws.amazon.com/blogs/aws/the-new-aws-tco-calculator/>

Incorrect options:

Application advertising - The application advertising is not relevant for a Total Cost of Ownership (TCO) estimate.

Number of end-users - The number of end-users is not relevant for a Total Cost of Ownership (TCO) estimate.

Electronic equipment at office - The electronic equipment at the office is not relevant for a Total Cost of Ownership (TCO) estimate.

References:

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

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

Question 39:

A company based in Sydney hosts its application on EC2 instances in ap-southeast-2. They would like to deploy the same EC2 instances in eu-south-1. Which of the following AWS entities can address this use-case?



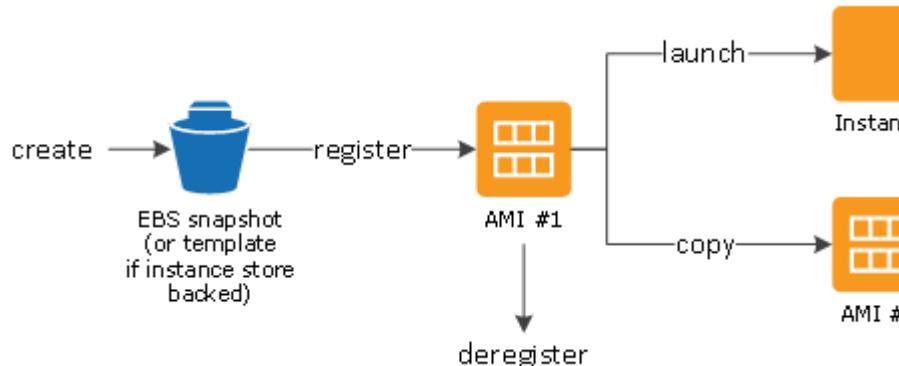
Explanation

Correct option:

Amazon Machine Image (AMI)

An Amazon Machine Image (AMI) provides the information required to launch an instance. You must specify an AMI when you launch an instance. You can launch multiple instances from a single AMI when you need multiple instances with the same configuration.

How to use an



AMI:

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

via

Incorrect options:

Elastic Load Balancing (ELB) - 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. It cannot be used to deploy the same EC2 instances across different Availability Zones (AZs).

AWS Lambda - AWS Lambda lets you run code without provisioning or managing servers. It cannot be used to deploy the same EC2 instances across different Availability Zones (AZs).

EBS snapshots - An EBS snapshot is a point-in-time copy of your Amazon EBS volume. EBS snapshots are one of the components of an AMI, but EBS snapshots alone cannot be used to deploy the same EC2 instances across different Availability Zones (AZs).

Reference:

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

Question 40:

A brand new startup would like to remove its need to manage the underlying infrastructure and focus on the deployment and management of its applications. Which type of Cloud Computing does this refer to?

Explanation

Correct option:

Platform as a Service (PaaS)

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

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.

Please review this overview of the types of Cloud Computing:

Cloud Computing Models

There are three main models for cloud computing. Each model represents a different part of the cloud computing stack.



Infrastructure as a Service (IaaS)

Infrastructure as a Service, sometimes abbreviated as IaaS, contains the basic building blocks for cloud IT and typically provide access to networking features, computers (virtual or on dedicated hardware), and data storage space. Infrastructure as a Service provides you with the highest level of flexibility and management control over your IT resources and is most similar to existing IT resources that many IT departments and developers are familiar with today.



Platform as a Service (PaaS)

Platforms as a service remove the need for organizations to manage the underlying infrastructure (usually hardware and operating systems) and allow you to focus on the deployment and management of your applications. This helps you be more efficient as you don't need to worry about resource procurement, capacity planning, software maintenance, patching, or any of the other undifferentiated heavy lifting involved in running your application.



Software as a Service (SaaS)

Software as a Service provides you with a completed product that is run and managed by the service provider. In most cases, people referring to Software as a Service are referring to end-user applications. With a SaaS offering you do not have to think about how the service is maintained or how the underlying infrastructure is managed; you only need to think about how you will use that particular piece of software. A common example of a SaaS application is web-based email where you can send and receive email without having to manage feature additions to the email product or maintaining the servers and operating systems that the email program is running on.

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

Incorrect options:

Infrastructure as a Service (IaaS) - 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.

Software as a Service (SaaS) - 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. AWS Rekognition is an example of a SaaS service.

On-premises - When an enterprise opts for on-premises, it needs to create, upgrade, and scale the on-premise IT infrastructure by investing in sophisticated hardware, compatible

software, and robust services. Also, the business needs to deploy dedicated IT staff to upkeep, scale, and manage the on-premise infrastructure continuously.

Reference:

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

Question 41:

Which of the following are the best practices when using AWS Organizations? (Select TWO)

-
-

Explanation

Correct option:

Create accounts per department

Restrict account privileges using Service Control Policies (SCP)

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.

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. Through integrations with other AWS services, you can use Organizations to define central configurations and resource sharing across accounts in your organization. AWS Organizations is available to all AWS customers at no additional charge.

You should create accounts per department based on regulatory restrictions (using SCP) for better resource isolation, and to have separate per-account service limits.

AWS Organizations allows you to restrict what services and actions are allowed in your accounts. You can use Service Control Policies (SCPs) to apply permission guardrails on AWS Identity and Access Management (IAM) users and roles.

Incorrect options:

Never use tags for billing - You should use tags standards to categorize AWS resources for billing purposes.

Disable CloudTrail on several accounts - You should enable CloudTrail to monitor activity on all accounts for governance, compliance, risk, and auditing purposes.

Do not use AWS Organizations to automate AWS account creation - AWS Organizations helps you simplify IT operations by automating AWS account creation and management. The Organizations APIs enable you to create new accounts programmatically, and to add the new accounts to a group. The policies attached to the group are automatically applied to the new account.

Reference:

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

Question 42:

Which security control tool can be used to deny traffic from a specific IP address?

-
- Explanation

Correct option:

Network ACL

A Network Access Control List (NACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets (i.e. it works at subnet level). A network ACL has separate inbound and outbound rules, and each rule can either allow or deny traffic.

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 - A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. Security groups act at the instance level, not at the subnet level. You can specify allow rules, but not deny rules. You can specify separate rules for inbound and outbound traffic.

AWS GuardDuty - Amazon GuardDuty is a threat detection service that continuously monitors for malicious or unauthorized behavior to help you protect your AWS accounts and workloads. It monitors for activity such as unusual API calls or potentially unauthorized deployments that indicate a possible account compromise. GuardDuty also detects potentially compromised instances or reconnaissance by attackers. It cannot deny traffic from a specific IP address.

VPC Flow Logs - VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. Flow log data can be published to Amazon CloudWatch Logs or Amazon S3. After you've created a flow log, you can retrieve and view its data in the chosen destination. However, it cannot deny traffic from a specific IP address.

Reference:

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

Question 43:

The IT infrastructure at a university is deployed on AWS Cloud and it's experiencing a read-intensive workload. As a Cloud Practitioner, which AWS service would you use to take the load off databases?

• **Explanation**

Correct option:

Amazon ElastiCache

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

If EC2 instances are intensively reading data from a database, ElastiCache can cache some values to take the load off the database.

How Amazon ElastiCache works:



via - <https://aws.amazon.com/elasticsearch/>)

Incorrect options:

Amazon Relational Database Service (RDS) - Amazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient and resizable capacity while automating time-consuming administration tasks such as hardware provisioning, database setup, patching and backups. It frees you to focus on your applications so you can give them the fast performance, high availability, security and compatibility they need. It cannot be used to take the load off databases. However, ElastiCache is often used with RDS to take the load off RDS.

AWS Glue - AWS Glue is a fully managed extract, transform, and load (ETL) service that makes it easy for customers to prepare and load their data for analytics. AWS Glue job is meant to be used for batch ETL data processing. It cannot be used to take the load off the databases.

Amazon EMR - Amazon EMR provides a managed Hadoop framework that makes it easy, fast, and cost-effective to process vast amounts of data across dynamically scalable Amazon EC2 instances. It cannot be used to take the load off the databases.

Reference:

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

Question 44:

A corporation would like to have a central user portal to log in to third-party business applications as well as accounts managed under AWS Organizations. As a Cloud Practitioner, which AWS service would you use for this task?

- **Explanation**

Correct option:

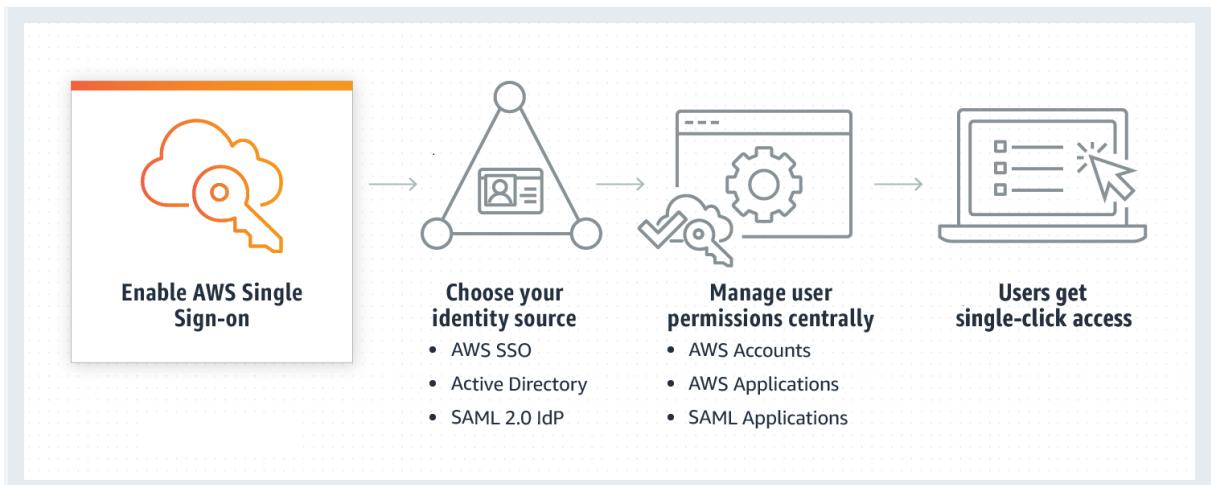
AWS Single Sign-On (SSO)

AWS SSO is an AWS service that enables you to make it easy to centrally manage access to multiple AWS accounts and business applications and provide users with single sign-on access to all their assigned accounts and applications from one place.

With AWS SSO, you can easily manage SSO access and user permissions to all of your accounts in AWS Organizations centrally. AWS SSO allows you to create and manage user identities in AWS SSO's identity store, or easily connect to your existing identity source including Microsoft Active Directory, Azure Active Directory (Azure AD), and Okta Universal Directory.

You can use AWS SSO to quickly and easily assign and manage your employees' access to multiple AWS accounts, SAML-enabled cloud applications (such as Salesforce, Office 365, and Box), and custom-built in-house applications, all from a central place.

How AWS SSO works:



via - <https://aws.amazon.com/single-sign-on/>

Incorrect options:

AWS Cognito - Amazon Cognito lets you add user sign-up, sign-in, and access control to your web and mobile apps quickly and easily. With Amazon Cognito, you also have the option to authenticate users through social identity providers such as Facebook, Twitter, or Amazon, with SAML identity solutions, or by using your own identity system. It is an identity management solution for customers/developers building B2C or B2B apps for their customers.

AWS Identity and Access Management (IAM) - AWS Identity and Access Management (IAM) enables you to securely control access to AWS services and resources for your users. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources. It is not used to log in but to manage users and roles.

AWS Command Line Interface (CLI) - The AWS Command Line Interface (CLI) is a unified tool to manage your AWS services. With just one tool to download and configure, you can control multiple AWS services from the command line and automate them through scripts. It is not a central user portal.

Reference:

<https://aws.amazon.com/single-sign-on/>

Question 45:

A company would like to optimize Amazon EC2 costs. Which of the following actions can help with this task? (Select TWO)

- **Explanation**

Correct option:

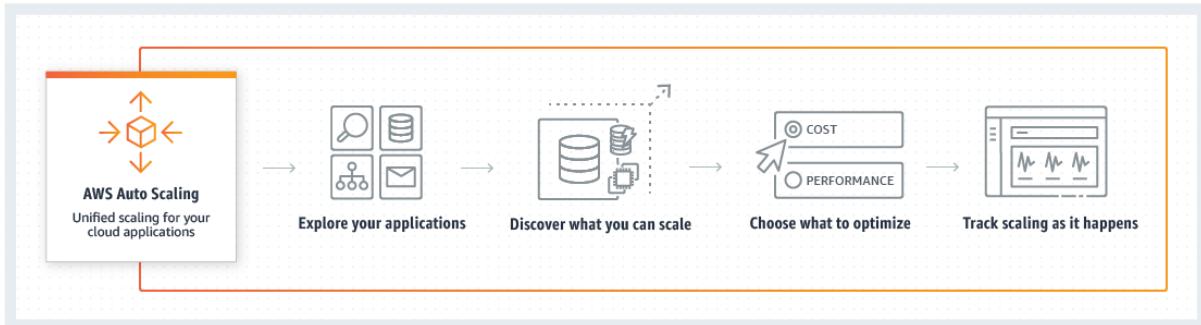
Set up Auto Scaling groups to align the number of instances with demand

Purchase EC2 Reserved instances

An Auto Scaling group contains a collection of Amazon EC2 instances that are treated as a logical grouping for automatic scaling and management. You can adjust its size to meet demand, either manually or by using automatic scaling.

AWS Auto Scaling can help you optimize your utilization and cost efficiencies when consuming AWS services so you only pay for the resources you need.

How AWS Auto Scaling works:



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

Amazon EC2 Reserved Instances (RI) provide a significant discount (up to 72%) compared to On-Demand pricing and provide a capacity reservation when used in a specific Availability Zone.

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:

Vertically scale the EC2 instances - Vertically scaling EC2 instances (increasing one computer performance by adding CPUs, memory, and storage) is limited and is way more expensive than scaling horizontally (adding more computers to the system).

Opt for a higher AWS Support plan - The AWS Support plans do not help with EC2 costs.

Build its own servers - Building your own servers is more expensive than using EC2 instances in the cloud. You're more likely to spend more money than saving money.

References:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/AutoScalingGroup.html>

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

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

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

Question 46:

Which of the following statements is an AWS best practice when architecting for the Cloud?



Explanation

Correct option:

Automation

Automation should be implemented to improve both your system's stability and the efficiency of your organization. There are many services to automate application architecture (AWS Elastic Beanstalk, Auto Scaling, AWS Lambda, etc.) to ensure more resiliency, scalability, and performance.

Incorrect options:

Servers, not services - The correct best practice is: "Services, not servers". AWS recommends to develop, manage, and operate applications, especially at scale, using the broad set of compute, storage, database, analytics, applications, and deployment services offered by AWS to move faster and lower IT costs.

Close coupling - The correct best practice is: "Loose coupling". AWS recommends that, as application complexity increases, IT systems should be designed in a way that reduces interdependencies. Therefore, a change or a failure in one component should not cascade to other components.

Security comes last - AWS allows you to improve your security in many, more simple ways. Therefore, you should take advantage of this and implement a high level of security.

Reference:

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

Question 47:

Which of the following statements is CORRECT regarding the scope of an Amazon Virtual Private Cloud (VPC)?



Explanation

Correct option:

A VPC spans all Availability Zones (AZs) within a region

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

A VPC spans all Availability Zones (AZs) within a region.

Incorrect options:

A VPC spans all subnets in all regions - A VPC is located within a region.

A VPC spans all Availability Zones (AZs) in all regions - A VPC is located within a region.

A VPC spans all regions within an Availability Zone (AZ) - AWS has the concept of a Region, which is a physical location around the world where AWS clusters data centers. Each AWS Region consists of multiple (two or more), isolated, and physically separate AZ's within a geographic area. An Availability Zone (AZ) is one or more discrete data centers with redundant power, networking, and connectivity in an AWS Region. Therefore, regions cannot be within an Availability Zone. Moreover, a VPC is located within a region.

AWS Regions and Availability Zones

Overview:

Regions

AWS has the concept of a Region, which is a physical location around the world where we cluster data centers. We call each group of logical data centers an Availability Zone. Each AWS Region consists of multiple, isolated, and physically separate AZ's within a geographic area. Unlike other cloud providers, who often define a region as a single data center, the multiple AZ design of every AWS Region offers advantages for customers. Each AZ has independent power, cooling, and physical security and is connected via redundant, ultra-low-latency networks. AWS customers focused on high availability can design their applications to run in multiple AZ's to achieve even greater fault-tolerance. AWS infrastructure Regions meet the highest levels of security, compliance, and data protection.

AWS provides a more extensive global footprint than any other cloud provider, and to support its global footprint and ensure customers are served across the world, AWS opens new Regions rapidly. AWS maintains multiple geographic Regions, including Regions in North America, South America, Europe, China, Asia Pacific, South Africa, and the Middle East.

Availability Zones

An Availability Zone (AZ) is one or more discrete data centers with redundant power, networking, and connectivity in an AWS Region. AZ's give customers the ability to operate production applications and databases that are more highly available, fault tolerant, and scalable than would be possible from a single data center. All AZ's in an AWS Region are interconnected with high-bandwidth, low-latency networking, over fully redundant, dedicated metro fiber providing high-throughput, low-latency networking between AZ's. All traffic between AZ's is encrypted. The network performance is sufficient to accomplish synchronous replication between AZ's. AZ's make partitioning applications for high availability easy. If an application is partitioned across AZ's, companies are better isolated and protected from issues such as power outages, lightning strikes, tornadoes, earthquakes, and more. AZ's are physically separated by a meaningful distance, many kilometers, from any other AZ, although all are within 100 km (60 miles) of each other.

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

Reference:

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

Question 48:

Which AWS serverless service allows you to prepare data for analytics?



Explanation

Correct option:

AWS Glue

AWS Glue - AWS Glue is a fully managed extract, transform, and load (ETL) service that makes it easy for customers to prepare and load their data for analytics. AWS Glue job is meant to be used for batch ETL data processing.

How AWS Glue

works:

How it works

Select a data source and data target. AWS Glue will generate ETL code in Scala or Python to extract data from the source, transform the data to match the target schema, and load it into the target. You can edit, debug and test this code via the Console, in your favorite IDE, or any notebook.

Step 1: Build your Data Catalog



First, use the AWS Management Console to register your data sources. AWS Glue will crawl your data sources and construct your Data Catalog using pre-built classifiers for many popular source formats and data types, including JSON, CSV, Parquet, and more.

Step 2: Generate and Edit Transformations



Next, select a data source and data target. AWS Glue will generate ETL code in Scala or Python to extract data from the source, transform the data to match the target schema, and load it into the target. You can edit, debug and test this code via the Console, in your favorite IDE, or any notebook.

Step 3: Schedule and Run Your Jobs



AWS Glue makes it easy to schedule recurring ETL jobs, chain multiple jobs together, or invoke jobs on-demand from other services like AWS Lambda. AWS Glue manages the dependencies between your jobs, automatically scales underlying resources, and retries jobs if they fail.

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

Incorrect options:

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. Athena is used for analytics and not to prepare data for analytics.

Amazon Redshift - Amazon Redshift is a fast, scalable data warehouse that makes it simple and cost-effective to analyze all your data across your data warehouse and data lake. Redshift is used for analytics and not to prepare data for analytics.

Amazon EMR - Amazon EMR provides a managed Hadoop framework that makes it easy, fast, and cost-effective to process vast amounts of data across dynamically scalable Amazon EC2 instances. EMR is used for analytics and not to prepare data for analytics.

Reference:

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

Question 49:

A company needs to keep sensitive data in its own data center due to compliance but would still like to deploy resources using AWS. Which Cloud deployment model does this refer to?



Explanation

Correct option:

Hybrid Cloud

A hybrid deployment is a way to connect infrastructure and applications between cloud-based resources and existing resources that are not located in the cloud. The most common method of hybrid deployment is between the cloud and existing on-premises infrastructure to extend, and grow, an organization's infrastructure into the cloud while connecting cloud resources to the internal system.

Overview of Cloud Computing Deployment Models:

Cloud Computing Deployment Models



Cloud

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](#). Cloud-based applications can be built on low-level infrastructure pieces or can use higher level services that provide abstraction from the management, architecting, and scaling requirements of core infrastructure.



Hybrid

A hybrid deployment is a way to connect infrastructure and applications between cloud-based resources and existing resources that are not located in the cloud. The most common method of hybrid deployment is between the cloud and existing on-premises infrastructure to extend, and grow, an organization's infrastructure into the cloud while connecting cloud resources to internal system. For more information on how AWS can help you with your hybrid deployment, please visit our [hybrid page](#).



On-premises

Deploying resources on-premises, using virtualization and resource management tools, is sometimes called "private cloud". On-premises deployment does not provide many of the benefits of cloud computing but is sometimes sought for its ability to provide [dedicated resources](#). In most cases this deployment model is the same as legacy IT infrastructure while using application management and virtualization technologies to try and increase resource utilization.

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

Incorrect options:

Public Cloud - A public 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 Cloud - Unlike a Public cloud, a Private cloud enables businesses to avail IT services that are provisioned and customized according to their precise needs. The business can further avail the IT services securely and reliably over a private IT infrastructure.

On-premises - This is not a cloud deployment model. When an enterprise opts for on-premises, it needs to create, upgrade, and scale the on-premise IT infrastructure by investing in sophisticated hardware, compatible software, and robust services. Also, the business needs to deploy dedicated IT staff to upkeep, scale, and manage the on-premise infrastructure continuously.

Reference:

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

Question 50:

A production company with predictable usage would like to reduce the cost of its Amazon EC2 instances by using reserved instances. Which of the following length terms are available for Amazon EC2 reserved instances? (Select TWO)

-
- **Explanation**

Correct option:

1 year

3 years

Reserved Instances provide you with a significant discount (up to 75%) compared to On-Demand instance pricing. Besides, 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.

Standard and Convertible reserved instances can be purchased for a 1-year or 3-year term.

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:

6 months - It is not possible to reserve instances for 6 months.

5 years - It is not possible to reserve instances for 5 years.

2 years - It is not possible to reserve instances for 2 years.

Reference:

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

Question 51:

According to the Well-Architected Framework, which of the following statements are design principles in the Performance Efficiency pillar? (Select TWO)



- **Explanation**

Correct option:

Use serverless architectures

Experiment more often

The Performance Efficiency pillar includes the ability to use computing resources efficiently to meet system requirements, and to maintain that efficiency as demand changes and technologies evolve.

In the cloud, serverless architectures remove the need for you to run and maintain servers to carry out traditional compute activities. For example, storage services can act as static websites, removing the need for web servers, and event services can host your code for you. This not only removes the operational burden of managing these servers, but also can lower transactional costs because these managed services operate at cloud scale.

With virtual and automatable resources, you can quickly carry out comparative testing using different types of instances, storage, or configurations.

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

The AWS Well-Architected Framework is based on five pillars — Operational Excellence, Security, Reliability, Performance Efficiency, and Cost Optimization.

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



Operational Excellence

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

[Operational Excellence whitepaper PDF | Kindle](#)



Security

The security pillar focuses on protecting information & systems. Key topics include confidentiality and integrity of data, identifying and managing who can do what with privilege management, protecting systems, and establishing controls to detect security events.

[Download the Security Pillar whitepaper PDF | Kindle](#)



Reliability

The reliability pillar focuses on the ability to prevent, and quickly recover from failures to meet business and customer demand. Key topics include foundational elements around setup, cross project requirements, recovery planning, and how we handle change.

[Download the Reliability Pillar whitepaper PDF | Kindle](#)



Performance Efficiency

The performance efficiency pillar focuses on using IT and computing resources efficiently. Key topics include selecting the right resource types and sizes based on workload requirements, monitoring performance, and making informed decisions to maintain efficiency as business needs evolve.

[Download the Performance Efficiency whitepaper PDF | Kindle](#)



Cost Optimization

Cost Optimization focuses on avoiding un-needed costs. Key topics include understanding and controlling where money is being spent, selecting the most appropriate and right number of resource types, analyzing spend over time, and scaling to meet business needs without overspending.

[Download the Cost Optimization whitepaper PDF | Kindle](#)

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

Incorrect options:

Automatically recover from failure - By monitoring a system for key performance indicators (KPIs), you can trigger automation when a threshold is breached. This allows for automatic notification and tracking of failures, and for automated recovery processes that work around or repair the failure. With more sophisticated automation, it's possible to anticipate and remediate failures before they occur. It is a design principle of the Reliability pillar.

Stop guessing about capacity - A common cause of failure in on-premises systems is resource saturation when the demands placed on a system exceed the capacity of that system (this is often the objective of denial of service attacks). In the cloud, you can monitor demand and system utilization, and automate the addition or removal of resources to maintain the optimal level to satisfy demand without over-provisioning or under-provisioning. It is a design principle of the Reliability pillar.

Enable traceability - Monitor, alert, and audit actions and changes to your environment in real-time. Integrate logs and metrics with systems to automatically respond and take action. It is a design principle of the Security pillar.

Reference:

<https://wa.aws.amazon.com/index.en.html>

Question 52:

A company would like to audit requests made to an S3 bucket. As a Cloud Practitioner, which S3 feature would you recommend addressing this use-case?

Explanation

Correct option:

S3 Access Logs

Server access logging provides detailed records for the requests that are made to a bucket. Server access logs are useful for many applications. For example, access log information can be useful in security and access audits.

It can also help you learn about your customer base and understand your Amazon S3 bill.

Incorrect options:

S3 Cross-Region Replication (CRR) - Replication enables automatic, asynchronous copying of objects across Amazon S3 buckets. Cross-Region replication (CRR) is used to copy objects across Amazon S3 buckets in different AWS Regions. It does not help with auditing requests made to your bucket.

S3 Bucket Policies - A bucket policy is a resource-based AWS Identity and Access Management (IAM) policy. You add a bucket policy to a bucket to grant other AWS accounts or IAM users access permissions for the bucket and the objects in it. Object permissions apply only to the objects that the bucket owner creates. It does not help with auditing requests made to your bucket.

S3 Versioning - Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. It does not help with auditing requests made to your bucket.

Reference:

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

Question 53:

Which of the following AWS Support plans offers a 15-minutes response time in case of a business-critical system going down?

- **Explanation**

Correct option:

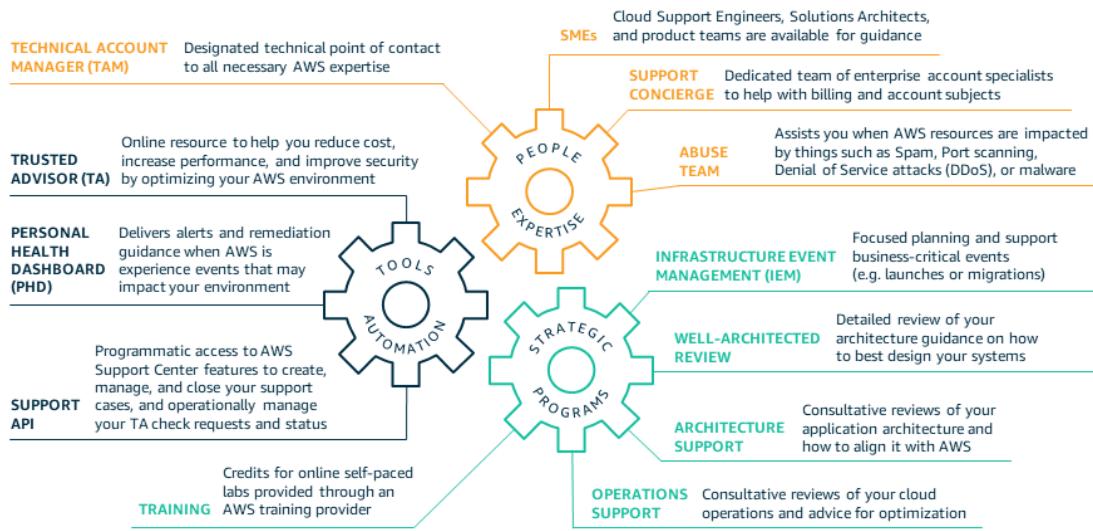
Enterprise

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 on helping the customer achieve their outcomes and find success in the cloud. With

Enterprise Support, you get access to online training with self-paced labs, 24x7 technical support from high-quality engineers, tools and technology to automatically manage the health of your environment, consultative architectural guidance, a designated Technical Account Manager (TAM) to coordinate access to proactive/preventative programs and AWS subject matter experts, as well as a 15-minutes response time in case of a business-critical system going down.

AWS Enterprise Support Plan Offerings:



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

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
	<i>Recommended if you are experimenting or testing in AWS.</i>	<i>Recommended if you have production workloads in AWS.</i>	<i>Recommended if you have business and/or mission critical workloads in AWS.</i>
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.

Basic - 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 access to technical support and architectural guidance in the context of your specific use-cases.

None of these three support plans offers a 15-minutes response time in case of a business-critical system going down.

References:

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

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

Question 54:

Which of the following entities allows AWS Lambda to get triggered?



Explanation

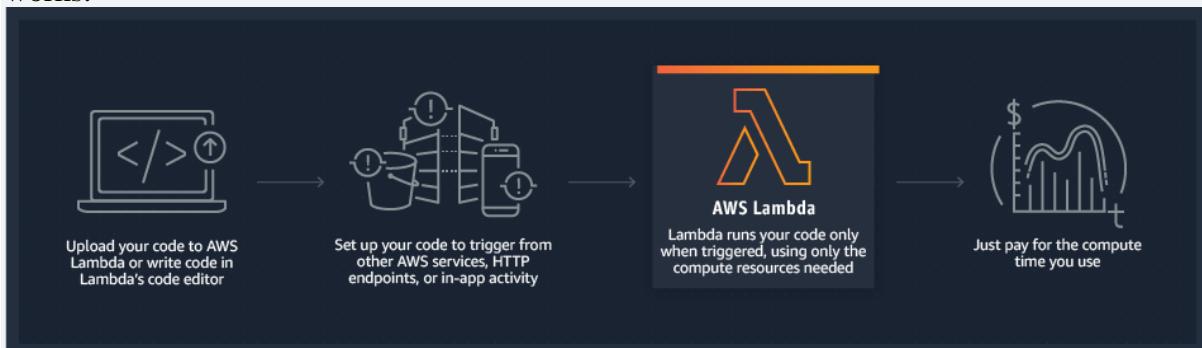
Correct option:

Events

AWS Lambda lets you run code without provisioning or managing servers. You pay only for the compute time you consume—there is no charge when your code is not running. With Lambda, you can run code for virtually any type of application or backend service—all with zero administration. Just upload your code, and Lambda takes care of everything required to run and scale your code with high availability. You can set up your code to automatically trigger from other AWS services, or you can call it directly from any web or mobile app.

Lambda functions that compose serverless applications are triggered by events.

How AWS Lambda works:



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

Incorrect options:

Metrics - Actions cannot trigger Lambda functions.

Timing - Actions cannot trigger Lambda functions.

Actions - Actions cannot trigger Lambda functions.

Reference:

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

Question 55:

An engineering team would like to cost-effectively run hundreds of thousands of batch computing workloads on AWS. As a Cloud Practitioner, which AWS service would you use for this task?

-  **Explanation**

Correct option:

AWS Batch

AWS Batch enables developers, scientists, and engineers to easily and efficiently run hundreds of thousands of batch computing jobs on AWS.

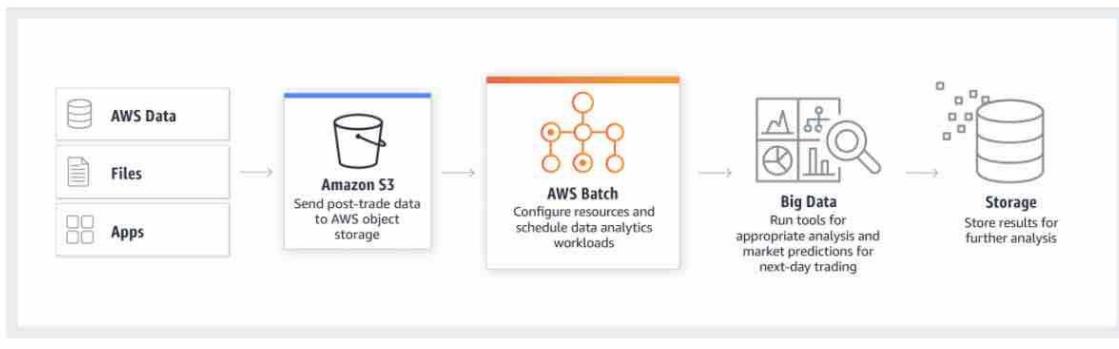
You can use AWS Batch to plan, schedule, and execute your batch computing workloads across the full range of AWS compute services. AWS Batch dynamically provisions the optimal quantity and type of compute resources (e.g., CPU or memory optimized instances) based on the volume and specific resource requirements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

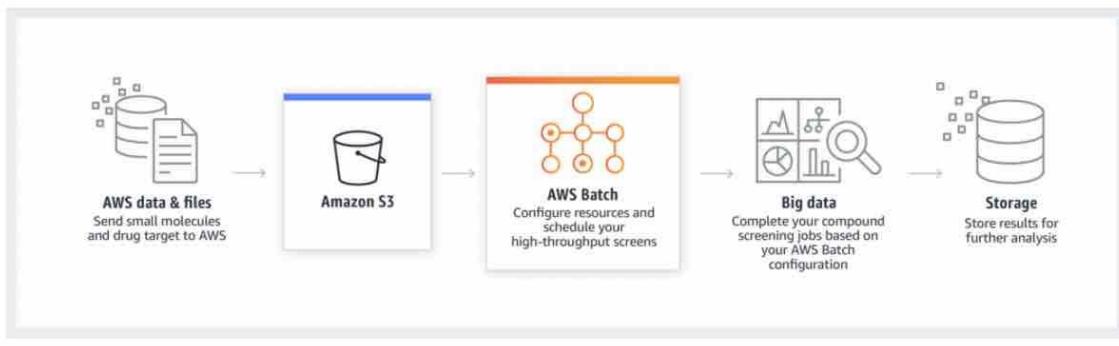
Financial services: Post-trade analytics

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



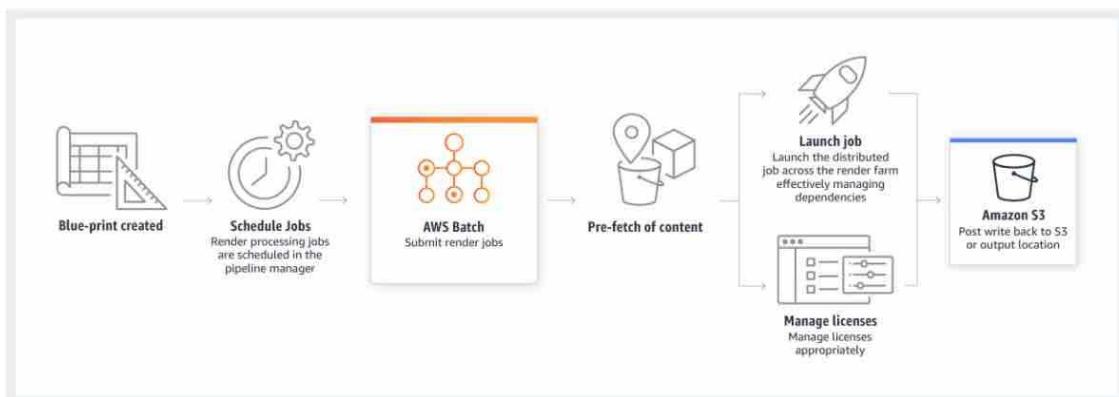
Life sciences: Drug screening for biopharma

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/>

Incorrect options:

AWS Lambda - AWS Lambda lets you run code without provisioning or managing servers. It can be used to run batch jobs, but has a time limit, and limited runtimes. It is usually used for smaller batch jobs.

Amazon Lightsail - Amazon Lightsail is designed to be the easiest way to launch and manage a virtual private server with AWS. Lightsail plans include everything you need to jumpstart your project – a virtual machine, SSD- based storage, data transfer, DNS

management, and a static IP address – for a low, predictable price. It is not used to run batch jobs.

AWS Fargate - AWS Fargate is a compute engine for Amazon ECS that allows you to run containers without having to manage servers or clusters. You can run batch jobs on Fargate, but it is more expensive than AWS Batch.

Reference:

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

Question 56:

An e-commerce company would like to build a chatbot for its customer service using Natural Language Understand (NLU). As a Cloud Practitioner, which AWS service would you use?



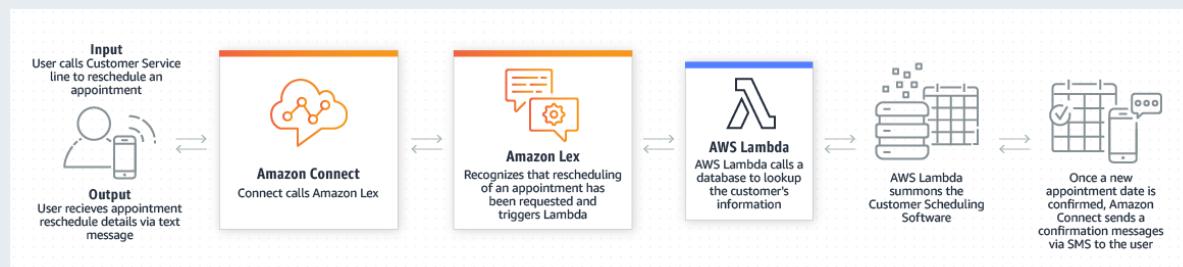
Amazon Rekognition

Explanation

Correct option:

Amazon Lex - Amazon Lex is a service for building conversational interfaces using voice and text. Powered by the same conversational engine as Alexa, Amazon Lex provides high-quality speech recognition and language understanding capabilities, enabling the addition of sophisticated, natural language ‘chatbots’ to new and existing applications.

Amazon Lex Use Cases:



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

Incorrect options:

Amazon Rekognition - With Amazon Rekognition, you can identify objects, people, text, scenes, and activities in images and videos, as well as to 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 SageMaker - Amazon SageMaker is a fully-managed platform that enables developers and data scientists to quickly and easily build, train, and deploy machine learning models at any scale. Amazon SageMaker removes all the barriers that typically slow down developers who want to use machine learning.

Amazon Comprehend - Amazon Comprehend is a natural language processing (NLP) service that uses machine learning to find meaning and insights in text. Natural Language Processing (NLP) is a way for computers to analyze, understand, and derive meaning from textual information in a smart and useful way. By utilizing NLP, you can extract important phrases, sentiment, syntax, key entities such as brand, date, location, person, etc., and the language of the text.

Reference:

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

Question 57:

Which Amazon EC2 Auto Scaling feature can help with fault tolerance?

- **Explanation**

Correct option:

Replacing unhealthy EC2 instances

Amazon EC2 Auto Scaling helps you maintain application availability and allows you to automatically add or remove EC2 instances according to conditions you define. You can use the fleet management features of EC2 Auto Scaling to maintain the health and availability of your fleet. You can also use the dynamic and predictive scaling features of EC2 Auto Scaling to add or remove EC2 instances.

Amazon EC2 Auto Scaling can detect when an instance is unhealthy, terminate it, and replace it with a new one.

Incorrect options:

Lower cost by adjusting the number of EC2 instances - Amazon EC2 Auto Scaling adds instances only when needed, and can scale across purchase options to optimize performance and cost. However, this will not help with fault tolerance.

Distributing load to EC2 instances - Even though this helps with fault tolerance and is often used with Amazon EC2 Auto Scaling, it is a feature of Elastic Load Balancing (ELB) and not Amazon EC2 Auto Scaling. 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.

Having the right amount of computing capacity - Amazon EC2 Auto Scaling ensures that your application always has the right amount of compute, so your application can handle the workload.

Reference:

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

Question 58:

A Cloud Practitioner would like to get operational insights of its resources to quickly identify any issues that might impact applications using those resources. Which AWS service can help with this task?

Explanation

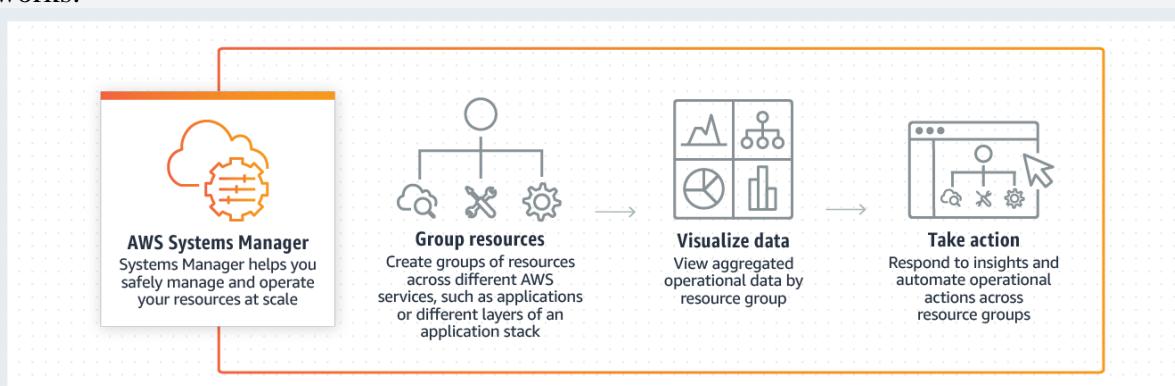
Correct option:

AWS Systems Manager

AWS Systems Manager allows you to centralize operational data from multiple AWS services and automate tasks across your AWS resources. You can create logical groups of resources such as applications, different layers of an application stack, or production versus development environments.

With Systems Manager, you can select a resource group and view its recent API activity, resource configuration changes, related notifications, operational alerts, software inventory, and patch compliance status. You can also take action on each resource group depending on your operational needs. Systems Manager provides a central place to view and manage your AWS resources, so you can have complete visibility and control over your operations.

How AWS Systems Manager works:



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

Incorrect options:

Amazon Inspector - Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. It is not used to get operational insights of AWS resources.

AWS Personal Health Dashboard - AWS Personal Health Dashboard provides alerts and remediation guidance when AWS is experiencing events that might affect you. It is not used to get operational insights of AWS resources.

AWS Trusted Advisor - AWS Trusted Advisor is an online resource to help you reduce cost, increase performance, and improve security by optimizing your AWS environment. Trusted Advisor provides real-time guidance to help you provision your resources following AWS best practices. It is not used to get operational insights of AWS resources.

Reference:

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

Question 59:

According to the Well-Architected Framework, which of the following statements are recommendations in the Operational Excellence pillar? (Select TWO)

- **Explanation**

Correct option:

Anticipate failure

Make frequent, small, reversible changes

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

Perform “pre-mortem” exercises to identify potential sources of failure so that they can be removed or mitigated. Test your failure scenarios and validate your understanding of their impact. Test your response procedures to ensure that they are effective, and that teams are familiar with their execution. Set up regular game days to test workloads and team responses to simulated events.

Design workloads to allow components to be updated regularly. Make changes in small increments that can be reversed if they fail (without affecting customers when possible).

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

The AWS Well-Architected Framework is based on five pillars — Operational Excellence, Security, Reliability, Performance Efficiency, and Cost Optimization.

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



Operational Excellence

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

[Operational Excellence whitepaper PDF | Kindle](#)



Security

The security pillar focuses on protecting information & systems. Key topics include confidentiality and integrity of data, identifying and managing who can do what with privilege management, protecting systems, and establishing controls to detect security events.

[Download the Security Pillar whitepaper PDF | Kindle](#)



Reliability

The reliability pillar focuses on the ability to prevent, and quickly recover from failures to meet business and customer demand. Key topics include foundational elements around setup, cross project requirements, recovery planning, and how we handle change.

[Download the Reliability Pillar whitepaper PDF | Kindle](#)



Performance Efficiency

The performance efficiency pillar focuses on using IT and computing resources efficiently. Key topics include selecting the right resource types and sizes based on workload requirements, monitoring performance, and making informed decisions to maintain efficiency as business needs evolve.

[Download the Performance Efficiency whitepaper PDF | Kindle](#)



Cost Optimization

Cost Optimization focuses on avoiding un-needed costs. Key topics include understanding and controlling where money is being spent, selecting the most appropriate and right number of resource types, analyzing spend over time, and scaling to meet business needs without overspending.

[Download the Cost Optimization whitepaper PDF | Kindle](#)

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

Incorrect options:

Enable traceability - Monitor, alert, and audit actions and changes to your environment in real-time. Integrate logs and metrics with systems to automatically respond and take action. It is a design principle of the Security pillar.

Automatically recover from failure - By monitoring a system for key performance indicators (KPIs), you can trigger automation when a threshold is breached. This allows for automatic notification and tracking of failures, and for automated recovery processes that work around or repair the failure. With more sophisticated automation, it's possible to anticipate and remediate failures before they occur. It is a design principle of the Reliability pillar.

Use serverless architectures - In the cloud, serverless architectures remove the need for you to run and maintain servers to carry out traditional compute activities. For example, storage services can act as static websites, removing the need for web servers, and event services can host your code for you. This not only removes the operational burden of managing these servers, but also can lower transactional costs because these managed services operate at cloud scale. It is a design principle of the Performance Efficiency pillar.

Reference:

<https://wa.aws.amazon.com/index.en.html>

Question 60:

Which of the following IAM Security Tools allows you to review permissions granted to a user?

- **Explanation**

Correct option:

IAM access advisor

Access advisor shows the service permissions granted to a user and when those services were last accessed. You can use this information to revise your policies.

Incorrect options:

IAM credentials report - You can generate and download a credential report that lists all users in your account and the status of their various credentials, including passwords, access keys, and MFA devices. It is not used to review permissions granted to a user.

IAM policies - IAM policies define permissions for an action regardless of the method that you use to perform the operation.

Multi-Factor Authentication (MFA) - AWS Multi-Factor Authentication (MFA) is a simple best practice that adds an extra layer of protection on top of your user name and password. With MFA enabled, when a user signs in to an AWS Management Console, they will be prompted for their user name and password (the first factor—what they know), as well as for an authentication code from their AWS MFA device (the second factor—what they have). Taken together, these multiple factors provide increased security for your AWS account settings and resources. It cannot be used to review permissions granted.

Reference:

<https://aws.amazon.com/about-aws/whats-new/2019/06/now-use-iam-access-advisor-with-aws-organizations-to-set-permission-guardrails-confidently/>

Question 61:

Which of the following statements is the MOST accurate when describing AWS Elastic Beanstalk?

- **Explanation**

Correct option:

It is a Platform as a Service (PaaS) which allows you to deploy and scale web applications and services

AWS Elastic Beanstalk makes it even easier for developers to quickly deploy and manage applications in the AWS Cloud. Developers simply upload their application, and Elastic Beanstalk automatically handles the deployment details of capacity provisioning, load balancing, auto-scaling, and application health monitoring.

It is a Platform as a Service as you only manage the applications and the data.

Please review this overview of the types of Cloud Computing:

Cloud Computing Models

There are three main models for cloud computing. Each model represents a different part of the cloud computing stack.



Infrastructure as a Service (IaaS)

Infrastructure as a Service, sometimes abbreviated as IaaS, contains the basic building blocks for cloud IT and typically provide access to networking features, computers (virtual or on dedicated hardware), and data storage space. Infrastructure as a Service provides you with the highest level of flexibility and management control over your IT resources and is most similar to existing IT resources that many IT departments and developers are familiar with today.



Platform as a Service (PaaS)

Platforms as a service remove the need for organizations to manage the underlying infrastructure (usually hardware and operating systems) and allow you to focus on the deployment and management of your applications. This helps you be more efficient as you don't need to worry about resource procurement, capacity planning, software maintenance, patching, or any of the other undifferentiated heavy lifting involved in running your application.



Software as a Service (SaaS)

Software as a Service provides you with a completed product that is run and managed by the service provider. In most cases, people referring to Software as a Service are referring to end-user applications. With a SaaS offering you do not have to think about how the service is maintained or how the underlying infrastructure is managed; you only need to think about how you will use that particular piece of software. A common example of a SaaS application is web-based email where you can send and receive email without having to manage feature additions to the email product or maintaining the servers and operating systems that the email program is running on.

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

Incorrect options:

It is an Infrastructure as Code which allows you to model and provision resources needed for an application - This is the definition of AWS CloudFormation. AWS CloudFormation gives developers and systems administrators an easy way to create and manage a collection of related AWS resources, provisioning and updating them in an orderly and predictable fashion. You can use the AWS CloudFormation sample templates or create your own templates to describe your AWS resources, and any associated dependencies or runtime parameters, required to run your application.

It is a Platform as a Service (PaaS) which allows you to model and provision resources needed for an application - AWS Elastic Beanstalk is a Platform as a Service. However, the service that allows you to model and provision resources needed for an application is AWS CloudFormation.

It is an Infrastructure as a Service (IaaS) which allows you to deploy and scale web applications and services - AWS Elastic Beanstalk allows you to deploy and scale web applications and services, but it is not an Infrastructure as a Service. With AWS Elastic Beanstalk, you do not manage the runtime, the middleware, and the operating system.

Reference:

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

Question 62:

Which AWS service can be used to view billing details for the past month?

-
- Explanation

Correct option:

AWS Cost & Usage Reports

The AWS Cost and Usage Reports (AWS CUR) contains the most comprehensive set of cost and usage data available. You can use Cost and Usage Reports to publish your AWS billing reports to an Amazon Simple Storage Service (Amazon S3) bucket that you own. You can receive reports that break down your costs by the hour or month, by product or product resource, or by tags that you define yourself.

AWS Cost and Usage Reports

Overview:

What are AWS Cost and Usage Reports?

[PDF](#) | [RSS](#)

The AWS Cost and Usage Reports (AWS CUR) contains the most comprehensive set of cost and usage data available. You can use Cost and Usage Reports to publish your AWS billing reports to an Amazon Simple Storage Service (Amazon S3) bucket that you own. You can receive reports that break down your costs by the hour or month, by product or product resource, or by tags that you define yourself. AWS updates the report in your bucket once a day in comma-separated value (CSV) format. You can view the reports using spreadsheet software such as Microsoft Excel or Apache OpenOffice Calc, or access them from an application using the Amazon S3 API.

AWS Cost and Usage Reports tracks your AWS usage and provides estimated charges associated with your account. Each report contains line items for each unique combination of AWS products, usage type, and operation that you use in your AWS account. You can customize the AWS Cost and Usage Reports to aggregate the information either by the hour or by the day.

AWS Cost and Usage Reports can do the following:

- Deliver report files to your Amazon S3 bucket
- Update the report up to three times a day
- Create, retrieve, and delete your reports using the AWS CUR API Reference

via - <https://docs.aws.amazon.com/cur/latest/userguide/what-is-cur.html>

Incorrect options:

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

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. AWS Cost Explorer cannot provide billing details for the past month.

AWS Total Cost of Ownership - TCO calculator helps to compare the cost of your applications in an on-premises or traditional hosting environment to AWS. 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 you to invest in the capacity you need and use it only when the business requires it. Once you describe your on-premises or hosting environment configuration, it produces a detailed cost comparison with AWS. TCO Calculator cannot provide billing details for the past month.

Exam Alert:

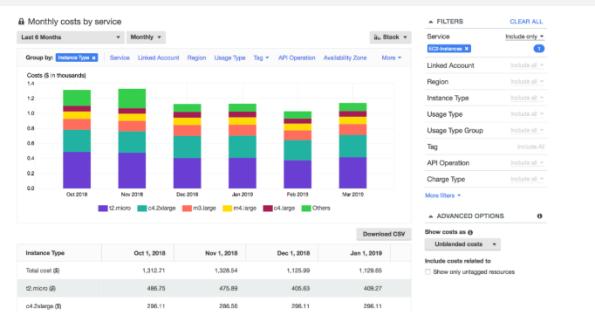
Please review the differences between "AWS Cost and Usage Reports" and "AWS Cost Explorer". Think of "AWS Cost and Usage Reports" as a cost management tool providing the most detailed cost and usage data for your AWS account. It can provide reports that break down your costs by the hour into your S3 bucket. On the other hand, "AWS Cost Explorer" is more of a high-level cost management tool that helps you visualize the costs and usage associated with your AWS account.

"AWS Cost Explorer" vs "AWS Cost and Usage Reports":

Monthly Costs by AWS Service

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.

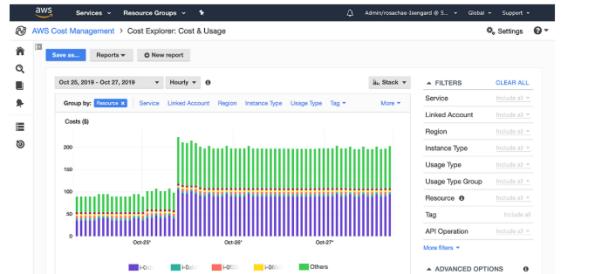
[Launch the Monthly Costs by AWS Service report »](#)



Hourly and Resource Level Granularity

AWS Cost Explorer helps you visualize, understand, and manage your AWS costs and usage over a daily or monthly granularity. The solution also lets you dive deeper using granular filtering and grouping dimensions such as Usage Type and Tags. You can also access your data with further granularity by enabling hourly and resource level granularity.

[Get started using Hourly and Resource Level Granularity »](#)



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

How does the AWS Cost & Usage Report work?

AWS delivers the AWS Cost & Usage Report (in CSV format) to whichever Amazon Simple Storage Service (S3) bucket you specify, and updates the reports at least once per day. You can download any of the reports using the Amazon S3 console, or you can retrieve the reports programmatically using the Amazon S3 APIs.

You can configure your Cost & Usage Reports to integrate with Amazon Athena. Once Amazon Athena integration has been enabled for your Cost & Usage Report, your data will be delivered in compressed Apache Parquet files to an Amazon S3 bucket of your choice. Your AWS Cost & Usage Report can also be ingested directly into Amazon Redshift or uploaded to Amazon QuickSight.

via - <https://aws.amazon.com/aws-cost-management/aws-cost-and-usage-reporting/>

References:

<https://docs.aws.amazon.com/cur/latest/userguide/what-is-cur.html>

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

<https://aws.amazon.com/aws-cost-management/aws-cost-and-usage-reporting/>

Question 63:

A company would like to move 50 petabytes (PBs) of data from its on-premises data centers to AWS in the MOST cost-effective way. As a Cloud Practitioner, which of the following solutions would you choose?

- **Explanation**

Correct option:

AWS Snowmobile

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

Incorrect options:

AWS Snowball Edge - Snowball Edge is an edge computing and data transfer device provided by the AWS Snowball service. It has on-board storage and compute power that provides select AWS services for use in edge locations. However, one Snowball Edge only provides up to 100 TB of capacity. Therefore, to transfer 50 PBs, AWS Snowball Edge is not the most cost-effective option.

AWS Snowball - AWS Snowball is a petabyte-scale data transport solution that uses secure appliances to transfer large amounts of data into and out of AWS. The use of Snowball addresses common challenges with large- scale data transfers including high network costs, long transfer times, and security concerns. Transferring data with Snowball is simple, fast, secure, and can be as little as one-fifth the cost of high-speed Internet. However, one Snowball only provides up to 80 TB of capacity. Therefore, to transfer 50 PBs, AWS Snowball is not the most cost-effective option.

AWS Storage Gateway - AWS Storage Gateway is a hybrid storage service that enables your on-premises applications to seamlessly use AWS cloud storage. You can use the service for backup and archiving, disaster recovery, cloud data processing, storage tiering, and migration. However, data transfer through AWS Storage Gateway takes longer even with great bandwidth. Moreover, to transfer 50 PBs of data, it will be more expensive than using AWS Snowmobile.

Reference:

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

Question 64: **Correct**

Which of the following billing timeframes is applied when running a Windows EC2 on-demand instance?

- **Explanation**

Correct option:

Pay per hour

With On-Demand instances you only pay for EC2 instances you use. The use of On-Demand instances frees you from the costs and complexities of planning, purchasing, and maintaining hardware and transforms what are commonly large fixed costs into much smaller variable costs.

When running a Windows EC2 on-demand instance, pay per hour pricing is applied.

Incorrect options:

Pay per second - Pay per second pricing is not available for Windows EC2 on-demand instances. It is available for Linux EC2 on demand-instances.

Pay per minute - Pay per minute pricing is not available for Windows EC2 on-demand instances, or any other type of on-demand EC2 instance.

Pay per day - Pay per day pricing is not available for Windows EC2 on-demand instances, or any other type of on-demand EC2 instance.

Reference:

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

Question 65:

A production company would like to establish an AWS managed VPN service between its on-premises network and AWS. Which item needs to be set up on the company's side?

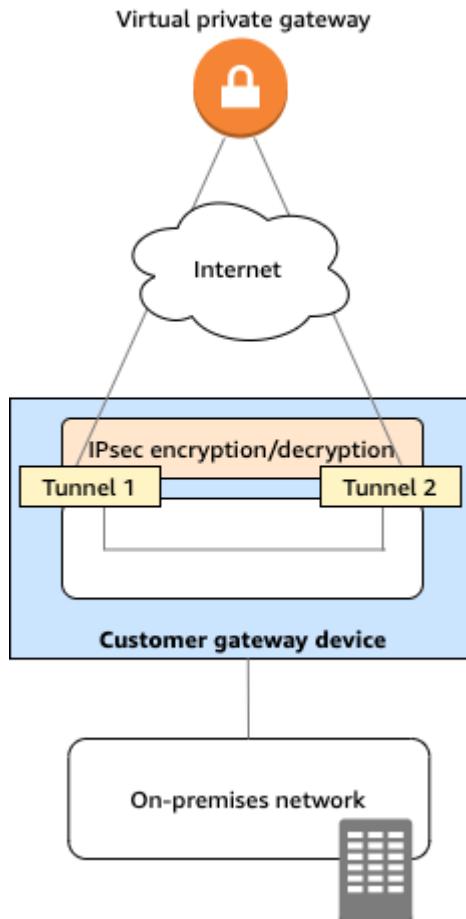
Explanation

Correct option:

A customer gateway

A customer gateway device is a physical or software appliance on your side of a Site-to-Site VPN connection. You or your network administrator must configure the device to work with the Site-to-Site VPN connection.

You can enable access to your remote network from your VPC by creating an AWS Site-to-Site VPN (Site-to-Site VPN) connection, and configuring routing to pass traffic through the connection.



- Schema:
 - <https://docs.aws.amazon.com/vpn/latest/s2svpn/your-cgw.html>

Incorrect options:

A security group - A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. It is not a component of a connection between on-premises network and AWS.

A VPC endpoint interface - An interface VPC endpoint (interface endpoint) enables you to connect to services powered by AWS PrivateLink. It is not a component of a connection between on-premises network and AWS.

A virtual private gateway - A virtual private gateway device is a physical or software appliance on AWS side of a Site-to-Site VPN connection.

References:

<https://docs.aws.amazon.com/vpn/latest/s2svpn/your-cgw.html>

https://docs.aws.amazon.com/vpn/latest/s2svpn/VPC_VPN.html