

Practice Test #1 - AWS Certified Cloud Practitioner - Results

Return to review

Chart

Pie chart with 3 slices.

End of interactive chart.

Attempt 2

All knowledge areas

All questions

Question 1: **Correct**

Which of the following entities applies patches to the underlying OS for AWS Aurora?

-
-

The AWS Product Team automatically

(Correct)

-
-

The AWS customer by using AWS Systems Manager

-
-

The AWS customer by SSHing on the instances

-
-

The AWS Support after receiving a request from the customer

Explanation

Correct option:

The AWS Product Team automatically

Amazon Aurora is a MySQL and PostgreSQL-compatible relational database built for the cloud. Amazon Aurora is fully managed by Amazon Relational Database Service (RDS), which automates time-consuming administration tasks like hardware provisioning, database setup, patching, and backups. The AWS Product team is responsible for applying patches to the underlying OS for AWS Aurora.

Incorrect options:

The AWS customer by using AWS Systems Manager - AWS Systems Manager gives you visibility and control of your infrastructure on AWS. Systems Manager provides a unified user interface so you can view operational data from multiple AWS services and allows you to automate operational tasks such as running commands, managing patches and configuring servers across AWS Cloud as well as on-premises infrastructure. You can only use AWS Systems Manager to apply patches to your EC2 instances or on-premises instances. You cannot use Systems Manager to apply patches to the underlying OS for AWS Aurora.

The AWS Support after receiving a request from the customer - AWS Support handles support tickets regarding AWS services. AWS Support is not responsible for applying patches to the underlying OS for AWS Aurora.

The AWS customer by SSHing on the instances - AWS customers are only responsible for patching their own EC2 instances.

Reference:

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

Question 2: **Correct**

A company wants to improve the resiliency of its flagship application so it wants to move from its traditional database system to a managed AWS database service to support active-active configuration in both the East and West US AWS regions. The active-active configuration with cross-region support is the prime criteria for any database solution that the company considers.

Which AWS database service is the right fit for this requirement?

-
-

Amazon DynamoDB with global tables

(Correct)

-
-

Amazon DynamoDB with DynamoDB Accelerator

-
-

Amazon Aurora with multi-master clusters

-
-

Amazon Relational Database Service (Amazon RDS) for MySQL

Explanation

Correct option: **Amazon DynamoDB with global tables**

Amazon DynamoDB is a fully managed, serverless, key-value NoSQL database designed to run high-performance applications at any scale. DynamoDB offers built-in security, continuous backups, automated multi-region replication, in-memory caching, and data export tools.

DynamoDB global tables replicate data automatically across your choice of AWS Regions and automatically scale capacity to accommodate your workloads. With global tables, your globally distributed applications can access data locally in the selected regions to get single-digit millisecond read and write performance. DynamoDB offers active-active cross-region support that is needed for the company.

Incorrect options:

Amazon DynamoDB with DynamoDB Accelerator - DynamoDB Accelerator (DAX) is an in-memory cache that delivers fast read performance for your tables at scale by enabling you to use a fully managed in-memory cache. Using DAX, you can improve the read performance of your DynamoDB tables by up to 10 times—taking the time required for reads from milliseconds to microseconds, even at millions of requests per second. DAX does not offer active-active cross-Region configuration.

Amazon Aurora with multi-master cluster - Amazon Aurora (Aurora) is a fully managed relational database engine that's compatible with MySQL and PostgreSQL. With some workloads, Aurora can deliver up to five times the throughput of MySQL and up to three times the throughput of PostgreSQL without requiring changes to most of your existing applications. In a multi-master cluster, all DB instances have read/write capability. Currently, all DB instances in a multi-master cluster must be in the same AWS Region. You can't enable cross-Region replicas from multi-master clusters.

Amazon Relational Database Service (Amazon RDS) for MYSQL - 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. RDS does not support active-active configuration with cross-region support.

References:

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

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-multi-master.html>

Question 3: **Correct**

A startup wants to set up its IT infrastructure on AWS Cloud. The CTO would like to get an estimate of the monthly AWS bill based on the AWS services that the startup wants to use. As a Cloud Practitioner, which AWS service would you suggest for this use-case?



AWS Cost Explorer



AWS Budgets



AWS Pricing Calculator

(Correct)



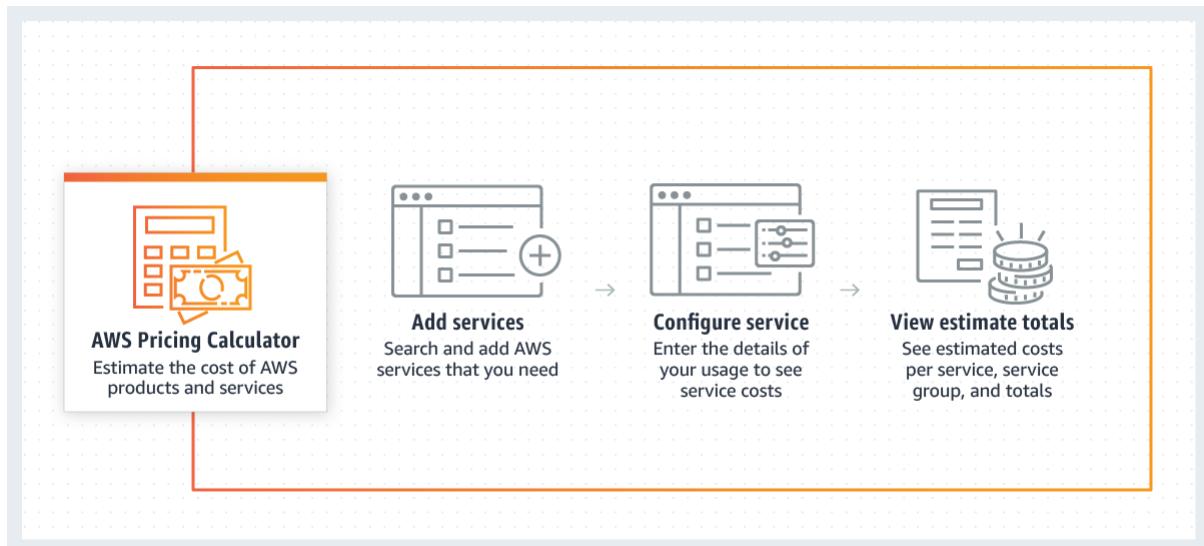
AWS Cost & Usage Report

Explanation

Correct option:

AWS Pricing Calculator

AWS Pricing Calculator lets you explore AWS services and create an estimate for the cost of your use cases on AWS. You can model your solutions before building them, explore the price points and calculations behind your estimate, and find the available instance types and contract terms that meet your needs. This enables you to make informed decisions about using AWS. You can plan your AWS costs and usage or price out setting up a new set of instances and services. AWS Pricing Calculator can provide the estimate of the AWS service usage based on the list of AWS services.



via - <https://calculator.aws/#/>

The AWS Pricing Calculator is accessible on : <https://calculator.aws/#/>

You should also note AWS is in the process of deprecating a similar tool called the Simple Monthly Calculator. This calculator provides an estimate of usage charges for AWS services based on certain information you provide. It helps customers and prospects estimate their monthly AWS bill more efficiently. This tool can be accessed on : <https://calculator.s3.amazonaws.com/index.html>

Incorrect options:

AWS Cost & Usage Report - The AWS Cost & Usage Report contains the most comprehensive set of AWS cost and usage data available, including additional metadata about AWS services, pricing, credit, fees, taxes, discounts, cost categories, Reserved Instances, and Savings Plans. The AWS Cost & Usage Report (CUR) itemizes usage at the account or Organization level by product code, usage type and operation. These costs can be further organized by Cost Allocation tags and Cost Categories. The AWS Cost & Usage Report is available at an hourly, daily, or monthly level of granularity, as well as at the management or member account level. The AWS Cost & Usage Report cannot provide the estimate of the monthly AWS bill based on the list of AWS services.

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 the estimate of the monthly AWS bill based on the list of AWS services.

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 the estimate of the monthly AWS bill based on the list of AWS services.

Reference:

<https://calculator.aws/#/>

Question 4: **Correct**

Which type of Cloud Computing does Amazon Elastic Compute Cloud (EC2) represent?

-
-

Infrastructure as a Service (IaaS)

(Correct)

-
-

Software as a Service (SaaS)

-
-

Platform as a Service (PaaS)

-
-

Network as a Service (NaaS)

Explanation

Correct option:

Infrastructure as a Service (IaaS)

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

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

EC2 gives you full control over managing the underlying OS, virtual network configurations, storage, data and applications. So EC2 is an example of an IaaS service.

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:

Platform as a Service (PaaS) - 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.

Elastic Beanstalk is an example of a PaaS service. You can simply upload your code and Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring.

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.

Network as a Service (NaaS) - This is a made-up option and has been added as a distractor.

Reference:

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

Question 5: **Correct**

AWS Shield Advanced provides expanded DDoS attack protection for web applications running on which of the following resources? (Select two)

-

AWS Elastic Beanstalk

-

Amazon API Gateway

-

AWS Global Accelerator

(Correct)

-

Amazon Route 53

(Correct)

-

AWS CloudFormation

Explanation

Correct options:

Amazon Route 53

AWS Global Accelerator

AWS Shield Standard is activated for all AWS customers, by default. For higher levels of protection against attacks, you can subscribe to AWS Shield Advanced. With Shield Advanced, you also have exclusive access to advanced, real-time metrics and reports for extensive visibility into attacks on your AWS resources. With the assistance of the DRT (DDoS response team), AWS Shield Advanced includes intelligent DDoS attack detection and mitigation for not only for network layer (layer 3) and transport layer (layer 4) attacks but also for application layer (layer 7) attacks.

AWS Shield Advanced provides expanded DDoS attack protection for web applications running on the following resources: Amazon Elastic Compute Cloud, Elastic Load Balancing (ELB), Amazon CloudFront, Amazon Route 53, AWS Global Accelerator.

Incorrect options:

Amazon API Gateway - Amazon API Gateway is a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale. APIs act as the "front door" for applications to access data, business logic, or functionality from your backend services. Amazon Web Application Firewall is used to monitor the HTTP and HTTPS requests that are forwarded to an Amazon API Gateway API. It is not covered under AWS Shield Advanced.

AWS CloudFormation - AWS CloudFormation allows you to use programming languages or a simple text file to model and provision, in an automated and secure manner, all the resources needed for your applications across all regions and accounts. CloudFormation is not covered under AWS Shield Advanced.

AWS Elastic Beanstalk - AWS Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services developed with various programming languages. You can simply upload your code and Elastic Beanstalk automatically handles the deployment, from capacity

provisioning, load balancing, auto-scaling to application health monitoring. Elastic Beanstalk is covered under AWS Shield Standard. Advanced coverage is not offered for this service.

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

Question 6: **Correct**

Which of the following statements are CORRECT regarding the Availability Zone (AZ) specific characteristics of EBS and EFS storage types?

-
-

EBS volume can be attached to a single instance in the same Availability Zone whereas EFS file system can be mounted on instances across multiple Availability Zones

(Correct)

-
-

EBS volume can be attached to one or more instances in multiple Availability Zones and EFS file system can be mounted on instances across multiple Availability Zones

-
-

EBS volume can be attached to one or more instances in multiple Availability Zones and EFS file system can be mounted on instances in the same Availability Zone

-
-

EBS volume can be attached to a single instance in the same Availability Zone and EFS file system can only be mounted on instances in the same Availability Zone

Explanation

Correct options:

EBS volume can be attached to a single instance in the same Availability Zone whereas EFS file system can be mounted on instances across multiple Availability Zones

Amazon Elastic File System (Amazon EFS) provides a simple, scalable, fully managed elastic NFS file system for use with AWS Cloud services and on-premises resources. It is built to scale on-demand to petabytes without disrupting applications, growing and shrinking automatically as you add and remove files, eliminating the need to provision and manage capacity to accommodate growth.

The service is designed to be highly scalable, highly available, and highly durable. Amazon EFS file systems store data and metadata across multiple Availability Zones in an AWS Region. EFS file system can be mounted on instances across multiple Availability Zones.

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

Designed for mission-critical systems, EBS volumes are replicated within an Availability Zone (AZ) and can easily scale to petabytes of data. You can attach an available EBS volume to one instance that is in the same Availability Zone as the volume.

Incorrect options:

EBS volume can be attached to one or more instances in multiple Availability Zones and EFS file system can be mounted on instances in the same Availability Zone

EBS volume can be attached to a single instance in the same Availability Zone and EFS file system can only be mounted on instances in the same Availability Zone

EBS volume can be attached to one or more instances in multiple Availability Zones and EFS file system can be mounted on instances across multiple Availability Zones

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

References:

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

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

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

Question 7: **Correct**

Compared to the On-demand prices, what is the highest possible discount offered for spot instances?

-

90

(Correct)

-

50

-

10

-

75

Explanation

Correct option:

90

Amazon EC2 Spot Instances let you take advantage of unused EC2 capacity in the AWS cloud. Spot Instances are available at up to a 90% discount compared to On-Demand prices. You can use Spot Instances for various stateless, fault-tolerant, or flexible applications such as big data, containerized workloads, CI/CD, web servers, high-performance computing (HPC), and other test & development workloads.

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:

75

10

50

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

Reference:

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

Question 8: **Correct**

Which of the following is the MOST cost-effective option to purchase an EC2 Reserved Instance?



Partial upfront payment option with standard 3-years term

(Correct)



All upfront payment option with standard 1-year term



No upfront payment option with standard 1-year term



No upfront payment option with standard 3-years term

Explanation

Correct option:

Partial upfront payment option with standard 3-years term

You can use Amazon EC2 Reserved Instances to reserve capacity and receive a discount on your instance usage compared to running On-Demand instances. The discounted usage price is reserved for the duration of your contract, allowing you to predict compute costs over the term of the Reserved Instance.

Please review this pricing comparison for EC2 Reserved Instances:

Standard 1-Year Term

Payment Option	Upfront	Monthly*	Effective Hourly	Savings over On-Demand	On-Demand Hourly
No Upfront	\$0	\$44.53	\$0.061	36%	\$0.096 per Hour
Partial Upfront	\$256	\$21.17	\$0.058	39%	
All Upfront	\$501	\$0	\$0.057	40%	

Standard 3-Year Term

Payment Option	Upfront	Monthly*	Effective Hourly	Savings over On-Demand
No Upfront	\$0	\$30.66	\$0.042	56%
Partial Upfront	\$515	\$14.60	\$0.040	59%
All Upfront	\$968	\$0	\$0.037	62%

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

So the percentage savings for each option is as follows:

"No upfront payment option with the standard 1-year term" - 36%

"All upfront payment option with the standard 1-year term" - 40%

"No upfront payment option with the standard 3-years term" - 56%

"Partial upfront payment option with the standard 3-years term" - 59%

Exam Alert:

For the exam, there is no need to memorize these savings numbers. All you need to remember is that a 3 years term would always be more cost-effective than a 1-year term. Then within a term, "all upfront" is better than "partial upfront" which in turn is better than "no upfront" from a cost savings perspective.

Incorrect options:

No upfront payment option with standard 1-year term

No upfront payment option with standard 1-year term

No upfront payment option with standard 3-years term

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

Reference:

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

Question 9: **Correct**

A startup wants to provision an EC2 instance for the lowest possible cost for a long-term duration but needs to make sure that the instance would never be interrupted. As a Cloud Practitioner, which of the following options would you recommend?

-

Reserved Instance

(Correct)

-

Dedicated Host

-

On-Demand Instance

-

Spot Instance

Explanation

Correct option:

Reserved Instance - Reserved Instances provide you with significant savings (up to 75%) on your Amazon EC2 costs compared to On-Demand Instance pricing. Reserved Instances are not physical instances, but rather a billing discount applied to the use of On-Demand Instances in your account. You can purchase a Reserved Instance for a one-year or three-year commitment, with the three-year commitment offering a bigger discount. Reserved instances cannot be interrupted. So this is the correct option.

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:

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

Spot Instance - A Spot Instance is an unused EC2 instance that is available for less than the On-Demand price. Because Spot Instances enable you to request unused EC2 instances at steep discounts (up to 90%), you can lower your Amazon EC2 costs significantly. Spot Instances are well-suited for data analysis, batch jobs, background processing, and optional tasks. These can be terminated at short notice, so these are not suitable for critical workloads that need to run at a specific point in time. So this option is not correct for the given use-case.

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

Reference:

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

Question 10: **Correct**

A multi-national corporation wants to get expert professional advice on migrating to AWS and managing their applications on AWS Cloud. Which of the following entities would you recommend for this engagement?



AWS Trusted Advisor



APN Consulting Partner

(Correct)



APN Technology Partner



Concierge Support Team

Explanation

Correct option:

APN Consulting Partner

The AWS Partner Network (APN) is the global partner program for technology and consulting businesses that leverage Amazon Web Services to build solutions and services for customers.

APN Consulting Partners are professional services firms that help customers of all types and sizes design, architect, build, migrate, and manage their workloads and applications on AWS, accelerating their migration to AWS cloud.

APN Partner Types

Overview:

APN Partner Types

APN Consulting Partners

APN Consulting Partners are professional services firms that help customers of all types and sizes design, architect, build, migrate, and manage their workloads and applications on AWS, accelerating their journey to the cloud. APN Consulting Partners often implement Technology Partner solutions in addition to the professional services they offer.

APN Consulting Partners include system integrators, strategic consultancies, agencies, managed service providers, and value-added resellers.

[Learn more »](#)

APN Technology Partners

APN Technology Partners provide hardware, connectivity services, or software solutions that are either hosted on, or integrated with, the AWS Cloud. Technology Partner products are often delivered as components to broader AWS customer solutions and can be delivered globally by Consulting Partners through AWS Marketplace, bundled solutions, or directly from APN Technology Partners.

APN Technology Partners include original equipment manufacturers (OEMs), semiconductor manufacturers, network carriers, SaaS Providers, and independent software vendors (ISVs).

[Learn more »](#)

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

Incorrect options:

APN Technology Partner - APN Technology Partners provide hardware, connectivity services, or software solutions that are either hosted on or integrated with, the AWS Cloud. APN Technology Partners cannot help in migrating to AWS and managing applications on AWS Cloud.

AWS Trusted Advisor - AWS Trusted Advisor is an online tool that provides you real-time guidance to help you provision your resources following AWS best practices on cost optimization, security, fault tolerance, service limits, and performance improvement. Whether establishing new workflows, developing applications, or as part of ongoing improvement, recommendations provided by Trusted Advisor regularly help keep your solutions provisioned optimally. All AWS customers get access to the seven core Trusted Advisor checks to help increase the security and performance of the AWS environment. Trusted Advisor cannot be used to migrate to AWS and manage applications on AWS Cloud.

Concierge Support Team - The Concierge Support Team are AWS billing and account experts that specialize in working with enterprise accounts. They will quickly and efficiently assist you with your billing and account inquiries. The Concierge Support Team is only available for the Enterprise Support plan. Concierge Support Team cannot help in migrating to AWS and managing applications on AWS Cloud.

Reference:

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

Question 11: **Correct**

Which of the following AWS services support VPC Endpoint Gateway for a private connection from a VPC? (Select two)

-

S3

(Correct)

-

Amazon SQS

-

DynamoDB

(Correct)

-

Amazon SNS

-

Amazon EC2

Explanation

Correct option:

S3

DynamoDB

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. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network.

There are two types of VPC endpoints: interface endpoints and gateway endpoints.

An interface endpoint is an elastic network interface with a private IP address from the IP address range of your subnet that serves as an entry point for traffic destined to a supported service. Interface endpoints are powered by AWS PrivateLink, a technology that enables you to privately access services by using private IP addresses.

A gateway endpoint is a gateway that you specify as a target for a route in your route table for traffic destined to a supported AWS service. The following AWS services are supported:

Amazon S3

DynamoDB

Exam Alert:

You may see a question around this concept in the exam. Just remember that only S3 and DynamoDB support VPC Endpoint Gateway. All other services that support VPC Endpoints use a VPC Endpoint Interface.

Incorrect options:

Amazon EC2

Amazon SQS

Amazon SNS

As explained earlier, these services support VPC Endpoint Interfaces.

Reference:

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

Question 12: **Correct**

A company uses reserved EC2 instances across multiple units with each unit having its own AWS account. However, some of the units under-utilize their reserved instances while other units need more reserved instances. As a Cloud Practitioner, which of the following would you recommend as the most cost-optimal solution?

-

Use AWS Systems Manager to manage AWS accounts of all units and then share the reserved EC2 instances amongst all units

-

Use AWS Cost Explorer to manage AWS accounts of all units and then share the reserved EC2 instances amongst all units

-

Use AWS Trusted Advisor to manage AWS accounts of all units and then share the reserved EC2 instances amongst all units

-

Use AWS Organizations to manage AWS accounts of all units and then share the reserved EC2 instances amongst all units

(Correct)

Explanation

Correct option:

Use AWS Organizations to manage AWS accounts of all units and then share the reserved EC2 instances amongst all units

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

Key Features of AWS Organizations:

CENTRALLY MANAGE POLICIES ACROSS MULTIPLE AWS ACCOUNTS

To improve control over your AWS environment, you can use AWS Organizations to create groups of accounts, and then attach policies to a group to ensure the correct policies are applied across the accounts without requiring custom scripts and manual processes.

AUTOMATE AWS ACCOUNT CREATION AND MANAGEMENT

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. For example, you can automate the creation of new accounts for workload or application isolation and grant entities in those accounts access only to the necessary AWS services.

CONSOLIDATE BILLING ACROSS MULTIPLE AWS ACCOUNTS

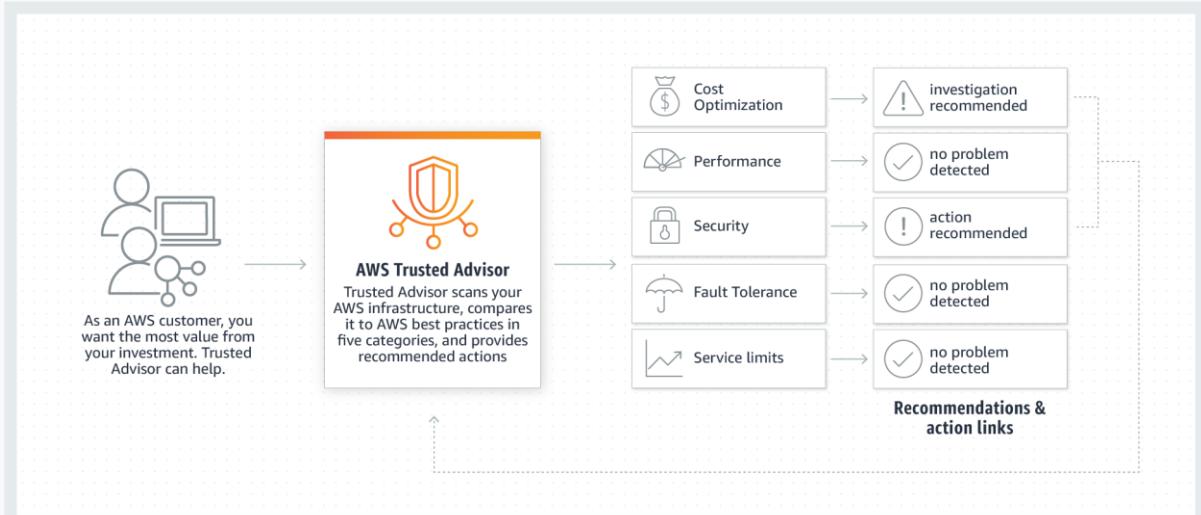
You can use AWS Organizations to set up a single payment method for all the AWS accounts in your organization through consolidated billing. With consolidated billing, you can see a combined view of charges incurred by all your accounts, as well as take advantage of pricing benefits from aggregated usage, such as volume discounts for [Amazon EC2](#) and [Amazon S3](#).

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

Incorrect options:

Use AWS Trusted Advisor to manage AWS accounts of all units and then share the reserved EC2 instances amongst all units - AWS Trusted Advisor is an online tool that provides you real-time guidance to help you provision your resources following AWS best practices on cost optimization, security, fault tolerance, service limits, and performance improvement. You cannot use Trusted Advisor to share the reserved EC2 instances amongst multiple AWS accounts.

How Trusted Advisor Works:



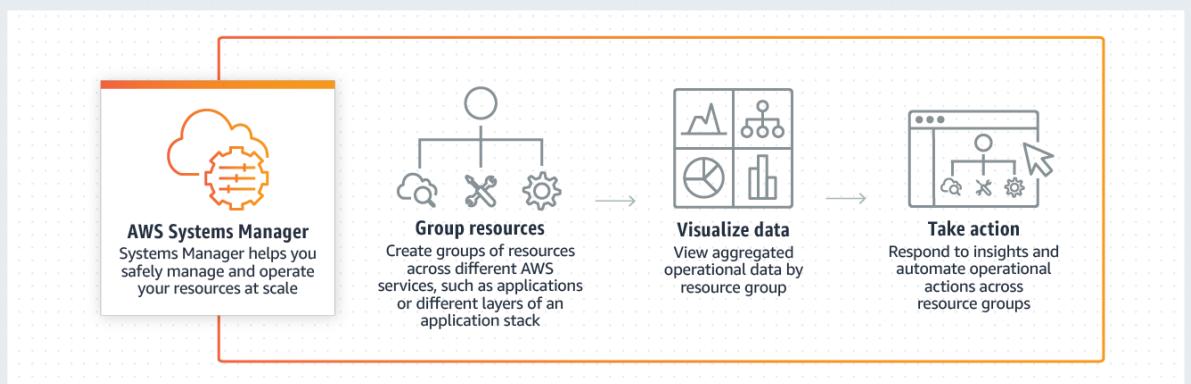
via - <https://aws.amazon.com/premiumsupport/technology/trusted-advisor/>

Use AWS Cost Explorer to manage AWS accounts of all units and then share the reserved EC2 instances amongst all units - 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). You cannot use Cost Explorer to share the reserved EC2 instances amongst multiple AWS accounts.

Use AWS Systems Manager to manage AWS accounts of all units and then share the reserved EC2 instances amongst all units - Systems Manager provides a unified user interface so you can view operational data from multiple AWS services and allows you to automate operational tasks across your AWS resources. With Systems Manager, you can group resources, like Amazon EC2 instances, Amazon S3 buckets, or Amazon RDS instances, by application, view operational data for monitoring and troubleshooting, and take action on your groups of resources. You cannot use Systems Manager to share the reserved EC2 instances amongst multiple AWS accounts.

How Systems Manager Works:



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

References:

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

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

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

Question 13: **Correct**

A Project Manager, working on AWS for the first time, is confused about how credits are used in AWS. There are two credits available in the manager's account. Credit one is for \$100, expires July 2022, and can be used for either Amazon S3 or Amazon EC2. Credit two is for \$50, expires December 2022, and can be used only for Amazon EC2. The manager's AWS account has incurred two charges: \$1000 for Amazon EC2 and \$500 for Amazon S3.

What will be the outcome on the overall bill once the credits are used? (Select two)

-

Then, credit two is applied to \$500 for Amazon S3 usage

-

Credit one is applied, which expires in July, to Amazon S3 usage which leaves you with a \$1000 Amazon EC2 charge and a \$400 Amazon S3 charge

-

Credit one is applied, which expires in July, to the Amazon EC2 charge which leaves you with a \$900 Amazon EC2 charge and a \$500 Amazon S3 charge

(Correct)

-

Only one credit can be used in one billing cycle and the customer has a choice to choose from the available ones

-

Then, credit two is applied to the remaining \$900 of Amazon EC2 usage

(Correct)

Explanation

Correct options:

Credit one is applied, which expires in July, to the Amazon EC2 charge which leaves you with a \$900 Amazon EC2 charge and a \$500 Amazon S3 charge

Then, credit two is applied to the remaining \$900 of Amazon EC2 usage

Credits are applied in the following order:

Soonest expiring

Least number of applicable products

Oldest credit

For the given use case, credit one is applied, which expires in July, to the Amazon EC2 charge which leaves you with a \$900 Amazon EC2 charge and a \$500 Amazon S3 charge. Then, credit two is applied to the remaining \$900 of Amazon EC2 usage. You need to pay \$850 for Amazon EC2 and \$500 for Amazon S3. All your credits are now exhausted.

Incorrect options:

Credit one is applied, which expires in July, to Amazon S3 usage which leaves you with a \$1000 Amazon EC2 charge and a \$400 Amazon S3 charge

Only one credit can be used in one billing cycle and the customer has a choice to choose from the available ones

Then, credit two is applied to \$500 for Amazon S3 usage

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

Reference:

<https://www.amazonaws.cn/en/support/faqs/>

Question 14: **Correct**

Which security service of AWS is enabled for all AWS customers, by default, at no additional cost?



AWS Shield Standard

(Correct)



AWS Secrets Manager



AWS Shield Advanced



AWS Web Application Firewall (AWS WAF)

Explanation

Correct option:

AWS Shield Standard

AWS Shield Standard defends against most common, frequently occurring network and transport layer DDoS attacks that target your website or applications. While AWS Shield Standard helps protect all AWS customers, you get better protection if you are using Amazon CloudFront and Amazon Route 53. All AWS customers benefit from the automatic protections of AWS Shield Standard, at no additional charge.

Incorrect options:

AWS Web Application Firewall (AWS WAF) - AWS WAF is a web application firewall that lets you monitor the HTTP(S) requests that are forwarded to an Amazon CloudFront distribution, an Amazon API Gateway API, or an Application Load Balancer. AWS WAF charges based on the number of web access control lists (web ACLs) that you create, the number of rules that you add per web ACL, and the number of web requests that you receive (it is not a free service).

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. With Secrets Manager, you pay based on the number of secrets stored and API calls made.

AWS Shield Advanced - AWS Shield Advanced includes intelligent DDoS attack detection and mitigation for not only for network layer (layer 3) and transport layer (layer 4) attacks but also for

application layer (layer 7) attacks. AWS Shield Advanced is a paid service that provides additional protections for internet-facing applications.

Reference: <https://docs.aws.amazon.com/waf/latest/developerguide/shield-chapter.html>

Question 15: **Correct**

A financial services company wants to ensure that its AWS account activity meets the governance, compliance and auditing norms. As a Cloud Practitioner, which AWS service would you recommend for this use-case?



Trusted Advisor



CloudTrail

(Correct)



Config



CloudWatch

Explanation

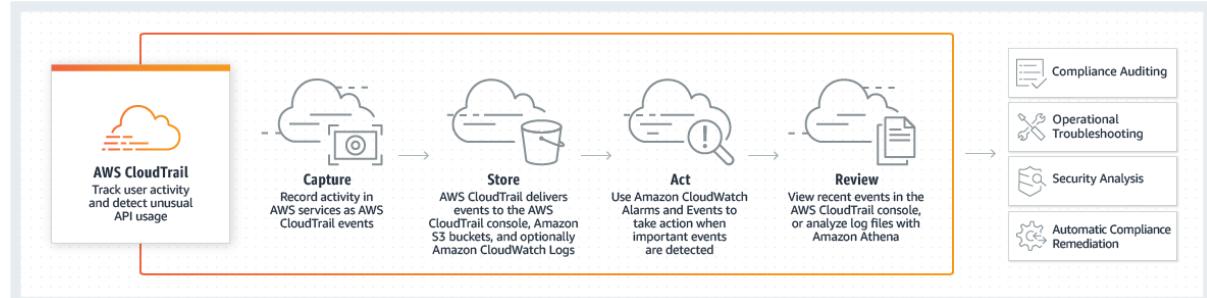
Correct option:

CloudTrail

You can use CloudTrail to log, monitor and retain account activity related to actions across your AWS infrastructure. CloudTrail provides an event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command-line tools, and other AWS services.

How CloudTrail

Works:



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

Incorrect options:

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.

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.

Trusted Advisor - AWS Trusted Advisor is an online tool that provides you real-time guidance to help you provision your resources following AWS best practices on cost optimization, security, fault tolerance, service limits and performance improvement.

Exam Alert:

You may see use-cases asking you to select one of CloudWatch vs CloudTrail vs Config. Just remember this thumb rule -

Think resource performance monitoring, events, and alerts; think CloudWatch.

Think account-specific activity and audit; think CloudTrail.

Think resource-specific change history, audit, and compliance; think Config.

Reference:

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

Question 16: **Incorrect**

Which of the following is an AWS database service?

-
-

Database Migration Service

(Incorrect)

-
-

Storage Gateway

-
-

Glue

-
-

Redshift

(Correct)

Explanation

Correct option:

Redshift - Amazon Redshift is a fully-managed petabyte-scale cloud-based data warehouse product designed for large scale data set storage and analysis.

Incorrect options:

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.

Storage Gateway - AWS Storage Gateway is a hybrid cloud storage service that connects your existing on-premises environments with the AWS Cloud. Customers use Storage Gateway to simplify storage management and reduce costs for key hybrid cloud storage use cases.

Database Migration Service - AWS Database Migration Service helps you migrate databases to AWS quickly and securely. The source database remains fully operational during the migration, minimizing downtime to applications that rely on the database. The AWS Database Migration Service can migrate your data to and from the most widely used commercial and open-source databases.

References:

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

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

Question 17: **Correct**

Which tool/service will help you access AWS services using programming language-specific APIs?

-

Language-specific Integrated Development Environments (IDE)

-

AWS Software Developer Kit (SDK)

(Correct)

-

AWS Management Console

-

AWS Command Line Interface (CLI)

Explanation

Correct option:

AWS Software Developer Kit (SDK) - SDKs take the complexity out of coding by providing language-specific APIs for AWS services. For example, the AWS SDK for JavaScript simplifies the use of

AWS Services by providing a set of libraries that are consistent and familiar for JavaScript developers. It provides support for API lifecycle considerations such as credential management, retries, data marshaling, serialization, and deserialization. AWS SDKs are offered in several programming languages to make it simple for developers working on different programming and scripting languages. So, AWS SDK can help with using AWS services from within an application using language-specific APIs.

Incorrect options:

AWS Management Console - The AWS Management Console is a web application that comprises and refers to a broad collection of service consoles for managing Amazon Web Services. When you first sign in, you see the console home page. The home page provides access to each service console as well as an intuitive user interface for exploring AWS and getting helpful tips.

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. CLI cannot be used with language-specific APIs.

Language-specific Integrated Development Environments (IDE) - An integrated development environment (IDE) provides a set of coding productivity tools such as a source code editor, a debugger, and build tools. Cloud9 IDE is an offering from AWS under IDEs.

References:

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

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

Question 18: **Correct**

A medical research startup wants to understand the compliance of AWS services concerning HIPAA guidelines. Which AWS service can be used to review the HIPAA compliance and governance-related documents on AWS?



AWS Artifact

(Correct)



AWS Trusted Advisor



AWS Systems Manager



AWS Secrets Manager

Explanation

Correct option:

AWS Artifact

AWS Artifact is your go-to, central resource for compliance-related information that matters to your organization. It provides on-demand access to AWS' security and compliance reports and select online agreements. Reports available in AWS Artifact include our Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, and certifications from accreditation bodies across geographies and compliance verticals that validate the implementation and operating effectiveness of AWS security controls. Different types of agreements are available in AWS Artifact Agreements to address the needs of customers subject to specific regulations. For example, the Business Associate Addendum (BAA) is available for customers that need to comply with the Health Insurance Portability and Accountability Act (HIPAA). It is not a service, it's a no-cost, self-service portal for on-demand access to AWS' compliance reports.

Incorrect options:

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

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

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

Reference:

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

Question 19: **Correct**

A web application stores all of its data on Amazon S3 buckets. A client has mandated that data be encrypted before sending it to Amazon S3.

Which of the following is the right technique for encrypting data as needed by the customer?

-

Encryption is enabled by default for all the objects written to Amazon S3. Additional configuration is not required

-

Enable client-side encryption using AWS encryption SDK

(Correct)

-

Enable server-side encryption with Amazon S3-Managed Keys (SSE-S3)

-

Enable server-side encryption with KMS keys stored in AWS Key Management Service (SSE-KMS)

Explanation

Correct option:

Enable client-side encryption using AWS encryption SDK

The act of encrypting data before sending it to Amazon S3 is termed as client-side encryption. The AWS encryption SDK is a client-side encryption library that is separate from the language-specific SDKs. You can use this encryption library to more easily implement encryption best practices in Amazon S3. Unlike the Amazon S3 encryption clients in the language-specific AWS SDKs, the AWS encryption SDK is not tied to Amazon S3 and can be used to encrypt or decrypt data to be stored anywhere.

Incorrect options:

Enable server-side encryption with Amazon S3-Managed Keys (SSE-S3) - When you use server-side encryption with Amazon S3-Managed Keys (SSE-S3), each object is encrypted with a unique key. As an additional safeguard, it encrypts the key itself with a root key that it regularly rotates.

Enable server-side encryption with KMS keys stored in AWS Key Management Service (SSE-KMS) - server-side encryption with AWS KMS keys (SSE-KMS) is similar to SSE-S3, but with some additional benefits and charges for using this service. There are separate permissions for the use of a KMS key that provides added protection against unauthorized access of your objects in Amazon S3. SSE-KMS also provides you with an audit trail that shows when your KMS key was used and by whom.

server-side encryption is the encryption of data at its destination by the application or service that receives it. Amazon S3 encrypts your data at the object level as it writes it to disks in its data centers and decrypts it for you when you access it. Hence, server-side encryption is not the right answer for the current scenario. So both these options are incorrect.

Encryption is enabled by default for all the objects written to Amazon S3. Additional configuration is not required - This statement is incorrect as encryption is not enabled by default on S3. You can protect data in transit using Secure Socket Layer/Transport Layer Security (SSL/TLS) or client-side encryption. Data at rest on Amazon S3 can be encrypted using server-side encryption or client-side encryption.

References:

https://docs.aws.amazon.com/en_us/AmazonS3/latest/userguide/UsingClientSideEncryption.html

https://docs.aws.amazon.com/en_us/AmazonS3/latest/userguide/serv-side-encryption.html

Question 20: **Correct**

Which of the following S3 storage classes takes the most time to retrieve data (also known as first byte latency)?



S3 Glacier



S3 Intelligent-Tiering



S3 Standard



S3 Glacier Deep Archive

(Correct)

Explanation

Correct option:

"S3 Glacier Deep Archive" - S3 Glacier Deep Archive is Amazon S3's lowest-cost storage class and supports long-term retention and digital preservation for data that may be accessed once or twice in a year. It is designed for customers — particularly those in highly-regulated industries, such as the Financial Services, Healthcare, and Public Sectors — that retain data sets for 7-10 years or longer to meet regulatory compliance requirements. S3 Glacier Deep Archive can also be used for backup and disaster recovery use cases. It has a retrieval time (first byte latency) of 12 to 48 hours.

Please review this illustration for S3 Storage Classes data retrieval times. You don't need to memorize the actual numbers, just remember that S3 Glacier Deep Archive takes the most time to retrieve data:

Performance across the S3 Storage Classes

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

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

Incorrect options:

S3 Standard - S3 Standard offers high durability, availability, and performance object storage for frequently accessed data. S3 Standard has a retrieval time (first byte latency) of milliseconds.

S3 Intelligent-Tiering - The S3 Intelligent-Tiering storage class is designed to optimize costs by automatically moving data to the most cost-effective access tier, without performance impact or operational overhead. It works by storing objects in two access tiers: one tier that is optimized for frequent access and another lower-cost tier that is optimized for infrequent access. S3 Intelligent-Tiering has a retrieval time (first byte latency) of milliseconds.

S3 Glacier - Amazon S3 Glacier is a secure, durable, and extremely low-cost Amazon S3 cloud storage class for data archiving and long-term backup. It is designed to deliver 99.999999999% durability, and provide comprehensive security and compliance capabilities that can help meet even the most stringent regulatory requirements. S3 Glacier has a retrieval time (first byte latency) of minutes or a few hours.

Reference:

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

Question 21: **Correct**

An IT company is planning to migrate from an on-premises environment to AWS Cloud. Which of the following expense areas would result in cost savings when the company moves to AWS Cloud? (Select two)

-

Computing hardware infrastructure expenditure

(Correct)

- - Project manager salary**
 -
 - SaaS application license fee**
 -
 - Developer salary**
 -
 - Data center physical security expenditure**
- (Correct)**

Explanation

Correct option:

Data center hardware infrastructure expenditure

Data center physical security expenditure

The company does not need to spend on the computing hardware infrastructure and data center physical security. So these expense areas would result in cost savings. The expenditure on the SaaS application license fee, developer salary, and project manager salary would remain the same.

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:

SaaS application license fee

Developer salary

Project manager salary

As explained earlier, the expenditure on the SaaS application license fee, developer salary, and project manager salary would remain the same, so these options are incorrect.

Reference:

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

Question 22: **Incorrect**

An e-commerce company has deployed an RDS database in a single Availability Zone. The engineering team wants to ensure that in case of an AZ outage, the database should continue working on the same endpoint without any manual administrative intervention. Which of the following solutions can address this use-case?

-

Configure the database in RDS Multi-AZ deployment with automatic failover to the standby

(Correct)

-

Configure the database in RDS read replica mode with automatic failover to the standby

(Incorrect)

-

Deploy the database via Elastic Beanstalk

-

Provision the database via CloudFormation

Explanation

Correct option:

Configure the database in RDS Multi-AZ deployment with automatic failover to the standby

When you provision a Multi-AZ DB Instance, Amazon RDS automatically creates a primary DB Instance and synchronously replicates the data to a standby instance in a different Availability Zone (AZ). In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby (or to a read replica in the case of Amazon Aurora), so that you can resume database operations as soon as

the failover is complete. Since the endpoint for your DB Instance remains the same after a failover, your application can resume database operation without the need for manual administrative intervention.

Incorrect options:

Deploy the database via Elastic Beanstalk - You cannot deploy only a database via Elastic Beanstalk as it's meant for automatic application deployment when you upload your code. Then Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring. Hence this option is incorrect.

Configure the database in RDS read replica mode with automatic failover to the standby - For RDS, Read replicas allow you to create read-only copies that are synchronized with your master database. There is no standby available while using read replicas. In case of infrastructure failure, you have to manually promote the read replica to be its own standalone DB Instance, which means that the database endpoint would change. Therefore, this option is incorrect.

Provision the database via CloudFormation - You can provision the database via CloudFront for sure, however, it does not provide any automatic recovery in case of a disaster.

References:

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

Question 23: **Correct**

Which AWS Service can be used to mitigate a Distributed Denial of Service (DDoS) attack?

-

AWS Shield

(Correct)

-

Amazon CloudWatch

-

AWS KMS

-

AWS Systems Manager

Explanation

Correct option:

AWS Shield

AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS. AWS Shield provides always-on detection and automatic inline

mitigations that minimize application downtime and latency, so there is no need to engage AWS Support to benefit from DDoS protection. There are two tiers of AWS Shield - Standard and Advanced.

All AWS customers benefit from the automatic protections of AWS Shield Standard, at no additional charge. AWS Shield Standard defends against most common, frequently occurring network and transport layer DDoS attacks that target your web site or applications. When you use AWS Shield Standard with Amazon CloudFront and Amazon Route 53, you receive comprehensive availability protection against all known infrastructure (Layer 3 and 4) attacks.

For higher levels of protection against attacks targeting your applications running on Amazon Elastic Compute Cloud (EC2), Elastic Load Balancing (ELB), Amazon CloudFront, AWS Global Accelerator and Amazon Route 53 resources, you can subscribe to AWS Shield Advanced. In addition to the network and transport layer protections that come with Standard, AWS Shield Advanced provides additional detection and mitigation against large and sophisticated DDoS attacks, near real-time visibility into attacks, and integration with AWS WAF, a web application firewall.

Incorrect options:

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

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

AWS KMS - AWS Key Management Service (KMS) makes it easy for you to create and manage cryptographic keys and control their use across a wide range of AWS services and in your applications. AWS KMS is a secure and resilient service that uses hardware security modules that have been validated under FIPS 140-2, or are in the process of being validated, to protect your keys.

Reference:

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

Question 24: **Correct**

Which of the following AWS services has encryption enabled by default?

-
-

Amazon S3

-
-

Elastic Block Storage (EBS)



Elastic File Storage (EFS)



CloudTrail Logs

(Correct)

Explanation

Correct option:

CloudTrail Logs

AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. CloudTrail can be used to record AWS API calls and other activity for your AWS account and save the recorded information to log files in an Amazon Simple Storage Service (Amazon S3) bucket that you choose. By default, the log files delivered by CloudTrail to your S3 bucket are encrypted using server-side encryption with Amazon S3-managed encryption keys (SSE-S3).

Incorrect options:

Elastic File Storage (EFS) - Amazon Elastic File System (Amazon EFS) provides a simple, scalable, fully managed elastic NFS file system for use with AWS Cloud services and on-premises resources. Amazon EFS supports two forms of encryption for file systems, encryption of data in transit and encryption at rest. This is an optional feature and has to be enabled by user if needed.

Elastic Block Storage (EBS) - Amazon Elastic Block Store (EBS) is an easy to use, high-performance block storage service designed for use with Amazon Elastic Compute Cloud (EC2) instances for both throughput and transaction-intensive workloads at any scale. Encryption (at rest and during transit) is an optional feature for EBS and has to be enabled by the user.

Amazon S3 - Amazon Simple Storage Service is storage for the Internet. To upload data into S3 you need to create an S3 bucket in one of the AWS Regions. Amazon S3 default encryption provides a way to set the default encryption behavior for an S3 bucket. Encryption for an S3 bucket is an additional feature and the user needs to enable it.

Reference: <https://docs.aws.amazon.com/awscloudtrail/latest/userguide/encrypting-cloudtrail-log-files-with-aws-kms.html>

Question 25: **Correct**

A big data analytics company is moving its IT infrastructure from an on-premises data center to AWS Cloud. The company has some server-bound software licenses that it wants to use on AWS. As a Cloud Practitioner, which of the following EC2 instance types would you recommend to the company?



Dedicated Host

(Correct)

-

On-Demand Instance

-

Reserved Instance

-

Dedicated Instance

Explanation

Correct option:

Dedicated host

Amazon EC2 Dedicated Hosts allow you to use your eligible software licenses from vendors such as Microsoft and Oracle on Amazon EC2. An Amazon EC2 Dedicated Host is a physical server fully dedicated for your use, so you can help address corporate compliance requirements.

Exam Alert:

Please review the differences between Dedicated hosts and Dedicated instances:

Differences between Dedicated Hosts and Dedicated Instances

Dedicated Hosts and Dedicated Instances can both be used to launch Amazon EC2 instances onto physical servers that are dedicated for your use.

There are no performance, security, or physical differences between Dedicated Instances and instances on Dedicated Hosts. However, there are some differences between the two. The following table highlights some of the key differences between Dedicated Hosts and Dedicated Instances:

	Dedicated Host	Dedicated Instance
Billing	Per-host billing	Per-instance billing
Visibility of sockets, cores, and host ID	Provides visibility of the number of sockets and physical cores	No visibility
Host and instance affinity	Allows you to consistently deploy your instances to the same physical server over time	Not supported
Targeted instance placement	Provides additional visibility and control over how instances are placed on a physical server	Not supported
Automatic instance recovery	Supported. For more information, see Host recovery .	Supported
Bring Your Own License (BYOL)	Supported	Not supported

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

Incorrect options:

Dedicated instance - Dedicated Instances are Amazon EC2 instances that run in a virtual private cloud (VPC) on hardware that's dedicated to a single customer. Dedicated Instances that belong to different AWS accounts are physically isolated at the hardware level. However, Dedicated Instances may share hardware with other instances from the same AWS account that are not Dedicated Instances. You cannot use Dedicated Instances for using server-bound software licenses.

Reserved Instance - Reserved Instances provide you with significant savings (up to 75%) on your Amazon EC2 costs compared to On-Demand Instance pricing. Reserved Instances are not physical instances, but rather a billing discount applied to the use of On-Demand Instances in your account. You can purchase a Reserved Instance for a one-year or three-year commitment, with the three-year commitment offering a bigger discount. You cannot use Reserved Instances for using server-bound software licenses.

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

Reference:

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

Question 26: **Correct**

Which AWS Support plan provides architectural guidance contextual to your specific use-cases?



Enterprise



Developer



Basic



Business

(Correct)

Explanation

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. You also get access to Infrastructure Event Management for an additional fee.

Incorrect options:

Developer - AWS recommends Developer Support if you are testing or doing early development on AWS and want the ability to get email-based technical support during business hours as well as general architectural guidance as you build and test. You do not get access to Infrastructure Event Management with this plan. This plan only supports general architectural guidance.

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

Customer Service & Communities - 24x7 access to customer service, documentation, whitepapers, and support forums. AWS Trusted Advisor - Access to the 7 core Trusted Advisor checks and guidance to

provision your resources following best practices to increase performance and improve security. AWS Personal Health Dashboard - A personalized view of the health of AWS services, and alerts when your resources are impacted. This plan does not support any architectural guidance.

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 review and guidance based on your applications, and a designated Technical Account Manager (TAM) to coordinate access to proactive/preventative programs and AWS subject matter experts. This plan supports architectural guidance contextual to your application.

Reference:

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

Question 27: **Correct**

Which of the following are the storage services offered by the AWS Cloud? (Select two)

-

S3

(Correct)

-

SQS

-

EFS

(Correct)

-

EC2

-

SNS

Explanation

Correct options:

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

EFS - Amazon Elastic File System (Amazon EFS) provides a simple, scalable, fully managed elastic NFS file system for use with AWS Cloud services and on-premises resources. It is built to scale on-demand

to petabytes without disrupting applications, growing and shrinking automatically as you add and remove files, eliminating the need to provision and manage capacity to accommodate growth.

Incorrect options:

EC2 - Amazon EC2 is a web service that provides secure, resizable compute capacity in the AWS cloud. You can use EC2 to provision virtual servers on AWS Cloud.

SQS - Amazon Simple Queue Service (SQS) is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. 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.

SNS - Amazon Simple Notification Service (SNS) is a highly available, durable, secure, fully managed pub/sub messaging service that enables you to decouple microservices, distributed systems, and serverless applications. Using Amazon SNS topics, your publisher systems can fan-out messages to a large number of subscriber endpoints for parallel processing, including Amazon SQS queues, AWS Lambda functions, and HTTP/S webhooks. Additionally, SNS can be used to fan out notifications to end users using mobile push, SMS, and email.

Reference:

Question 28: **Correct**

A research group wants to use EC2 instances to run a scientific computation application that has a fault tolerant architecture. The application needs high-performance hardware disks that provide fast I/O performance. As a Cloud Practitioner, which of the following storage options would you recommend as the MOST cost-effective solution?

-
-

Instance Store

(Correct)

-
-

EBS

-
-

S3

-
-

EFS

Explanation

Correct option:

Instance Store

An instance store provides temporary block-level storage for your instance. This storage is located on disks that are physically attached to the host computer. This is a good option when you need storage with very low latency, but you don't need the data to persist when the instance terminates or you can take advantage of fault-tolerant architectures. For this use-case, the computation application itself has a fault tolerant architecture, so it can automatically handle any failures of Instance Store volumes.

As the Instance Store volumes are included as part of the instance's usage cost, therefore this is the correct option.

EC2 Instances Store

Overview:

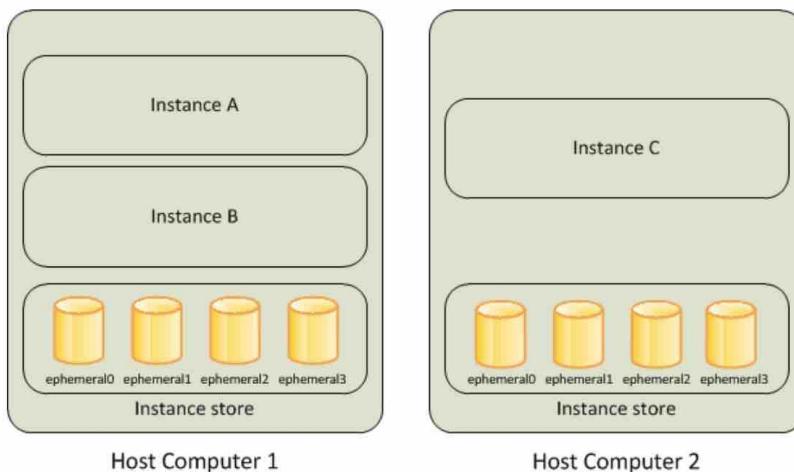
Amazon EC2 Instance Store

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

An *instance store* provides temporary block-level storage for your instance. This storage is located on disks that are physically attached to the host computer. Instance store is ideal for temporary storage of information that changes frequently, such as buffers, caches, scratch data, and other temporary content, or for data that is replicated across a fleet of instances, such as a load-balanced pool of web servers.

An instance store consists of one or more instance store volumes exposed as block devices. The size of an instance store as well as the number of devices available varies by instance type.

The virtual devices for instance store volumes are ephemeral [0-23]. Instance types that support one instance store volume have ephemeral0. Instance types that support two instance store volumes have ephemeral0 and ephemeral1, and so on.



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

Incorrect options:

EFS - Amazon Elastic File System (Amazon EFS) provides a simple, scalable, fully managed, elastic NFS file system. EFS is not available as a hardware disk on the instance, so this option is not correct.

EBS - Amazon Elastic Block Store (EBS) is an easy to use, high-performance block storage service designed for use with Amazon Elastic Compute Cloud (EC2) for both throughput and transaction-intensive workloads at any scale. EBS is not available as a hardware disk on the instance, so this option is not correct.

S3 - Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. S3 is not available as a hardware disk on the instance, so this option is not correct.

Reference:

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

Question 29: **Correct**

Which of the following AWS Support plans provide access to guidance, configuration, and troubleshooting of AWS interoperability with third-party software? (Select two)

-
- **Corporate**
-
- **Developer**
-
- **Business**
- **(Correct)**
-
- **Basic**
-
- **Enterprise**
- **(Correct)**

Explanation

Correct options:

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. You get access to guidance, configuration, and troubleshooting of AWS interoperability with many common operating systems, platforms, and application stack components.

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. You get

access to guidance, configuration, and troubleshooting of AWS interoperability with many common operating systems, platforms, and application stack components.

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	General guidance: < 24 hours System impaired: < 12 hours Production system impaired: < 4 hours Production system down: < 1 hour Business-critical system down: < 15 minutes
Architectural Guidance	General	Contextual to your use-cases	Consultative review and guidance based on your applications
Programmatic Case Management		AWS Support API	AWS Support API
Third-Party Software Support		Interoperability & configuration guidance and troubleshooting	Interoperability & configuration guidance and troubleshooting

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

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

Incorrect options:

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

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

Developer - AWS recommends Developer Support plan if you are testing or doing early development on AWS and want the ability to get email-based technical support during business hours. This plan also supports general guidance on how services can be used for various use cases, workloads, or applications. You do not get access to Infrastructure Event Management with this plan.

Both these plans do not support access to guidance, configuration, and troubleshooting of AWS interoperability with third-party software.

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

Reference:

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

Question 30: **Correct**

The DevOps team at an e-commerce company is trying to debug performance issues for its serverless application built using a microservices architecture. As a Cloud Practitioner, which AWS service would you recommend addressing this use-case?



AWS CloudFormation



Amazon Pinpoint



AWS Trusted Advisor



AWS X-Ray

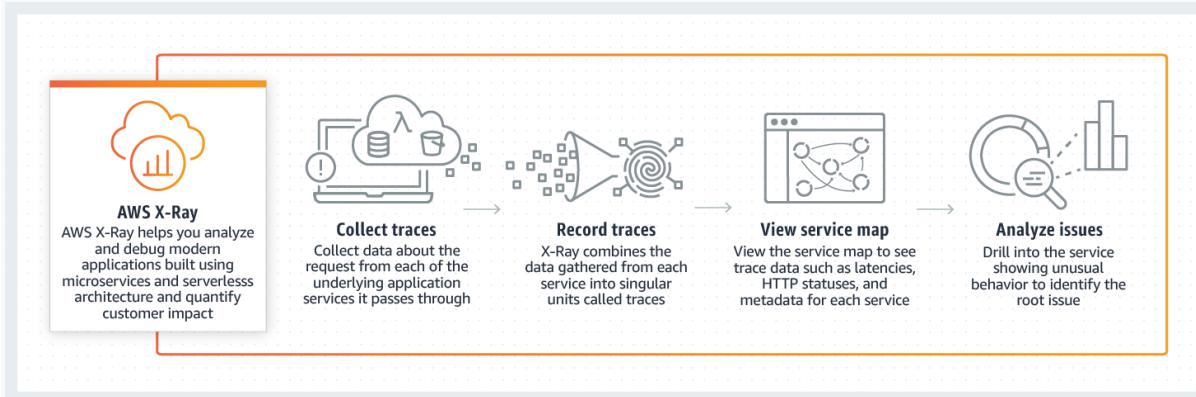
(Correct)

Explanation

Correct option:

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

How X-Ray Works:



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

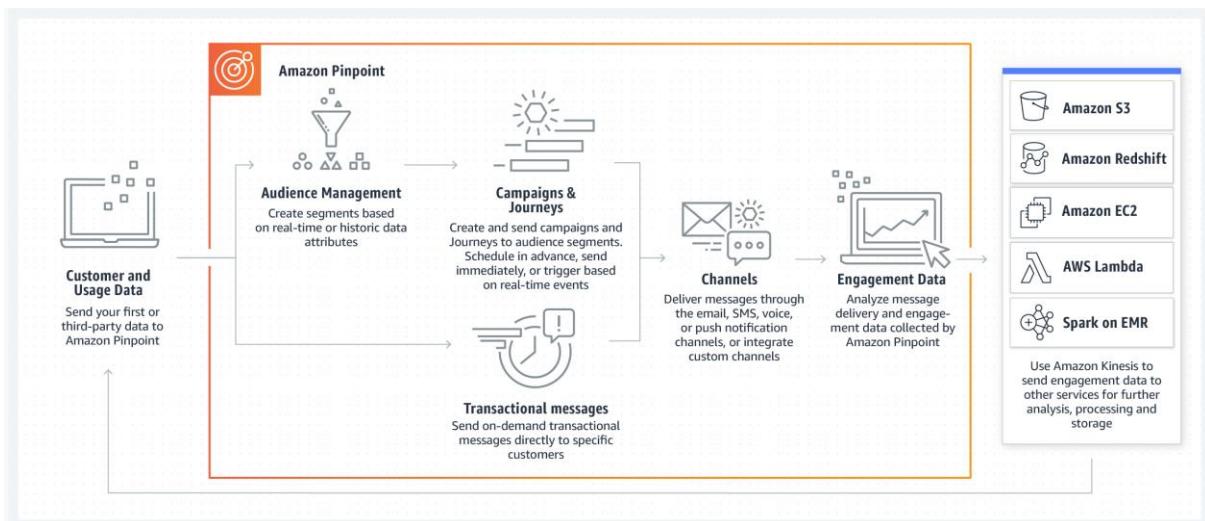
Incorrect options:

AWS Trusted Advisor - AWS Trusted Advisor is an online tool that provides you real-time guidance to help you provision your resources following AWS best practices on cost optimization, security, fault tolerance, service limits and performance improvement. Whether establishing new workflows, developing applications, or as part of ongoing improvement, recommendations provided by Trusted Advisor regularly help keep your solutions provisioned optimally. Trusted Advisor cannot be used to debug performance issues for this serverless application built using a microservices architecture.

Amazon Pinpoint - Amazon Pinpoint allows marketers and developers to deliver customer-centric engagement experiences by capturing customer usage data to draw real-time insights. Pinpoint cannot be used to debug performance issues for this serverless application built using a microservices architecture.

AWS CloudFormation - AWS CloudFormation allows you to use programming languages or a simple text file to model and provision, in an automated and secure manner, all the resources needed for your applications across all Regions and accounts. Think infrastructure as code; think CloudFormation. CloudFormation cannot be used to debug performance issues for this serverless application built using a microservices architecture.

How Amazon Pinpoint Works:



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

Reference:

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

Question 31: **Correct**

AWS Web Application Firewall (WAF) offers protection from common web exploits at which layer?

-

Layer 7

(Correct)

-

Layer 4 and 7

-

Layer 3

-

Layer 4

Explanation

Correct option:

Layer 7

AWS WAF is a web application firewall that lets you monitor the HTTP and HTTPS requests that are forwarded to an Amazon API Gateway API, Amazon CloudFront or an Application Load Balancer. HTTP and HTTPS requests are part of the Application layer, which is layer 7.

Incorrect options:

Layer 3 - Layer 3 is the Network layer and this layer decides which physical path data will take when it moves on the network. AWS Shield offers protection at this layer. WAF does not offer protection at this layer.

Layer 4 - Layer 4 is the Transport layer and this layer data transmission occurs using TCP or UDP protocols. AWS Shield offers protection at this layer. WAF does not offer protection at this layer.

Layer 4 and 7 - This option has been added as a distractor.

Reference: <https://docs.aws.amazon.com/waf/latest/developerguide/what-is-aws-waf.html>

Question 32: **Incorrect**

A company wants to identify the optimal AWS resource configuration for its workloads so that the company can reduce costs and increase workload performance. Which of the following services can be used to meet this requirement?

-

AWS Cost Explorer

(Incorrect)

-

AWS Compute Optimizer

(Correct)

-

AWS Budgets

-

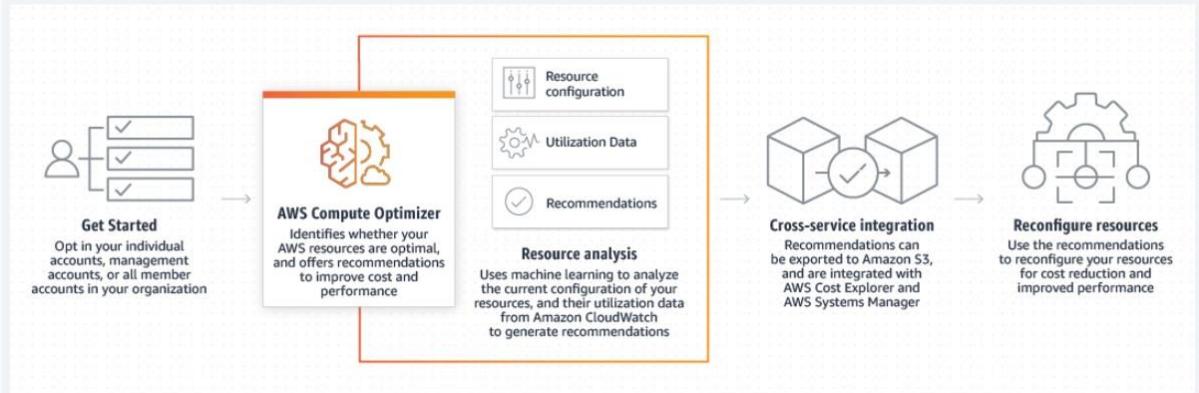
AWS Systems Manager

Explanation

Correct option: **AWS Compute Optimizer** - AWS Compute Optimizer recommends optimal AWS resources for your workloads to reduce costs and improve performance by using machine learning to analyze historical utilization metrics. Over-provisioning resources can lead to unnecessary infrastructure costs, and under-provisioning resources can lead to poor application performance. Compute Optimizer helps you choose optimal configurations for three types of AWS resources: Amazon EC2 instances, Amazon EBS volumes, and AWS Lambda functions, based on your utilization data.

Compute Optimizer recommends up to 3 options from 140+ EC2 instance types, as well as a wide range of EBS volume and Lambda function configuration options, to right-size your workloads. Compute Optimizer also projects what the CPU utilization, memory utilization, and run time of your workload would have been on recommended AWS resource options. This helps you understand how your workload would have performed on the recommended options before implementing the recommendations.

How Compute Optimizer works:



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

Incorrect options:

AWS Systems Manager - AWS Systems Manager is the operations hub for AWS. Systems Manager provides a unified user interface so you can track and resolve operational issues across your AWS applications and resources from a central place. With Systems Manager, you can automate operational tasks for Amazon EC2 instances or Amazon RDS instances. You can also group resources by application, view operational data for monitoring and troubleshooting, implement pre-approved change workflows, and audit operational changes for your groups of resources. Systems Manager simplifies resource and application management, shortens the time to detect and resolve operational problems, and makes it easier to operate and manage your infrastructure at scale. Systems Manager cannot be used to identify the optimal resource configuration for workloads running on AWS.

AWS Budgets - AWS Budgets allows you to set custom budgets to track your cost and usage from the simplest to the most complex use cases. With AWS Budgets, you can choose to be alerted by email or SNS notification when actual or forecasted cost and usage exceed your budget threshold, or when your actual RI and Savings Plans' utilization or coverage drops below your desired threshold. With AWS Budget Actions, you can also configure specific actions to respond to cost and usage status in your accounts, so that if your cost or usage exceeds or is forecasted to exceed your threshold, actions can be executed automatically or with your approval to reduce unintentional over-spending.

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. Cost Explorer Resource Rightsizing Recommendations and Compute Optimizer use the same recommendation engine. The Compute Optimizer recommendation engine delivers recommendations to help customers identify optimal EC2 instance types for their workloads. The Cost Explorer console and API surface a subset of these recommendations that may lead to cost savings, and augments them with customer-specific cost and savings information (e.g. billing information, available credits, RI, and Savings Plans) to help Cost Management owners quickly identify savings opportunities through infrastructure rightsizing. Compute Optimizer console and its API delivers all recommendations regardless of the cost implications.

Reference:

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

Question 33: **Correct**

Which of the following AWS Support plans provide access to only 7 core checks from the AWS Trusted Advisor Best Practice Checks? (Select two)

-

Basic

(Correct)

-

Corporate

-

Business

-

Enterprise

-

Developer

(Correct)

Explanation

Correct option:

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

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

Developer - AWS recommends Developer Support if you are testing or doing early development on AWS and want the ability to get email-based technical support during business hours as well as general architectural guidance as you build and test. This plan provides access to just the 7 core Trusted Advisor checks.

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**	General guidance: < 24 hours	General guidance: < 24 hours System impaired: < 12 hours
	System impaired: < 12 business hours**	Production system impaired: < 4 hours	Production system impaired: < 4 hours Production system down: < 1 hour
		Production system down: < 1 hour	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:

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 also get full access to AWS Trusted Advisor Best Practice Checks.

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 and a designated Technical Account Manager (TAM) to coordinate access to proactive/preventative programs and AWS subject matter experts. You also get full access to AWS Trusted Advisor Best Practice Checks.

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

Reference:

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

Question 34: **Correct**

A silicon valley based healthcare startup stores anonymized patient health data on Amazon S3. The CTO further wants to ensure that any sensitive data on S3 is discovered and identified to prevent any sensitive data leaks. As a Cloud Practitioner, which AWS service would you recommend addressing this use-case?



Amazon Macie

(Correct)



Amazon Polly



AWS Secrets Manager



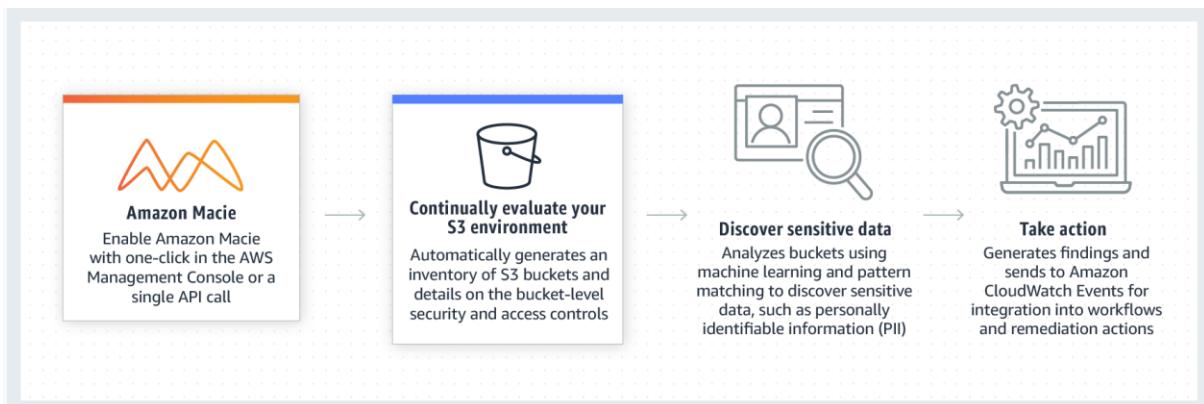
AWS Glue

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. Macie automatically provides an inventory of Amazon S3 buckets including a list of unencrypted buckets, publicly accessible buckets, and buckets shared with AWS accounts outside those you have defined in AWS Organizations. Then, Macie applies machine learning and pattern matching techniques to the buckets you select to identify and alert you to sensitive data, such as personally identifiable information (PII).

How Macie
Works:



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

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. It cannot be used to discover and protect your sensitive data in AWS.

Amazon Polly - Amazon Polly is a service that turns text into lifelike speech, allowing you to create applications that talk, and build entirely new categories of speech-enabled products. Polly's Text-to-Speech (TTS) service uses advanced deep learning technologies to synthesize natural sounding human speech. It cannot be used to discover and protect your 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. Users and applications retrieve secrets with a call to Secrets Manager APIs, eliminating the need to hardcode sensitive information in plain text. It cannot be used to discover and protect your sensitive data in AWS.

Reference:

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

Question 35: **Correct**

Which of the following is CORRECT regarding removing an AWS account from AWS Organizations?

- **The AWS account can be removed from AWS Systems Manager**
 - **The AWS account must be able to operate as a standalone account. Only then it can be removed from AWS organizations**
- (Correct)**
-

The AWS account must not have any Service Control Policies (SCPs) attached to it. Only then it can be removed from AWS organizations

-

Raise a support ticket with AWS Support to remove the account

Explanation

Correct option:

The AWS account must be able to operate as a standalone account. Only then it can be removed from AWS organizations

You can remove an account from your organization only if the account has the information that is required for it to operate as a standalone account. For each account that you want to make standalone, you must accept the AWS Customer Agreement, choose a support plan, provide and verify the required contact information, and provide a current payment method. AWS uses the payment method to charge for any billable (not AWS Free Tier) AWS activity that occurs while the account isn't attached to an organization.

Incorrect options:

Raise a support ticket with AWS Support to remove the account - AWS Support does not need to help you in removing an AWS account from AWS Organizations.

The AWS account can be removed from AWS Systems Manager - AWS Systems Manager gives you visibility and control of your infrastructure on AWS. Systems Manager provides a unified user interface so you can view operational data from multiple AWS services and allows you to automate operational tasks such as running commands, managing patches, and configuring servers across AWS Cloud as well as on-premises infrastructure. Systems Manager cannot be used to remove an AWS account from AWS Organizations.

The AWS account must not have any Service Control Policies (SCPs) attached to it. Only then it can be removed from AWS organizations - This is not a pre-requisite to remove the AWS account. The principals in the AWS account are no longer affected by any service control policies (SCPs) that were defined in the organization. This means that restrictions imposed by those SCPs are gone, and the users and roles in the account might have more permissions than they had before.

Reference:

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_accounts_remove.html

Question 36: **Correct**

A data analytics company is running a proprietary batch analytics application on AWS and wants to use a storage service which would be accessed by hundreds of EC2 instances simultaneously to append data to existing files. As a Cloud Practitioner, which AWS service would you suggest for this use-case?

-

EFS

(Correct)



S3



Instance Store



EBS

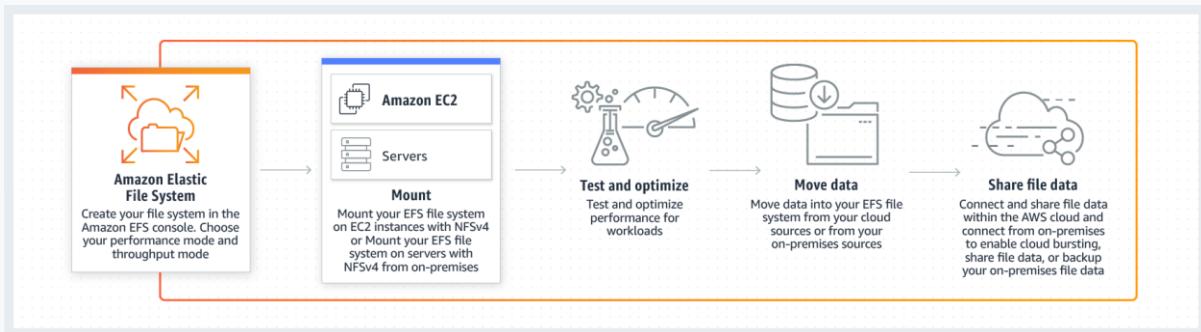
Explanation

Correct option:

"EFS" - Amazon EFS is a file storage service for use with Amazon EC2. Amazon EFS provides a file system interface, file system access semantics, and concurrently-accessible storage for up to thousands of Amazon EC2 instances. Amazon EFS uses the Network File System protocol.

How EFS

works:



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

Incorrect options:

EBS - Amazon Elastic Block Store (EBS) is an easy to use, high-performance block storage service designed for use with Amazon Elastic Compute Cloud (EC2) for both throughput and transaction-intensive workloads at any scale. EBS volumes cannot be accessed simultaneously by multiple EC2 instances, so this option is incorrect.

Instance Store - An instance store provides temporary block-level storage for your instance. This storage is located on disks that are physically attached to the host computer. Instance Store volumes cannot be accessed simultaneously by multiple EC2 instances, so this option is incorrect.

S3 - Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. S3 is object storage and it does not support file append operations, so this option is incorrect.

Reference:

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

Question 37: **Correct**

Which of the following is an INCORRECT statement about Scaling, a design principle of Reliability pillar of the AWS Well-Architected Framework.

-
- Vertical Scaling implies you scale by adding more power (CPU, RAM) to your existing machine/node**
-
- Fault tolerance is achieved by Horizontal scaling**
-
- Horizontal Scaling implies you scale by adding more instances to your existing pool of resources**
-
- Fault tolerance is achieved by Vertical Scaling**

(Correct)

Explanation

Correct option:

Fault tolerance is achieved by Vertical Scaling

A "vertically scalable" system, is constrained to be 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. Fault tolerance is not possible on vertically scalable systems since a single instance is prone to failure.

Incorrect options:

Vertical Scaling implies you scale by adding more power (CPU, RAM) to your existing machine/node - A "vertically scalable" system runs on a single instance. Adding power is only possible through the addition of resources in the form of CPU, RAM, or storage to enhance performance.

Horizontal Scaling implies you scale by adding more instances to your existing pool of resources - A "horizontally scalable" system is one that can increase capacity by adding more computers to the system. Horizontally scalable systems are oftentimes able to outperform vertically scalable systems by enabling parallel execution of workloads and distributing those across many different computers.

Fault tolerance is achieved by Horizontal scaling - Horizontal scaling adds more instances to its existing pool to scale. This implies, there is no single point of failure. If an instance is down, the workload is taken up by other healthy instances. Distributed systems are an example of horizontal scaling.

Reference:

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

Question 38: **Correct**

The DevOps team at an IT company is moving 500 GB of data from an EC2 instance to an S3 bucket in the same region. Which of the following scenario captures the correct charges for this data transfer?



The company would only be charged for the inbound data transfer into the S3 bucket



The company would only be charged for the outbound data transfer from EC2 instance



The company would be charged for both the outbound data transfer from EC2 instance as well as the inbound data transfer into the S3 bucket



The company would not be charged for this data transfer

(Correct)

Explanation

Correct option:

The company would not be charged for this data transfer

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

Per AWS pricing, data transfer between S3 and EC2 instances within the same region is not charged, so there would be no data transfer charge for moving 500 GB of data from an EC2 instance to an S3 bucket in the same region.

Incorrect options:

The company would only be charged for the outbound data transfer from EC2 instance

The company would only be charged for the inbound data transfer into the S3 bucket

The company would be charged for both the outbound data transfer from EC2 instance as well as the inbound data transfer into the S3 bucket

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

Reference:

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

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

Question 39: **Correct**

A company wants to have control over creating and using its own keys for encryption on AWS services. Which of the following can be used for this use-case?

-
- **Secrets Manager**
-
- **AWS Owned CMK**
-
- **AWS Managed CMK**
-
- **Customer Managed CMK**

(Correct)

Explanation

Correct option:

Customer Managed CMK

A customer master key (CMK) is a logical representation of a master key. The CMK includes metadata, such as the key ID, creation date, description, and key state. The CMK also contains the key material used to encrypt and decrypt data. These are created and managed by the AWS customer. Access to these can be controlled using the AWS IAM service.

Incorrect options:

Secrets Manager - AWS Secrets Manager helps you protect secrets needed to access your applications, services, and IT resources. The service enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle. You cannot use Secrets Manager for creating and using your own keys for encryption on AWS services.

AWS Managed CMK - AWS managed CMKs are CMKs in your account that are created, managed, and used on your behalf by an AWS service that is integrated with AWS KMS.

AWS Owned CMK - AWS owned CMKs are a collection of CMKs that an AWS service owns and manages for use in multiple AWS accounts. AWS owned CMKs are not in your AWS account. You cannot view or manage these CMKs.

Reference:

https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#master_keys

Question 40: **Correct**

Which of the following AWS Support plans provides access to online training with self-paced labs?



Enterprise

(Correct)



Basic



Developer



Business

Explanation

Correct option:

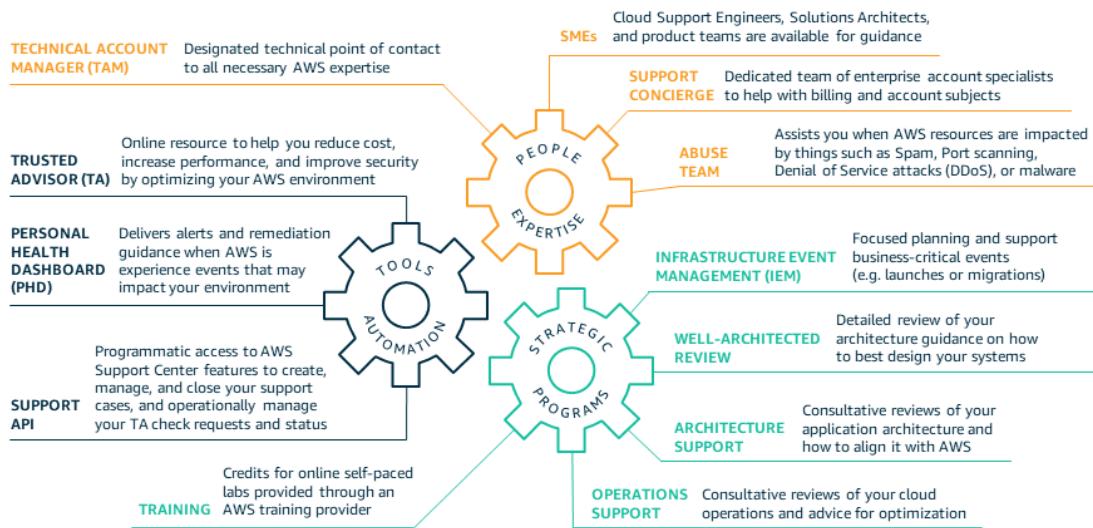
Enterprise

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.

AWS Enterprise Support Plan

Offerings:



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

Incorrect options:

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

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

Basic - A basic support plan is included for all AWS customers.

None of these three support plans provide access to online training with self-paced labs.

References:

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

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

Question 41: **Correct**

Under the AWS Shared Responsibility Model, which of the following is a shared responsibility of both AWS and the customer?

-

Infrastructure maintenance of Amazon S3 storage servers

-

Configuration Management

(Correct)

-

Guarantee data separation among various AWS customers

-

Availability Zone infrastructure maintenance

Explanation

Correct option:

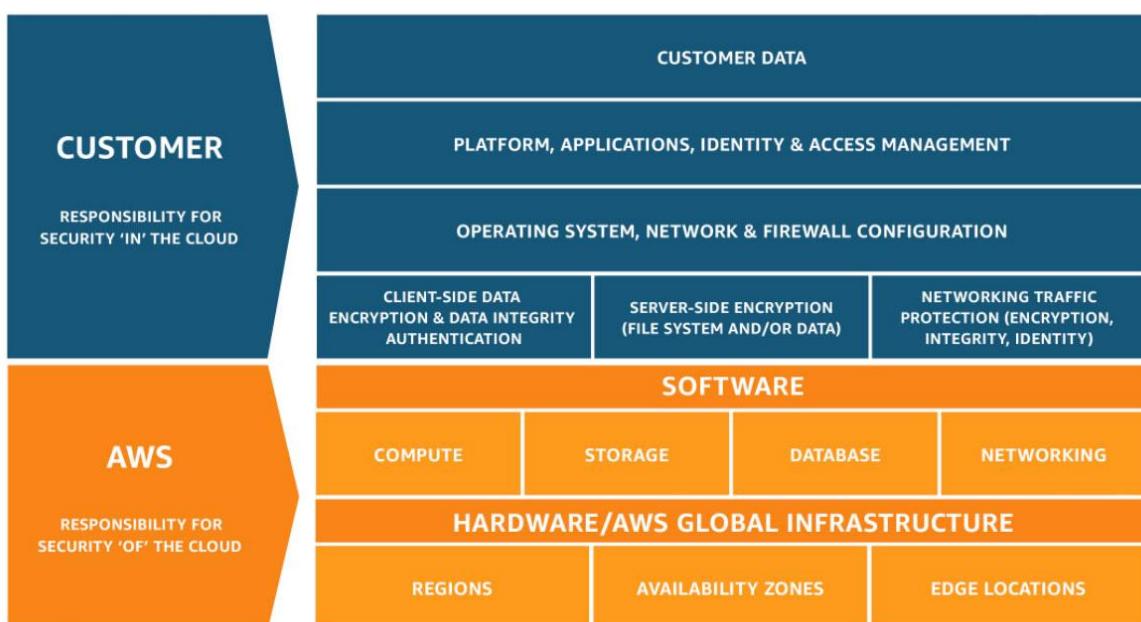
Configuration Management

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

Controls that apply to both the infrastructure layer and customer layers, but in completely separate contexts or perspectives are called shared controls. 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 forms a part of shared controls - AWS maintains the configuration of its infrastructure devices, but a customer is responsible for configuring their own guest operating systems, databases, and applications.

Shared Responsibility Model

Overview:



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

Incorrect options:

Infrastructure maintenance of Amazon S3 storage servers - AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud.

Guarantee data separation among various AWS customers - 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.

Availability Zone infrastructure maintenance - AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud.

Reference:

https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#master_keys

Question 42: **Correct**

A company needs a storage solution for a project wherein the data is accessed less frequently but needs rapid access when required. Which S3 storage class is the MOST cost-effective for the given use-case?



Amazon S3 Standard



Amazon S3 Glacier (S3 Glacier)



Amazon S3 Intelligent-Tiering (S3 Intelligent-Tiering)



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

(Correct)

Explanation

Correct option:

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

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 make S3 Standard-IA ideal for long-term storage, backups, and as a data store for disaster recovery files.

Incorrect options:

Amazon S3 Standard - The S3 Standard offers high durability, availability, and performance object storage for frequently accessed data. S3 standard would turn out to be costlier than S3 Standard-IA for the given use-case, so this option is not correct.

Amazon S3 Intelligent-Tiering (S3 Intelligent-Tiering) - The S3 Intelligent-Tiering storage class is designed to optimize costs by automatically moving data to the most cost-effective access tier, without performance impact or operational overhead. It works by storing objects in two access tiers: one tier that is optimized for frequent access and another lower-cost tier that is optimized for infrequent access. S3 Intelligent-Tiering would turn out to be costlier than S3 Standard-IA for the given use-case, so this option is not correct.

Amazon S3 Glacier (S3 Glacier) - Amazon S3 Glacier is a secure, durable, and extremely low-cost Amazon S3 cloud storage class for data archiving and long-term backup. It is designed to deliver 99.99999999% durability, and provide comprehensive security and compliance capabilities that can help meet even the most stringent regulatory requirements. S3 Glacier does not support rapid data retrieval, so this option is ruled out.

Reference:

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

Question 43: **Correct**

A startup wants to migrate its data and applications from the on-premises data center to AWS Cloud. Which of the following options can be used by the startup to help with this migration? (Select two)

-

Use AWS Trusted Advisor to automate the infrastructure migration

-

Consult moderators on AWS Developer Forums

-

Raise a support ticket with AWS Support for further assistance

-

Leverage AWS Professional Services to accelerate the infrastructure migration

(Correct)

-

Utilize AWS Partner Network (APN) to build a custom solution for this infrastructure migration

(Correct)

Explanation

Correct options:

Leverage AWS Professional Services to accelerate the infrastructure migration

The AWS Professional Services organization is a global team of experts that can help you realize your desired business outcomes when using the AWS Cloud. AWS Professional Services consultants can supplement your team with specialized skills and experience that can help you achieve quick results. Therefore, leveraging AWS Professional Services can accelerate the infrastructure migration for the startup.

Utilize AWS Partner Network (APN) to build a custom solution for this infrastructure migration

The AWS Partner Network (APN) is the global partner program for technology and consulting businesses that leverage Amazon Web Services to build solutions and services for customers. The startup can work with experts from APN to build a custom solution for this infrastructure migration.

Incorrect options:

Raise a support ticket with AWS Support for further assistance - AWS Support cannot help with complex infrastructure migration of this nature. Hence this option is incorrect.

Consult moderators on AWS Developer Forums - This is a made-up option and has been added as a distractor.

Use AWS Trusted Advisor to automate the infrastructure migration - AWS Trusted Advisor is an online tool that provides you real-time guidance to help you provision your resources following AWS best practices on cost optimization, security, fault tolerance, service limits, and performance improvement. Trusted Advisor cannot automate the infrastructure migration.

References:

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

<https://aws.amazon.com/professional-services/>

<https://aws.amazon.com/solutions/implementations/aws-landing-zone/>

Question 44: **Correct**

Which of the following statements are CORRECT regarding the AWS VPC service? (Select two)

-

A NAT Gateway is managed by AWS

(Correct)

-

A Security Group can have allow rules only

(Correct)

-

A NACL can have allow rules only

-

A Security Group can have both allow and deny rules

-

A NAT Instance is managed by AWS

Explanation

Correct options:

A Security Group can have allow rules only

A NAT Gateway is managed by AWS

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.

Security Group

Overview:

Security group basics

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

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

 **Note**

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

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

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

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>

You can use a network address translation (NAT) gateway or a NAT Instance to enable instances in a private subnet to connect to the internet or other AWS services, but prevent the internet from initiating a connection with those instances. NAT Gateway is managed by AWS but NAT Instance is managed by you.

Please see this comparison table for differences between NAT Gateway and NAT Instance:

Comparison of NAT instances and NAT gateways

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

The following is a high-level summary of the differences between NAT instances and NAT gateways.

Attribute	NAT gateway	NAT instance
Availability	Highly available. NAT gateways in each Availability Zone are implemented with redundancy. Create a NAT gateway in each Availability Zone to ensure zone-independent architecture.	Use a script to manage failover between instances.
Bandwidth	Can scale up to 45 Gbps.	Depends on the bandwidth of the instance type.
Maintenance	Managed by AWS. You do not need to perform any maintenance.	Managed by you, for example, by installing software updates or operating system patches on the instance.
Performance	Software is optimized for handling NAT traffic.	A generic Amazon Linux AMI that's configured to perform NAT.
Cost	Charged depending on the number of NAT gateways you use, duration of usage, and amount of data that you send through the NAT gateways.	Charged depending on the number of NAT instances that you use, duration of usage, and instance type and size.
Type and size	Uniform offering; you don't need to decide on the type or size.	Choose a suitable instance type and size, according to your predicted workload.
Public IP addresses	Choose the Elastic IP address to associate with a NAT gateway at creation.	Use an Elastic IP address or a public IP address with a NAT instance. You can change the public IP address at any time by associating a new Elastic IP address with the instance.
Private IP addresses	Automatically selected from the subnet's IP address range when you create the gateway.	Assign a specific private IP address from the subnet's IP address range when you launch the instance.
Security groups	Cannot be associated with a NAT gateway. You can associate security groups with your resources behind the NAT gateway to control inbound and outbound traffic.	Associate with your NAT instance and the resources behind your NAT instance to control inbound and outbound traffic.
Network ACLs	Use a network ACL to control the traffic to and from the subnet in which your NAT gateway resides.	Use a network ACL to control the traffic to and from the subnet in which your NAT instance resides.
Flow logs	Use flow logs to capture the traffic.	Use flow logs to capture the traffic.
Port forwarding	Not supported.	Manually customize the configuration to support port forwarding.
Bastion	Not supported.	Use as a bastion server.

via - <https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-comparison.html>

Incorrect options:

A Security Group can have both allow and deny rules

A NAT Instance is managed by AWS

A NACL can have allow rules only

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

References:

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

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

Question 45: **Correct**

Which of the following is a benefit of using AWS managed services such as Amazon RDS?

-

The customer needs to patch the underlying OS

-

The customer needs to manage database backups

-

There is no need to optimize database instance type and size

-

The performance of AWS managed RDS instance is better than a customer-managed database instance

(Correct)

Explanation

Correct option:

The performance of AWS managed RDS instance is better than a customer-managed database instance

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.

Amazon RDS provides a selection of instance types optimized to fit different relational database use cases. Instance types comprise varying combinations of CPU, memory, storage, and networking capacity and give you the flexibility to choose the appropriate mix of resources for your database to optimize the database for your use-case by selecting the correct instance type and size.

As the RDS instances are optimized for memory, performance, or I/O, therefore the performance of AWS managed RDS instance is better than a customer-managed database instance.

Incorrect options:

The customer needs to patch the underlying OS

The customer needs to manage database backups

There is no need to optimize database instance type and size

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

Reference:

<https://aws.amazon.com/rds/instance-types/>

Question 46: **Correct**

Which AWS services can be used to decouple components of a microservices based application on AWS Cloud? (Select two)

-

Step Function

-

SQS

(Correct)

-

Lambda

-

SNS

(Correct)

-

EC2

Explanation

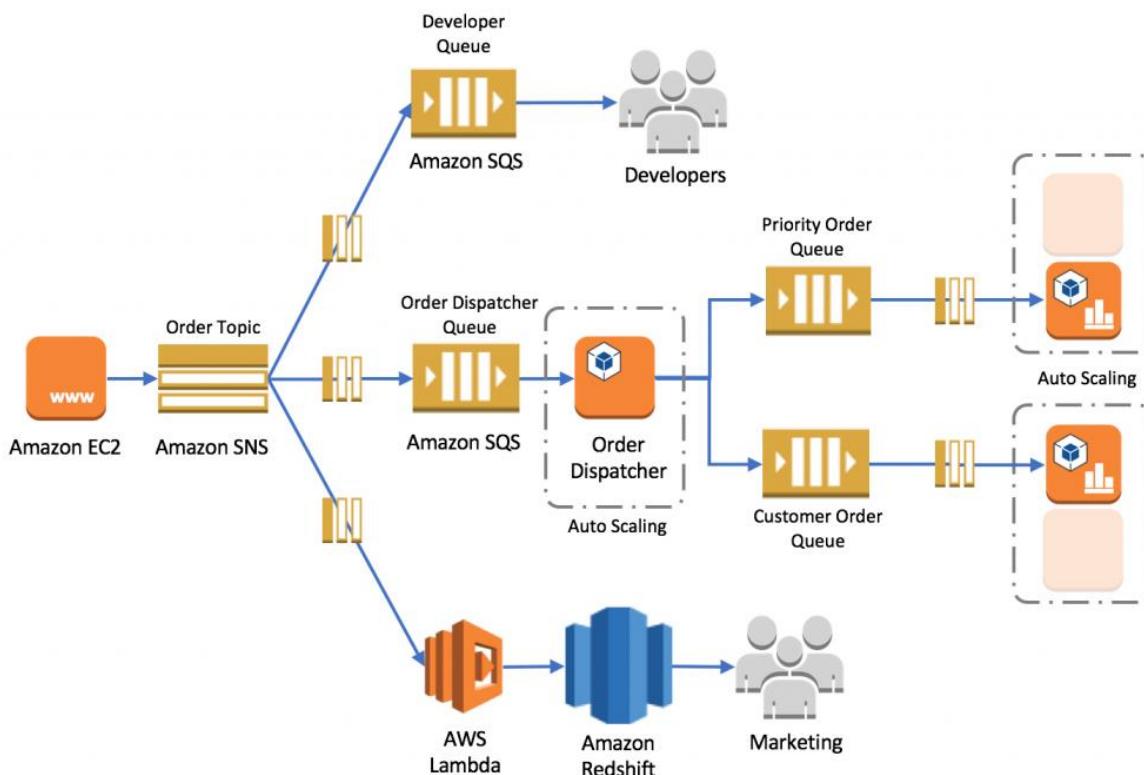
Correct option:

SQS - Amazon Simple Queue Service (SQS) is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. 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.

SNS - Amazon Simple Notification Service (SNS) is a highly available, durable, secure, fully managed pub/sub messaging service that enables you to decouple microservices, distributed systems, and serverless applications. Using Amazon SNS topics, your publisher systems can fan-out messages to a large number of subscriber endpoints for parallel processing, including Amazon SQS queues, AWS Lambda functions, and HTTP/S webhooks. Additionally, SNS can be used to fan out notifications to end users using mobile push, SMS, and email.

Therefore, both SNS and SQS can be used to decouple components of a microservices-based application.

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-c-applications-with-amazon-sqs-and-amazon-sns/>

Incorrect options:

EC2 - Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud with support for per-second billing. It is the easiest way to provision

servers on AWS Cloud and access the underlying OS. EC2 cannot be used to decouple components of a microservices-based application.

Lambda - AWS Lambda lets you run code without provisioning or managing servers. You pay only for the compute time you consume. Lambda cannot be used to decouple components of a microservices-based application.

Step Function - AWS Step Function lets you coordinate multiple AWS services into serverless workflows. You can design and run workflows that stitch together services such as AWS Lambda, AWS Glue and Amazon SageMaker. Step Function cannot be used to decouple components of a microservices-based application.

Reference:

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

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

Question 47: **Correct**

A company wants to move to AWS cloud and release new features with quick iterations by utilizing relevant AWS services whenever required. Which of the following characteristics of AWS Cloud does it want to leverage?

-

Reliability

-

Agility

(Correct)

-

Scalability

-

Elasticity

Explanation

Correct option:

Agility

In the world of cloud computing, "Agility" refers to the ability to rapidly develop, test and launch software applications that drive business growth. Another way to explain "Agility" - AWS provides a massive global cloud infrastructure that allows you to quickly innovate, experiment and iterate. Instead of waiting weeks or months for hardware, you can instantly deploy new applications. This ability is called Agility.

Incorrect options:

Elasticity - This refers to the ability to acquire resources as you need and release when they are no longer needed is termed as Elasticity of the Cloud.

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

Scalability - Scalability is the measurement of a system's ability to grow to accommodate an increase in demand, or shrink down to a diminishing demand.

Reference:

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

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

Question 48: **Correct**

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

-

Maintaining Amazon S3 data in different availability zones to keep it durable

(Correct)

-

Creating IAM role for accessing Amazon EC2 instances

-

Replacing faulty hardware of Amazon EC2 instances

(Correct)

-

Creating S3 bucket policies for appropriate user access

-

Enabling Multi Factor Authentication on AWS accounts in your organization

Explanation

Correct option:

According to the AWS Shared Responsibility Model, AWS is responsible for "Security of the Cloud". This includes protecting the infrastructure that runs all of the services offered in the AWS Cloud. This

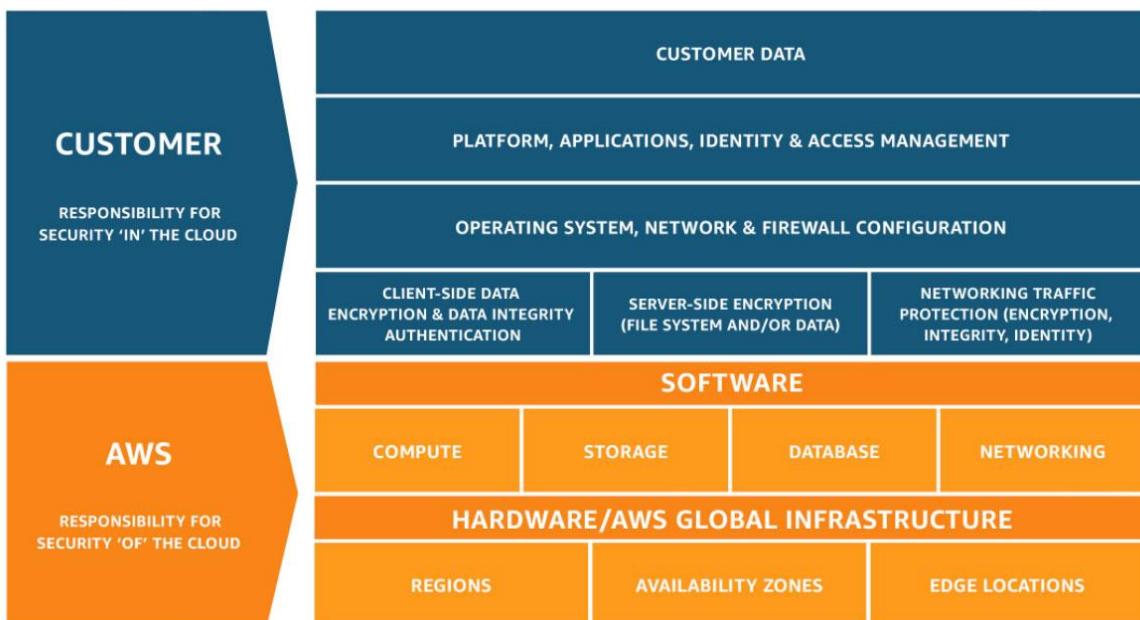
infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services.

Replacing faulty hardware of Amazon EC2 instances - Replacing faulty hardware of Amazon EC2 instances comes under the infrastructure maintenance "of" the cloud. This is the responsibility of AWS.

Maintaining Amazon S3 data in different availability zones to keep it durable - AWS is responsible for keeping data on AWS Cloud Secure, Durable, Available and Reliable. Keeping data infrastructure safe from failures is the responsibility of AWS.

Shared Responsibility Model

Overview:



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

Incorrect options:

Enabling Multi Factor Authentication on AWS accounts in your organization - Enabling Multi Factor Authentication for AWS accounts in your organization is your responsibility. On the other hand, AWS is responsible for making sure that the user data created and their relationships and policies are stored on fail-proof infrastructure.

Creating IAM role for accessing Amazon EC2 instances - Creating user roles, policies is the responsibility of the customer. Customers will decide "which" resources get "what" access.

Creating S3 bucket policies for appropriate user access - Creating bucket policies for Amazon S3 data access is the responsibility of the customer. The customer decides who gets access to the data he stores on S3 and will use AWS tools to implement these requirements. AWS on the other hand is responsible for keeping the data safe from hardware and software failure.

Reference:

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

Question 49: **Correct**

Which of the following AWS services should be used to automatically distribute incoming traffic across multiple targets?

-
-

AWS Elastic Beanstalk

-
-

AWS Elastic Load Balancing

(Correct)

-
-

AWS Auto Scaling

-
-

Amazon Elasticsearch

Explanation

Correct option:

AWS Elastic Load Balancing

Elastic Load Balancing is used to automatically distribute your incoming application traffic across all the EC2 instances that you are running. You can use Elastic Load Balancing to manage incoming requests by optimally routing traffic so that no one instance is overwhelmed. Your load balancer acts as a single point of contact for all incoming web traffic to your application. When an instance is added, it needs to register with the load balancer or no traffic is routed to it. When an instance is removed, it must deregister from the load balancer or traffic continues to be routed to it.

Incorrect options:

AWS Elastic Beanstalk - AWS Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services developed in a variety of programming languages. You can simply upload your code and Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring. You cannot use Beanstalk to distribute incoming traffic across multiple targets.

Amazon Elasticsearch - The term "Elasticsearch" is used to define a distributed, open source search and analytics engine for all types of data, including textual, numerical, geospatial, structured, and unstructured. Amazon Elasticsearch Service is a fully managed service that makes it easy to deploy, secure, and run Elasticsearch cost effectively at scale. It is a search and analytics service from Amazon.

AWS Auto Scaling - AWS Auto Scaling monitors your applications and automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost. Using AWS Auto Scaling, it's easy to setup application scaling for multiple resources across multiple services in minutes. This is a scaling service that helps you spin up resources as and when you need them and scale down when the

high demand reduces. Auto Scaling can be used with Elastic Load Balancing to build high performance applications.

Reference:

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

Question 50: **Correct**

Which of the following is a serverless AWS service?



Beanstalk



EMR



EC2



Lambda

(Correct)

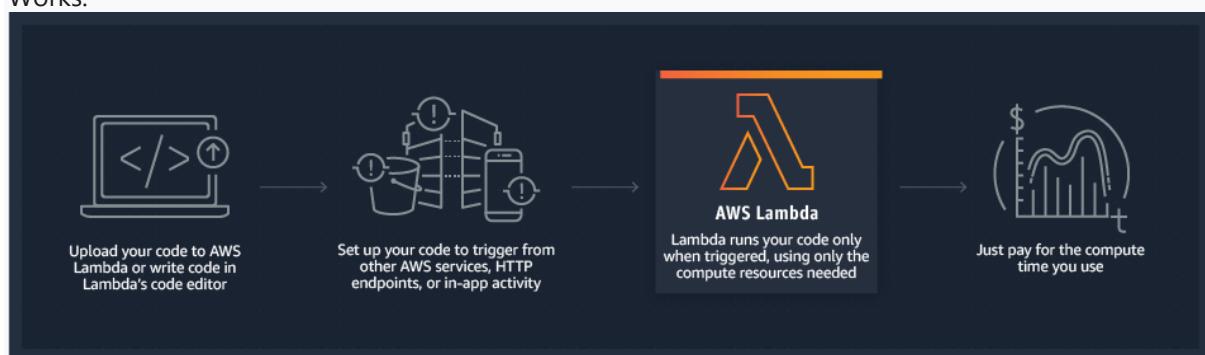
Explanation

Correct option:

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

How Lambda

Works:



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

Incorrect options:

EC2 - Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud with support for per-second billing. It is the easiest way to provision servers on AWS Cloud and access the underlying OS. EC2 is not a serverless service.

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. EMR is not a serverless service.

Beanstalk - AWS Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services. You simply upload your code and Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring. Beanstalk provisions servers so it is not a serverless service.

Reference:

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

Question 51: **Correct**

Which AWS service will help you receive alerts when the reservation utilization falls below the defined threshold?

-

AWS CloudTrail

-

AWS Budgets

(Correct)

-

AWS Pricing Calculator

-

AWS Trusted Advisor

Explanation

Correct option:

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 reservation utilization or coverage targets and receive alerts when your utilization drops below the threshold you define. Reservation alerts are supported for

Amazon EC2, Amazon RDS, Amazon Redshift, Amazon ElastiCache, and Amazon Elasticsearch reservations.

Incorrect options:

AWS Pricing Calculator - AWS Pricing Calculator lets you explore AWS services and create an estimate for the cost of your use cases on AWS. You can model your solutions before building them, explore the price points and calculations behind your estimate, and find the available instance types and contract terms that meet your needs. This enables you to make informed decisions about using AWS. You cannot use this service to receive alerts when the reservation utilization falls below the defined threshold.

AWS CloudTrail - AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command-line tools, and other AWS services. You cannot use this service to receive alerts when the reservation utilization falls below the defined threshold.

AWS Trusted Advisor - AWS Trusted Advisor is an online tool that provides real-time guidance to help provision your resources following AWS best practices. Whether establishing new workflows, developing applications, or as part of ongoing improvement, recommendations provided by Trusted Advisor regularly help keep your solutions provisioned optimally. AWS Trusted Advisor analyzes your AWS environment and provides best practice recommendations in five categories: Cost Optimization, Performance, Security, Fault Tolerance, Service Limits. You cannot use this service to receive alerts when the reservation utilization falls below the defined threshold.

References:

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

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

Question 52: **Correct**

Which of the following are the advantages of Cloud Computing? (Select three)

-

Trade capital expense for variable expense

(Correct)

-

Spend money on building and maintaining data centers

-

Trade variable expense for capital expense

-

Allocate a few months of planning for your infrastructure capacity needs

-

Benefit from massive economies of scale

(Correct)

-

Go global in minutes and deploy applications in multiple regions around the world with just a few clicks

(Correct)

Explanation

Correct options:

Benefit from massive economies of scale

Trade capital expense for variable expense

Go global in minutes and deploy applications in multiple regions around the world with just a few clicks

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:

Spend money on building and maintaining data centers - With Cloud Computing, you can focus on projects that differentiate your business, not the infrastructure. You don't need to spend money on building and maintaining data centers as the Cloud provider takes care of that.

Allocate a few months of planning for your infrastructure capacity needs - With Cloud Computing, you don't need to guess on your infrastructure capacity needs. 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. There is no need to allocate a few months of infrastructure planning.

Trade variable expense for capital expense - With Cloud Computing, you actually trade capital expense for variable expense.

Reference:

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

Question 53: **Correct**

A multi-national company has just moved its infrastructure from its on-premises data center to AWS Cloud. As part of the shared responsibility model, AWS is responsible for which of the following?

- - Patching guest OS**
 -
 - Configuring customer applications**
 -
 - Physical and Environmental controls**
- (Correct)**
- - Service and Communications Protection or Zone Security**

Explanation

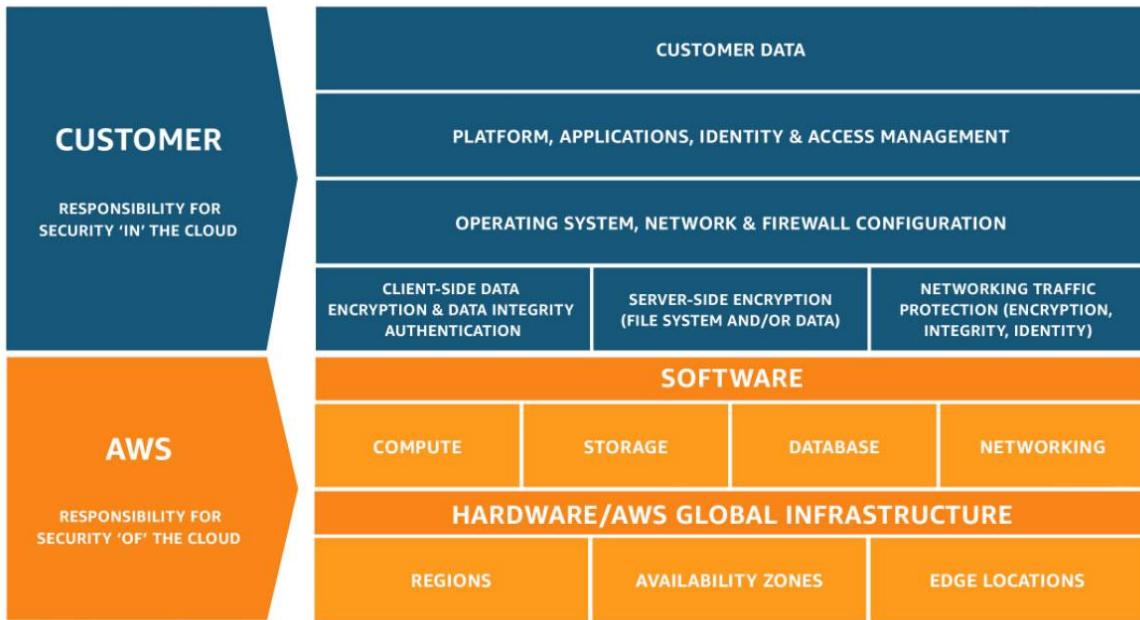
Correct option:

Physical and Environmental controls

As part of the shared responsibility model, Physical and Environmental controls are part of the inherited controls and hence these are the responsibility of AWS.

Shared Responsibility Model

Overview:



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

Incorrect options:

Patching guest OS

Configuring customer applications

The customers must provide their own control implementation within their use of AWS services. Therefore, the customers are responsible for patching their guest OS as well as for configuring their applications.

Service and Communications Protection or Zone Security - Customers are responsible for Service and Communications Protection or Zone Security which may require the customers to route or zone data within specific security environments.

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/>

Reference:

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

Question 54: **Correct**

Which AWS Route 53 routing policy would you use to route traffic to multiple resources and also choose how much traffic is routed to each resource?

-

Failover routing policy

-

Weighted routing policy

(Correct)

-

Simple routing policy

-

Latency routing policy

Explanation

Correct option:

Weighted routing policy

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

Weighted routing lets you associate multiple resources with a single domain name (example.com) or subdomain name (acme.example.com) and choose how much traffic is routed to each resource. This can be useful for a variety of purposes, including load balancing and testing new versions of software. To configure weighted routing, you create records that have the same name and type for each of your resources. You assign each record a relative weight that corresponds with how much traffic you want to send to each resource. Amazon Route 53 sends traffic to a resource based on the weight that you assign to the record as a proportion of the total weight for all records in the group.

Route 53 Routing Policy

Overview:

Choosing a routing policy

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

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

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

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

Incorrect options:

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

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

Latency routing policy - This routing policy is used when you have resources in multiple AWS Regions and you want to route traffic to the region that provides the best latency.

Reference:

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

Question 55: **Correct**

An intern at an IT company provisioned a Linux based On-demand EC2 instance with per-second billing but terminated it within 30 seconds as he wanted to provision another instance type. What is the duration for which the instance would be charged?



30 seconds

-

60 seconds

(Correct)

-

600 seconds

-

300 seconds

Explanation

Correct option:

60 seconds - There is a one-minute minimum charge for Linux based EC2 instances, so this is the correct option.

Incorrect options:

30 seconds

300 seconds

600 seconds

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

Reference:

<https://aws.amazon.com/blogs/aws/new-per-second-billing-for-ec2-instances-and-ebs-volumes/>

Question 56: **Correct**

Which of the following AWS Support plans provides access to Infrastructure Event Management for an additional fee?

-

Basic

-

Developer

-

Business

(Correct)

-
-

Enterprise

Explanation

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. Also, you get access to Infrastructure Event Management for an additional fee.

Incorrect options:

Developer - AWS recommends Developer Support if you are testing or doing early development on AWS and want the ability to get email-based technical support during business hours as well as general architectural guidance as you build and test. You do not get access to Infrastructure Event Management with this plan.

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

Customer Service & Communities - 24x7 access to customer service, documentation, whitepapers, and support forums. AWS Trusted Advisor - Access to the 7 core Trusted Advisor checks and guidance to provision your resources following best practices to increase performance and improve security. AWS Personal Health Dashboard - A personalized view of the health of AWS services, and alerts when your resources are impacted. You do not get access to Infrastructure Event Management with this plan.

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. Access to Infrastructure Event Management is included in the plan.

Reference:

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

Question 57: **Correct**

Which of the following is a recommended way to provide programmatic access to AWS resources?

-
-

Use Multi Factor Authentication to access AWS resources programmatically

-
-

Use IAM groups to access AWS resources programmatically

-

Create a new IAM user and share the username and password

-

Use Access Key ID and Secret Access Key to access AWS resources programmatically

(Correct)

Explanation

Correct option:

Use Access Key ID and Secret Access Key to access AWS resources programmatically

Access keys are long-term credentials for an IAM user or the AWS account root user. You can use access keys to sign programmatic requests to the AWS CLI or AWS API (directly or using the AWS SDK). Access keys consist of two parts: an access key ID and a secret access key. As a user name and password, you must use both the access key ID and secret access key together to authenticate your requests. When you create an access key pair, save the access key ID and secret access key in a secure location. The secret access key is available only at the time you create it. If you lose your secret access key, you must delete the access key and create a new one.

Incorrect options:

Create a new IAM user and share the username and password - This is not a viable option, IAM user credentials are not needed to access resources programmatically.

Use Multi Factor Authentication to access AWS resources programmatically - For increased security, AWS recommends that you configure multi-factor authentication (MFA) to help protect your AWS resources. You can enable MFA for IAM users or the AWS account root user. MFA adds extra security because it requires users to provide unique authentication from an AWS supported MFA mechanism in addition to their regular sign-in credentials when they access AWS websites or services. MFA cannot be used for programmatic access to AWS resources.

Use IAM Groups to access AWS resources programmatically - An IAM Group is a collection of IAM users. Groups let you specify permissions for multiple users, which can make it easier to manage the permissions for those users. IAM Group is for managing users and not for programmatic access to AWS resources.

Reference:

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

Question 58: **Correct**

Which AWS services can be used to facilitate organizational change management, part of the Reliability pillar of AWS Well-Architected Framework? (Select three)

-

Amazon GuardDuty

-
- Amazon Inspector**
-
- AWS CloudTrail**
- (Correct)
-
- AWS Trusted Advisor**
-
- Amazon CloudWatch**
- (Correct)
-
- AWS Config**
- (Correct)

Explanation

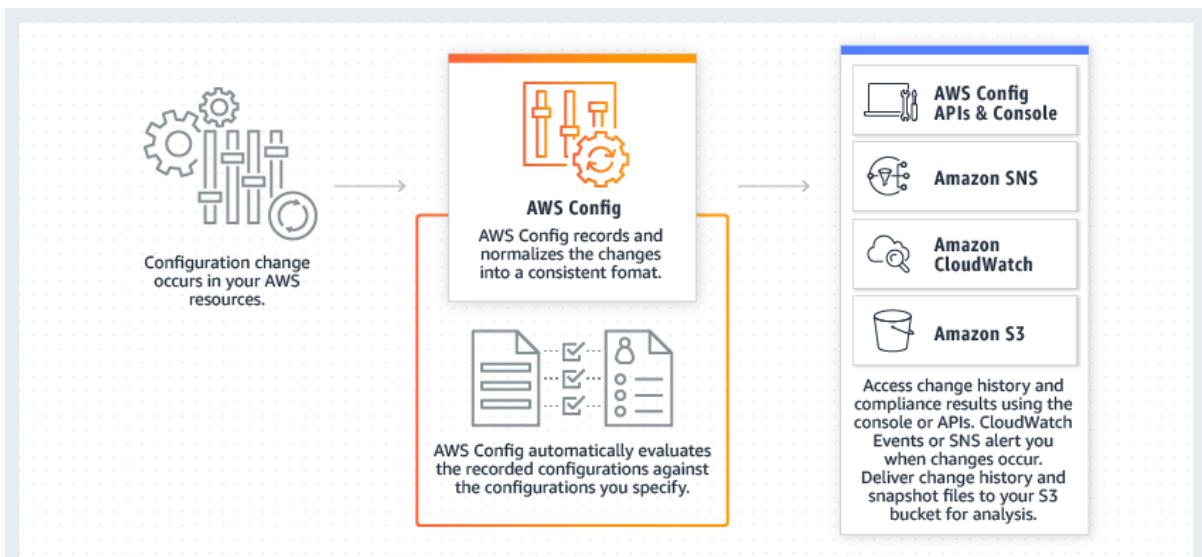
Correct options:

There are three best practice areas for Reliability in the cloud - Foundations, Change Management, Failure Management. Being aware of how change affects a system (change management) allows you to plan proactively, and monitoring allows you to quickly identify trends that could lead to capacity issues or SLA breaches.

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

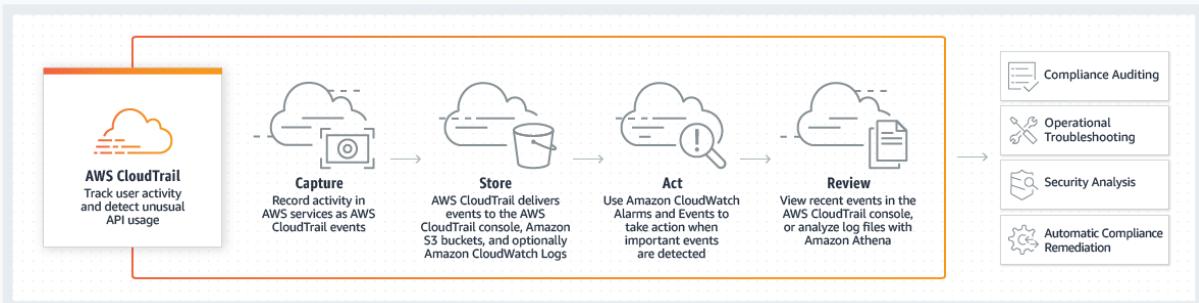
Works:



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

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

How CloudTrail Works:



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

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.

Incorrect options:

AWS Trusted Advisor - AWS Trusted Advisor is an online tool that provides you real-time guidance to help you provision your resources following AWS best practices on cost optimization, security, fault tolerance, service limits, and performance improvement.

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 GuardDuty - Amazon GuardDuty is a threat detection service that monitors malicious activity and unauthorized behavior to protect your AWS account. GuardDuty analyzes billions of events across your AWS accounts from AWS CloudTrail (AWS user and API activity in your accounts), Amazon VPC Flow Logs (network traffic data), and DNS Logs (name query patterns). This service is for AWS account level access, not for instance-level management like an EC2. GuardDuty cannot be used to check OS vulnerabilities.

References:

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

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

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

Question 59: **Correct**

What are the advantages that AWS Cloud offers over a traditional on-premises IT infrastructure?
(Select two)

- **Make a capacity decision before deploying an application, to reduce costs**
 - **Provide lower latency to applications by maintaining servers on-premises**
 - **Increase speed and agility by keeping servers and other required resources ready before time in your data centers**
 - **Eliminate guessing on your infrastructure capacity needs**
- (Correct)**
- **Trade capital expense for variable expense**
- (Correct)**

Explanation

Correct options:

Trade capital expense for variable expense - In a traditional on-premises environment, you have to invest heavily in data centers and servers before you know how you're going to use them. With Cloud Computing, you can pay only when you consume computing resources, and pay only for how much you consume.

Eliminate guessing on your infrastructure capacity needs - When you make a capacity decision before 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. You can Stop guessing capacity.

Incorrect options:

Make a capacity decision before deploying an application, to reduce costs - As explained above, when you make a capacity decision before deploying an application, you often end up either sitting on expensive idle resources or dealing with limited capacity.

Provide lower latency to applications by maintaining servers on-premises - Maintaining servers on-premises involves costly capital expenses and costly ongoing expenses to maintain, manage and upgrade them.

Increase speed and agility by keeping servers and other required resources ready before time in your data centers - This again is indicative of maintaining on-premises infrastructure which is neither a cost-effective or time effective way of managing the resources.

Reference:

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

Question 60: **Correct**

Which of the following are correct statements regarding the AWS Global Infrastructure? (Select two)

-

Each AWS Region consists of two or more Edge Locations

-

Each AWS Region consists of two or more Availability Zones

(Correct)

-

Each Availability Zone (AZ) consists of one or more discrete data centers

(Correct)

-

Each Availability Zone (AZ) consists of two or more discrete data centers

-

Each AWS Region consists of one or more Availability Zones

Explanation

Correct options:

Each AWS Region consists of two or more Availability Zones

Each Availability Zone (AZ) consists of one or more discrete data centers

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. Each AZ has independent power, cooling, and physical security and is connected via redundant, ultra-low-latency networks.

An Availability Zone (AZ) is one or more discrete data centers with redundant power, networking, and connectivity in an AWS Region. 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.

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/

Incorrect options:

Each AWS Region consists of one or more Availability Zones

Each Availability Zone (AZ) consists of two or more discrete data centers

Each AWS Region consists of two or more Edge Locations

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

Reference:

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

Question 61: **Correct**

Which of the following AWS services can be used to connect a company's on-premises environment to a VPC without using the public internet?



Internet Gateway



Site-to-Site VPN



Amazon VPC Endpoint



AWS Direct Connect

(Correct)

Explanation

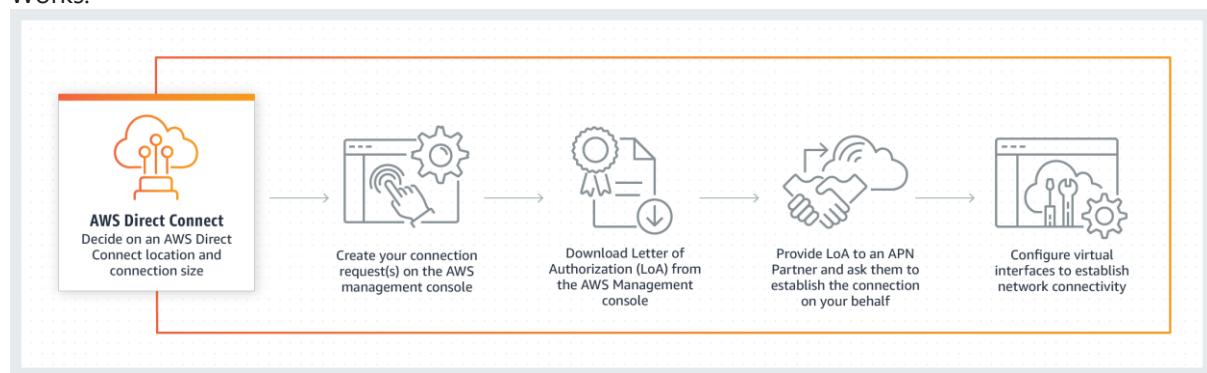
Correct option:

AWS Direct Connect

AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS. You can use AWS Direct Connect to establish a private virtual interface from your on-premise network directly to your Amazon VPC, providing you with a private, high bandwidth network connection between your network and your VPC. This connection is private and does not go over the public internet. It takes at least a month to establish this physical connection.

How Direct Connect

Works:



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

Incorrect options:

Amazon VPC Endpoint - 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. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network. VPC Endpoint cannot be used to privately connect on-premises data center to AWS Cloud.

Internet Gateway - An Internet Gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between your VPC and the internet. An internet gateway serves two purposes: to provide a target in your VPC route tables for internet-routable traffic and to perform network address translation (NAT) for instances. Internet Gateway cannot be used to privately connect on-premises data center to AWS Cloud.

Site-to-Site VPN - AWS Site-to-Site VPN creates a secure connection between your data center or branch office and your AWS cloud resources. This connection goes over the public internet.

References:

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

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

Question 62: **Correct**

A company runs an application on a fleet of EC2 instances. The company wants to automate the traditional maintenance job of running timely assessments and checking for OS vulnerabilities. As a Cloud Practitioner, which service will you suggest for this use case?

-
-

Amazon Inspector

(Correct)

-
-

AWS Shield

-
-

Amazon GuardDuty

-
-

Amazon Macie

Explanation

Correct option:

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. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity. These findings can be reviewed directly or as part of detailed assessment reports which are available via the Amazon Inspector console or API.

Incorrect options:

Amazon GuardDuty - Amazon GuardDuty is a threat detection service that monitors malicious activity and unauthorized behavior to protect your AWS account. GuardDuty analyzes billions of events across your AWS accounts from AWS CloudTrail (AWS user and API activity in your accounts), Amazon VPC Flow Logs (network traffic data), and DNS Logs (name query patterns). This service is for AWS account level access, not for instance-level management like an EC2. GuardDuty cannot be used to check OS vulnerabilities.

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. Macie helps identify and alert you to sensitive data, such as personally identifiable information (PII). This service is for securing data and has nothing to do with an EC2 security assessment. Macie cannot be used to check OS vulnerabilities.

AWS Shield - AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS. AWS Shield provides always-on detection and automatic inline mitigations that minimize application downtime and latency, so there is no need to engage AWS Support to benefit from DDoS protection. Shield is general protection against DDoS attacks for all resources in the AWS network, and not an instance-level security assessment service. Shield cannot be used to check OS vulnerabilities.

Reference:

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

Question 63: **Correct**

Which of the following AWS services support reservations to optimize costs? (Select three)

-

DocumentDB

-

RDS

(Correct)

-

EC2 Instances

(Correct)

-

DynamoDB

(Correct)

-

Lambda

-

S3

Explanation

Correct options:

EC2 Instances

DynamoDB

RDS

The following AWS services support reservations to optimize costs:

Amazon EC2 Reserved Instances: You can use Amazon EC2 Reserved Instances to reserve capacity and receive a discount on your instance usage compared to running On-Demand instances.

Amazon DynamoDB Reserved Capacity: If you can predict your need for Amazon DynamoDB read-and-write throughput, Reserved Capacity offers significant savings over the normal price of DynamoDB provisioned throughput capacity.

Amazon ElastiCache Reserved Nodes: Amazon ElastiCache Reserved Nodes give you the option to make a low, one-time payment for each cache node you want to reserve and, in turn, receive a significant discount on the hourly charge for that node.

Amazon RDS RIs: Like Amazon EC2 RIs, Amazon RDS RIs can be purchased using No Upfront, Partial Upfront, or All Upfront terms. All Reserved Instance types are available for Aurora, MySQL, MariaDB, PostgreSQL, Oracle, and SQL Server database engines.

Amazon Redshift Reserved Nodes: If you intend to keep an Amazon Redshift cluster running continuously for a prolonged period, you should consider purchasing reserved-node offerings. These offerings provide significant savings over on-demand pricing, but they require you to reserve compute nodes and commit to paying for those nodes for either a 1- or 3-year duration.

Incorrect options:

DocumentDB - Amazon DocumentDB (with MongoDB compatibility) is a fast, scalable, highly available, and fully managed document database service that supports MongoDB workloads. As a document database, Amazon DocumentDB makes it easy to store, query, and index JSON data.

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

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

None of these AWS services support reservations to optimize costs.

Reference:

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

Question 64: **Correct**

A cyber forensics team has detected that AWS owned IP-addresses are being used to carry out malicious attacks. As this constitutes prohibited use of AWS services, which of the following is the correct solution to address this issue?



Contact AWS Support



Contact AWS Developer Forum moderators



Contact AWS Abuse Team

(Correct)



Write an email to Jeff Bezos, the CEO of Amazon, with the details of the incident

Explanation

Correct option:

Contact AWS Abuse Team

The AWS Abuse team can assist you when AWS resources are used to engage in abusive behavior.

Please see details of the various scenarios that the AWS Abuse team can address:

How do I report abuse of AWS resources?

Last updated: 2020-04-30

I suspect that Amazon Web Services (AWS) resources are used for abusive or illegal purposes. How do I let AWS know?

Resolution

The AWS Abuse team can assist you when AWS resources are used to engage in the following types of abusive behavior:

- **Spam:** You are receiving unwanted emails from an AWS-owned IP address, or AWS resources are used to spam websites or forums.
- **Port scanning:** Your logs show that one or more AWS-owned IP addresses are sending packets to multiple ports on your server, and you believe this is an attempt to discover unsecured ports.
- **Denial-of-service (DoS) attacks:** Your logs show that one or more AWS-owned IP addresses are used to flood ports on your resources with packets, and you believe that this is an attempt to overwhelm or crash your server or the software running on your server.
- **Intrusion attempts:** Your logs show that one or more AWS-owned IP addresses are used to attempt to log in to your resources.
- **Hosting objectionable or copyrighted content:** You have evidence that AWS resources are used to host or distribute illegal content or distribute copyrighted content without the consent of the copyright holder.
- **Distributing malware:** You have evidence that AWS resources are used to distribute software that was knowingly created to compromise or cause harm to computers or machines on which it is installed.

via - <https://aws.amazon.com/premiumsupport/knowledge-center/report-aws-abuse/>

Incorrect options:

Contact AWS Support - You need to contact the AWS Abuse team for prohibited use of AWS services.

Contact AWS Developer Forum moderators - You need to contact the AWS Abuse team for prohibited use of AWS services.

Write an email to Jeff Bezos, the CEO of Amazon, with the details of the incident - This has been added as a distractor. For the record, please let us know if you do get a reply from Mr. Bezos.

Reference:

<https://aws.amazon.com/premiumsupport/knowledge-center/report-aws-abuse/>

Question 65: **Correct**

A unicorn startup is building an analytics application with support for a speech-based interface. The application will accept speech-based input from users and then convey results via speech. As a Cloud Practitioner, which solution would you recommend for the given use-case?

-

Use Amazon Polly to convert speech to text for downstream analysis. Then use Amazon Translate to convey the text results via speech

-

Use Amazon Transcribe to convert speech to text for downstream analysis. Then use Amazon Polly to convey the text results via speech

(Correct)

-

Use Amazon Polly to convert speech to text for downstream analysis. Then use Amazon Transcribe to convey the text results via speech

-

Use Amazon Translate to convert speech to text for downstream analysis. Then use Amazon Polly to convey the text results via speech

Explanation

Correct option:

Use Amazon Transcribe to convert speech to text for downstream analysis. Then use Amazon Polly to convey the text results via speech

You can use Amazon Transcribe to add speech-to-text capability to your applications. Amazon Transcribe uses a deep learning process called automatic speech recognition (ASR) to convert speech to text quickly and accurately. Amazon Transcribe can be used to transcribe customer service calls, to automate closed captioning and subtitling, and to generate metadata for media assets.

Amazon Transcribe Use-

Cases:

Improving Customer Service

By converting audio input into text, Amazon Transcribe helps you build text analytics applications that can search and analyze voice input. Customer contact centers can use Amazon Transcribe to transcribe calls, and mine the data for insights using other AWS services like [Amazon Comprehend](#) to extract meaning and intent from conversations.

Captioning & Subtitling Workflows

Amazon Transcribe can help content producers and media distributors improve reach and accessibility by automatically generating time-stamped subtitles that can be displayed along with the video content. By combining this text with [Amazon Translate](#), you can also easily localize videos.

Cataloging Audio Archives

You can use Amazon Transcribe to transcribe audio and video assets into fully searchable archives for compliance monitoring and risk management. Convert audio to text and use [Amazon Elasticsearch](#) to index and search across your audio/video library.

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

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 Polly

Benefits:

Natural sounding voices

Amazon Polly provides dozens of languages and a wide selection of natural-sounding male and female voices. Amazon Polly's fluid pronunciation of text enables you to deliver high-quality voice output for a global audience.

Store & redistribute speech

Amazon Polly allows for unlimited replays of generated speech without any additional fees. You can create speech files in standard formats like MP3 and OGG, and serve them from the cloud or locally with apps or devices for offline playback.

Real-time streaming

Delivering lifelike voices and conversational user experiences requires consistently fast response times. When you send text to Amazon Polly's API, it returns the audio to your application as a stream so you can play the voices immediately.

Customize & control speech output

Modify Amazon Polly voices to best suit your needs – Amazon Polly supports lexicons and SSML tags which enable you to control aspects of speech, such as pronunciation, volume, pitch, speed rate, etc.

Low cost

Amazon Polly's pay-as-you-go pricing, low cost per character converted, and unlimited replays make it a cost-effective way to voice your applications.

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

Amazon Translate is used for language translation. Amazon Translate uses neural machine translation via deep learning models to deliver more accurate and more natural-sounding translation than traditional statistical and rule-based translation algorithms.

Incorrect options:

Use Amazon Polly to convert speech to text for downstream analysis. Then use Amazon Transcribe to convey the text results via speech - Amazon Polly cannot be used to convert speech to text, so this option is incorrect.

Use Amazon Translate to convert speech to text for downstream analysis. Then use Amazon Polly to convey the text results via speech - Amazon Translate cannot convert speech to text, so this option is incorrect.

Use Amazon Polly to convert speech to text for downstream analysis. Then use Amazon Translate to convey the text results via speech - Amazon Polly cannot be used to convert speech to text, so this option is incorrect.

References:

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

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

Practice Test #2 - AWS Certified Cloud Practitioner - Results

Return to review

Chart

Pie chart with 3 slices.

End of interactive chart.

Attempt 2

All knowledge areas

All questions

Question 1: **Correct**

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

-

AWS Trusted Advisor

-

AWS Key Management Service (KMS)

-

AWS CloudHSM

(Correct)

-

AWS Secrets Manager

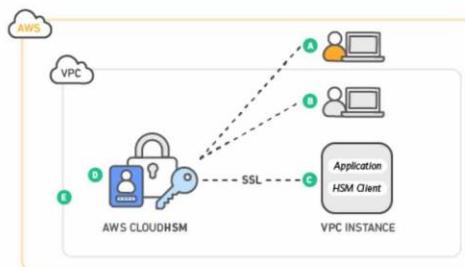
Explanation

Correct option:

AWS CloudHSM

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

Please review this detailed description of how CloudHSM works:



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

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

B: You control and manage your own keys

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

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

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

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

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

Incorrect options:

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

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

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

Reference:

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

Question 2: **Correct**

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

-
-

AWS Web Application Firewall (WAF)

(Correct)

-
-

AWS CloudWatch

-
-

Amazon Inspector

-
-

Amazon GuardDuty

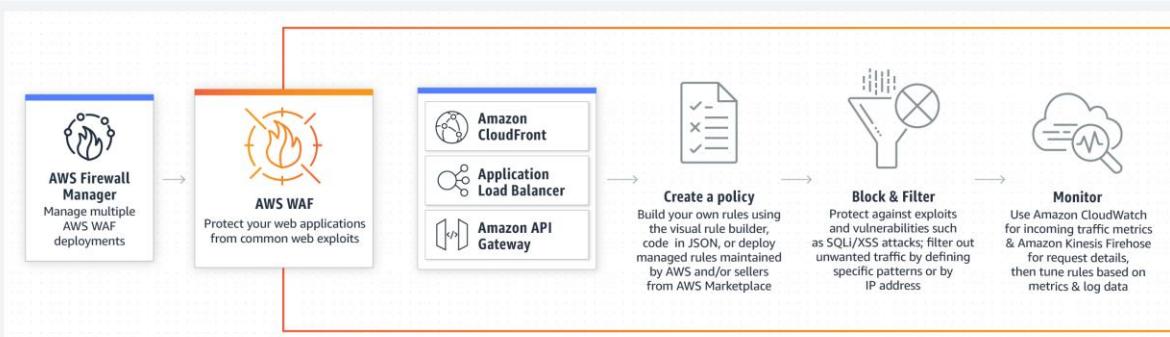
Explanation

Correct option:

AWS Web Application Firewall (WAF)

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

How WAF Works:



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

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

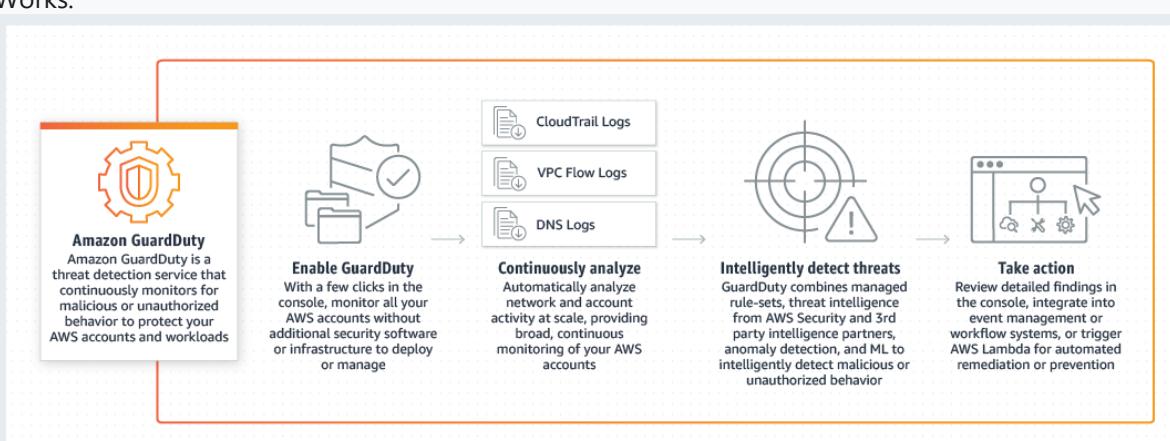
Similar to an SQL injection attack, a cross-site scripting attack also involves injecting malicious code into a website, but in this case, the website itself is not being attacked. Instead, the malicious code the attacker has injected only runs in the user's browser when they visit the attacked website,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

Incorrect options:

Amazon GuardDuty

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

How GuardDuty Works:



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

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

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

Reference:

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

Question 3: **Correct**

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

- A VPC spans all of the Availability Zones in the Region whereas a subnet spans only one Availability Zone in the Region
(Correct)
- A subnet spans all of the Availability Zones in the Region whereas a VPC spans only one Availability Zone in the Region
- Both the VPC and the subnet span only one Availability Zone in the Region
- Both the VPC and the subnet span all of the Availability Zones in the Region

Explanation

Correct option:

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

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

subnets, and configuration of route tables and network gateways. A VPC spans all of the Availability Zones in the Region.

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

VPC and Subnet

Overview:

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



The main route table has the following routes.

Destination	Target
10.0.0.0/16	local

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

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

Incorrect options:

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

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

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

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

Reference:

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

Question 4: **Correct**

A company wants a fully managed, flexible, and scalable file storage system, with low latency access, for its Windows-based applications. Which AWS service is the right choice for the company?



Amazon FSx for Lustre



Amazon Elastic File System (Amazon EFS)



Amazon FSx for Windows File Server

(Correct)



Amazon Elastic Block Storage (Amazon EBS)

Explanation

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

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

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

Incorrect options:

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

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

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

Reference:

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

Question 5: **Incorrect**

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

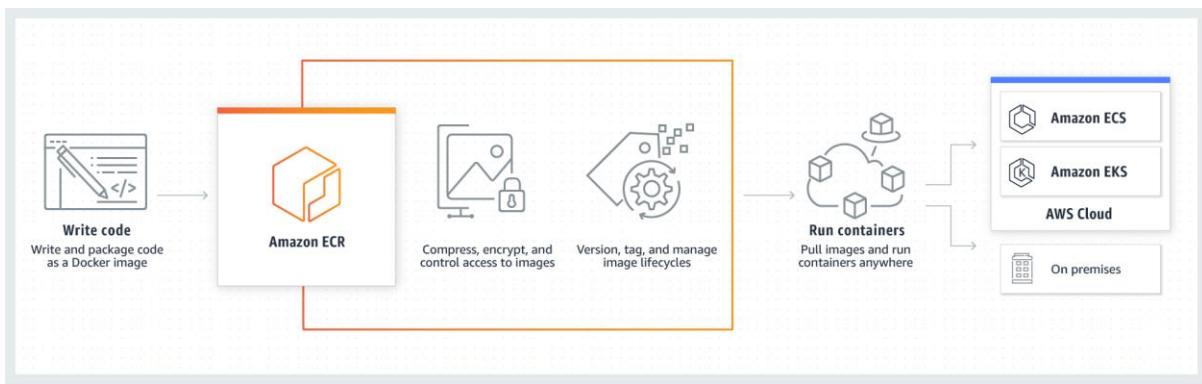
-
- Amazon Lambda**
-
- Amazon EC2**
-
- Amazon Elastic Container Registry (ECR)**
- (Correct)**
-
- Amazon Elastic Container Service (ECS)**
- (Incorrect)**

Explanation

Correct option:

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

Please see this schematic diagram to understand how ECR works:

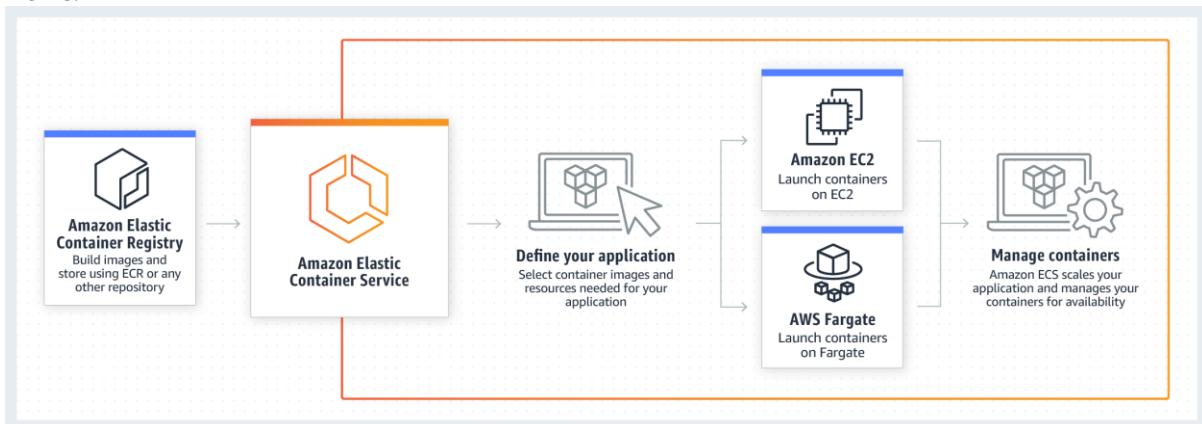


via - <https://aws.amazon.com/ecr/>

Incorrect options:

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

Please see this schematic diagram to understand how ECS works:



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

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

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

References:

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

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

Question 6: **Correct**

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

-

Scalability

-

Elasticity

-

Reliability

(Correct)

-

Cost Optimization

(Correct)

-

Availability

Explanation

Correct option:

Reliability

Cost Optimization

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

Incorrect options:

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

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

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

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

Reference:

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

Question 7: Correct

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

-

Enterprise

(Correct)

-

Developer

-

Business & Enterprise

-

Business

Explanation

Correct option:

"Enterprise"

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

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

Exam Alert:

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

	Developer	Business	Enterprise
	<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.

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

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

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

Question 8: **Correct**

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

-

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

(Correct)

-

Root user account password cannot be changed once it is set

-

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

-

Root user credentials should only be shared with managers requiring administrative responsibilities to complete their jobs

-

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

(Correct)

Explanation

Correct options:

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

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

The Email address and the password used for signing up for AWS services are the AWS account root user credentials. Root account, therefore, has full permissions on all AWS resources under that account. Restricting root account access is not possible. As a best practice, Multi-Factor Authentication (MFA) should be set on the root account. The root account password can be changed

after account creation. For all employees performing various administrative jobs, create individual user accounts using AWS IAM, and give administrative permissions as needed.

AWS Root Account Security Best Practices:

The AWS Account Root User

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

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

Important

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

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

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

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

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

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

Lock Away Your AWS Account Root User Access Keys

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

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

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

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

Incorrect options:

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

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

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

References:

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

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

Question 9: **Correct**

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

-

AWS Applicable Use Policy

-

AWS Fair Use Policy

-

AWS Trusted Advisor

-

AWS Acceptable Use Policy

(Correct)

Explanation

Correct option:

AWS Acceptable Use Policy

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

Incorrect options:

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

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

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

Reference:

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

Question 10: **Correct**

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

-

AWS OpsWorks

- AWS CloudFormation
 - AWS Cost Explorer
 - AWS Auto Scaling
- (Correct)**

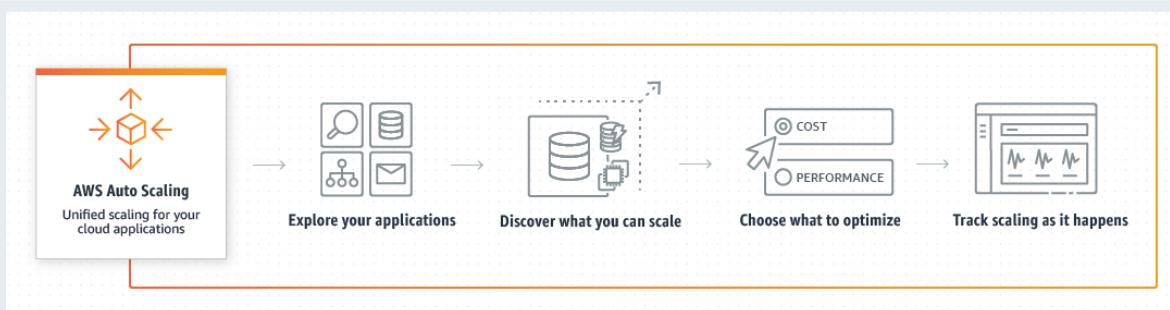
Explanation

Correct option: **AWS Auto Scaling**

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

How Auto Scaling

Works:



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

Incorrect options:

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

AWS OpsWorks - AWS OpsWorks is a configuration management service that provides managed instances of Chef and Puppet. Chef and Puppet are automation platforms that allow you to use code to automate the configurations of your servers. OpsWorks lets you use Chef and Puppet to automate how servers are configured, deployed and managed across your Amazon EC2 instances or on-premises compute environments. OpsWorks cannot auto-scale resources.

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

References:

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

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

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

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

Question 11: **Correct**

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

-
- **Enterprise**
-
- **Developer**
-
- **Business**
- **(Correct)**
-
- **Basic**

Explanation

Correct option:

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

A basic support plan is included for all AWS customers.

Business - AWS recommends Business Support if you have production workloads on AWS and want 24x7 phone, email and chat access to technical support and architectural guidance in the context of your specific use-cases. Enterprise Support plan also provides 24x7 phone, email and chat access to technical support however it's much costlier than Business Support plan. Developer plan does not provide 24x7 phone based technical support. Therefore Business Support plan is the correct option for the given use-case.

Exam Alert:

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

	Developer	Business	Enterprise
	<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:

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

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

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

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

Reference:

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

Question 12: **Correct**

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



Elasticity

(Correct)



Durability



Reliability



Resiliency

Explanation

Correct option: **Elasticity**

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

What is
Elasticity:

Elasticity

With cloud computing, you don't have to over-provision resources up front to handle peak levels of business activity in the future. Instead, you provision the amount of resources that you actually need. You can scale these resources up or down to instantly to grow and shrink capacity as your business needs change.



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

Incorrect options:

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

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

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

References:

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

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

Question 13: **Incorrect**

Which of the following AWS services are part of the AWS Foundation services for the Reliability pillar of the Well-Architected Framework in AWS Cloud? (Select two)

-

AWS Service Quotas

(Correct)

-

AWS CloudFormation

-

AWS Trusted Advisor

(Correct)

-

Amazon CloudWatch

(Incorrect)

-

AWS CloudTrail

Explanation

Correct options:

AWS Trusted Advisor

AWS Service Quotas

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

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

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

Incorrect options:

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

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

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

Reference:

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

Question 14: **Correct**

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



Amazon S3



EC2 Instance Store



Elastic Block Store (EBS) Volume



Elastic File System (EFS)

(Correct)

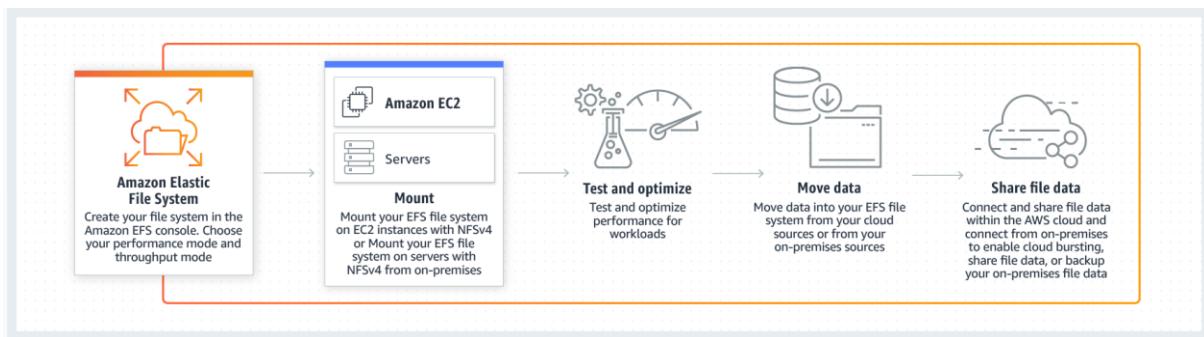
Explanation

Correct option:

Elastic File System (EFS)

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

How EFS
Works:



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

Incorrect options:

Elastic Block Store (EBS) Volume - Amazon Elastic Block Store (EBS) is an easy to use, high-performance block storage service designed for use with Amazon Elastic Compute Cloud (EC2) for both throughput and transaction-intensive workloads at any scale. A broad range of workloads, such as relational and non-relational databases, enterprise applications, containerized applications, big data analytics engines, file systems, and media workflows are widely deployed on Amazon EBS. An EBS can only be mounted to one EC2 instance at a time, so this option is not correct for the given use-case.

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

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

Reference:

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

Question 15: **Correct**

Which tool will help you review your workloads against current AWS best practices for cost optimization, security, and performance improvement and then obtain advice to architect them better?

- ○

AWS Cost Explorer

- ○

Amazon Inspector

-

AWS Trusted Advisor

(Correct)

-

Amazon CloudWatch

Explanation

Correct option: **AWS Trusted Advisor**

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

How Trusted Advisor

Works:



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

AWS Trusted Advisor

Recommendations:

Like your customized cloud expert, AWS Trusted Advisor analyzes your AWS environment and provides best practice recommendations in five categories:



Core Checks & Recommendations

All AWS customers get access to the seven core Trusted Advisor checks to help increase the security and performance of the AWS environment. Checks include:

Security

- S3 Bucket Permissions
- Security Groups - Specific Ports Unrestricted
- IAM Use
- MFA on Root Account
- EBS Public Snapshots
- RDS Public Snapshots

Service Limits

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

Incorrect options:

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

Amazon CloudWatch - Amazon CloudWatch is a monitoring and observability service built for DevOps engineers, developers, site reliability engineers (SREs), and IT managers. CloudWatch provides data and actionable insights to monitor applications, respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health. This is an excellent service for building Resilient systems. Think resource performance monitoring, events, and alerts; think CloudWatch. CloudWatch does not offer any recommendations vis-a-vis AWS best practices for cost optimization, security, and performance improvement.

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

Reference:

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

Question 16: **Correct**

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

-

SNS

(Correct)

-

Lambda

-

CloudTrail

-

CloudWatch

(Correct)

-

SQS

Explanation

Correct options:

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

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

How SNS Works:



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

Incorrect options:

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

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

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

References:

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

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

Question 17: **Correct**

What are the fundamental drivers of cost with AWS Cloud?

-

Compute, Databases and Outbound Data Transfer

-

Compute, Storage and Outbound Data Transfer

(Correct)

-

Compute, Databases and Inbound Data Transfer

-

Compute, Storage and Inbound Data Transfer

Explanation

Correct options:

Compute, Storage and Outbound Data Transfer

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

AWS Cloud Pricing

Fundamentals:

Understand the fundamentals of pricing

There are three fundamental drivers of cost with AWS: compute, storage, and outbound data transfer. These characteristics vary somewhat, depending on the AWS product and pricing model you choose.

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

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

Incorrect options:

Compute, Storage and Inbound Data Transfer

Compute, Databases and Outbound Data Transfer

Compute, Databases and Inbound Data Transfer

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

Reference:

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

Question 18: **Correct**

An IT company wants to run a log backup process every Monday at 2 AM. The usual runtime of the process is 5 minutes. As a Cloud Practitioner, which AWS services would you recommend to build a serverless solution for this use-case? (Select two)

-

EC2 Instance

-

Systems Manager

-

Lambda

(Correct)

-

Step Function

-

CloudWatch

(Correct)

Explanation

Correct option:

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

Lambda - AWS Lambda lets you run code without provisioning or managing servers. You pay only for the compute time you consume. The lambda has a maximum execution time of 15 minutes, so it can be used to run this log backup process.

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

Incorrect options:

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

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

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

Reference:

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

Question 19: **Correct**

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

-

Amazon Kinesis Data Stream

-

Amazon Simple Queue Service (SQS)

-

Amazon Simple Notification Service (SNS)

-

Amazon MQ

(Correct)

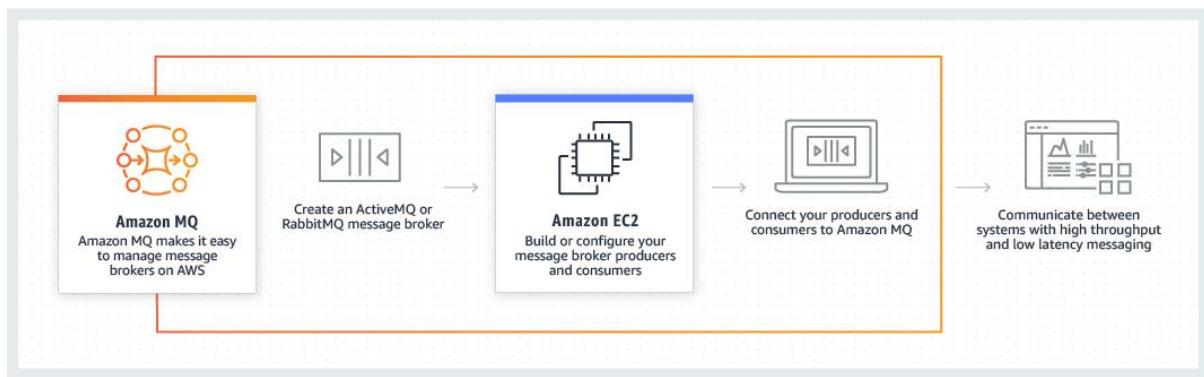
Explanation

Correct option:

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

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

How MQ
works:



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

Incorrect options:

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

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

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

Reference:

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

Question 20: **Correct**

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

-

Performance Efficiency

-

Vertical Scaling

-

Horizontal Scaling

-
-

High Availability

(Correct)

Explanation

Correct option:

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

Incorrect options:

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

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

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

References:

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

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

Question 21: **Correct**

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

-
-

Allows unlimited contacts to open unlimited cases

-
-

Allows one contact to open unlimited cases

(Correct)

-
- **Allows unlimited contacts to open a limited number of cases per month**
-

Allows one contact to open a limited number of cases per month

Explanation

Correct option:

Allows one contact to open unlimited cases

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

Incorrect options:

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

Allows unlimited contacts to open unlimited cases - This is supported by AWS "Business" and "Enterprise" Support plans. So this is incorrect for AWS "Developer" Support plan.

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

Reference:

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

Question 22: **Correct**

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

-

Amazon CloudFront

(Correct)

-

Amazon S3

-

AWS Identity and Access Management (IAM)

(Correct)

-

Amazon Relational Database Service (Amazon RDS)

-

Amazon Elastic Compute Cloud (Amazon EC2)

Explanation

Correct options:

AWS Identity and Access Management (IAM)

Amazon CloudFront

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

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

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

Incorrect options:

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

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

Exam Alert:

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

References:

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

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

Question 23: **Correct**

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

-

AWS WAF

(Correct)

-

AWS Shield

-

Route 53

(Correct)

-

AWS Protect

-

CloudWatch

Explanation

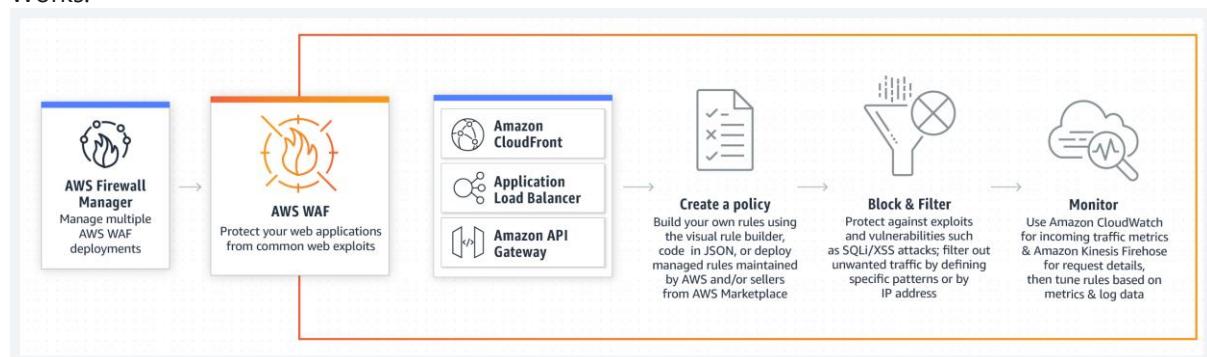
Correct options:

AWS WAF

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

How WAF

Works:



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

Route 53

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

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

Incorrect options:

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

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

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

References:

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

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

Question 24: **Incorrect**

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

- Edge Location Management**
(Correct)
- Server-side Encryption**
- Customer Data**
- Identity and Access Management**
(Incorrect)

Explanation

Correct option:

Edge Location Management

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

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

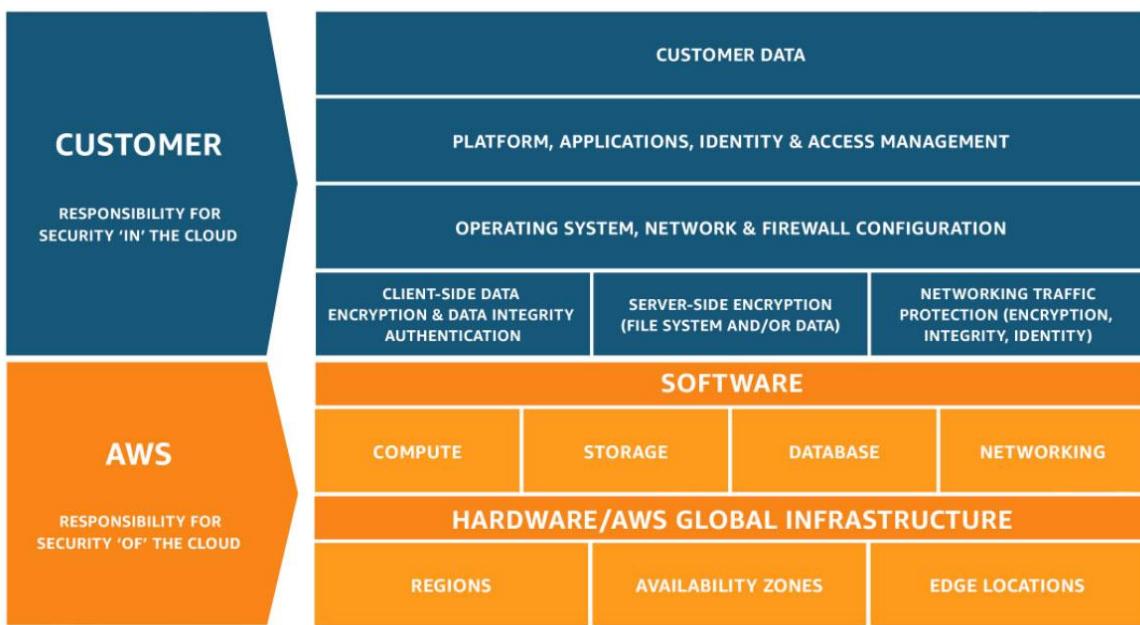
Incorrect options:

Customer Data**Identity and Access Management****Server-side Encryption**

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

Exam Alert:

Please review the Shared Responsibility Model in detail as you can expect multiple questions on the shared responsibility model in the exam:



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

Reference:

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

Question 25: **Correct**

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

-

Use S3 Standard to store the thumbnails

-

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

-

Use S3 Glacier to store the thumbnails

-

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

(Correct)

Explanation

Correct option:

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

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

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

Exam Alert:

Please review this detailed comparison on S3 Storage Classes as you can expect a few questions on this aspect of

S3:

Performance across the S3 Storage Classes

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

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

Incorrect options:

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

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

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

Reference:

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

Question 26: **Correct**

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

- IAM Role**
- IAM User**
- IAM Group**
- AWS Policy**

Explanation

Correct option: **IAM User**

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

Incorrect options:

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

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

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

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

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

Question 27: **Correct**

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

-

Multi-AZ reduces database usage costs

-

Multi-AZ enhances database availability

(Correct)

-

Multi-AZ protects the database from a regional failure

-

Multi-AZ improves database performance for read-heavy workloads

Explanation

Correct option:

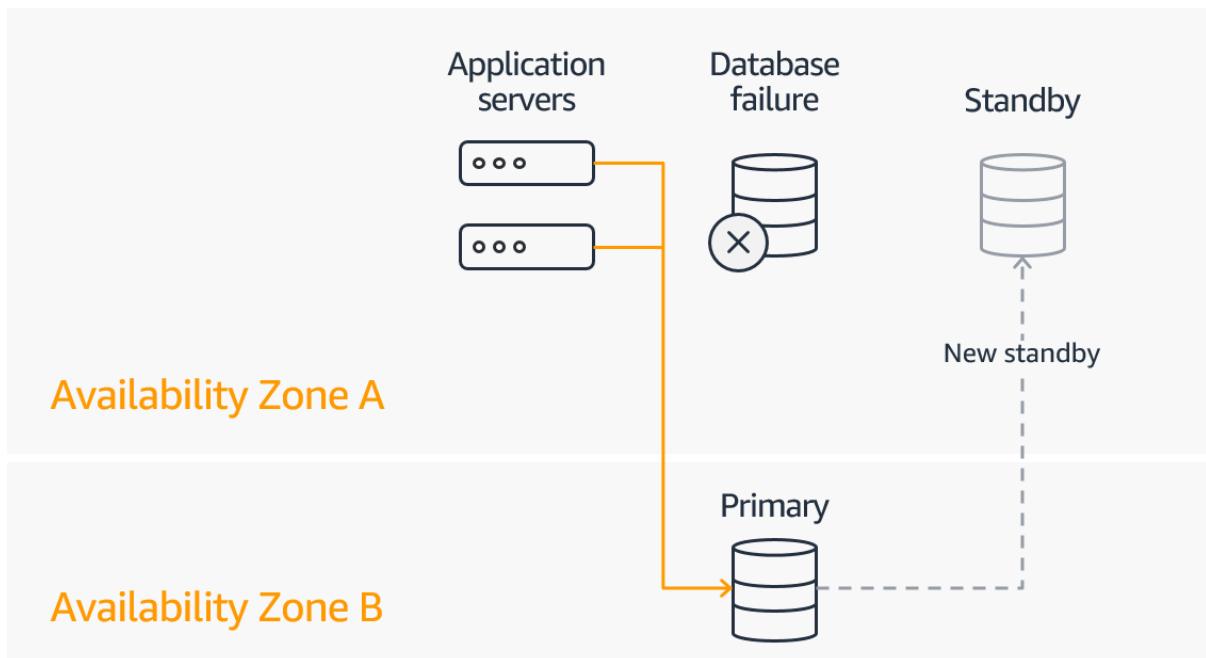
Multi-AZ enhances database availability

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

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

How Multi-AZ

Works:



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

Exam Alert:

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

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

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

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

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

Incorrect options:

Multi-AZ improves database performance for read-heavy workloads - Read Replicas allow you to create read-only copies that are synchronized with your master database. Read Replicas are used for improved read performance. Therefore, this option is incorrect.

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

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

Reference:

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

Question 28: **Correct**

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

-

AWS Service Catalog

(Correct)

-

Amazon CloudWatch

-

AWS Organizations

-

AWS CloudTrail

-

AWS Partner Network

(Correct)

Explanation

Correct options:

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

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

Incorrect options:

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

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

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

References:

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

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

Question 29: **Correct**

An organization deploys its IT infrastructure in a combination of its on-premises data center along with AWS Cloud. How would you categorize this deployment model?

-

Cloud deployment

-

Hybrid deployment

(Correct)

-

Mixed deployment

-

Private deployment

Explanation

Correct option:

Hybrid deployment

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

Overview of Cloud Computing Deployment Models

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:

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

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

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

References:

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

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

Question 30: **Correct**

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

- AWS VPN
(Correct)
- Amazon Route 53
- AWS Direct Connect
(Correct)
- Internet Gateway

Amazon VPC

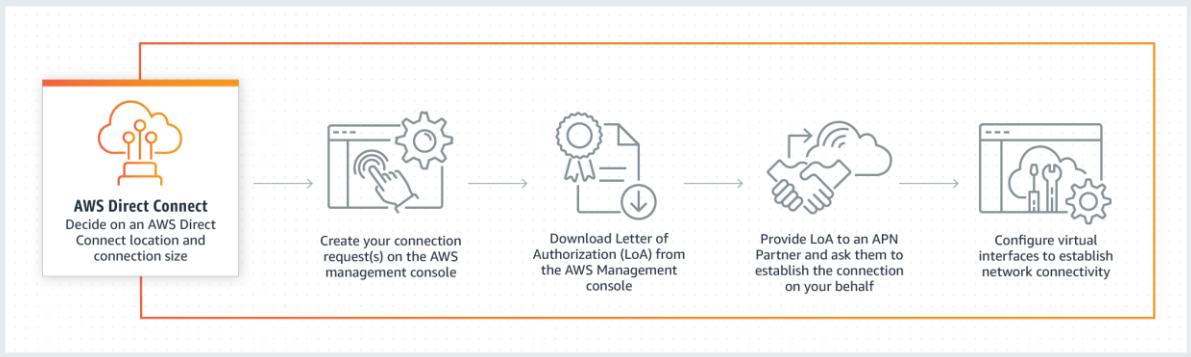
Explanation

Correct options:

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

How AWS Direct Connect

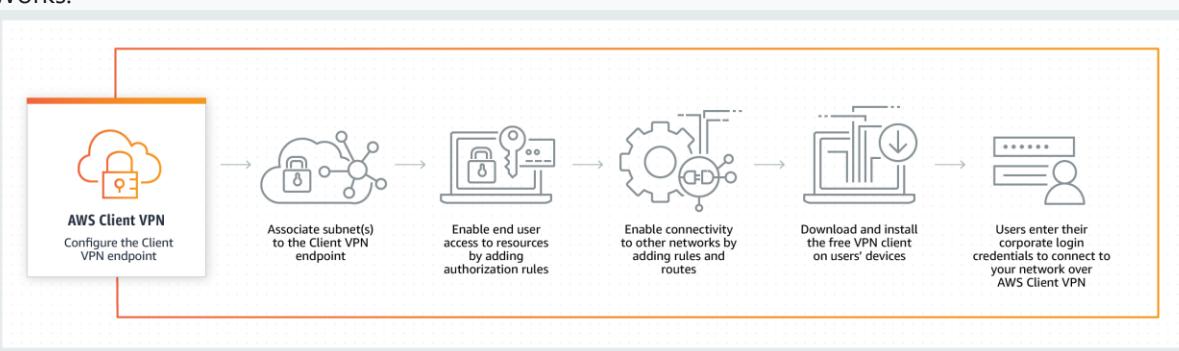
Works:



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

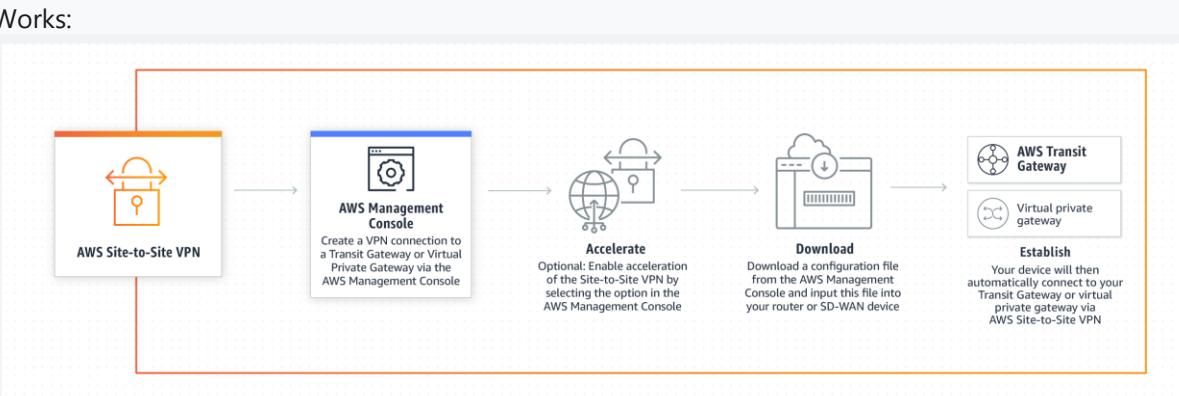
AWS VPN - AWS Virtual Private Network (VPN) solutions establish secure connections between on-premises networks, remote offices, client devices, and the AWS global network. AWS VPN is comprised of two services: AWS Site-to-Site VPN and AWS Client VPN. Together, they deliver a highly-available, managed,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

How AWS Client VPN Works:



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

How AWS Site-to-Site VPN Works:



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

Incorrect options:

Amazon VPC - Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including the selection of your IP address range, creation of subnets, and configuration of route tables and network gateways. You cannot use Amazon VPC to connect your on-premises network with AWS Cloud.

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

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

References:

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

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

Question 31: **Correct**

An e-commerce company wants to assess its applications deployed on EC2 instances for vulnerabilities and deviations from AWS best practices. Which AWS service can be used to facilitate this?



AWS CloudHSM



Amazon Inspector

(Correct)



AWS Trusted Advisor



AWS Secrets Manager

Explanation

Correct option:

Amazon Inspector

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

Overview of Amazon Inspector:

IDENTIFY APPLICATION SECURITY ISSUES

Amazon Inspector helps you to identify security vulnerabilities as well as deviations from security best practices in applications, both before they are deployed, and while they are running in a production environment. This helps improve the overall security posture of your applications deployed on AWS.

INTEGRATE SECURITY INTO DEVOPS

Amazon Inspector is an API-driven service that analyzes network configurations in your AWS account and uses an optional agent for visibility into your Amazon EC2 instances. This makes it easy for you to build Inspector assessments right into your existing DevOps process, decentralizing and automating vulnerability assessments, and empowering your development and operations teams to make security assessments an integral part of the deployment process.

INCREASE DEVELOPMENT AGILITY

Amazon Inspector helps you reduce the risk of introducing security issues during development and deployment by automating the security assessment of your applications and proactively identifying vulnerabilities. This allows you to develop and iterate on new applications quickly and assess compliance with best practices and policies.

LEVERAGE AWS SECURITY EXPERTISE

The AWS security organization is continuously assessing the AWS environment and updating a knowledge base of security best practices and rules. Amazon Inspector makes this expertise available to you in the form of a service that simplifies the process of establishing and enforcing best practices within your AWS environment.

STREAMLINE SECURITY COMPLIANCE

Amazon Inspector gives security teams and auditors visibility into the security testing that is being performed during development of applications on AWS. This streamlines the process of validating and demonstrating that security and compliance standards and best practices are being followed throughout the development process.

ENFORCE SECURITY STANDARDS

Amazon Inspector allows you to define standards and best practices for your applications and validate adherence to these standards. This simplifies enforcement of your organization's security standards and best practices, and helps to proactively manage security issues before they impact your production application.

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

Incorrect options:

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

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

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

Reference:

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

Question 32: **Correct**

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

-
-

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

-
-

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

(Correct)

-
-

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

-
-

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

Explanation

Correct option:

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

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

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

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

Incorrect options:

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

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

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

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

References:

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

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

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

Question 33: **Correct**

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

-

Configuration management for AWS global infrastructure

-

Managing patches of the guest operating system on Amazon EC2

(Correct)

-

Patching/fixing flaws within the AWS infrastructure

-

Availability Zone infrastructure management

Explanation

Correct option:

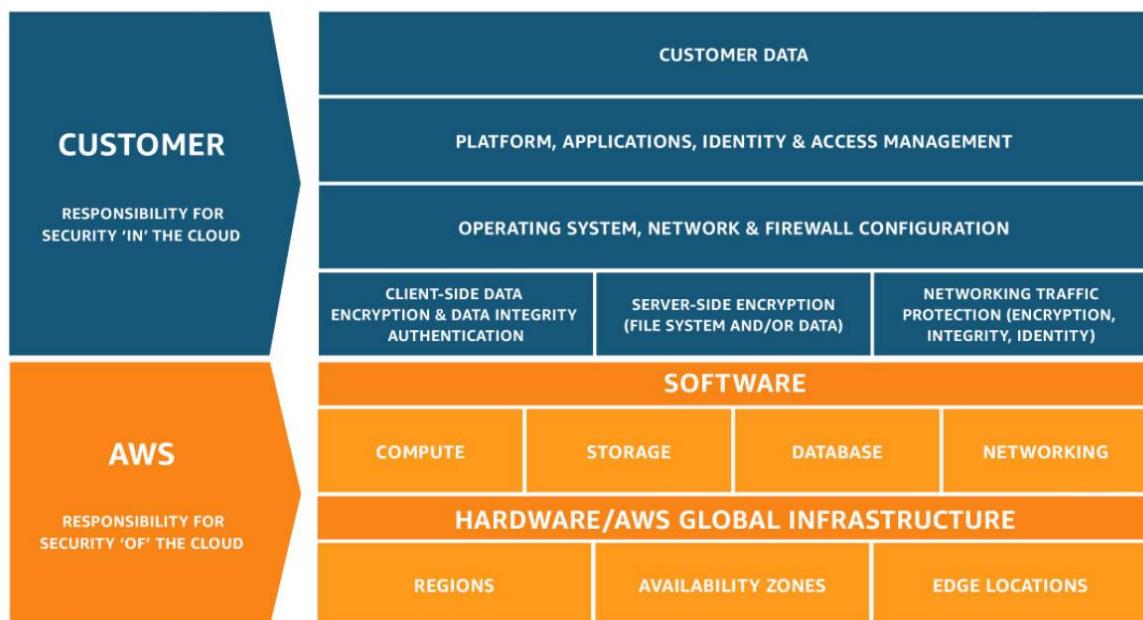
Managing patches of the guest operating system on Amazon EC2

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

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

Exam Alert:

Please review the Shared Responsibility Model in detail as you can expect multiple questions on the shared responsibility model in the exam:



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

Incorrect options:

Configuration management for AWS global infrastructure

Availability Zone infrastructure management

Patching/fixing flaws within the AWS infrastructure

AWS is responsible for "Security of the Cloud". AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services. Hence, all of the above options -

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

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

Question 34: **Correct**

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



Amazon Elastic Compute Cloud (Amazon EC2)



Amazon Elastic Container Service - EC2 launch type



Amazon Elastic Container Service - Fargate launch type

(Correct)



AWS Lambda

Explanation

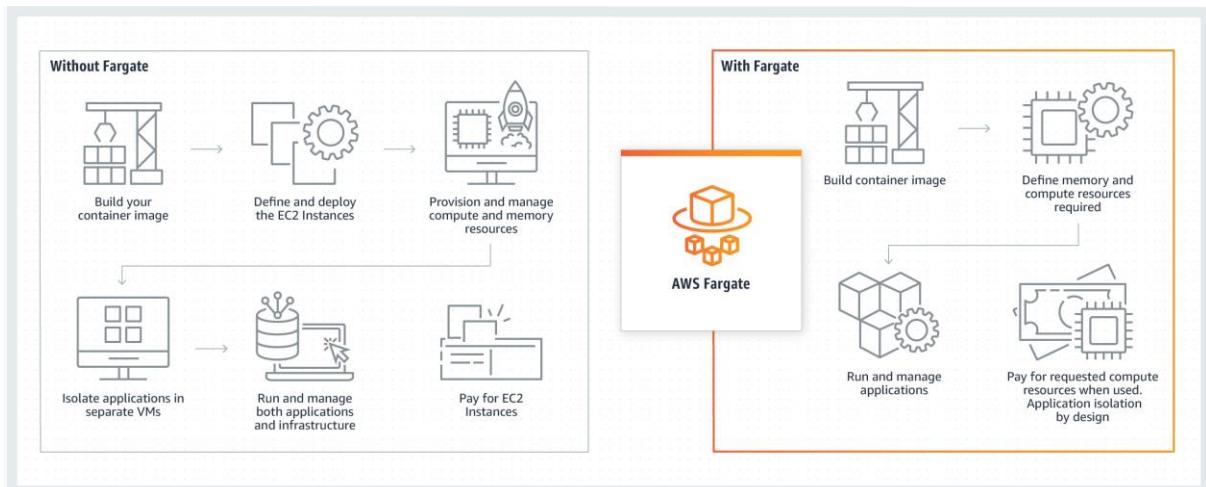
Correct option:

Amazon Elastic Container Service - Fargate launch type

AWS Fargate is a serverless compute engine for containers. It works with both Amazon Elastic Container Service (ECS) and Amazon Elastic Kubernetes Service (EKS). Fargate makes it easy for you to focus on building your applications. Fargate removes the need to provision and manage servers, lets you specify and pay for resources per application, and improves security through application isolation by design. Fargate allocates the right amount of compute, eliminating the need to choose instances and scale cluster capacity. You only pay for the resources required to run your containers, so there is no over-provisioning and paying for additional servers. Fargate runs each task or pod in its kernel providing the tasks and pods their own isolated compute environment. This enables your application to have workload isolation and improved security by design.

How Fargate

Works:



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

Incorrect options:

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

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

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

Reference:

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

Question 35: **Incorrect**

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

-

Applying patches to the RDS database

-

Database encryption

(Correct)

-

Applying patches to the underlying OS

(Incorrect)

-

Managing the underlying server hardware on which RDS runs

Explanation

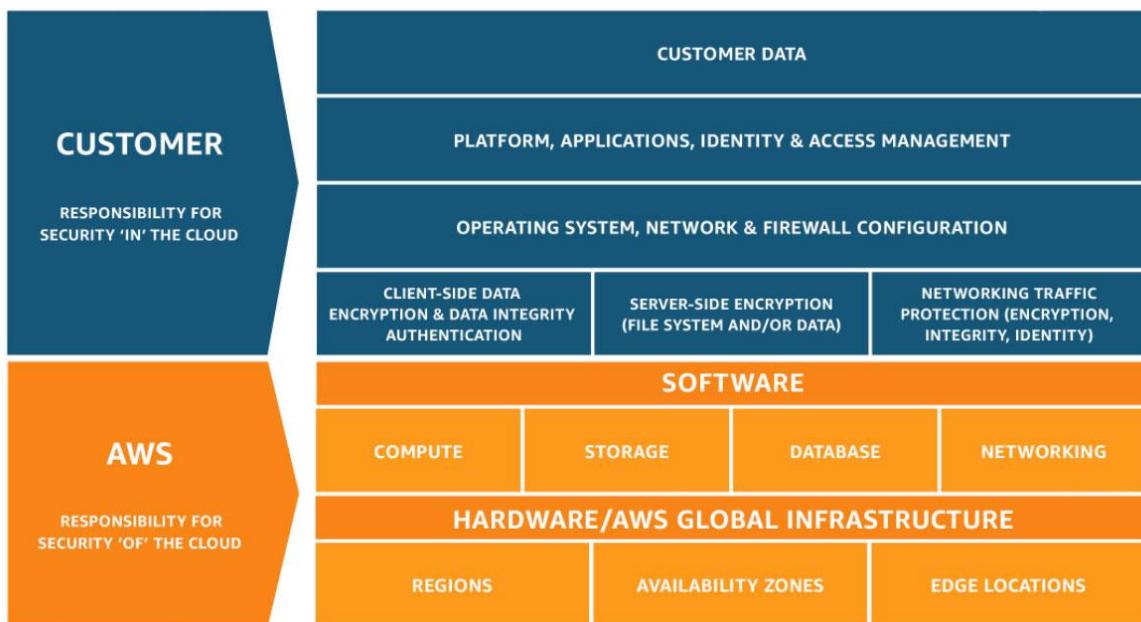
Correct option:

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

Database encryption - Under the shared model, customers are responsible for managing their data, including data encryption.

Shared Responsibility Model

Overview:



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

Incorrect options:

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

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

Managing the underlying server hardware on which RDS runs - Since RDS is a managed service, the underlying infrastructure is the responsibility of AWS.

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

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

Reference:

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

Question 36: **Correct**

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



Latency routing policy

(Correct)



Simple routing policy



Failover routing policy



Weighted routing policy

Explanation

Correct option:

Latency routing policy

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

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

Choosing a routing policy

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

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

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

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

Incorrect options:

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

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

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

Reference:

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

Question 37: **Correct**

AWS Compute Optimizer delivers recommendations for which of the following AWS resources? (Select two)

-

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

-

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

-

Amazon EC2 instances, Amazon EC2 Auto Scaling groups

(Correct)

-

Amazon EBS volumes, AWS Lambda functions

(Correct)

-

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

Explanation

Correct options:

Amazon EC2 instances, Amazon EC2 Auto Scaling groups

Amazon EBS volumes, AWS Lambda functions

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

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

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

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

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

Incorrect options:

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

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

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

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

Reference:

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

Question 38: **Correct**

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



Amazon EMR

(Correct)



AWS Step Function



Amazon EC2



AWS Batch

Explanation

Correct option:

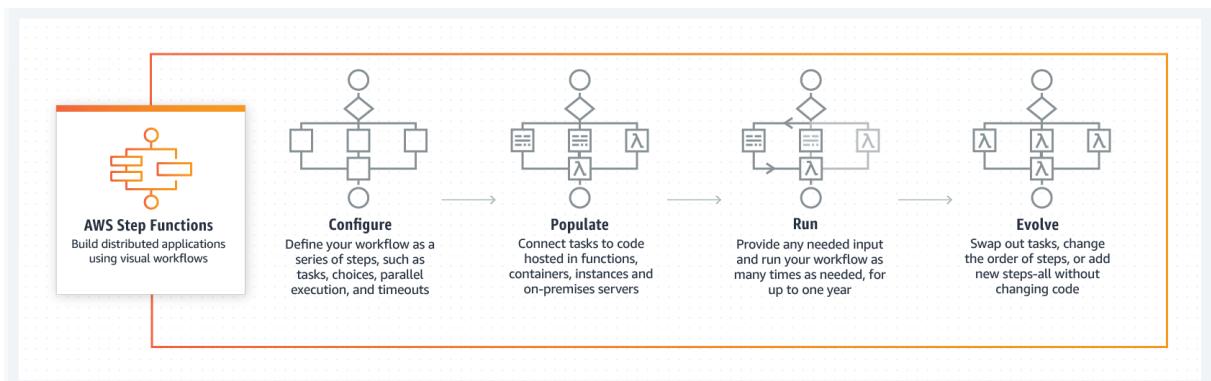
Amazon EMR - Amazon EMR is the industry-leading cloud big data platform for processing vast amounts of data using open source tools such as Hadoop, Apache Spark, Apache Hive, Apache HBase, Apache Flink, Apache Hudi, and Presto. Amazon EMR can be used to provision resources to run big data workloads on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

Incorrect options:

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

AWS Step Functions

Overview:



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

AWS Batch

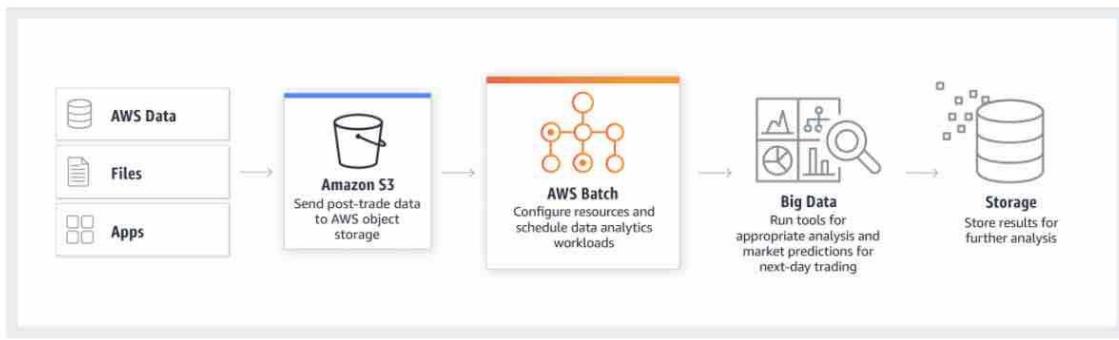
You can use AWS Batch to plan, schedule and execute your batch computing workloads across the full range of AWS compute services. AWS Batch dynamically provisions the optimal quantity and type of compute resources (e.g., CPU or memory optimized instances) based on the volume and specific resource requirements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

Please review the common use-cases for AWS Batch:

Use cases

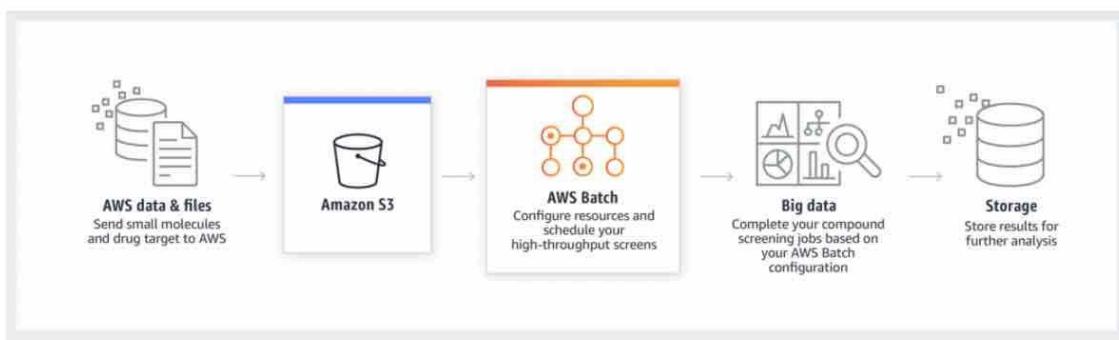
Financial services: Post-trade analytics

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



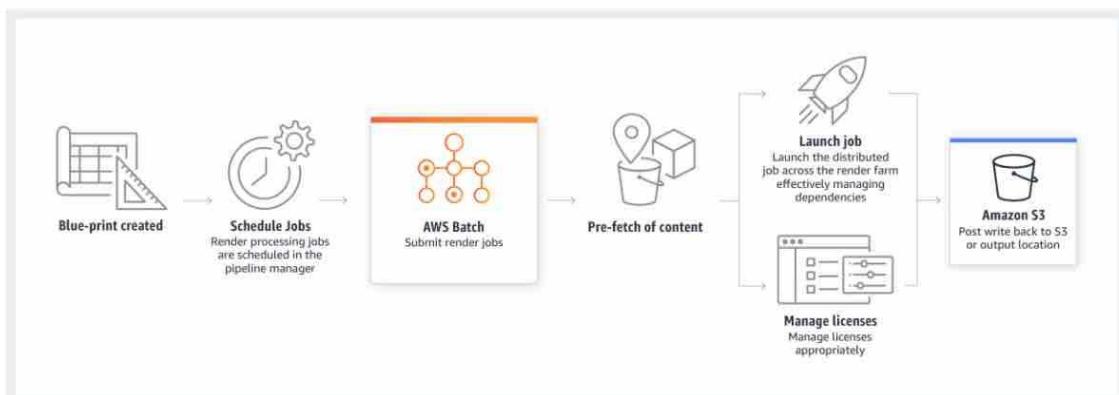
Life sciences: Drug screening for biopharma

Rapidly search libraries of small molecules for drug discovery.



Digital media: Visual effects rendering

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



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

Exam Alert:

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

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

References:

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

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

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

Question 39: **Correct**

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

-

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

(Correct)

-

Security Group acts as a firewall at the VPC level whereas Network Access Control List acts as a firewall at the AZ level

-

Security Group acts as a firewall at the AZ level whereas Network Access Control List acts as a firewall at the VPC level

-

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

Explanation

Correct option:

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

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

Security Group

Overview:

Security group basics

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

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

 **Note**

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

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

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

Network Access Control List (NACL)

Overview:

Network ACL basics

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

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

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

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

Incorrect options:

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

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

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

References:

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

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

Question 40: **Correct**

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



Only outbound data transfer is charged

(Correct)

-

Neither inbound nor outbound data transfer are charged

-

Only inbound data transfer is charged

-

Both inbound data transfer and outbound data transfer are charged

Explanation

Correct option:

Only outbound data transfer is charged

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

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

Incorrect options:

Only inbound data transfer is charged

Both inbound data transfer and outbound data transfer are charged

Neither inbound nor outbound data transfer are charged

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

Reference:

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

Question 41: **Correct**

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

-

Modify an EC2 instance type from t2.nano to u-12tb1.metal

-

Add a bigger CPU to a computer

-

Read Replicas in Amazon RDS

(Correct)

-

Modify a Database instance to higher CPU and RAM

-

Elastic Load Balancing

(Correct)

Explanation

Correct options: **Elastic Load Balancing**

Read Replicas in Amazon RDS

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

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

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

Incorrect options:

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

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

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

Reference:

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

Question 42: **Correct**

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



AWS Identity and Access Management (IAM)

(Correct)



Amazon CloudWatch



AWS WAF



AWS Shield

Explanation

Correct option:

AWS Identity and Access Management (IAM)

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

Incorrect options:

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

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

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

Reference:

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

Question 43: **Correct**

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

- **Elastic Compute Cloud (Amazon EC2)**
- **DynamoDB**
- **AWS Auto Scaling**
(Correct)
- **Simple Storage Service (Amazon S3)**
- **Identity and Access Management (IAM)**
(Correct)

Explanation

Correct options:

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

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

Incorrect options:

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

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

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

References:

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

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

Question 44: **Correct**

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



AWS CloudTrail



AWS Config

(Correct)



AWS CloudFormation



AWS Service Catalog

Explanation

Correct option:

AWS Config

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

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

Incorrect options:

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

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

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

Reference:

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

Question 45: **Correct**

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

-

AWS Organizations

(Correct)

-

AWS Budgets

-

AWS Secrets Manager

-

AWS Cost Explorer

Explanation

Correct option:

AWS Organizations

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

Key Features of AWS Organizations:

CENTRALLY MANAGE POLICIES ACROSS MULTIPLE AWS ACCOUNTS

To improve control over your AWS environment, you can use AWS Organizations to create groups of accounts, and then attach policies to a group to ensure the correct policies are applied across the accounts without requiring custom scripts and manual processes.

GOVERN ACCESS TO AWS SERVICES, RESOURCES, AND REGIONS

AWS Organizations allows you to restrict what services and actions are allowed in your accounts. You can use Service Control Policies (SCPs) to apply permission guardrails on AWS Identity and Access Management (IAM) users and roles. For example, you can apply an SCP that restricts users in accounts in your organization from launching any resources in regions that you do not explicitly allow.

AUTOMATE AWS ACCOUNT CREATION AND MANAGEMENT

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. For example, you can automate the creation of new accounts for workload or application isolation and grant entities in those accounts access only to the necessary AWS services.

CONFIGURE AWS SERVICES ACROSS MULTIPLE ACCOUNTS

AWS Organizations helps you configure AWS services and share resources across accounts in your organization. For example, Organizations integrates with AWS Single Sign-on to enable you to easily provision access for all of your developers to accounts in your organization from a single place. You can make central changes to access permissions and have them automatically updated on accounts in your organization.

CONSOLIDATE BILLING ACROSS MULTIPLE AWS ACCOUNTS

You can use AWS Organizations to set up a single payment method for all the AWS accounts in your organization through consolidated billing. With consolidated billing, you can see a combined view of charges incurred by all your accounts, as well as take advantage of pricing benefits from aggregated usage, such as volume discounts for Amazon EC2 and Amazon S3.

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

Incorrect options:

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

understanding of your cost trends. You cannot use Cost Explorer to set up consolidated billing and a single payment method for multiple AWS accounts.

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

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

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

Question 46: **Correct**

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

-
-

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

(Correct)

-
-

You can automatically remove unhealthy instances

-
-

You can scale out and add more EC2 instances to match an increase in demand as well as scale in and remove EC2 instances to match a reduced demand

-
-

You can automatically register new instances to a Load Balancer

Explanation

Correct option:

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

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

Incorrect options:

AWS Auto Scaling monitors your applications and automatically adjusts the capacity to maintain steady, predictable performance at the lowest possible cost. Using AWS Auto Scaling, it's easy to

setup application scaling for multiple resources across multiple services in minutes. The service provides a simple, powerful user interface that lets you build scaling plans for resources including Amazon EC2 instances and Spot Fleets, Amazon ECS tasks, Amazon DynamoDB tables and indexes, and Amazon Aurora Replicas.

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

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

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

Reference:

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

Question 47: **Correct**

A data analytics company has some data stored on Amazon S3 and wants to do SQL based analysis on this data with minimum effort. As a Cloud Practitioner, which of the following AWS services will you suggest for this use case?

-

Amazon Aurora

-

DynamoDB

-

Redshift

-

Amazon Athena

(Correct)

Explanation

Correct option:

Amazon Athena

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

Key features of Amazon Athena:

Start querying instantly	Pay per query
Serverless, no ETL Athena is serverless. You can quickly query your data without having to setup and manage any servers or data warehouses. Just point to your data in Amazon S3, define the schema, and start querying using the built-in query editor. Amazon Athena allows you to tap into all your data in S3 without the need to set up complex processes to extract, transform, and load the data (ETL).	Only pay for data scanned With Amazon Athena, you pay only for the queries that you run. You are charged \$5 per terabyte scanned by your queries. You can save from 30% to 90% on your per-query costs and get better performance by compressing, partitioning, and converting your data into columnar formats. Athena queries data directly in Amazon S3. There are no additional storage charges beyond S3.
Open, powerful, standard	Fast, really fast
Built on Presto, runs standard SQL Amazon Athena uses Presto with ANSI SQL support and works with a variety of standard data formats, including CSV, JSON, ORC, Avro, and Parquet. Athena is ideal for quick, ad-hoc querying but it can also handle complex analysis, including large joins, window functions, and arrays. Amazon Athena is highly available; and executes queries using compute resources across multiple facilities and multiple devices in each facility. Amazon Athena uses Amazon S3 as its underlying data store, making your data highly available and durable.	Interactive performance even for large datasets With Amazon Athena, you don't have to worry about having enough compute resources to get fast, interactive query performance. Amazon Athena automatically executes queries in parallel, so most results come back within seconds.

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

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

Incorrect options:

Amazon Aurora - Amazon Aurora is a MySQL and PostgreSQL-compatible relational database built for the cloud, that combines the performance and availability of traditional enterprise databases with the simplicity and cost-effectiveness of open source databases. You cannot use Aurora for SQL analysis on S3 based data.

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

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

Reference:

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

Question 48: **Correct**

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



Amazon CloudFront

- -
- Amazon Route 53**
- -
- Elastic Load Balancer**
- -
- Global Accelerator**
- (Correct)**

Explanation

Correct option:

Global Accelerator

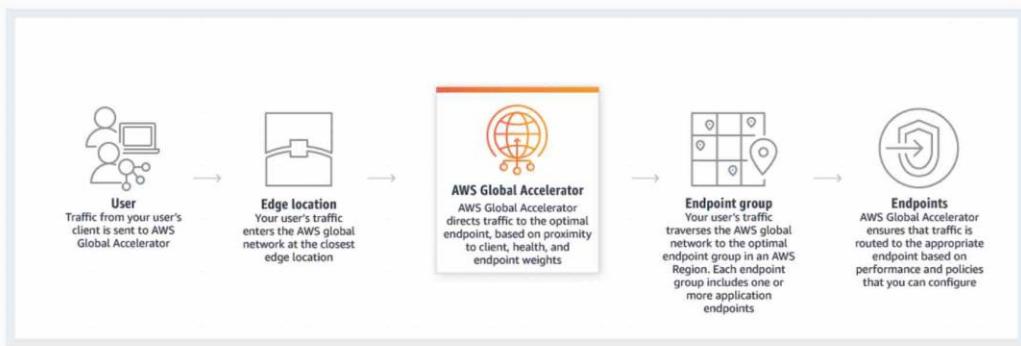
AWS Global Accelerator is a service that improves the availability and performance of your applications with local or global users. It provides static IP addresses that act as a fixed entry point to your application endpoints in a single or multiple AWS Regions, such as your Application Load Balancers,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

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

How Global Accelerator

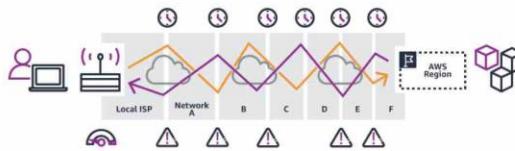
Works:

How it works



Directly access web applications

Without AWS Global Accelerator



It can take many networks to reach the application. Paths to and from the application may differ. Each hop impacts performance and can introduce risks.

With AWS Global Accelerator



Adding AWS Global Accelerator removes these inefficiencies. It leverages the Global AWS Network, resulting in improved performance.

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

Exam Alert:

Please review the differences between CloudFront and Global Accelerator:

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

A: AWS Global Accelerator and Amazon CloudFront are separate services that use the AWS global network and its edge locations around the world. CloudFront improves performance for both cacheable content (such as images and videos) and dynamic content (such as API acceleration and dynamic site delivery). Global Accelerator improves performance for a wide range of applications over TCP or UDP by proxying packets at the edge to applications running in one or more AWS Regions. Global Accelerator is a good fit for non-HTTP use cases, such as gaming (UDP), IoT (MQTT), or Voice over IP, as well as for HTTP use cases that specifically require static IP addresses or deterministic, fast regional failover. Both services integrate with AWS Shield for DDoS protection.

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

Incorrect options:

Amazon CloudFront - Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a developer-friendly environment. CloudFront cannot be used to improve application availability and performance using the AWS global network.

Elastic Load Balancer - Elastic Load Balancer distributes incoming application or network traffic across multiple targets, such as Amazon EC2 instances, containers, and IP addresses, in multiple Availability Zones. Elastic Load Balancing scales your load balancer as traffic to your application

changes over time. It can automatically scale to the vast majority of workloads. Elastic Load Balancer cannot be used to improve application availability and performance using the AWS global network.

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

Reference:

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

Question 49: **Correct**

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

Which tool/service will help you achieve this requirement?

-

AWS Systems Manager Session Manager

(Correct)

-

Amazon Inspector

-

Amazon EC2 Instance Connect

-

Amazon Route 53

Explanation

Correct option:

AWS Systems Manager Session Manager

AWS SSM Session Manager is a fully-managed service that provides you with an interactive browser-based shell and CLI experience. It helps provide secure and auditable instance management without the need to open inbound ports, maintain bastion hosts, and manage SSH keys. Session Manager helps to enable compliance with corporate policies that require controlled access to instances, increase security and auditability of access to the instances while providing simplicity and cross-platform instance access to end-users.

Incorrect options:

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

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

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

Reference:

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

Question 50: **Correct**

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



AWS Elastic Beanstalk

(Correct)



AWS CloudFormation



Amazon EC2



AWS Elastic Container Service (ECS)

Explanation

Correct option:

AWS Elastic Beanstalk

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

Key Benefits of Elastic Beanstalk:

Fast and simple to begin

Elastic Beanstalk is the fastest and simplest way to deploy your application on AWS. You simply use the AWS Management Console, a Git repository, or an integrated development environment (IDE) such as Eclipse or Visual Studio to upload your application, and Elastic Beanstalk automatically handles the deployment details of capacity provisioning, load balancing, auto-scaling, and application health monitoring. Within minutes, your application will be ready to use without any infrastructure or resource configuration work on your part.

Impossible to outgrow

Elastic Beanstalk automatically scales your application up and down based on your application's specific need using easily adjustable Auto Scaling settings. For example, you can use CPU utilization metrics to trigger Auto Scaling actions. With Elastic Beanstalk, your application can handle peaks in workload or traffic while minimizing your costs.

Developer productivity

Elastic Beanstalk provisions and operates the infrastructure and manages the application stack (platform) for you, so you don't have to spend the time or develop the expertise. It will also keep the underlying platform running your application up-to-date with the latest patches and updates. Instead, you can focus on writing code rather than spending time managing and configuring servers, databases, load balancers, firewalls, and networks.

Complete resource control

You have the freedom to select the AWS resources, such as Amazon EC2 instance type, that are optimal for your application. Additionally, Elastic Beanstalk lets you "open the hood" and retain full control over the AWS resources powering your application. If you decide you want to take over some (or all) of the elements of your infrastructure, you can do so seamlessly by using Elastic Beanstalk's management capabilities.

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

Incorrect options:

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

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

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

Reference:

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

Question 51: **Correct**

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

- -
 -
 -
- AWS OpsWorks**
- AWS Systems Manager**
- AWS Marketplace**
- (Correct)**
- AWS Config**

Explanation

Correct option:

AWS Marketplace

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

Incorrect options:

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

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

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

Reference:

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

Question 52: **Correct**

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

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



AWS Direct Connect



AWS Wavelength



AWS Edge Locations



AWS Local Zones

(Correct)

Explanation

Correct option:

AWS Local Zones

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

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

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

Incorrect options:

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

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

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

Reference:

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

Question 53: **Incorrect**

Which AWS service publishes up-to-the-minute information on the general status and availability of all AWS services in all the Regions of AWS Cloud?

-
- Amazon CloudWatch**
-
- AWS CloudFormation**
-
- AWS Personal Health Dashboard**
- (Incorrect)**
-
- AWS Service Health Dashboard**
- (Correct)**

Explanation

Correct option: **AWS Service Health Dashboard**

AWS Service Health Dashboard publishes most up-to-the-minute information on the status and availability of all AWS services in tabular form for all Regions that AWS is present in. You can check on this page <https://status.aws.amazon.com/> to get current status information.

AWS Service Health Dashboard

Overview:

The screenshot shows the AWS Service Health Dashboard. At the top, there's a navigation bar with the AWS logo and a "SERVICE HEALTH DASHBOARD" link. Below it, a breadcrumb trail says "Amazon Web Services » Service Health Dashboard". A main heading "Get a personalized view of AWS service health" is followed by a button "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).

Region	Service	Status	Details	RSS
North America	No recent events.			
South America	Alexa for Business (N. Virginia)	Service is operating normally		
Europe	Amazon API Gateway (Montreal)	Service is operating normally		
Africa	Amazon API Gateway (N. California)	Service is operating normally		
Asia Pacific	Amazon API Gateway (N. Virginia)	Service is operating normally		
Middle East	Amazon API Gateway (Ohio)	Service is operating normally		
Contact Us	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:

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

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

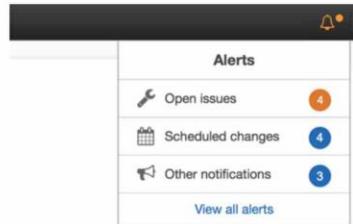
AWS Personal Health Dashboard

Overview:

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.

A screenshot of the AWS Service Health Dashboard. It shows a summary bar with 4 Open issues, 4 Scheduled changes, and 3 Other notifications. Below this is a table titled "Dashboard" with columns: Event type, Service, Region(s), Start date, and End date. It lists several events for various AWS services like S3, Lambda, and RDS.

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

Exam Alert:

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

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

Reference:

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

Question 54: **Correct**

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



Elastic Load Balancing



Amazon Rekognition

(Correct)



AWS Elastic Beanstalk



Amazon EC2

Explanation

Correct option: **Amazon Rekognition**

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

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

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

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

Overview of Cloud Computing

Types:

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/>

You can use Amazon Rekognition to add image and video analysis to your applications using proven, highly scalable, deep learning technology that requires no machine learning expertise. With Amazon

Rekognition, you can identify objects, people, text, scenes, and activities in images and videos as well as detect any inappropriate content. Rekognition is an example of Software as a Service model.

Incorrect options:

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

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

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

References:

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

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

Question 55: **Correct**

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

-

AWS Shield

(Correct)

-

Amazon CloudFront with Route 53

(Correct)

-

AWS CloudHSM

-

AWS Trusted Advisor

-

Amazon Inspector

-

AWS WAF

(Correct)

Explanation

Correct options:

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

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

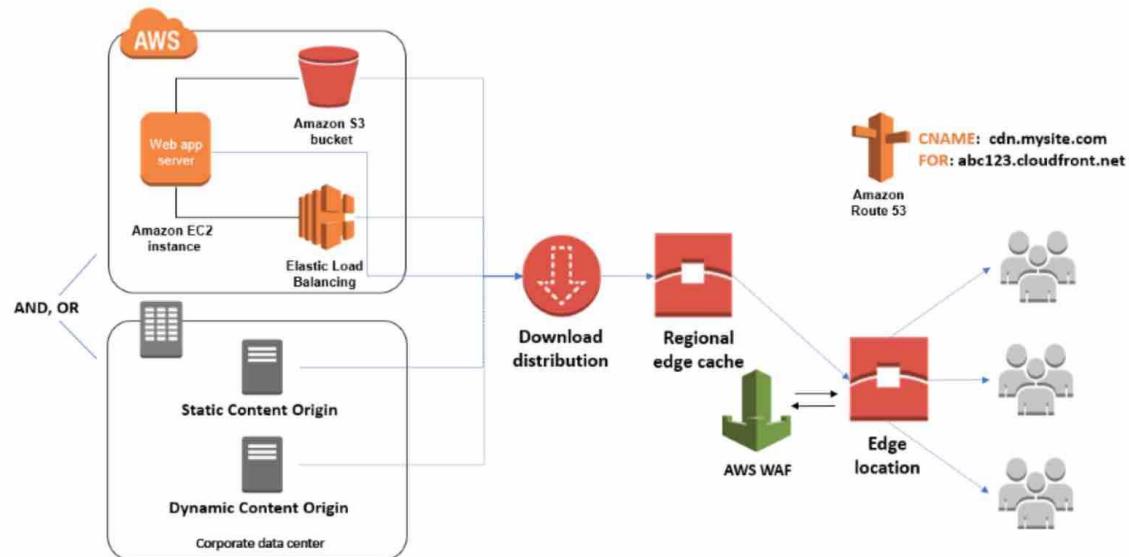
Amazon CloudFront with Route 53 - AWS hosts CloudFront and Route 53 services on a distributed network of proxy servers in data centers throughout the world called edge locations. Using the global Amazon network of edge locations for application delivery and DNS service plays an important part in building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

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

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

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

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



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

Incorrect options:

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

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

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

automatically assesses applications for exposure, vulnerabilities, and deviations from best practices. Amazon Inspector cannot be used to prevent Distributed Denial-of-Service (DDoS) attack.

References:

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

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

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

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

Question 56: **Correct**

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



AWS Budgets

(Correct)



AWS Cost Explorer



AWS Organizations



AWS Pricing Calculator

Explanation

Correct option:

AWS Budgets

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

AWS Budgets

Overview:

AWS Budgets Features

Create and manage budgets

Set custom cost and usage budgets to more easily manage your AWS spend. Monitor your budget status from the AWS Budgets dashboard or AWS Budgets reports.

Refine your budget using filters

Track your cost or usage across multiple dimensions by adding filters related to Service, Linked Account(s), Region, Tag, and more.

Add notifications to your budget

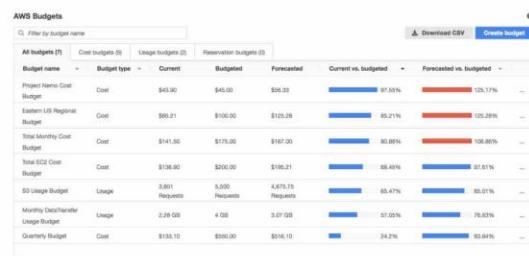
Set up to five alert thresholds for each budget. Each alert can notify up to ten email recipients as well as publish updates to a Slack channel, Amazon Chime room, or Amazon SNS topic of your choice.

Getting Started

AWS Budgets Dashboard

The AWS Budgets Dashboard is your hub for creating, tracking, and inspecting your budgets. From the AWS Budgets Dashboard, you can create, edit, and manage your budgets, as well as view the status of each of your budgets. You can also view additional details about your budgets, such as a high-level variance analysis and a budget criteria summary.

Budgets can be created at the monthly, quarterly, or yearly level, and you can customize the start and end dates. You can further refine your budget to track costs associated with multiple dimensions, such as AWS service, linked account, tag, and others. Budget alerts can be sent via email and/or Amazon Simple Notification Service (SNS) topic.



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

Exam Alert:

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

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

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

Incorrect options:

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

AWS Cost Explorer

Reports:

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 »](#)



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

Exam Alert:

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

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

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

Reference:

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

Question 57: **Correct**

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

-

Quickly resize photos to create thumbnails

(Correct)

-

Label objects in a photo

-

Identify person in a photo

-

Detect text in a photo

Explanation

Correct options:

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

With Amazon Rekognition, you can identify objects, people, text, scenes, and activities in images and videos, as well as detect any inappropriate content. Amazon Rekognition also provides highly accurate

facial analysis and facial search capabilities that you can use to detect, analyze, and compare faces for a wide variety of user verification, people counting, and public safety use cases.

Amazon Rekognition Use-Cases:

Key features



Labels

With Amazon Rekognition, you can identify thousands of objects (such as bike, telephone, building), and scenes (such as parking lot, beach, city). When analyzing video, you can also identify specific activities such as "delivering a package" or "playing soccer". [Learn more »](#)



Custom labels

With Amazon Rekognition Custom Labels, you can extend the detection capabilities of Amazon Rekognition to extract information from images that is uniquely helpful to your business. For example, you can find your corporate logo in social media, identify your products on store shelves, classify your machine parts in an assembly line, or detect your animated characters in videos. [Learn more »](#)



Content moderation

Amazon Rekognition helps you identify potentially unsafe or inappropriate content across both image and video assets and provides you with detailed labels that allow you to accurately control what you want to allow based on your needs. Use [Amazon AI](#) to enhance the accuracy of Amazon Rekognition image moderation predictions using human review. [Learn more »](#)

Text detection

In photos and videos, text appears very differently than neat words on a printed page. Amazon Rekognition can read skewed and distorted text to capture information like store names, forced narratives overlaid on media, street signs, and text on product packaging. [Learn more »](#)

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



Face detection and analysis

With Amazon Rekognition, you can easily detect when faces appear in images and videos and get attributes such as gender, age range, eyes open, glasses, facial hair for each. In video, you can also measure how these face attributes change over time, such as constructing a timeline of the emotions expressed by an actor. [Learn more »](#)



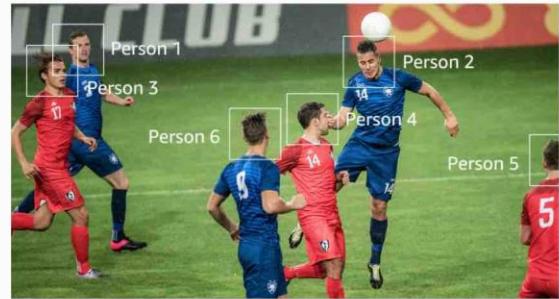
Face search and verification

Amazon Rekognition provides fast and accurate face search, allowing you to identify a person in a photo or video using your private repository of face images. You can also verify identity by analyzing a face image against images you have stored for comparison. [Learn more »](#)



Celebrity recognition

You can quickly identify well known people in your video and image libraries to catalog footage and photos for marketing, advertising, and media industry use cases. [Learn more »](#)



Pathing

You can capture the path of people in the scene when using Amazon Rekognition with video files. For example, you can use the movement of athletes during a game to identify plays for post-game analysis. [Learn more »](#)

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

Incorrect options:

Identify person in a photo

Detect text in a photo

Label objects in a photo

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

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

Question 58: **Correct**

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

-

Reserved Instances

Dedicated Hosts

Spot Instances

On-demand Instances

(Correct)

Explanation

Correct option:

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

EC2 Pricing Options

Overview:

On-Demand

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

On-Demand instances are recommended for:

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

[See On-Demand pricing »](#)

Spot instances

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

Spot instances are recommended for:

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

[See Spot pricing »](#)

Savings Plans

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

Dedicated Hosts

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

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

[See Dedicated pricing »](#)

Reserved Instances

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

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

Reserved Instances are recommended for:

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

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

Incorrect options:

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

Spot Instances - A Spot Instance is an unused EC2 instance that is available for less than the On-Demand price. Because Spot Instances enable you to request unused EC2 instances at steep discounts, you can lower your Amazon EC2 costs significantly. Spot Instances are well-suited for data analysis, batch jobs, background processing, and optional tasks. These can be terminated at short notice, so these are not suitable for critical workloads that need to run at a specific point in time. So this option is not correct for the given use-case.

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

Reference:

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

Question 59: **Correct**

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

-

Amazon Lightsail

-

Amazon Elastic Compute Cloud (EC2)

(Correct)

-

Amazon Elastic Container Service (ECS)

-

AWS Lambda

Explanation

Correct option:

Amazon Elastic Compute Cloud (EC2)

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

Amazon EC2

Overview:

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

To use Amazon EC2, you simply:

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

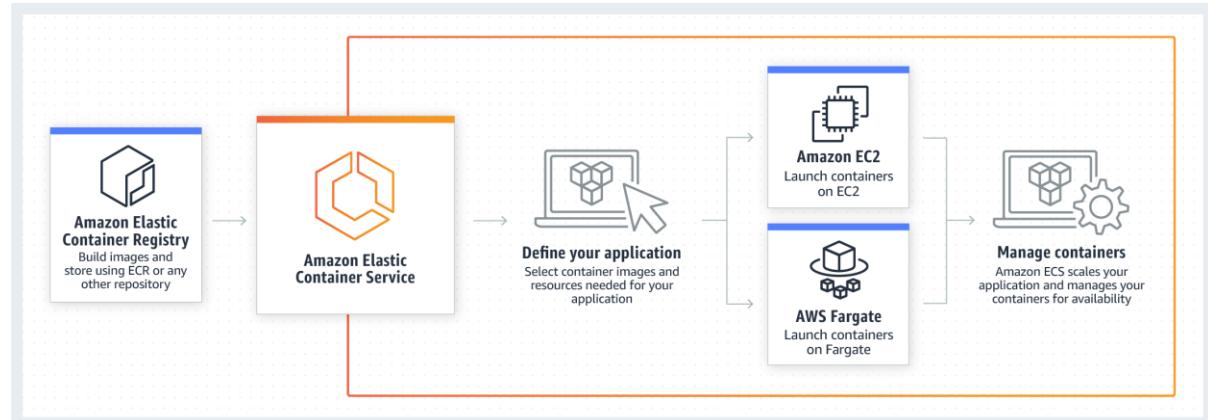
via - <https://aws.amazon.com/ec2/>

Incorrect options:

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

How ECS

Works:



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

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

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

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

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

Question 60: **Correct**

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



Developer



Individual



Business



Enterprise

(Correct)

Explanation

Correct option:

Enterprise

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

Exam Alert:

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

	Developer	Business	Enterprise
	<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**	General guidance: < 24 hours System impaired: < 12 hours	General guidance: < 24 hours System impaired: < 12 hours Production system impaired: < 4 hours Production system down: < 1 hour
Architectural Guidance	General	Contextual to your use-cases	Consultative review and guidance based on your applications
Programmatic Case Management		AWS Support API	AWS Support API
Third-Party Software Support		Interoperability & configuration guidance and troubleshooting	Interoperability & configuration guidance and troubleshooting
	Developer	Business	Enterprise
Proactive Programs		Access to Infrastructure Event Management for additional fee.	Infrastructure Event Management Well-Architected Reviews Operations Reviews Technical Account Manager (TAM) coordinates access to programs and other AWS experts as needed.
Technical Account Management			Designated Technical Account Manager (TAM) to proactively monitor your environment and assist with optimization.
Training			Access to online self-paced labs
Account Assistance			Concierge Support Team
Pricing	Greater of \$29 / month*** - or - 3% of monthly AWS usage See pricing detail and example.	Greater of \$100 / month*** - or - 10% of monthly AWS usage for the first \$0-\$10K 7% of monthly AWS usage from \$10K-\$80K 5% of monthly AWS usage from \$80K-\$250K 3% of monthly AWS usage over \$250K See pricing detail and example.	Greater of \$15,000 - or - 10% of monthly AWS usage for the first \$0-\$150K 7% of monthly AWS usage from \$150K-\$500K 5% of monthly AWS usage from \$500K-\$1M 3% of monthly AWS usage over \$1M See pricing detail and example.

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

Incorrect options:

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

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

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

Reference:

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

Question 61: **Correct**

Which service gives a personalized view of the status of the AWS services that are part of your Cloud architecture so that you can quickly assess the impact on your business when AWS service(s) are experiencing issues?

-

AWS Personal Health Dashboard

(Correct)

-

AWS Inspector

-

Amazon CloudWatch

-

AWS Service Health Dashboard

Explanation

Correct option: **AWS Personal Health Dashboard**

AWS Personal Health Dashboard provides alerts and remediation guidance when AWS is experiencing events that may impact you. With Personal Health Dashboard, alerts are triggered by changes in the health of your AWS resources, giving you event visibility, and guidance to help quickly diagnose and resolve issues.

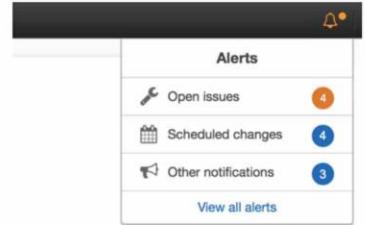
AWS Personal Health Dashboard

Overview:

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.

A screenshot of the AWS Service Health Dashboard. At the top, there is a header with the AWS logo and a search bar. Below the header is a navigation menu with 'Dashboard' and 'All services'. The main content area is titled 'Dashboard' and shows a table of service status. The table has columns: Event type, Service, Impact, Start time, and End time. It lists four entries: 'Service Maintenance End', 'AWS Lambda Function Update', 'EC2 Maintenance Scheduled', and 'RDS Maintenance Scheduled'. All entries show 'Opening' under 'Impact' and various dates/times under 'Start time' and 'End time'.

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

Incorrect options:

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

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

AWS Service Health Dashboard - AWS Service Health Dashboard publishes most up-to-the-minute information on the status and availability of all AWS services in tabular form for all Regions that AWS is present in. You can check on this page (<https://status.aws.amazon.com/>) any time to get current status information or subscribe to an RSS feed to be notified of interruptions to each service.

AWS Service Health Dashboard

Overview:



[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/>

Exam Alert:

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

Reference:

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

Question 62: **Correct**

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

Tape Gateway, File Gateway and Block Gateway

Object Gateway, File Gateway and Block Gateway

-
-

Tape Gateway, Object Gateway and Volume Gateway

-
-

Tape Gateway, File Gateway and Volume Gateway

(Correct)

Explanation

Correct option:

Tape Gateway, File Gateway and Volume Gateway

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

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

Gateway Storage Types

Overview:

Gateway Types

File Gateway

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

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

[Learn More »](#)

Tape Gateway

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

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

[Learn More »](#)

Volume Gateway

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

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

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

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

Incorrect options:

Object Gateway, File Gateway and Block Gateway

Tape Gateway, Object Gateway and Volume Gateway

Tape Gateway, File Gateway and Block Gateway

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

Reference:

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

Question 63: **Correct**

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

-
- **AWS Systems Manager**
- **AWS Command Line Interface (CLI)**
(Correct)
- **AWS Software Developer Kit (SDK)**
(Correct)
-
- **Amazon API Gateway**
- **AWS Management Console**
(Correct)
-

AWS Secrets Manager

Explanation

Correct options:

AWS services can be accessed in three different ways:

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

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

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

Incorrect options:

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

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

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

Question 64: **Incorrect**

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

-

Allows you to install databases on the underlying serverless Operating System

(Incorrect)

-

You pay for the compute time you consume

(Correct)

-

AWS Lambda lets you run code without provisioning or managing servers

(Correct)

-

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

-

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

Explanation

Correct options:

AWS Lambda lets you run code without provisioning or managing servers

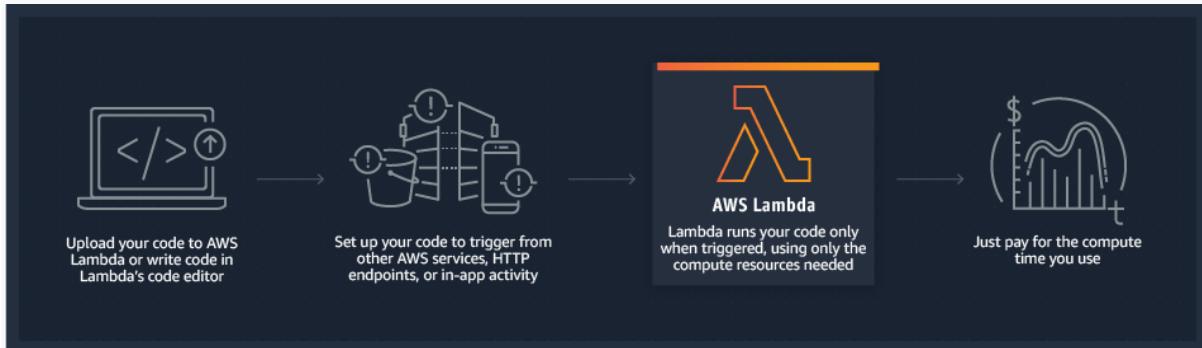
You pay for the compute time you consume

AWS Lambda is a compute service that lets you run code without provisioning or managing servers. AWS Lambda executes your code only when needed and scales automatically, from a few requests per day to thousands per second. You pay for the compute time and the number of requests for your Lambda function - there is no charge when your code is not running. With AWS Lambda, you can run code for virtually any type of application or backend service - all with zero administration. AWS

Lambda runs your code on a high-availability compute infrastructure and performs all of the administration of the compute resources, including server and operating system maintenance, capacity provisioning and automatic scaling, code monitoring and logging.

How Lambda

Works:



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

Incorrect options:

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

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

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

Reference:

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

Question 65: **Correct**

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

-

Amazon RDS for PostgreSQL

-

Amazon DynamoDB

(Correct)

-

Amazon Aurora

-

Amazon Redshift

Explanation

Correct option:

Amazon DynamoDB

Amazon DynamoDB is a NoSQL database that supports key-value and document data models and enables developers to build modern, serverless applications that can start small and scale globally to support petabytes of data and tens of millions of read and write requests per second. DynamoDB supports both key-value and document data models. This enables DynamoDB to have a flexible schema, so each row can have any number of columns at any point in time. This allows you to easily adapt the tables as your business requirements change, without having to redefine the table schema as you would in relational databases.

Incorrect options:

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

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

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

Reference:

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

Practice Test #3 - AWS Certified Cloud Practitioner - Results

Return to review

Chart

Pie chart with 3 slices.

End of interactive chart.

Attempt 1

All knowledge areas

All questions

Question 1: **Correct**

Which AWS service can help you create data-driven business cases for transitioning your business from on-premises to AWS Cloud?

-
-

AWS Migration Evaluator

(Correct)

-
-

AWS Trusted Advisor

-
-

AWS Budgets

-
-

AWS Billing and Cost Management

Explanation

Correct option:

AWS Migration Evaluator

Migration Evaluator (Formerly TSO Logic) is a complimentary service to create data-driven business cases for AWS Cloud planning and migration.

Migration Evaluator quickly provides a business case to make sound AWS planning and migration decisions. With Migration Evaluator, your organization can build a data-driven business case for AWS, gets access to AWS expertise, visibility into the costs associated with multiple migration strategies, and insights on how reusing existing software licensing reduces costs further.

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. You cannot use this service to create data-driven business cases for transitioning your business from on-premises to AWS Cloud.

AWS Trusted Advisor - AWS Trusted Advisor is an online tool that provides real-time guidance to help provision your resources following AWS best practices. Whether establishing new workflows, developing applications, or as part of ongoing improvement, recommendations provided by Trusted

Advisor regularly help keep your solutions provisioned optimally. AWS Trusted Advisor analyzes your AWS environment and provides best practice recommendations in five categories: Cost Optimization, Performance, Security, Fault Tolerance, Service Limits. You cannot use this service to create data-driven business cases for transitioning your business from on-premises to AWS Cloud.

AWS Billing and Cost Management - AWS Billing and Cost Management is the service that you use to pay your AWS bill, monitor your usage, and analyze and control your costs. It is the billing department for AWS services - with necessary tools and services under its hood. You cannot use this service to create data-driven business cases for transitioning your business from on-premises to AWS Cloud.

Reference:

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/ce-exploring-data.html>

Question 2: **Incorrect**

Amazon CloudWatch billing metric data is stored in which AWS Region?

-
-

US East (N. Virginia) - us-east-1

(Correct)

-
-

In the AWS Region where the AWS resource is provisioned

(Incorrect)

-
-

US West (N. California) - us-west-1

-
-

In the AWS Region where the AWS account is created

Explanation

Correct option:

US East (N. Virginia) - us-east-1

You can monitor your estimated AWS charges by using Amazon CloudWatch. Billing metric data is stored in the US East (N. Virginia) Region and represents worldwide charges. This data includes the estimated charges for every service in AWS that you use, in addition to the estimated overall total of your AWS charges.

Incorrect options:

In the AWS Region where the AWS account is created

In the AWS Region where the AWS resource is provisioned

US West (N. California) - us-west-1

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

Reference:

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

Question 3: **Correct**

Which of the following improves the availability for a fleet of EC2 instances?

-

Deploy the EC2 instances across different Availability Zones in the same AWS Region

(Correct)

-

Deploy the EC2 instances across different AWS Regions of the same Availability Zone

-

Deploy the EC2 instances in the same Availability Zone of an AWS Region

-

Deploy the EC2 instances in the same Availability Zone across two different AWS Regions

Explanation

Correct option:

Deploy the EC2 instances across different Availability Zones in the same AWS Region

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. Each AZ has independent power, cooling, and physical security and is connected via redundant, ultra-low-latency networks.

An Availability Zone (AZ) is one or more discrete data centers with redundant power, networking, and connectivity in an AWS Region. An AWS Region refers to a physical location around the world where AWS clusters data centers. 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.

AWS Regions and Availability Zones Explained:

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/

Incorrect options:

Deploy the EC2 instances in the same Availability Zone of an AWS Region - Deploying EC2 instances within the same AZ will not improve availability.

Deploy the EC2 instances in the same Availability Zone across two different AWS Regions - An Availability Zone cannot belong to two different AWS Regions. So this option is incorrect.

Deploy the EC2 instances across different AWS Regions of the same Availability Zone - You cannot have an AWS Region inside an Availability Zone. So this option is incorrect.

Reference:

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

Question 4: **Incorrect**

A cyber-security agency uses AWS Cloud and wants to carry out security assessments on their own AWS infrastructure without any prior approval from AWS. Which of the following describes/facilitates this practice?



Penetration Testing

(Correct)

- **AWS Secrets Manager**
- **Network Stress Testing**
- **Amazon Inspector**
(Incorrect)

Explanation

Correct option:

Penetration Testing

AWS customers can carry out security assessments or penetration tests against their AWS infrastructure without prior approval for few common AWS services. Customers are not permitted to conduct any security assessments of AWS infrastructure, or the AWS services themselves.

Incorrect options:

Network Stress Testing - AWS considers "network stress test" to be when a test sends a large volume of legitimate or test traffic to a specific intended target application. The endpoint and infrastructure are expected to be able to handle this traffic.

Amazon Inspector - Amazon Inspector is an automated, security assessment service that helps you check for unintended network accessibility of your Amazon EC2 instances and for vulnerabilities on those EC2 instances. Amazon Inspector assessments are offered to you as pre-defined rules packages mapped to common security best practices and vulnerability definitions.

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

Reference:

<https://aws.amazon.com/security/penetration-testing/>

Question 5:

Skipped

An AWS user is trying to launch an EC2 instance in a given region. What is the region-specific constraint that the Amazon Machine Image (AMI) must meet so that it can be used for this EC2 instance?

-

You must use an AMI from the same region as that of the EC2 instance. The region of the AMI has no bearing on the performance of the EC2 instance

(Correct)

-

An AMI is a global entity, so the region is not applicable

-

You should use an AMI from the same region, as it improves the performance of the EC2 instance

-

You can use an AMI from a different region, but it degrades the performance of the EC2 instance

Explanation

Correct option:

You must use an AMI from the same region as that of the EC2 instance. The region of the AMI has no bearing on the performance of the EC2 instance

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.

The AMI must be in the same region as that of the EC2 instance to be launched. If the AMI exists in a different region, you can copy that AMI to the region where you want to launch the EC2 instance. The region of AMI has no bearing on the performance of the EC2 instance.

Amazon Machine Images (AMI)

Overview:

Amazon Machine Images (AMI)

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

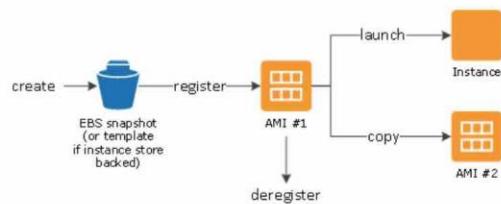
An Amazon Machine Image (AMI) provides the information required to launch an instance. You must specify an AMI when you launch an instance. You can launch multiple instances from a single AMI when you need multiple instances with the same configuration. You can use different AMIs to launch instances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

An AMI includes the following:

- One or more EBS snapshots, or, for instance-store-backed AMIs, a template for the root volume of the instance (for example, an operating system, an application server, and applications).
- Launch permissions that control which AWS accounts can use the AMI to launch instances.
- A block device mapping that specifies the volumes to attach to the instance when it's launched.

Using an AMI

The following diagram summarizes the AMI lifecycle. After you create and register an AMI, you can use it to launch new instances. (You can also launch instances from an AMI if the AMI owner grants you launch permissions.) You can copy an AMI within the same Region or to different Regions. When you no longer require an AMI, you can deregister it.



You can search for an AMI that meets the criteria for your instance. You can search for AMIs provided by AWS or AMIs provided by the community. For more information, see [AMI types](#) and [Finding a Linux AMI](#).

After you launch an instance from an AMI, you can connect to it. When you are connected to an instance, you can use it just like you use any other server. For information about launching, connecting, and using your instance, see [Amazon EC2 instances](#).

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

Incorrect options:

You can use an AMI from a different region, but it degrades the performance of the EC2 instance

You should use an AMI from the same region, as it improves the performance of the EC2 instance

An AMI is a global entity, so the region is not applicable

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

Reference:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html>

Question 6:

Skipped

Which of the following statements are true about Cost Allocation Tags in AWS Billing? (Select two)

-

Tags helps in organizing resources and are a mandatory configuration item to run reports

-

For each resource, each tag key must be unique, and each tag key can have only one value

(Correct)

-

Only user-defined tags need to be activated before they can appear in Cost Explorer or on a cost allocation report

-

For each resource, each tag key must be unique, but can have multiple values

-

You must activate both AWS generated tags and user-defined tags separately before they can appear in Cost Explorer or on a cost allocation report

(Correct)

Explanation

Correct options:

For each resource, each tag key must be unique, and each tag key can have only one value

You must activate both AWS generated tags and user-defined tags separately before they can appear in Cost Explorer or on a cost allocation report

A Cost Allocation Tag is a label that you or AWS assigns to an AWS resource. Each tag consists of a key and a value. For each resource, each tag key must be unique, and each tag key can have only one value. You can use tags to organize your resources, and cost allocation tags to track your AWS costs on a detailed level.

AWS provides two types of cost allocation tags, an AWS generated tags and user-defined tags. AWS defines, creates, and applies the AWS generated tags for you, and you define, create, and apply user-defined tags. You must activate both types of tags separately before they can appear in Cost Explorer or on a cost allocation report.

AWS Cost Allocation Tags

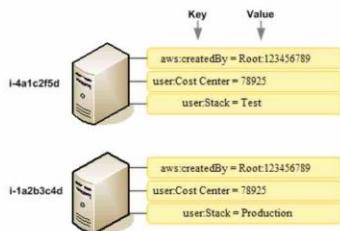
Overview:

Using Cost Allocation Tags

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

A tag is a label that you or AWS assigns to an AWS resource. Each tag consists of a *key* and a *value*. For each resource, each tag key must be unique, and each tag key can have only one value. You can use tags to organize your resources, and cost allocation tags to track your AWS costs on a detailed level. After you activate cost allocation tags, AWS uses the cost allocation tags to organize your resource costs on your cost allocation report, to make it easier for you to categorize and track your AWS costs. AWS provides two types of cost allocation tags, an *AWS generated tags* and *user-defined tags*. AWS defines, creates, and applies the AWS generated tags for you, and you define, create, and apply user-defined tags. You must activate both types of tags separately before they can appear in Cost Explorer or on a cost allocation report.

The following diagram illustrates the concept. In the example, you've assigned and activated tags on two Amazon EC2 instances, one tag called Cost Center and another tag called Stack. Each of the tags has an associated value. You also activated the AWS generated tags, createdBy before creating these resources. The createdBy tag tracks who created a resource. The user-defined tags use the user prefix, and the AWS generated tag uses the aws: prefix.



After you or AWS applies tags to your AWS resources (such as Amazon EC2 instances or Amazon S3 buckets) and you activate the tags in the Billing and Cost Management console, AWS generates a cost allocation report as a comma-separated value (CSV file) with your usage and costs grouped by your active tags. You can apply tags that represent business categories (such as cost centers, application names, or owners) to organize your costs across multiple services.

The cost allocation report includes all of your AWS costs for each billing period. The report includes both tagged and untagged resources, so that you can clearly organize the charges for resources. For example, if you tag resources with an application name, you can track the total cost of a single application that runs on those resources. The following screenshot shows a partial report with columns for each tag.

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

via - <https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/cost-alloc-tags.html>

Incorrect options:

Tags helps in organize resources and are a mandatory configuration item to run reports - Tags definitely help organize resources as per an organization's requirement; they are not mandatory though.

For each resource, each tag key must be unique, but can have multiple values - For each resource, each tag key must be unique, and each tag key can have only one value.

Only user-defined tags need to be activated before they can appear in Cost Explorer or on a cost allocation report - As explained above, both kinds of tags (user-defined and AWS generated) need to be activated separately before they can appear in report generation.

Reference:

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/cost-alloc-tags.html>

Question 7: **Incorrect**

Which of the following AWS services offer block-level storage? (Select two)

-

S3

-

Instance Store

(Correct)

-

EBS

(Correct)

-

ECS

-

EFS

Explanation

Correct options:

EBS - Amazon Elastic Block Store (EBS) is an easy to use, high-performance block storage service designed for use with Amazon Elastic Compute Cloud (EC2) for both throughput and transaction-intensive workloads at any scale. A broad range of workloads, such as relational and non-relational databases, enterprise applications, containerized applications, big data analytics engines, file systems, and media workflows are widely deployed on Amazon EBS.

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

Incorrect options:

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

S3 - Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. This means customers of all sizes and industries can use it to store and protect any amount of data for a range of use cases, such as websites, mobile applications, backup and restore, archive, enterprise applications, IoT devices, and big data analytics.

ECS - Amazon Elastic Container Service (ECS) is a highly scalable, high-performance container management service that supports Docker containers and allows you to easily run applications on a

managed cluster of Amazon EC2 instances. This is not a storage service and has been added as a distractor.

References:

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

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

Question 8: **Incorrect**

An IT company would like to move its IT resources (including any data and applications) from an AWS Region in the US to another AWS Region in Europe. Which of the following represents the correct solution for this use-case?



The company should just start creating new resources in the destination AWS Region and then migrate the relevant data and applications into this new AWS Region

(Correct)



The company should raise a ticket with AWS Support for this resource migration



The company should use Database Migration Service to move the resources (including any data and applications) from source AWS Region to destination AWS Region

(Incorrect)



The company should use CloudFormation to move the resources (including any data and applications) from source AWS Region to destination AWS Region

Explanation

Correct option:

The company should just start creating new resources in the destination AWS Region and then migrate the relevant data and applications into this new AWS Region - The company needs to create resources in the new AWS Region and then move the relevant data and applications into the new AWS Region. There is no off-the-shelf solution or service that the company can use to facilitate this transition.

Incorrect options:

The company should use CloudFormation to move the resources (including any data and applications) from source AWS Region to destination AWS Region - AWS CloudFormation allows you to use programming languages or a simple text file to model and provision, in an automated and

secure manner, all the resources needed for your applications across all regions and accounts. CloudFormation cannot help with moving data and applications into another Region.

The company should use Database Migration Service to move the resources (including any data and applications) from source AWS Region to destination AWS Region - AWS Database

Migration Service helps you migrate databases to AWS quickly and securely. The source database remains fully operational during the migration, minimizing downtime to applications that rely on the database. The AWS Database Migration Service can migrate your data to and from the most widely used commercial and open-source databases. Database Migration Service cannot help with the entire IT resources migration.

The company should raise a ticket with AWS Support for this resource migration - This option has been added as a distractor. AWS Support cannot help with IT resources migration.

Question 9: **Correct**

A research lab wants to optimize the caching capabilities for its scientific computations application running on EC2 instances. Which EC2 storage option is best suited for this use-case?

-

Amazon S3

-

Amazon EC2 Instance Store

(Correct)

-

Amazon EFS

-

Amazon EBS

Explanation

Correct option:

Amazon EC2 Instance Store

An Instance Store provides temporary block-level storage for your EC2 instance. This storage is located on disks that are physically attached to the host computer. Instance store is ideal for the temporary storage of information that changes frequently, such as buffers, caches, scratch data, and other temporary content, or for data that is replicated across a fleet of instances, such as a load-balanced pool of web servers. Instance storage is temporary, data is lost if instance experiences failure or is terminated.

Instance Store

Overview:

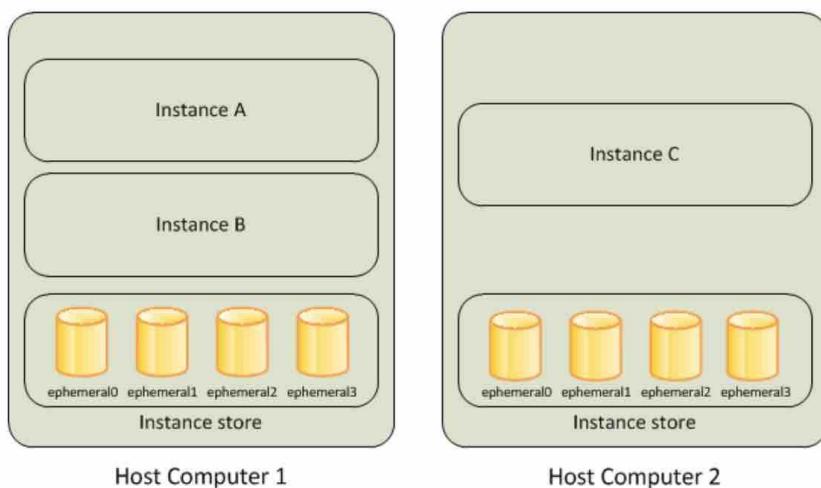
Amazon EC2 Instance Store

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

An *instance store* provides temporary block-level storage for your instance. This storage is located on disks that are physically attached to the host computer. Instance store is ideal for temporary storage of information that changes frequently, such as buffers, caches, scratch data, and other temporary content, or for data that is replicated across a fleet of instances, such as a load-balanced pool of web servers.

An instance store consists of one or more instance store volumes exposed as block devices. The size of an instance store as well as the number of devices available varies by instance type.

The virtual devices for instance store volumes are ephemeral [0-23]. Instance types that support one instance store volume have ephemeral0. Instance types that support two instance store volumes have ephemeral0 and ephemeral1, and so on.



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

Incorrect options:

Amazon EBS - Amazon Elastic Block Store (EBS) is an easy to use, high-performance block storage service designed for use with Amazon Elastic Compute Cloud (EC2) for both throughput and transaction-intensive workloads at any scale. A broad range of workloads, such as relational and non-relational databases, enterprise applications, containerized applications, big data analytics engines, file systems, and media workflows are widely deployed on Amazon EBS. EBS is not a good fit for caching information on EC2 instances.

Amazon EFS - Amazon Elastic File System (Amazon EFS) provides a simple, scalable, fully managed, elastic NFS file system. It is built to scale on-demand to petabytes without disrupting applications, growing and shrinking automatically as you add and remove files, eliminating the need to provision and manage capacity to accommodate growth. Amazon EFS is designed to provide massively parallel shared access to thousands of Amazon EC2 instances, enabling your applications to achieve high levels of aggregate throughput and IOPS with consistent low latencies. EFS is not a good fit for caching information on EC2 instances.

Amazon S3 - Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. S3 is not a good fit for caching information on EC2 instances.

Reference:

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

Question 10: **Correct**

Which of the following is correct regarding the AWS Shield Advanced pricing?

-

AWS Shield Advanced is a free service for AWS Enterprise Support plan

-

AWS Shield Advanced is a free service for all AWS Support plans

-

AWS Shield Advanced offers protection against higher fees that could result from a DDoS attack

(Correct)

-

AWS Shield Advanced is a free service for AWS Business Support plan

Explanation

Correct option:

AWS Shield Advanced offers protection against higher fees that could result from a DDoS attack

AWS Shield Advanced offers some cost protection against spikes in your AWS bill that could result from a DDoS attack. This cost protection is provided for your Elastic Load Balancing load balancers, Amazon CloudFront distributions, Amazon Route 53 hosted zones, Amazon Elastic Compute Cloud instances, and your AWS Global Accelerator accelerators.

AWS Shield Advanced is a paid service for all customers, irrespective of the Support plan.

Incorrect options:

AWS Shield Advanced is a free service for AWS Enterprise Support plan

AWS Shield Advanced is a free service for AWS Business Support plan

AWS Shield Advanced is a free service for all AWS Support plans

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

Reference:

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

Question 11: **Incorrect**

Which of the following use cases is best suited for Amazon Elastic File System (EFS) Standard–Infrequent Access (Standard–IA) storage class?

-

Use as boot volume for highly available Amazon EC2 instances

-

Object storage for workloads that need sub-second latency speeds for accessing the data

(Incorrect)

-

Storing files in an accessible location to satisfy audit requirements

(Correct)

-

Storing data in a single AWS Availability Zone

Explanation

Correct option: **Storing files in an accessible location to satisfy audit requirements** - The Standard–IA storage class reduces storage costs for files that are not accessed every day. It does this without sacrificing the high availability, high durability, elasticity, and POSIX file system access that Amazon EFS provides.

AWS recommends Standard–IA storage if you need your full dataset to be readily accessible and want to automatically save on storage costs for files that are less frequently accessed. Examples include keeping files accessible to satisfy audit requirements, performing historical analysis, or performing backup and recovery. Standard–IA storage is compatible with all Amazon EFS features, and is available in all AWS Regions where Amazon EFS is available.

Incorrect options:

Storing data in a single AWS Availability Zone - EFS One Zone storage class is used to store data in a single AWS Availability Zone. Data stored in this storage class may be lost in the event of a disaster or other fault that affects all copies of the data within the Availability Zone, or in the event of Availability Zone destruction.

Object storage for workloads that need sub-second latency speeds for accessing the data - EFS is a file system service and not an object storage service. You should use S3 for object storage. So, this option is incorrect.

Use as boot volume for highly available Amazon EC2 instances - Amazon EFS cannot be used as a boot volume for Amazon EC2 instances. For boot volumes, Amazon Elastic Block Storage (Amazon EBS) volumes are used.

Reference:

<https://docs.aws.amazon.com/efs/latest/ug/storage-classes.html>

Question 12: **Correct**

Which AWS Support plan guarantees a case response time of 15 minutes when Business Critical systems are down?



Enterprise

(Correct)



Basic



Developer



Business

Explanation

Correct option:

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. This plan provides Enhanced Technical Support as follows:

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

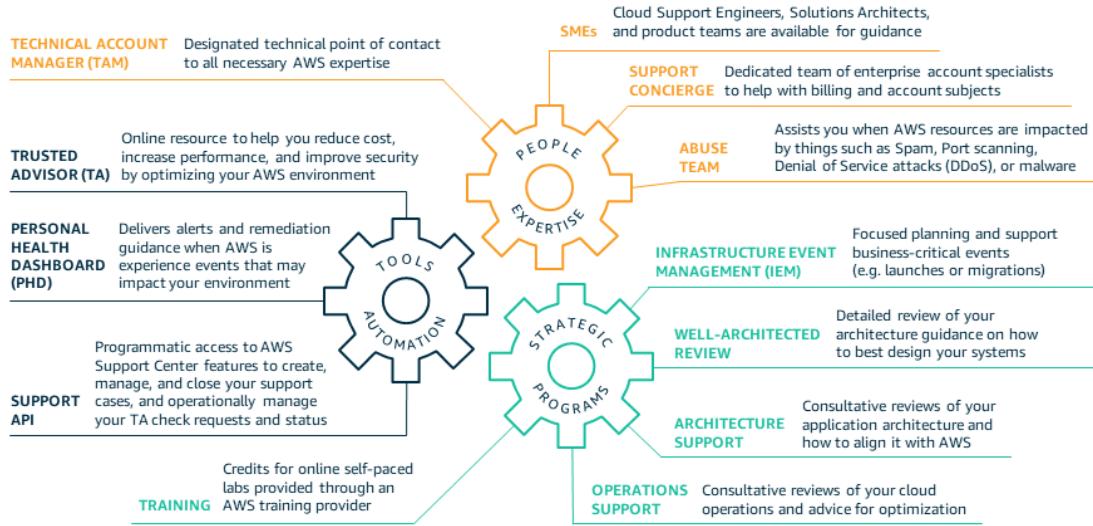
System Impaired - < 12 hours

Production System Impaired - < 4 hours

Production System Down - < 1 hour

Business Critical System Down - <15 min

Benefits of AWS Enterprise Support
Plan:



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

Incorrect options:

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. This plan does not guarantee any specific response time for Business Critical systems.

Developer - AWS recommends Developer Support if you are testing or doing early development on AWS and want the ability to get email-based technical support during business hours as well as general architectural guidance as you build and test. You do not get access to Infrastructure Event Management with this plan. This plan does not guarantee any specific response time for Business Critical systems.

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

Customer Service & Communities - 24x7 access to customer service, documentation, whitepapers, and support forums. AWS Trusted Advisor - Access to the 7 core Trusted Advisor checks and guidance to provision your resources following best practices to increase performance and improve security. AWS Personal Health Dashboard - A personalized view of the health of AWS services, and alerts when your resources are impacted. This plan does not guarantee any specific response time for Business Critical systems.

Reference:

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

Question 13: **Correct**

Which S3 storage class offers the lowest availability?

-

S3 Intelligent-Tiering

-

S3 One Zone-IA

(Correct)

-

S3 Standard

-

S3 Glacier

Explanation

Correct option:

S3 One Zone-IA

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.

Please review this illustration for S3 Storage Classes availability. You don't need to memorize the actual numbers, just remember that S3 One Zone-IA offers the lowest availability:

Performance across the S3 Storage Classes

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

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

Incorrect options:

S3 Standard - S3 Standard offers high durability, availability, and performance object storage for frequently accessed data.

S3 Intelligent-Tiering - The S3 Intelligent-Tiering storage class is designed to optimize costs by automatically moving data to the most cost-effective access tier, without performance impact or operational overhead. It works by storing objects in two access tiers: one tier that is optimized for frequent access and another lower-cost tier that is optimized for infrequent access.

S3 Glacier - Amazon S3 Glacier is a secure, durable, and extremely low-cost Amazon S3 cloud storage class for data archiving and long-term backup. It is designed to deliver 99.999999999% durability, and provide comprehensive security and compliance capabilities that can help meet even the most stringent regulatory requirements.

References:

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

Question 14: **Correct**

Which of the following statements are CORRECT about the AWS Auto Scaling group? (Select two)

-

Auto Scaling group scales down and downgrades to a less powerful EC2 instance to match a decrease in demand

-

Auto Scaling group scales down and reduces the number of EC2 instances to match a decrease in demand

-

Auto Scaling group scales in and reduces the number of EC2 instances to match a decrease in demand

(Correct)

-

Auto Scaling group scales out and adds more number of EC2 instances to match an increase in demand

(Correct)

-

Auto Scaling group scales up and upgrades to a more powerful EC2 instance to match an increase in demand

Explanation

Correct option:

Auto Scaling group scales out and adds more number of EC2 instances to match an increase in demand

Auto Scaling group scales in and reduces the number of EC2 instances to match a decrease in demand

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

You can use scaling policies to increase or decrease the number of instances in your group dynamically to meet changing conditions. When the scaling policy is in effect, the Auto Scaling group adjusts the desired capacity of the group, between the minimum and maximum capacity values that you specify, and launches or terminates the instances as needed. You can also scale on a schedule.

Incorrect options:

Auto Scaling group scales down and reduces the number of EC2 instances to match a decrease in demand - A scale down refers to a downgrade to a less powerful EC2 instance. Therefore this option is incorrect.

Auto Scaling group scales down and downgrades to a less powerful EC2 instance to match a decrease in demand

Auto Scaling group scales up and upgrades to a more powerful EC2 instance to match an increase in demand

An Auto Scaling group does not scale up or scale down, so these two options are incorrect.

Reference:

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

Question 15: **Correct**

Which feature of AWS Cloud offers the ability to innovate faster and rapidly develop, test and launch software applications?

-

Cost savings

-

Elasticity

-

Agility

(Correct)

-

Ability to deploy globally in minutes

Explanation

Correct option:

Cloud computing is the on-demand delivery of IT resources over the Internet with pay-as-you-go pricing. Instead of buying, owning, and maintaining physical data centers and servers, you can access technology services, such as computing power, storage, and databases, on an as-needed basis from a cloud provider like Amazon Web Services (AWS).

Agility - Agility refers to the ability of the cloud to give you easy access to a broad range of technologies so that you can innovate faster and build nearly anything that you can imagine. You can quickly spin up resources as you need them – from infrastructure services, such as compute, storage, and databases, to Internet of Things, machine learning, data lakes and analytics, and much more.

Incorrect options:

Elasticity - With cloud computing elasticity, you don't have to over-provision resources upfront to handle peak levels of business activity in the future. Instead, you provision the number of resources that you actually need. You can scale these resources up or down instantly to grow and shrink capacity as your business needs change.

Cost savings - The cloud allows you to trade capital expenses (such as data centers and physical servers) for variable expenses, and only pay for IT as you consume it. Plus, the variable expenses are much lower than what you would pay to do it yourself because of the economies of scale.

Ability to deploy globally in minutes - With the cloud, you can expand to new geographic regions and deploy globally in minutes. For example, AWS has infrastructure all over the world, so you can deploy your application in multiple physical locations with just a few clicks. Putting applications in closer proximity to end users reduces latency and improves their experience.

Exam Alert:

Please review the benefits of Cloud Computing:

Benefits of cloud computing

Agility



The cloud gives you easy access to a broad range of technologies so that you can innovate faster and build nearly anything that you can imagine. You can quickly spin up resources as you need them—from infrastructure services, such as compute, storage, and databases, to Internet of Things, machine learning, data lakes and analytics, and much more.

You can deploy technology services in a matter of minutes, and get from idea to implementation several orders of magnitude faster than before. This gives you the freedom to experiment, test new ideas to differentiate customer experiences, and transform your business.

Elasticity

With cloud computing, you don't have to over-provision resources up front to handle peak levels of business activity in the future. Instead, you provision the amount of resources that you actually need. You can scale these resources up or down to instantly grow and shrink capacity as your business needs change.



Cost savings

The cloud allows you to trade capital expenses (such as data centers and physical servers) for variable expenses, and only pay for IT as you consume it. Plus, the variable expenses are much lower than what you would pay to do it yourself because of the economies of scale.

Deploy globally in minutes

With the cloud, you can expand to new geographic regions and deploy globally in minutes. For example, AWS has infrastructure all over the world, so you can deploy your application in multiple physical locations with just a few clicks. Putting applications in closer proximity to end users reduces latency and improves their experience.



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

Reference:

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

Question 16: **Correct**

An organization maintains separate VPCs for each of its departments. With expanding business, the organization now wants to connect all VPCs for better departmental collaboration. Which AWS service will help the organization tackle the issue effectively?

-
-

Site to Site VPN

-
-

AWS Transit Gateway

(Correct)

-
-

VPC Peering

-
-

AWS Direct Connect

Explanation

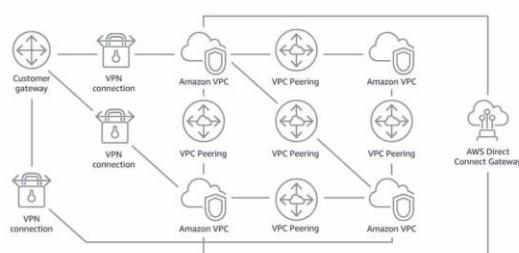
Correct option:

AWS Transit Gateway

AWS Transit Gateway connects VPCs and on-premises networks through a central hub. This simplifies your network and puts an end to complex peering relationships. It acts as a cloud router – each new connection is only made once. As you expand globally, inter-Region peering connects AWS Transit Gateways using the AWS global network. Your data is automatically encrypted and never travels over the public internet.

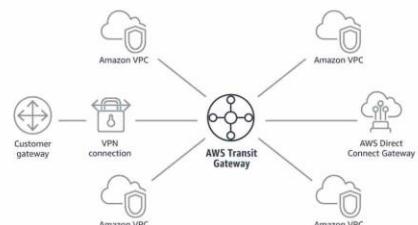
How Transit Gateway can simplify your network:

Without AWS Transit Gateway



Complexity increases with scale. You must maintain routing tables within each VPC and connect to each onsite location using separate network gateways.

With AWS Transit Gateway

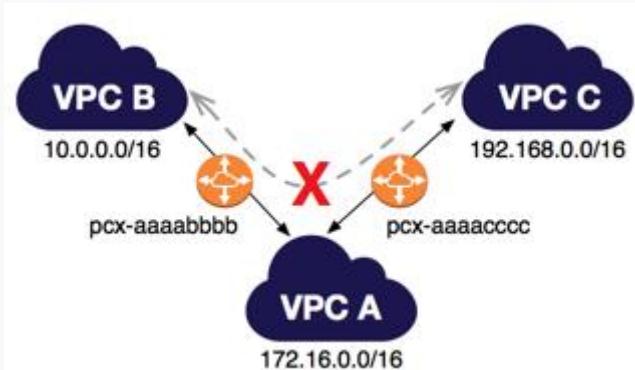


Your network is streamlined and scalable. AWS Transit Gateway routes all traffic to and from each VPC or VPN, and you have one place to manage and monitor it all.

via - <https://aws.amazon.com/transit-gateway/>

Incorrect options:

VPC Peering - A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them privately. VPC peering is not transitive, a separate VPC peering connection has to be made between two VPCs that need to talk to each other. With growing VPCs, this gets difficult to manage.



Transitive VPC Peering is not allowed:

- <https://docs.aws.amazon.com/vpc/latest/peering/invalid-peering-configurations.html>

via

AWS Direct Connect - AWS Direct Connect creates a dedicated private connection from a remote network to your VPC. This is a private connection and does not use the public internet. Takes at least a month to establish this connection. Direct Connect cannot be used to interconnect VPCs.

Site to Site VPN - AWS Site-to-Site VPN creates a secure connection between your data center or branch office and your AWS cloud resources. This connection goes over the public internet. Site to Site VPN cannot be used to interconnect VPCs.

Reference:

<https://aws.amazon.com/transit-gateway/>

Question 17: **Correct**

A leading research firm needs to access information available in old patents and documents (such as PDFs, Text Files, Word documents, etc) present in its huge knowledge base. The firm is looking for a powerful search tool that can dig into these knowledge resources and return the most relevant files/documents. Which of the following is the correct service to address this requirement?

-

Amazon Personalize

-

Amazon Comprehend

-

Amazon Kendra

(Correct)

-

Amazon Lex

Explanation

Correct option: **Amazon Kendra** - Amazon Kendra is an intelligent search service powered by machine learning. Kendra reimagines enterprise search for your websites and applications so your employees and customers can easily find the content they are looking for, even when it's scattered across multiple locations and content repositories within your organization.

Using Amazon Kendra, you can stop searching through troves of unstructured data and discover the right answers to your questions, when you need them. Amazon Kendra is a fully managed service, so there are no servers to provision, and no machine learning models to build, train, or deploy. Kendra supports unstructured and semi-structured data in .html, MS Office (.doc, .ppt), PDF, and text formats.

Unlike conventional search technology, natural language search capabilities return the answers you're looking for quickly and accurately, no matter where the information lives within your organization.

Kendra's deep learning models come pre-trained across 14 industry domains, allowing it to extract more accurate answers across a wide range of business use cases from the get-go. You can also fine-tune search results by manually adjusting the importance of data sources, authors, freshness, or using custom tags.

Incorrect options:

Amazon Personalize - Amazon Personalize enables developers to build applications with the same machine learning (ML) technology used by Amazon.com for real-time personalized recommendations. Amazon Personalize makes it easy for developers to build applications capable of delivering a wide array of personalization experiences, including specific product recommendations, personalized product re-ranking, and customized direct marketing.

Amazon Comprehend - Amazon Comprehend is a natural-language processing (NLP) service that uses machine learning to uncover information in unstructured data. Instead of combing through documents, the process is simplified and unseen information is easier to understand.

Amazon Kendra provides ML-powered search capabilities for all unstructured data customers store in AWS. Kendra offers easy-to-use native connectors to popular AWS repository types such as S3 and RDS databases. Other AI services such as Amazon Comprehend, Amazon Transcribe, and Amazon Comprehend Medical can be used to pre-process documents, generate searchable text, extract entities, and enrich their metadata for more specialized search experiences.

Amazon Lex - Amazon Lex is a service for building conversational interfaces into any application using voice and text. Amazon Lex provides the advanced deep learning functionalities of automatic speech recognition (ASR) for converting speech to text, and natural language understanding (NLU) to recognize the intent of the text, to enable you to build applications with highly engaging user experiences and lifelike conversational interactions.

Reference:

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

Question 18: **Correct**

Which of the following is the best way to protect your data from accidental deletion on Amazon S3?

-
-

S3 Transfer Acceleration

-
-

S3 Versioning

(Correct)

-
-

S3 lifecycle configuration

-
-

S3 Storage Classes

Explanation
Correct option:

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.

Versioning-enabled buckets enable you to recover objects from accidental deletion or overwrite. For example: if you delete an object, instead of removing it permanently, Amazon S3 inserts a delete marker, which becomes the current object version.

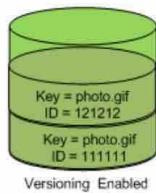
S3 Versioning
Overview:

Using versioning

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

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. When you enable versioning for a bucket, if Amazon S3 receives multiple write requests for the same object simultaneously, it stores all of the objects.

If you enable versioning for a bucket, Amazon S3 automatically generates a unique version ID for the object being stored. In one bucket, for example, you can have two objects with the same key, but different version IDs, such as `photo.gif` (version 111111) and `photo.gif` (version 121212).



Versioning-enabled buckets enable you to recover objects from accidental deletion or overwrite. For example:

- If you delete an object, instead of removing it permanently, Amazon S3 inserts a delete marker, which becomes the current object version. You can always restore the previous version. For more information, see [Deleting object versions](#).
- If you overwrite an object, it results in a new object version in the bucket. You can always restore the previous version.

via - <https://docs.aws.amazon.com/AmazonS3/latest/dev/ObjectVersioning.html>

Incorrect options:

S3 lifecycle configuration - To manage your S3 objects so that they are stored cost-effectively throughout their lifecycle, configure their Amazon S3 Lifecycle. With S3 Lifecycle configuration rules, you can tell Amazon S3 to transition objects to less expensive storage classes, or archive or delete them. Lifecycle configuration will do the hard lifting of moving your data into cost-effective storage classes without user intervention. Lifecycle configuration is not meant to protect from accidental deletion of data.

S3 Storage Classes - Amazon S3 offers a range of storage classes designed for different use cases. These include S3 Standard for general-purpose storage of frequently accessed data; S3 Intelligent-Tiering for data with unknown or changing access patterns; S3 Standard-Infrequent Access (S3 Standard-IA) and S3 One Zone-Infrequent Access (S3 One Zone-IA) for long-lived, but less frequently accessed data; and Amazon S3 Glacier (S3 Glacier) and Amazon S3 Glacier Deep Archive (S3 Glacier Deep Archive) for long-term archive and digital preservation. Storage classes are for different storage pattern needs that customers have, and not a data protection mechanism for S3.

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. Transfer Acceleration takes advantage of Amazon CloudFront's globally distributed edge locations. As the data arrives at an edge location, data is routed to Amazon S3 over an optimized network path. Transfer Acceleration cannot be used to protect from accidental deletion of data.

Reference:

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

Question 19: **Incorrect**

Which AWS service will you use if you have to move large volumes of on-premises data to AWS Cloud from a remote location with limited bandwidth?

-

AWS Transit Gateway

(Incorrect)

-

AWS Snowball

(Correct)

-

AWS Direct Connect

-

AWS Virtual Private Network (VPN)

Explanation

Correct option:

AWS Snowball

AWS Snowball, a part of the AWS Snow Family, is a data migration and edge computing device. If you have large quantities of data you need to migrate into AWS, offline data transfer with AWS Snowball can overcome the challenge of limited bandwidth, and avoid the need to lease additional bandwidth. Snowball moves terabytes of data in about a week. You can use it to move things like databases, backups, archives, healthcare records, analytics datasets, IoT sensor data and media content, especially when network conditions prevent realistic timelines for transferring large amounts of data both into and out of AWS.

Incorrect options:

AWS Virtual Private Network (VPN) - A VPN connection refers to the connection between your Virtual Private Cloud and your on-premises network. 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. VPN aids regular connectivity of AWS and your private on-premises network, it is not a data migration solution.

AWS Direct Connect - AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS. You can use AWS Direct Connect to establish a private virtual interface from your on-premise network directly to your Amazon VPC, providing you with a private, high bandwidth network connection between your network and your

VPC. This connection is private and does not go over the public internet. It takes at least a month to establish this physical connection. It is not feasible to set up AWS Direct Connect in remote locations.

AWS Transit Gateway - AWS Transit Gateway connects VPCs and on-premises networks through a central hub. This simplifies your network and puts an end to complex peering relationships. It acts as a cloud router – each new connection is only made once. VPC peering across large connections is made possible using Transit Gateway without ending up with a complex VPC peering network. Transit Gateway is not a data migration solution.

Reference:

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

Question 20: **Correct**

Which AWS service can be used to automate code deployment to EC2 instances as well as on-premises instances?



AWS CodeDeploy

(Correct)



AWS CodePipeline



AWS CloudFormation



AWS CodeCommit

Explanation

Correct option:

AWS CodeDeploy

AWS CodeDeploy is a service that automates code deployments to any instance, including Amazon EC2 instances and instances running on-premises. AWS CodeDeploy makes it easier for you to rapidly release new features, helps you avoid downtime during deployment, and handles the complexity of updating your applications. You can use AWS CodeDeploy to automate deployments, eliminating the need for error-prone manual operations, and the service scales with your infrastructure so you can easily deploy to one instance or thousands.

Incorrect options:

AWS CodeCommit - AWS CodeCommit is a fully-managed source control service that hosts secure Git-based repositories. It makes it easy for teams to collaborate on code in a secure and highly

scalable ecosystem. CodeCommit eliminates the need to operate your own source control system or worry about scaling its infrastructure. It cannot be used to automate code deployment.

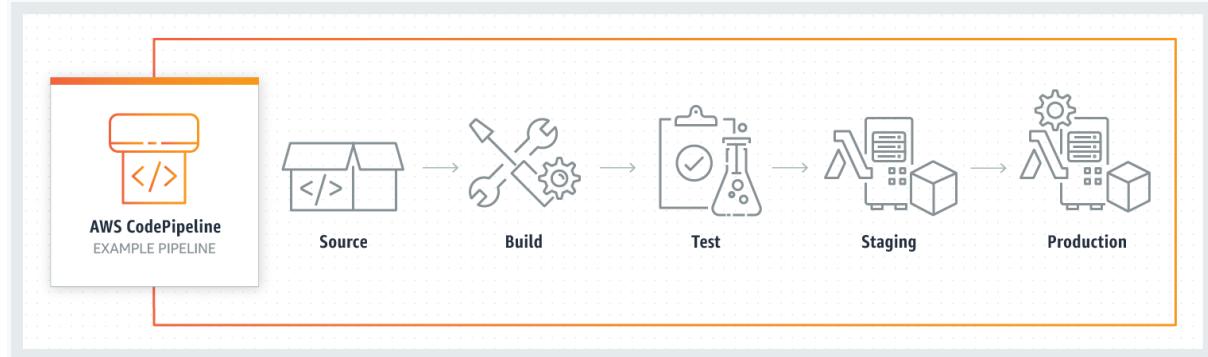
AWS CloudFormation - AWS CloudFormation allows you to use programming languages or a simple text file to model and provision, in an automated and secure manner, all the resources needed for your applications across all regions and accounts. It cannot be used to automate code deployment.

AWS CodePipeline - AWS CodePipeline is a continuous delivery service that enables you to model, visualize, and automate the steps required to release your software. With AWS CodePipeline, you model the full release process for building your code, deploying to pre-production environments, testing your application and releasing it to production.

AWS CodePipeline integrates with AWS services such as AWS CodeCommit, Amazon S3, AWS CodeBuild, AWS CodeDeploy, AWS Elastic Beanstalk, AWS CloudFormation, AWS OpsWorks, Amazon ECS, and AWS Lambda. To further elucidate, CodePipeline cannot by itself deploy the code, it can integrate with CodeDeploy for the actual deployment.

How CodePipeline

Works:



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

Reference:

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

Question 21: **Correct**

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

-

Amazon Rekognition

(Correct)

-

AWS WAF

-

AWS Identity and Access Management (IAM)

-

AWS Lambda

(Correct)

-

Amazon CloudFront

Explanation

Correct options:

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

AWS Lambda - AWS Lambda is a compute service that lets you run code without provisioning or managing servers. AWS Lambda executes your code only when needed and scales automatically, from a few requests per day to thousands per second. Lambda is a regional service.

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

Incorrect options:

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

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.

AWS WAF - By using AWS WAF, you can configure web access control lists (Web ACLs) on your CloudFront distributions or Application Load Balancers to filter and block requests based on request signatures.

As mentioned earlier, these three services are global in scope.

Exam Alert:

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

Question 22: **Correct**

A financial services company must meet compliance requirements that mandate storing multiple copies of data in geographically distant locations. As the company uses S3 as its main storage service, which of the following represents the MOST resource-efficient solution for this use-case?

-

Run a daily job on an EC2 instance to copy objects into another Region

-

Use Same-Region replication (SRR) to replicate data between distant AWS Regions

-

For every new object, trigger a lambda function to write data into a bucket in another AWS Region

-

Use Cross-Region replication (CRR) to replicate data between distant AWS Regions

(Correct)

Explanation

Correct option:

Use Cross-Region replication (CRR) to replicate data between distant AWS Regions

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

Replication enables automatic, asynchronous copying of objects across Amazon S3 buckets. Buckets that are configured for object replication can be owned by the same AWS account or by different accounts. You can copy objects between different AWS Regions or within the same Region.

Although Amazon S3 stores your data across multiple geographically distant Availability Zones by default, compliance requirements might dictate that you store data at even greater distances. Cross-Region Replication (CRR) allows you to replicate data between distant AWS Regions to satisfy these requirements.

Incorrect options:

Use Same-Region replication (SRR) to replicate data between distant AWS Regions - SRR is used to copy objects across Amazon S3 buckets in the same AWS Region, so this option is incorrect.

Exam Alert:

Please review the differences between SRR and CRR:

When to Use CRR

Cross-Region replication can help you do the following:

- **Meet compliance requirements** — Although Amazon S3 stores your data across multiple geographically distant Availability Zones by default, compliance requirements might dictate that you store data at even greater distances. Cross-Region replication allows you to replicate data between distant AWS Regions to satisfy these requirements.
- **Minimize latency** — If your customers are in two geographic locations, you can minimize latency in accessing objects by maintaining object copies in AWS Regions that are geographically closer to your users.
- **Increase operational efficiency** — If you have compute clusters in two different AWS Regions that analyze the same set of objects, you might choose to maintain object copies in those Regions.

When to Use SRR

Same-Region replication can help you do the following:

- **Aggregate logs into a single bucket** — If you store logs in multiple buckets or across multiple accounts, you can easily replicate logs into a single, in-Region bucket. This allows for simpler processing of logs in a single location.
- **Configure live replication between production and test accounts** — If you or your customers have production and test accounts that use the same data, you can replicate objects between those multiple accounts, while maintaining object metadata, by implementing SRR rules.
- **Abide by data sovereignty laws** — You might be required to store multiple copies of your data in separate AWS accounts within a certain Region. Same-Region replication can help you automatically replicate critical data when compliance regulations don't allow the data to leave your country.

via - <https://docs.aws.amazon.com/AmazonS3/latest/dev/replication.html>

For every new object, trigger a lambda function to write data into a bucket in another AWS Region - Although this solution is feasible, it's not resource efficient as the lambda is used to do something which S3 CRR can achieve off-the-shelf.

Run a daily job on an EC2 instance to copy objects into another Region - Creating a daily job on EC2 instance to copy objects into another Region involves a lot of development effort. It is much better to use S3 CRR for this task.

Reference:

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

Question 23: **Incorrect**

What is the primary benefit of deploying an RDS database in a Read Replica configuration?

-

Read Replica protects the database from a regional failure

(Incorrect)

-

Read Replica improves database scalability

(Correct)

-

Read Replica enhances database availability

-

Read Replica reduces database usage costs

Explanation

Correct option:

Read Replica improves database scalability

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

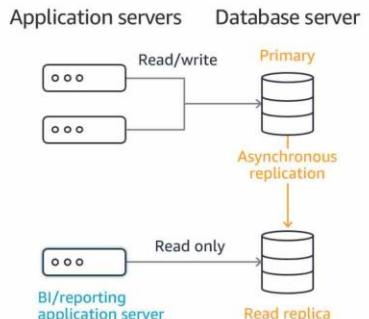
Read Replica

Overview:

Amazon RDS Read Replicas provide enhanced performance and durability for RDS database (DB) instances. They make it easy to elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads. You can create one or more replicas of a given source DB instance and serve high-volume application read traffic from multiple copies of your data, thereby increasing aggregate read throughput. Read replicas can also be promoted when needed to become standalone DB instances. Read replicas are available in Amazon RDS for MySQL, MariaDB, PostgreSQL, Oracle, and SQL Server as well as Amazon Aurora.

For the MySQL, MariaDB, PostgreSQL, Oracle, and SQL Server database engines, Amazon RDS creates a second DB instance using a snapshot of the source DB instance. It then uses the engines' native asynchronous replication to update the read replica whenever there is a change to the source DB instance. The read replica operates as a DB instance that allows only read-only connections; applications can connect to a read replica just as they would to any DB instance. Amazon RDS replicates all databases in the source DB instance.

Amazon Aurora further extends the benefits of read replicas by employing an SSD-backed virtualized storage layer purpose-built for database workloads. Amazon Aurora replicas share the same underlying storage as the source instance, lowering costs and avoiding the need to copy data to the replica nodes. For more information about replication with Amazon Aurora, see the [online documentation](#).



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

Exam Alert:

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

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

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

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

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

Incorrect options:

Read Replica enhances database availability -Amazon RDS Multi-AZ deployments provide enhanced availability and durability for RDS database (DB) instances, making them a natural fit for production database workloads. When you provision a Multi-AZ DB Instance, Amazon RDS automatically creates a primary DB Instance and synchronously replicates the data to a standby instance in a different Availability Zone (AZ). Read Replica cannot enhance database availability.

Read Replica protects the database from a regional failure - You need to use RDS in Multi-Region deployment configuration to protect from a regional failure. Read Replica cannot protect from a regional failure.

Read Replica reduces database usage costs - RDS with Read Replicas increases the database costs compared to the standard deployment. So this option is incorrect.

Reference:

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

Question 24: **Correct**

Which AWS service can be used as an in-memory database with high-performance and low latency?



Amazon ElastiCache

(Correct)



Amazon DynamoDB



Amazon Athena



Amazon RDS

Explanation

Correct option:

Amazon ElastiCache

Amazon ElastiCache allows you to seamlessly set up, run, and scale popular open-Source compatible in-memory data stores in the cloud. Build data-intensive apps or boost the performance of your existing databases by retrieving data from high throughput and low latency in-memory data stores. Amazon ElastiCache is a popular choice for real-time use cases like Caching, Session Stores, Gaming, Geospatial Services, Real-Time Analytics, and Queuing. ElastiCache cannot be used for online analytical processing.

How ElastiCache

Works:



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

Incorrect options:

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. RDS cannot be used as an in-memory database.

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

to have a flexible schema, so each row can have any number of columns at any point in time. This allows you to easily adapt the tables as your business requirements change, without having to redefine the table schema as you would in relational databases. DynamoDB cannot be used as an in-memory database.

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 cannot be used as an in-memory database.

Reference:

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

Question 25: **Correct**

AWS Lambda pricing is based on which of the following criteria? (Select two)

-

The size of the deployment package for the lambda function

-

The time it takes for the lambda function to execute

(Correct)

-

Number of requests for the lambda function

(Correct)

-

The number of lines of code for the lambda function

-

The language runtime of the lambda function

Explanation

Correct options:

Number of requests for the lambda function

The time it takes for the lambda function to execute

AWS Lambda lets you run code without provisioning or managing servers. With Lambda, you can run code for virtually any type of application or backend service - all with zero administration. Just upload your code and Lambda takes care of everything required to run and scale your code with high availability.

With AWS Lambda, you pay only for what you use. You are charged based on the number of requests for your functions and the duration, the time it takes for your code to execute. Lambda counts a request each time it starts executing in response to an event notification or invoke call, including test invokes from the console. Duration is calculated from the time your code begins executing until it returns or otherwise terminates, rounded up to the nearest 100ms.

Incorrect options:

The language runtime of the lambda function - Lambda supports many programming language runtimes such as NodeJS, Python, Go, C# etc. The pricing for a lambda function is not dependent on the language runtime of the lambda function.

The number of lines of code for the lambda function - The pricing for a lambda function is not dependent on the number of lines of code for the lambda function.

The size of the deployment package for the lambda function - The pricing for a lambda function is not dependent on the size of the deployment package for the lambda function.

Reference:

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

Question 26: **Correct**

Gmail is an example of which of the following Cloud Computing Models?

-

Function as a Service (FaaS)

-

Platform as a Service (PaaS)

-

Infrastructure as a Service (IaaS)

-

Software as a Service (SaaS)

(Correct)

Explanation

Correct option:

Software as a Service (SaaS)

Software as a Service (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. Gmail is an example of a SaaS service.

Overview of Cloud Computing

Types:

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) - Infrastructure as a Service (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. EC2 is an example of an IaaS service.

Platform as a Service (PaaS) - Platform as a Service (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. Beanstalk is an example of a PaaS service.

Function as a Service (FaaS) - Function as a service (FaaS) is a category of cloud computing services that provides a platform allowing customers to develop, run, and manage application functionalities without the complexity of building and maintaining the infrastructure typically associated with developing and launching an app. Lambda is an example of a FaaS service.

Reference:

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

Question 27: **Correct**

Which AWS service can be used for online analytical processing?



Amazon Redshift

(Correct)

-

Amazon RDS

-

Amazon DynamoDB

-

Amazon ElastiCache

Explanation

Correct option:

Amazon Redshift

Amazon Redshift is a fast, fully managed cloud data warehouse that makes it simple and cost-effective to analyze all your data using standard SQL and your existing Business Intelligence (BI) tools. It allows you to run complex analytic queries against terabytes to petabytes of structured data, using sophisticated query optimization, columnar storage on high-performance storage, and massively parallel query execution.

Incorrect options:

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.

Customers use Amazon RDS databases primarily for online-transaction processing (OLTP) workload while Redshift is used primarily for reporting and analytics.

Amazon DynamoDB - Amazon DynamoDB is a NoSQL database that supports key-value and document data models and enables developers to build modern, serverless applications that can start small and scale globally to support petabytes of data and tens of millions of read and write requests per second. DynamoDB supports both key-value and document data models. This enables DynamoDB to have a flexible schema, so each row can have any number of columns at any point in time. This allows you to easily adapt the tables as your business requirements change, without having to redefine the table schema as you would in relational databases. DynamoDB cannot be used for online analytical processing.

Amazon ElastiCache - Amazon ElastiCache allows you to seamlessly set up, run, and scale popular open-Source compatible in-memory data stores in the cloud. Build data-intensive apps or boost the performance of your existing databases by retrieving data from high throughput and low latency in-memory data stores. Amazon ElastiCache is a popular choice for real-time use cases like Caching, Session Stores, Gaming, Geospatial Services, Real-Time Analytics, and Queuing. ElastiCache cannot be used for online analytical processing.

Reference:

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

Question 28: **Correct**

An AWS hardware failure has impacted one of your EBS volumes. Which AWS service will alert you of the affected resources and provide a remedial action?



Amazon GuardDuty



AWS Personal Health Dashboard

(Correct)



AWS Config



AWS Trusted Advisor

Explanation

Correct option:

AWS Personal Health Dashboard

AWS Personal Health Dashboard provides alerts and remediation guidance when AWS is experiencing events that may impact you. 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. 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. For example, in the event of an AWS hardware failure impacting one of your EBS volumes, you will get an alert that includes a list of your affected resources, a recommendation to restore your volume, and links to the steps to help you restore it from a snapshot.

Incorrect options:

Amazon GuardDuty - Amazon GuardDuty is a threat detection service that monitors malicious activity and unauthorized behavior to protect your AWS account. GuardDuty analyzes billions of events across your AWS accounts from AWS CloudTrail (AWS user and API activity in your accounts), Amazon VPC Flow Logs (network traffic data), and DNS Logs (name query patterns).

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.

AWS Trusted Advisor - AWS Trusted Advisor is an online tool that provides real-time guidance to help you provision your resources following AWS best practices. Whether establishing new workflows, developing applications, or as part of ongoing improvement, recommendations provided by Trusted Advisor on a regular basis help keep your solutions provisioned optimally.

Reference:

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

Question 29: **Incorrect**

Which of the following are correct statements regarding the AWS Shared Responsibility Model?
(Select two)

- **AWS is responsible for training AWS and customer employees on AWS products and services**
- **AWS is responsible for Security "of" the Cloud**
(Correct)
- **For a service like Amazon EC2, that falls under Infrastructure as a Service, AWS is responsible for maintaining guest operating system**
- **Configuration Management is the responsibility of the customer**
(Incorrect)
- **For abstracted services like Amazon S3, AWS operates the infrastructure layer, the operating system, and platforms**

Explanation

Correct options:

Security and Compliance is a shared responsibility between AWS and the customer. This shared model can help relieve the customer's operational burden as AWS operates, manages and controls the

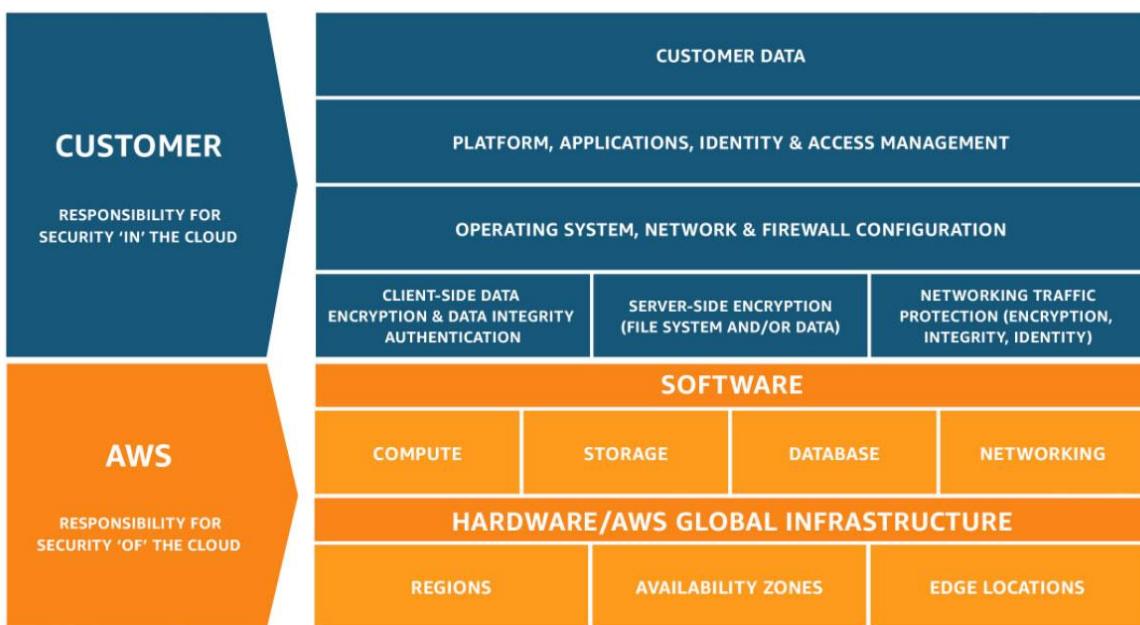
components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates.

AWS is responsible for Security "of" the Cloud - AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services.

"For abstracted services like Amazon S3, AWS operates the infrastructure layer, the operating system, and platforms" - For abstracted services, such as Amazon S3 and Amazon DynamoDB, AWS operates the infrastructure layer, the operating system, and platforms, and customers access the endpoints to store and retrieve data.

Shared Responsibility Model

Overview:



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

Incorrect options:

For a service like Amazon EC2, that falls under Infrastructure as a Service, AWS is responsible for maintaining guest operating system - A service such as Amazon Elastic Compute Cloud (Amazon EC2) is categorized as Infrastructure as a Service (IaaS) and, as such, requires the customer to perform all of the necessary security configuration and management tasks. Customers are responsible for the management of the guest operating system (including updates and security patches), any application software or utilities installed by the customer on the instances, and the configuration of the AWS-provided firewall (called a security group) on each instance.

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

AWS is responsible for training AWS and customer employees on AWS products and services - Awareness & Training is also a shared responsibility. AWS trains AWS employees, but a customer must train their own employees.

Reference:

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

Question 30: **Incorrect**

AWS Trusted Advisor analyzes your AWS environment and provides best practice recommendations for which of the following categories? (Select two)?

-

Cost Optimization

(Correct)

-

Change Management

-

Service Limits

(Correct)

-

Elasticity

-

Documentation

(Incorrect)

Explanation

Correct options:

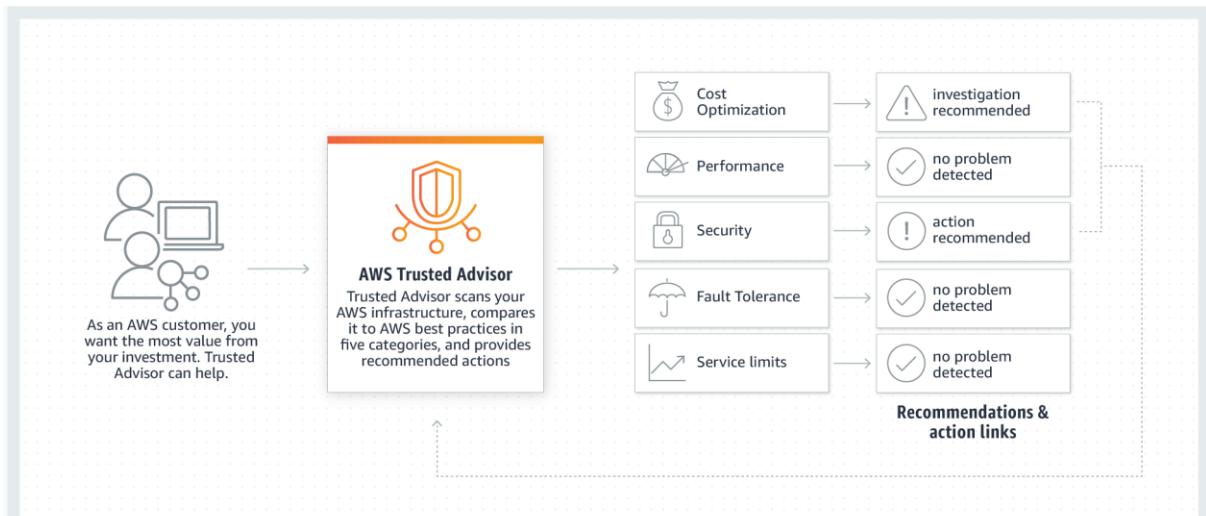
Cost Optimization

Service Limits

AWS Trusted Advisor is an online tool that provides real-time guidance to help provision your resources following AWS best practices. Whether establishing new workflows, developing applications, or as part of ongoing improvement, recommendations provided by Trusted Advisor on a regular basis help keep your solutions provisioned optimally. AWS Trusted Advisor analyzes your AWS environment and provides best practice recommendations in five categories: Cost Optimization, Performance, Security, Fault Tolerance, Service Limits.

How Trusted Advisor

Works:



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

AWS Trusted Advisor Recommendations:

Like your customized cloud expert, AWS Trusted Advisor analyzes your AWS environment and provides best practice recommendations in five categories:



Core Checks & Recommendations

All AWS customers get access to the seven core Trusted Advisor checks to help increase the security and performance of the AWS environment. Checks include:

Security

- S3 Bucket Permissions
- Security Groups - Specific Ports Unrestricted
- IAM Use
- MFA on Root Account
- EBS Public Snapshots
- RDS Public Snapshots

Service Limits

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

Incorrect options:

Elasticity

Documentation

Change Management

These three options are made-up and have no importance in the context of AWS Trusted Advisor.

Reference:

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

Question 31: **Correct**

Which of the following are recommended best practices for AWS IAM service? (Select two)

-

Create a minimum number of accounts and share these account credentials among employees

-

Enable MFA for all users

(Correct)

-

Rotate credentials regularly

(Correct)

-

Grant maximum privileges to avoid assigning privileges again

-

Share AWS account root user access keys with other administrators

Explanation

Correct option:

Enable MFA for all users - AWS recommends that you require multi-factor authentication (MFA) for all users in your account. With MFA, users have a device that generates a response to an authentication challenge. Both the user's credentials and the device-generated response are required to complete the sign-in process.

Rotate credentials regularly - AWS recommends that you change your own passwords and access keys regularly, and make sure that all IAM users in your account do as well. That way, if a password or access key is compromised without your knowledge, you limit how long the credentials can be used to access your resources. You can apply a password policy to your account to require all your IAM users to rotate their passwords.

AWS IAM security best practices:

Security Best Practices in IAM

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

To help secure your AWS resources, follow these recommendations for the AWS Identity and Access Management (IAM) service.

Topics

- [Lock Away Your AWS Account Root User Access Keys](#)
- [Create Individual IAM Users](#)
- [Use Groups to Assign Permissions to IAM Users](#)
- [Grant Least Privilege](#)
- [Get Started Using Permissions with AWS Managed Policies](#)
- [Use Customer Managed Policies Instead of Inline Policies](#)
- [Use Access Levels to Review IAM Permissions](#)
- [Configure a Strong Password Policy for Your Users](#)
- [Enable MFA](#)
- [Use Roles for Applications That Run on Amazon EC2 Instances](#)
- [Use Roles to Delegate Permissions](#)
- [Do Not Share Access Keys](#)
- [Rotate Credentials Regularly](#)
- [Remove Unnecessary Credentials](#)
- [Use Policy Conditions for Extra Security](#)
- [Monitor Activity in Your AWS Account](#)

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

Incorrect options: **Create a minimum number of accounts and share these account credentials among employees** - AWS recommends that user account credentials should not be shared between users.

Grant maximum privileges to avoid assigning privileges again - AWS recommends granting the least privileges required to complete a certain job and avoid giving excessive privileges which can be misused.

Share AWS account root user access keys with other administrators - The access key for your AWS account root user gives full access to all your resources for all AWS services, including your billing information. You cannot reduce the permissions associated with your AWS account root user access key. You should never share these access keys with any other users, not even the administrators.

Reference:

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

Question 32: **Correct**

Compared to the On-demand prices, what is the highest possible discount offered for reserved instances?

50

72

(Correct)

90

40

Explanation

Correct option:

72

Reserved Instances provide you with significant savings (up to 72%) on your Amazon EC2 costs compared to On-Demand Instance pricing. Reserved Instances are not physical instances, but rather a billing discount applied to the use of On-Demand Instances in your account. You can purchase a Reserved Instance for a one-year or three-year commitment, with the three-year commitment offering a bigger discount.

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 »](#)

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

Incorrect options:

90

50

40

Reference:

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

Question 33: **Correct**

An IT company has a hybrid cloud architecture and it wants to centralize the server logs for its EC2 instances and on-premises servers. Which of the following is the MOST effective for this use-case?



Use CloudWatch Logs for both the EC2 instance and the on-premises servers

(Correct)



Use AWS Lambda to send log data from EC2 instance as well as on-premises servers to CloudWatch Logs

-

Use CloudTrail for the EC2 instance and CloudWatch Logs for the on-premises servers

-

Use CloudWatch Logs for the EC2 instance and CloudTrail for the on-premises servers

Explanation

Correct option:

Use CloudWatch Logs for both the EC2 instance and the on-premises servers

You can use Amazon CloudWatch Logs to monitor, store, and access your log files from Amazon Elastic Compute Cloud (Amazon EC2) instances, AWS CloudTrail, Route 53, and other sources such as on-premises servers.

CloudWatch Logs enables you to centralize the logs from all of your systems, applications, and AWS services that you use, in a single, highly scalable service. You can then easily view them, search them for specific error codes or patterns, filter them based on specific fields, or archive them securely for future analysis.

Incorrect options:

Use AWS Lambda to send log data from EC2 instance as well as on-premises servers to CloudWatch Logs

AWS Lambda lets you run code without provisioning or managing servers. You pay only for the compute time you consume. Lambda cannot be used to centralize the logs from EC2 instances and on-premises servers.

Use CloudWatch Logs for the EC2 instance and CloudTrail for the on-premises servers

Use CloudTrail for the EC2 instance and CloudWatch Logs for the on-premises servers

AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command-line tools, and other AWS services. CloudTrail cannot be used to centralize the server logs for EC2 instances or on-premises servers, so both these options are incorrect.

References:

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

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

Question 34: **Correct**

Which AWS Route 53 routing policy would you use when you want to route your traffic in an active-passive configuration?

-
-

Failover routing policy

(Correct)

-
-

Simple routing policy

-
-

Weighted routing policy

-
-

Latency routing policy

Explanation

Correct option:

Failover routing policy

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

Failover routing policy is used when you want to configure active-passive failover. Failover routing lets you route traffic to a resource when the resource is healthy or to a different resource when the first resource is unhealthy. The primary and secondary records can route traffic to anything from an Amazon S3 bucket that is configured as a website to a complex tree of records.

Route 53 Routing Policy

Overview:

Choosing a routing policy

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

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

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

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

Incorrect options:

Simple routing policy - Simple routing lets you configure standard DNS records, with no special Route 53 routing such as weighted or latency. With simple routing, you typically route traffic to a single resource, for example, to a web server for your website.

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

Latency routing policy - This routing policy is used when you have resources in multiple AWS Regions and you want to route traffic to the region that provides the best latency.

Reference:

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

Question 35: **Incorrect**

Which AWS services support High Availability by default? (Select two)

-

EFS

(Correct)

-

Instance Store

-

DynamoDB

(Correct)

-

Redshift

-

EBS

(Incorrect)

Explanation

Correct options:

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. All of your data is stored on solid-state disks (SSDs) and is automatically replicated across multiple Availability Zones in an AWS Region, providing built-in high availability and data durability.

DynamoDB High

Availability:

High Availability and Durability

DynamoDB automatically spreads the data and traffic for your tables over a sufficient number of servers to handle your throughput and storage requirements, while maintaining consistent and fast performance. All of your data is stored on solid-state disks (SSDs) and is automatically replicated across multiple Availability Zones in an AWS Region, providing built-in high availability and data durability. You can use global tables to keep DynamoDB tables in sync across AWS Regions. For more information, see [Global Tables: Multi-Region Replication with DynamoDB](#).

via - <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Introduction.html>

EFS - Amazon Elastic File System (Amazon EFS) provides a simple, scalable, fully managed elastic NFS file system for use with AWS Cloud services and on-premises resources. It is built to scale on-demand to petabytes without disrupting applications, growing and shrinking automatically as you add and remove files, eliminating the need to provision and manage capacity to accommodate growth. Amazon EFS is a regional service storing data within and across multiple Availability Zones (AZs) for high availability and durability.

EFS High

Availability:

Q. What is Amazon Elastic File System?

Amazon EFS is a fully-managed service that makes it easy to set up, scale, and cost-optimize file storage in the Amazon Cloud. With a few clicks in the AWS Management Console, you can create file systems that are accessible to Amazon EC2 instances via a file system interface (using standard operating system file I/O APIs) and support full file system access semantics (such as strong consistency and file locking).

Amazon EFS file systems can automatically scale from gigabytes to petabytes of data without needing to provision storage. Tens, hundreds, or even thousands of Amazon EC2 instances can access an Amazon EFS file system at the same time, and Amazon EFS provides consistent performance to each Amazon EC2 instance. Amazon EFS is designed to be highly durable and highly available. With Amazon EFS, there is no minimum fee or setup costs, and you pay only for what you use.

via - <https://aws.amazon.com/efs/faq/>

Incorrect options:

Redshift - Amazon Redshift is a fast, fully managed cloud data warehouse that makes it simple and cost-effective to analyze all your data using standard SQL and your existing Business Intelligence (BI) tools.

Amazon Redshift only supports Single-AZ deployments:

Q: Does Amazon Redshift support Multi-AZ Deployments?

Currently, Amazon Redshift only supports Single-AZ deployments. You can run data warehouse clusters in multiple AZ's by loading data into two Amazon Redshift data warehouse clusters in separate AZs from the same set of Amazon S3 input files. With Redshift Spectrum, you can spin up multiple clusters across AZs and access data in Amazon S3 without having to load it into your cluster. In addition, you can also restore a data warehouse cluster to a different AZ from your data warehouse cluster snapshots.

via - <https://aws.amazon.com/redshift/faqs/>

EBS - Amazon Elastic Block Store (EBS) is an easy to use, high-performance block storage service designed for use with Amazon Elastic Compute Cloud (EC2) for both throughput and transaction-intensive workloads at any scale. EBS volumes are replicated within an Availability Zone (AZ) and can easily scale to petabytes of data.

Instance Store - As Instance Store volumes are tied to an EC2 instance, they are also single AZ entities.

References:

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

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Introduction.html>

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

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

Question 36: **Correct**

A medical device company is looking for a durable and cost-effective way of storing their historic data. Due to compliance requirements, the data must be stored for 10 years. Which AWS Storage solution will you suggest?

-
-

S3 Glacier Deep Archive

(Correct)

-
-

S3 Glacier

-
-

AWS Storage Gateway

-
-

Amazon EFS

Explanation

Correct option:

S3 Glacier Deep Archive

S3 Glacier Deep Archive is Amazon S3's lowest-cost storage class and supports long-term retention and digital preservation for data that may be accessed once or twice in a year. It is designed for customers — particularly those in highly-regulated industries, such as the Financial Services, Healthcare, and Public Sectors — that retain data sets for 7-10 years or longer to meet regulatory compliance requirements. S3 Glacier Deep Archive can also be used for backup and disaster recovery use cases. It has a retrieval time (first byte latency) of 12 to 48 hours.

S3 Glacier Deep Archive

Overview:

Amazon S3 Glacier Deep Archive (S3 Glacier Deep Archive)

S3 Glacier Deep Archive is Amazon S3's lowest-cost storage class and supports long-term retention and digital preservation for data that may be accessed once or twice in a year. It is designed for customers — particularly those in highly-regulated industries, such as the Financial Services, Healthcare, and Public Sectors — that retain data sets for 7-10 years or longer to meet regulatory compliance requirements. S3 Glacier Deep Archive can also be used for backup and disaster recovery use cases, and is a cost-effective and easy-to-manage alternative to magnetic tape systems, whether they are on-premises libraries or off-premises services. S3 Glacier Deep Archive complements Amazon S3 Glacier, which is ideal for archives where data is regularly retrieved and some of the data may be needed in minutes. All objects stored in S3 Glacier Deep Archive are replicated and stored across at least three geographically-dispersed Availability Zones, protected by 99.99999999% of durability, and can be restored within 12 hours.

Key Features:

- Designed for durability of 99.99999999% of objects across multiple Availability Zones
- Lowest cost storage class designed for long-term retention of data that will be retained for 7-10 years
- Ideal alternative to magnetic tape libraries
- Retrieval time within 12 hours
- S3 PUT API for direct uploads to S3 Glacier Deep Archive, and S3 Lifecycle management for automatic migration of objects

via - <https://aws.amazon.com/s3/storage-classes/>

Incorrect options:

S3 Glacier - Amazon S3 Glacier is a secure, durable, and extremely low-cost Amazon S3 cloud storage class for data archiving and long-term backup. It is designed to deliver 99.99999999% durability, and provide comprehensive security and compliance capabilities that can help meet even the most stringent regulatory requirements. Glacier Deep Archive is a better fit as it is more cost-optimal than Glacier for the given use-case.

AWS Storage Gateway - AWS Storage Gateway is a hybrid cloud storage service that gives you on-premises access to virtually unlimited cloud storage. All data transferred between the gateway and AWS storage is encrypted using SSL (for all three types of gateways - File, Volume and Tape Gateways). Storage Gateway cannot be used for data archival.

Amazon EFS - Amazon Elastic File System (Amazon EFS) provides a simple, scalable, fully managed elastic NFS file system for use with AWS Cloud services and on-premises resources. It is built to scale on-demand to petabytes without disrupting applications, growing and shrinking automatically as you add and remove files, eliminating the need to provision and manage capacity to accommodate growth.

Reference:

<https://aws.amazon.com/s3/storage-classes/>

Question 37: **Correct**

Which of the following statements is correct regarding the AWS Elastic File System (EFS) storage service?

-

EC2 instances can access files on an EFS file system across many Availability Zones but not across VPCs and Regions

-

EC2 instances can access files on an EFS file system only in one Availability Zone

-

EC2 instances can access files on an EFS file system across many Availability Zones, Regions and VPCs

(Correct)

-

EC2 instances can access files on an EFS file system across many Availability Zones and VPCs but not across Regions

Explanation

Correct option:

EC2 instances can access files on an EFS file system across many Availability Zones, Regions and VPCs

Amazon EFS is a regional service storing data within and across multiple Availability Zones (AZs) for high availability and durability. Amazon EC2 instances can access your file system across AZs, regions, and VPCs, while on-premises servers can access using AWS Direct Connect or AWS VPN.

Amazon EFS

Overview:

Amazon Elastic File System (Amazon EFS) provides a simple, scalable, fully managed elastic NFS file system for use with AWS Cloud services and on-premises resources. It is built to scale on demand to petabytes without disrupting applications, growing and shrinking automatically as you add and remove files, eliminating the need to provision and manage capacity to accommodate growth.

Amazon EFS offers two storage classes: the Standard storage class, and the [Infrequent Access storage class \(EFS IA\)](#). EFS IA provides price/performance that's cost-optimized for files not accessed every day. By simply enabling EFS Lifecycle Management on your file system, files not accessed according to the lifecycle policy you choose will be automatically and transparently moved into EFS IA. The EFS IA storage class costs only \$0.025/GB-month*.

While workload patterns vary, customers typically find that 80% of files are infrequently accessed (and suitable for EFS IA), and 20% are actively used (suitable for EFS Standard), resulting in an effective storage cost as low as \$0.08/GB-month*. Amazon EFS transparently serves files from both storage classes in a common file system namespace.

Amazon EFS is designed to provide massively parallel shared access to thousands of Amazon EC2 instances, enabling your applications to achieve high levels of aggregate throughput and IOPS with consistent low latencies.

Amazon EFS is well suited to support a broad spectrum of use cases from home directories to business-critical applications. Customers can use EFS to lift-and-shift existing enterprise applications to the AWS Cloud. Other use cases include: big data analytics, web serving and content management, application development and testing, media and entertainment workflows, database backups, and container storage.

Amazon EFS is a regional service storing data within and across multiple Availability Zones (AZs) for high availability and durability. Amazon EC2 instances can access your file system across AZs, regions, and VPCs, while on-premises servers can access using AWS Direct Connect or AWS VPN.

via - <https://aws.amazon.com/efs/>

Incorrect options:

EC2 instances can access files on an EFS file system only in one Availability Zone

EC2 instances can access files on an EFS file system across many Availability Zones but not across VPCs and Regions

EC2 instances can access files on an EFS file system across many Availability Zones and VPCs but not across Regions

These three options contradict the details provided earlier in the explanation, so these options are incorrect.

Reference:

<https://aws.amazon.com/efs/>

Question 38: **Correct**

An IT company has deployed a static website on S3, but the website is still inaccessible. As a Cloud Practitioner, which of the following solutions would you suggest to address this issue?

-
-

Fix the S3 bucket policy

(Correct)

-
-

Enable S3 replication

-
-

Enable S3 versioning

-
-

Disable S3 encryption

Explanation

Correct options:

Fix the S3 bucket policy

To host a static website on Amazon S3, you configure an Amazon S3 bucket for website hosting and then upload your website content to the bucket. When you configure a bucket as a static website, you must enable website hosting, set permissions, and create and add an index document.

Hosting a static website on Amazon S3:

Hosting a static website on Amazon S3

[PDF](#) | [Kindle](#) | [RSS](#)

You can use Amazon S3 to host a static website. On a *static* website, individual webpages include static content. They might also contain client-side scripts.

By contrast, a *dynamic* website relies on server-side processing, including server-side scripts such as PHP, JSP, or ASP.NET. Amazon S3 does not support server-side scripting, but AWS has other resources for hosting dynamic websites. To learn more about website hosting on AWS, see [Web Hosting](#).

To configure your bucket for static website hosting, you can use the AWS Management Console without writing any code. You can also create, update, and delete the website configuration *programmatically* by using the AWS SDKs. The SDKs provide wrapper classes around the Amazon S3 REST API. If your application requires it, you can send REST API requests directly from your application.

To host a static website on Amazon S3, you configure an Amazon S3 bucket for website hosting and then upload your website content to the bucket. When you configure a bucket as a static website, you must [enable website hosting](#), [set permissions](#), and [create and add an index document](#). Depending on your website requirements, you can also [configure redirects](#), [web traffic logging](#), and a [custom error document](#).

After you configure your bucket as a static website, you can access the bucket through the AWS Region-specific Amazon S3 website endpoints for your bucket. Website endpoints are different from the endpoints where you send REST API requests. For more information, see [Website endpoints](#).

via - <https://docs.aws.amazon.com/AmazonS3/latest/dev/WebsiteHosting.html>

If you want to configure an existing bucket as a static website that has public access, you must edit block public access settings for that bucket. You may also have to edit your account-level block public access settings. Amazon S3 applies the most restrictive combination of the bucket-level and account-level block public access settings.

Here is how you can edit Public Access settings for S3 buckets:

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)



Account settings for Block Public Access are currently turned on

Account settings for Block Public Access that are enabled apply even if they are disabled for this bucket.

Block all public access

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

Block public access to buckets and objects granted through new access control lists (ACLs)

S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

Block public access to buckets and objects granted through any access control lists (ACLs)

S3 will ignore all ACLs that grant public access to buckets and objects.

Block public access to buckets and objects granted through new public bucket or access point policies

S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

Block public and cross-account access to buckets and objects through any public bucket or access point policies

S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

via - <https://docs.aws.amazon.com/AmazonS3/latest/dev/WebsiteAccessPermissionsReqd.html>

Incorrect options:

Disable S3 encryption

Enable S3 versioning

Enable S3 replication

Disabling S3 encryption, enabling S3 versioning or replication have no bearing on deploying a static website on S3, so these options are not correct.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/WebsiteHosting.html>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/WebsiteAccessPermissionsReqd.html>

Question 39: **Correct**

Which of the following statements are CORRECT regarding Security Groups and Network Access Control Lists (NACLs)? (Select two)

-

A NACL is stateful, that is, it automatically allows the return traffic

-

A Security Group contains a numbered list of rules and evaluates these rules in the increasing order while deciding whether to allow the traffic

-

A Security Group is stateless, that is, the return traffic must be explicitly allowed

-

A Security Group is stateful, that is, it automatically allows the return traffic

(Correct)

-

A NACL contains a numbered list of rules and evaluates these rules in the increasing order while deciding whether to allow the traffic

(Correct)

Explanation

Correct options:

A Security Group is stateful, that is, it automatically allows the return traffic

A NACL contains a numbered list of rules and evaluates these rules in the increasing order while deciding whether to allow the traffic

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. Security groups are stateful — if you send a request from your instance, the response traffic for that request is allowed to flow in regardless of inbound security group rules. A security group evaluates all rules before deciding whether to allow traffic.

Security Group

Overview:

Security group basics

The following are the basic characteristics of security groups for your VPC:

- There are quotas on the number of security groups that you can create per VPC, the number of rules that you can add to each security group, and the number of security groups that you can associate with a network interface. For more information, see [Amazon VPC quotas](#).
- You can specify allow rules, but not deny rules.
- You can specify separate rules for inbound and outbound traffic.
- When you create a security group, it has no inbound rules. Therefore, no inbound traffic originating from another host to your instance is allowed until you add inbound rules to the security group.
- By default, a security group includes an outbound rule that allows all outbound traffic. You can remove the rule and add outbound rules that allow specific outbound traffic only. If your security group has no outbound rules, no outbound traffic originating from your instance is allowed.
- Security groups are stateful — if you send a request from your instance, the response traffic for that request is allowed to flow in regardless of inbound security group rules. Responses to allowed inbound traffic are allowed to flow out, regardless of outbound rules.

Note

Some types of traffic are tracked differently from other types. For more information, see [Connection tracking in the Amazon EC2 User Guide for Linux Instances](#).

- Instances associated with a security group can't talk to each other unless you add rules allowing the traffic (exception: the default security group has these rules by default).
- Security groups are associated with network interfaces. After you launch an instance, you can change the security groups that are associated with the instance, which changes the security groups associated with the primary network interface (eth0). You can also specify or change the security groups associated with any other network interface. By default, when you create a network interface, it's associated with the default security group for the VPC, unless you specify a different security group. For more information about network interfaces, see [Elastic network interfaces](#).
- When you create a security group, you must provide it with a name and a description. The following rules apply:
 - Names and descriptions can be up to 255 characters in length.
 - Names and descriptions are limited to the following characters: a-z, A-Z, 0-9, spaces, and _-:/()#@[]+=&;!\$*.
 - A security group name cannot start with Sg- as these indicate a default security group.
 - A security group name must be unique within the VPC.
- A security group can only be used in the VPC that you specify when you create the security group.

via - https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html

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 contains a numbered list of rules. A NACL evaluates 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. AWS recommends 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.

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:

A Security Group contains a numbered list of rules and evaluates these rules in the increasing order while deciding whether to allow the traffic

A NACL is stateful, that is, it automatically allows the return traffic

A Security Group is stateless, that is, the return traffic must be explicitly allowed

These three options contradict the details provided earlier in the explanation, so these options are incorrect.

References:

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html>

Question 40: **Correct**

Which of the following capabilities does Amazon Rekognition provide as a ready-to-use feature?



Human pose detection



Identify objects in a photo

(Correct)

-

Resize images quickly

-

Convert images into greyscale

Explanation

Correct option:

Identify objects in a photo

With Amazon Rekognition, you can identify objects, people, text, scenes, and activities in images and videos, as well as detect any inappropriate content. Amazon Rekognition also provides highly accurate facial analysis and facial search capabilities that you can use to detect, analyze, and compare faces for a wide variety of user verification, people counting, and public safety use cases.

Amazon Rekognition Use-Cases:

Key features



Labels

With Amazon Rekognition, you can identify thousands of objects (such as bike, telephone, building), and scenes (such as parking lot, beach, city). When analyzing video, you can also identify specific activities such as "delivering a package" or "playing soccer". [Learn more »](#)



Content moderation

Amazon Rekognition helps you identify potentially unsafe or inappropriate content across both image and video assets and provides you with detailed labels that allow you to accurately control what you want to allow based on your needs. Use [Amazon A2I](#) to enhance the accuracy of Amazon Rekognition image moderation predictions using human review. [Learn more »](#)

via - <https://aws.amazon.com/rekognition/>

Custom labels

With Amazon Rekognition Custom Labels, you can extend the detection capabilities of Amazon Rekognition to extract information from images that is uniquely helpful to your business. For example, you can find your corporate logo in social media, identify your products on store shelves, classify your machine parts in an assembly line, or detect your animated characters in videos. [Learn more »](#)



Text detection

In photos and videos, text appears very differently than neat words on a printed page. Amazon Rekognition can read skewed and distorted text to capture information like store names, forced narratives overlaid on media, street signs, and text on product packaging. [Learn more »](#)



Face detection and analysis

With Amazon Rekognition, you can easily detect when faces appear in images and videos and get attributes such as gender, age range, eyes open, glasses, facial hair for each. In video, you can also measure how these face attributes change over time, such as constructing a timeline of the emotions expressed by an actor. [Learn more »](#)



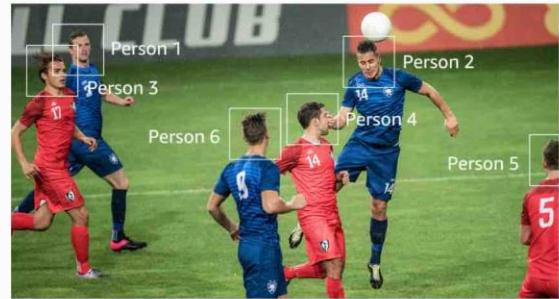
Face search and verification

Amazon Rekognition provides fast and accurate face search, allowing you to identify a person in a photo or video using your private repository of face images. You can also verify identity by analyzing a face image against images you have stored for comparison. [Learn more »](#)



Celebrity recognition

You can quickly identify well known people in your video and image libraries to catalog footage and photos for marketing, advertising, and media industry use cases. [Learn more »](#)



Pathing

You can capture the path of people in the scene when using Amazon Rekognition with video files. For example, you can use the movement of athletes during a game to identify plays for post-game analysis. [Learn more »](#)

via - <https://aws.amazon.com/rekognition/>

Incorrect options:

Convert images into greyscale

Resize images quickly

Human pose detection

Amazon Rekognition does not do image processing tasks such as converting images to greyscale or resizing images. Human pose detection is not available in Amazon Rekognition.

Reference:

Question 41: **Correct**

AWS Identity and Access Management (IAM) policies are written as JSON documents. Which of the following are mandatory elements of an IAM policy?

-

Effect, Action

(Correct)

- ○
Sid, Principal
- ○
Action, Condition

- ○
Effect, Sid

Explanation

Correct option:

Effect, Action - Most policies are stored in AWS as JSON documents. Identity-based policies and policies used to set permissions boundaries are JSON policy documents that you attach to a user or role. Resource-based policies are JSON policy documents that you attach to a resource.

A JSON policy document includes these elements:

1. Optional policy-wide information at the top of the document
2. One or more individual statements

Each statement includes information about a single permission. The information in a statement is contained within a series of elements.

1. Version – Specify the version of the policy language that you want to use. As a best practice, use the latest 2012-10-17 version.
2. Statement – Use this main policy element as a container for the following elements. You can include more than one statement in a policy.
 - a. Sid (Optional) – Include an optional statement ID to differentiate between your statements.
 - b. Effect – Use Allow or Deny to indicate whether the policy allows or denies access.
 - c. Principal (Required in only some circumstances) – If you create a resource-based policy, you must indicate the account, user, role, or federated user to which you would like to allow or deny access. If you are creating an IAM permissions policy to attach to a user or role, you cannot include this element. The principal is implied as that user or role.
 - d. Action – Include a list of actions that the policy allows or denies.
 - e. Resource (Required in only some circumstances) – If you create an IAM permissions policy, you must specify a list of resources to which the actions apply. If you create a resource-based policy, this element is optional. If you do not include this element, then the resource to which the action applies is the resource to which the policy is attached.
 - f. Condition (Optional) – Specify the circumstances under which the policy grants permission.

Incorrect options:

Sid, Principal

Action, Condition

Effect, Sid

These three options contradict the explanation provided above, so these options are incorrect.

Reference:

https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html#access_policies-json

Question 42: **Correct**

A development team is looking out for a forum where the most frequent questions and requests from AWS customers are listed along with AWS provided solutions.

Which AWS forum/service is the optimal place to start when looking for troubleshooting an issue or checking for a solution?



AWS Marketplace



AWS Support Center



AWS Service Health Dashboard



AWS Knowledge Center

(Correct)

Explanation

Correct option:

AWS Knowledge Center - AWS Knowledge Center contains the most frequent & common questions and requests and AWS provided solutions for the same. This should be the starting point of checking for a solution or troubleshooting an issue with AWS services. The URL for Knowledge Center is <https://aws.amazon.com/premiumsupport/knowledge-center/>.

Incorrect options:

AWS Marketplace - The AWS Marketplace enables qualified partners to market and sell their software to AWS Customers. AWS Marketplace is an online software store that helps customers find, buy, and immediately start using the software and services that run on AWS.

AWS Marketplace is designed for Independent Software Vendors (ISVs), Value-Added Resellers (VARs), and Systems Integrators (SIs) who have software products they want to offer to customers in the

cloud. Partners use AWS Marketplace to be up and running in days and offer their software products to customers around the world.

AWS Support Center - AWS Support Center is the hub for managing your Support cases. The Support Center is accessible through the AWS Management Console, providing federated access support. All Developer-level and higher Support customers can open a Technical Support case online through the Support Center. Business and Enterprise-level customers can ask Support to call at a convenient phone number or strike up a conversation with one of our engineers via chat. Enterprise-level customers can have direct access to their dedicated Technical Account Manager.

AWS Service Health Dashboard - Amazon Web Services publishes up-to-the-minute information on service availability in a tabular form through its Service Health Dashboard page. You can check the page any time to get current status information or subscribe to an RSS feed to be notified of interruptions to each service. The page can be accessed via the URL - <https://status.aws.amazon.com/>.

References:

<https://aws.amazon.com/premiumsupport/knowledge-center/>

<https://status.aws.amazon.com/>

Question 43: **Correct**

A multi-national company has its business-critical data stored on a fleet of Amazon EC2 instances, in various countries, configured in region-specific compliance rules. To demonstrate compliance, the company needs to submit historical configurations on a regular basis. Which AWS service is best suited for this requirement?

-
-

AWS CloudTrail

-
-

AWS Config

(Correct)

-
-

Amazon Macie

-
-

Amazon GuardDuty

Explanation

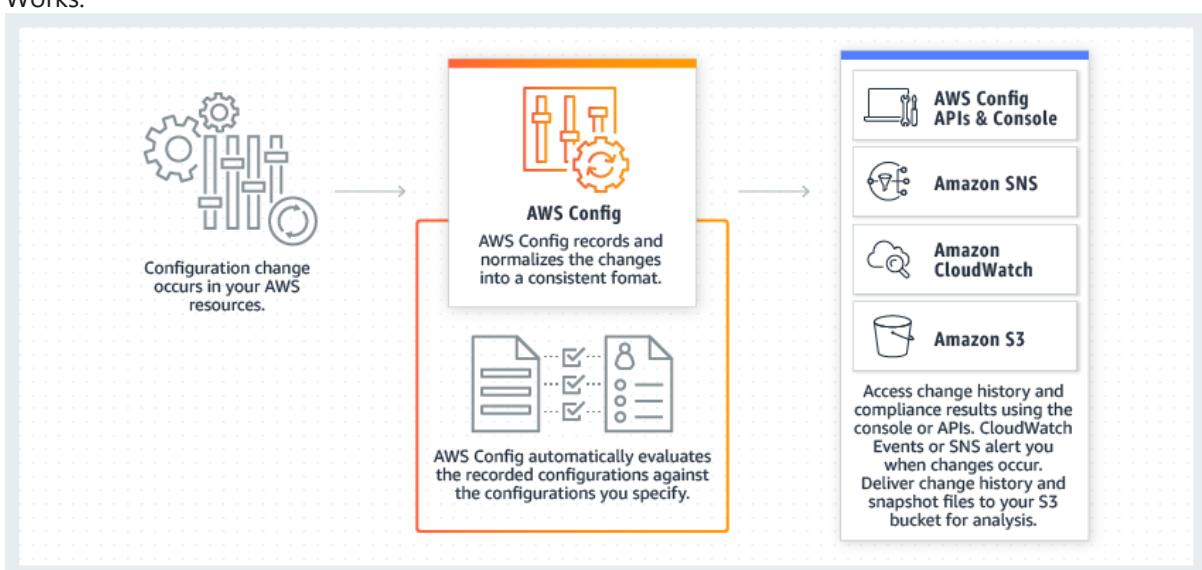
Correct option:

AWS Config

AWS Config provides a detailed view of the configuration of AWS resources in your AWS account. This includes how the resources are related to one another and how they were configured in the past so

that you can see how the configurations and relationships change over time. AWS Config is designed to help you oversee your application resources in the following scenarios: Resource Administration, Auditing and Compliance, Managing and Troubleshooting Configuration Changes, Security Analysis.

How AWS Config Works:



via - <https://aws.amazon.com/config/>

Incorrect options:

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. Macie helps identify and alert you to sensitive data, such as personally identifiable information (PII). This service is an added security feature for data privacy and is not the best fit for the current requirement.

AWS CloudTrail - AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. CloudTrail provides an event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command-line tools, and other AWS services.

Config is focused on the configuration of your AWS resources and reports with detailed snapshots on how your resources have changed. Whereas CloudTrail focuses on the events or API calls, that drive those changes. It focuses on the user, application, and activity performed on the system.

Amazon GuardDuty - Amazon GuardDuty is a threat detection service that monitors malicious activity and unauthorized behavior to protect your AWS account. GuardDuty analyzes billions of events across your AWS accounts from AWS CloudTrail, Amazon VPC Flow Logs, and DNS Logs. Its a threat detection service and not a configuration management and tracking service.

References:

<https://aws.amazon.com/config/>

<https://docs.aws.amazon.com/config/latest/developerguide/WhatIsConfig.html>

Question 44: **Incorrect**

A financial services enterprise plans to enable Multi-Factor Authentication (MFA) for its employees. For ease of travel, they prefer not to use any physical devices to implement MFA. Which of the below options is best suited for this use case?



Virtual MFA device

(Correct)



U2F security key

(Incorrect)



Hardware MFA device



Soft Token MFA device

Explanation

Correct option:

Virtual MFA device

A software app that runs on a phone or other device and emulates a physical device. The device generates a six-digit numeric code based upon a time-synchronized one-time password algorithm. The user must type a valid code from the device on a second webpage during sign-in. Each virtual MFA device assigned to a user must be unique. A user cannot type a code from another user's virtual MFA device to authenticate.

Google Authenticator is an example of a Virtual MFA device:

The screenshot shows the Google Authenticator app interface. At the top, there is a blue header bar with a menu icon (three horizontal lines), the text "Authenticator", a plus sign (+) for adding new accounts, and a pencil icon for editing. Below the header, there are three account entries, each consisting of a large blue QR code and a service name followed by a smaller blue QR code.

Service	Code
Amazon Web Services	361 806
Amazon Web Services	710 897
Incorrect options:	

U2F security key - A device that you plug into a USB port on your computer. U2F is an open authentication standard hosted by the FIDO Alliance. When you enable a U2F security key, you sign in by entering your credentials and then tapping the device instead of manually entering a code.

Hardware MFA device - A hardware device that generates a six-digit numeric code based upon a time-synchronized one-time password algorithm. The user must type a valid code from the device on a second webpage during sign-in. Each MFA device assigned to a user must be unique. A user cannot type a code from another user's device to be authenticated.

Soft Token MFA device - This is a made-up option and has been added as a distractor.

Reference:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa.html

Question 45: **Incorrect**

Which AWS Support plan provides general architectural guidance on how services can be used for various use-cases, workloads, or applications?

-

Enterprise

-

Basic

-

Business

(Incorrect)

-

Developer

(Correct)

Explanation

Correct option:

Developer - AWS recommends Developer Support plan if you are testing or doing early development on AWS and want the ability to get email-based technical support during business hours. This plan also supports general guidance on how services can be used for various use cases, workloads, or applications. You do not get access to Infrastructure Event Management with this plan.

Developer Support Plan

Overview:

We recommend 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. In addition to what is available with Basic Support, Developer Support provides:

AWS Trusted Advisor - Access to the 7 core 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.

Technical Support - Business hours* access to Cloud Support Engineers via email. One named contact can open an unlimited amount of cases. Response times are as follows:

- General Guidance - < 24 business hours
- System Impaired - < 12 business hours

Architecture Support - General guidance on how services can be used for various use cases, workloads, or applications.

via - <https://aws.amazon.com/premiumsupport/plans/developers/>

Incorrect options:

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.

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.

Basic - The basic plan only provides access to the following:

Customer Service & Communities - 24x7 access to customer service, documentation, whitepapers, and support forums. AWS Trusted Advisor - Access to the 7 core Trusted Advisor checks and guidance to provision your resources following best practices to increase performance and improve security. AWS Personal Health Dashboard - A personalized view of the health of AWS services, and alerts when your resources are impacted.

Reference:

<https://aws.amazon.com/premiumsupport/plans/developers/>

Question 46: **Incorrect**

Data encryption is automatically enabled for which of the following AWS services? (Select two)?

-

Amazon EFS drives

-

Amazon S3 Glacier

(Correct)

-

AWS Storage Gateway

(Correct)

-

Amazon EBS volumes

(Incorrect)

-

Amazon Redshift

Explanation

Correct option:

Amazon S3 Glacier - Amazon S3 Glacier (S3 Glacier), is a storage service optimized for infrequently used data, or "cold data. Data at rest stored in S3 Glacier is automatically server-side encrypted using 256-bit Advanced Encryption Standard (AES-256) with keys maintained by AWS.

AWS Storage Gateway - AWS Storage Gateway is a hybrid cloud storage service that gives you on-premises access to virtually unlimited cloud storage. All data transferred between the gateway and AWS storage is encrypted using SSL (for all three types of gateways - File, Volume and Tape Gateways).

Incorrect options:

Amazon EBS volumes - Amazon EBS volumes are not encrypted, by default. You can configure your AWS account to enforce the encryption of the new EBS volumes and snapshot copies that you create.

Amazon Redshift - Encryption is an optional setting in Amazon Redshift. When you enable encryption for a cluster, the data-blocks and system metadata are encrypted for the cluster and its snapshots.

Amazon EFS drives - Encryption is not a default setting, but an optional configuration for EFS drives. Amazon EFS supports two forms of encryption for file systems, encryption of data in transit and encryption at rest.

References:

<https://aws.amazon.com/storagegateway/faqs/>

<https://docs.aws.amazon.com/amazonglacier/latest/dev/DataEncryption.html>

Question 47: **Incorrect**

Which pillar of the AWS Well-Architected Framework recommends maintaining infrastructure as code?

-

Cost Optimization

-

Security

-

Performance Efficiency

(Incorrect)

-

Operational Excellence

(Correct)

Explanation

Correct option:

Operational Excellence

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 six pillars — Operational Excellence, Security, Reliability, Performance Efficiency, Cost Optimization and Sustainability.

The Operational Excellence pillar includes the ability to run and monitor systems to deliver business value and to continually improve supporting processes and procedures. In the cloud, you can apply the same engineering discipline that you use for application code to your entire environment. You can define your entire workload (applications, infrastructure) as code and update it with code. You can implement your operations procedures as code and automate their execution by triggering them in response to events.

Incorrect options:

Cost Optimization - Cost Optimization focuses on avoiding un-needed costs. Key topics include understanding and controlling where the 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.

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.

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.

Reference:

<https://wa.aws.amazon.com/wat.pillar.operationalExcellence.en.html>

Question 48: **Incorrect**

According to the AWS Shared Responsibility Model, which of the following are responsibilities of the customer (select 2)?

-

Compliance validation of Cloud infrastructure

-

Operating system patches and updates of an EC2 instance

(Correct)

-

Ensuring AWS employees cannot access customer data

-

AWS Global Network Security

(Incorrect)

-

Enabling data encryption of data stored in S3 buckets

(Correct)

Explanation

Correct options:

Under the Shared Responsibility Model, 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. Customer's responsibility is determined by the AWS Cloud services that a customer selects.

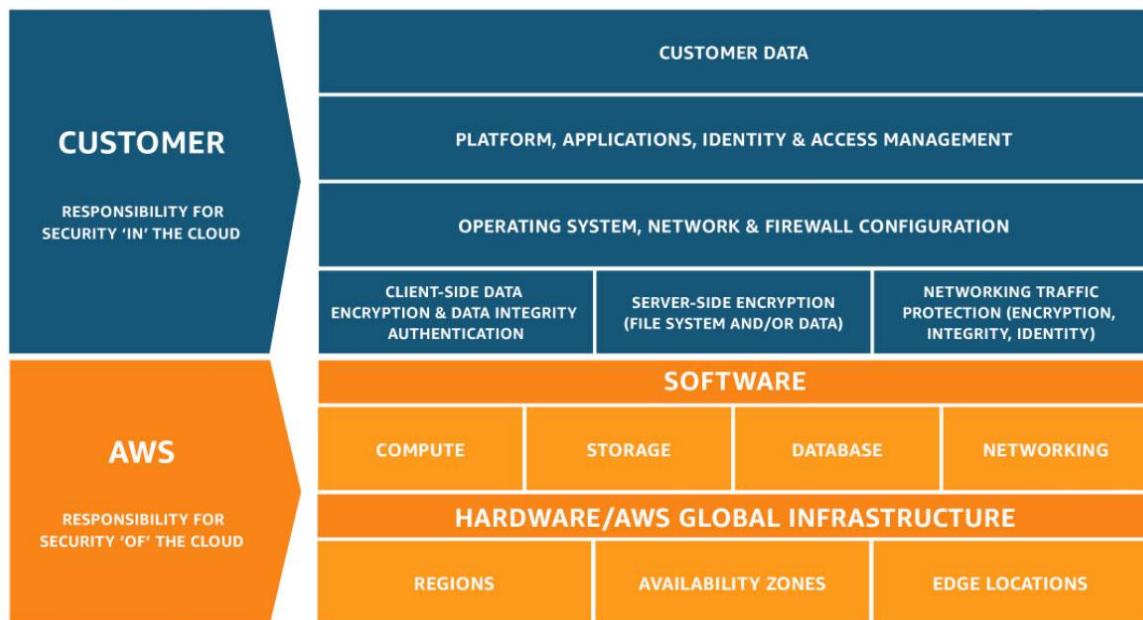
Security and Compliance is a shared responsibility between AWS and the customer. This shared model can help relieve the customer's operational burden as AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates.

Operating system patches and updates of an EC2 instance - Security "in" the cloud is the responsibility of the customer. A service such as Amazon Elastic Compute Cloud (Amazon EC2) is categorized as Infrastructure as a Service (IaaS) and, as such, requires the customer to perform all of the necessary security configuration and management tasks.

Enabling data encryption of data stored in S3 buckets - In the Shared Responsibility Model, customers are responsible for managing their data (including encryption options), classifying their assets, and using IAM tools to apply the appropriate permissions.

Shared Responsibility Model

Overview:



via - <https://aws.amazon.com/compliance/shared-responsibility-model/>

Incorrect options:

AWS Global Network Security - Cloud infrastructure management is the responsibility of AWS.

Ensuring AWS employees cannot access customer data - Ensuring protection of customer data and keeping it safe from AWS employees is the responsibility of AWS.

Compliance validation of Cloud infrastructure - Cloud security and compliance are the responsibilities of AWS.

Reference:

<https://aws.amazon.com/compliance/shared-responsibility-model/>

Question 49: **Correct**

A company has a static website hosted on an S3 bucket in an AWS Region in Asia. Although most of its users are in Asia, now it wants to drive growth globally. How can it improve the global performance of its static website?

- ○

Use S3 Transfer Acceleration to improve the performance of your website

-

Use CloudWatch to improve the performance of your website

-

Use WAF to improve the performance of your website

-

Use CloudFront to improve the performance of your website

(Correct)

Explanation

Correct option:

Use CloudFront to improve the performance of your website

You can use Amazon CloudFront to improve the performance of your website. CloudFront makes your website files (such as HTML, images, and video) available from data centers around the world (called edge locations). When a visitor requests a file from your website, CloudFront automatically redirects the request to a copy of the file at the nearest edge location. This results in faster download times than if the visitor had requested the content from a data center that is located farther away.

Incorrect options:

Use CloudFormation to improve the performance of your website - AWS CloudFormation allows you to use programming languages or a simple text file to model and provision, in an automated and secure manner, all the resources needed for your applications across all regions and accounts. CloudFormation cannot be used to improve the performance of a static website.

Use WAF to improve the performance of your website - By using AWS WAF, you can configure web access control lists (Web ACLs) on your CloudFront distributions or Application Load Balancers to filter and block requests based on request signatures. Besides, by using AWS WAF's rate-based rules, you can automatically block the IP addresses of bad actors when requests matching a rule exceed a threshold that you define. WAF cannot be used to improve the performance of a static website.

Use S3 Transfer Acceleration to improve the performance of your website - Amazon S3 Transfer Acceleration enables fast, easy, and secure transfers of files over long distances between your client and an S3 bucket. Transfer Acceleration takes advantage of Amazon CloudFront's globally distributed edge locations. As the data arrives at an edge location, data is routed to Amazon S3 over an optimized network path. Transfer Acceleration cannot be used to improve the performance of a static website.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/website-hosting-cloudfront-walkthrough.html>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/transfer-acceleration.html>

Question 50: **Correct**

Which AWS service will you use to privately connect your VPC to Amazon S3?



Amazon API Gateway



AWS Direct Connect



VPC Endpoint Gateway

(Correct)



AWS Transit Gateway

Explanation

Correct option:

VPC Endpoint Gateway

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. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network.

There are two types of VPC endpoints: interface endpoints and gateway endpoints.

An interface endpoint is an elastic network interface with a private IP address from the IP address range of your subnet that serves as an entry point for traffic destined to a supported service. Interface endpoints are powered by AWS PrivateLink, a technology that enables you to privately access services by using private IP addresses.

A gateway endpoint is a gateway that you specify as a target for a route in your route table for traffic destined to a supported AWS service. The following AWS services are supported:

Amazon S3

DynamoDB

Exam Alert:

You may see a question around this concept in the exam. Just remember that only S3 and DynamoDB support VPC Endpoint Gateway. All other services that support VPC Endpoints use a VPC Endpoint Interface.

Incorrect options:

AWS Direct Connect - AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS. You can use AWS Direct Connect to establish a private virtual interface from your on-premise network directly to your Amazon VPC. This private connection takes at least one month for completion.

AWS Transit Gateway - AWS Transit Gateway connects VPCs and on-premises networks through a central hub. This simplifies your network and puts an end to complex peering relationships. It acts as a cloud router – each new connection is only made once. This service is helpful in reducing the complex topology of VPC peering when a lot of systems are involved.

Amazon API Gateway - Amazon API Gateway is a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale. APIs act as the "front door" for applications to access data, business logic, or functionality from your backend services.

Reference:

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints.html>

Question 51: **Correct**

A research group wants to provision an EC2 instance for a flexible application that can be interrupted. As a Cloud Practitioner, which of the following would you recommend as the MOST cost-optimal option?



Dedicated Host



Reserved Instance



Spot Instance

(Correct)



On-Demand Instance

Explanation

Correct option:

Spot Instance - A Spot Instance is an unused EC2 instance that is available for less than the On-Demand price. Because Spot Instances enable you to request unused EC2 instances at steep discounts

(up to 90%), you can lower your Amazon EC2 costs significantly. Spot Instances are well-suited for data analysis, batch jobs, background processing, and other flexible tasks that can be interrupted. These can be terminated at short notice, so these are not suitable for critical workloads that need to run at a specific point in time.

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:

On-Demand Instance - An On-Demand Instance is an instance that you use on-demand. You have full control over its lifecycle — you decide when to launch, stop, hibernate, start, reboot, or terminate it. There is no long-term commitment required when you purchase On-Demand Instances. There is no upfront payment and you pay only for the seconds that your On-Demand Instances are running. The price per second for running an On-Demand Instance is fixed. On-demand instances cannot be interrupted. However, On-demand instances are not as cost-effective as spot instances, so this option is not correct.

Reserved Instance - Reserved Instances provide you with significant savings (up to 75%) on your Amazon EC2 costs compared to On-Demand Instance pricing. Reserved Instances are not physical instances, but rather a billing discount applied to the use of On-Demand Instances in your account. You can purchase a Reserved Instance for a one-year or three-year commitment, with the three-year commitment offering a bigger discount. Reserved instances cannot be interrupted. Reserved instances are not as cost-effective as spot instances, so this option is not correct.

Dedicated Host - Amazon EC2 Dedicated Hosts allow you to use your eligible software licenses from vendors such as Microsoft and Oracle on Amazon EC2 so that you get the flexibility and cost-

effectiveness of using your licenses, but with the resiliency, simplicity, and elasticity of AWS. An Amazon EC2 Dedicated Host is a physical server fully dedicated for your use, so you can help address corporate compliance requirement. They're not cost-efficient compared to spot instances. So this option is not correct.

Reference:

<https://aws.amazon.com/ec2/pricing/>

Question 52: **Correct**

Which AWS service protects your AWS account by monitoring malicious activity and detecting threats?



Trusted Advisor



GuardDuty

(Correct)



CloudTrail



CloudWatch

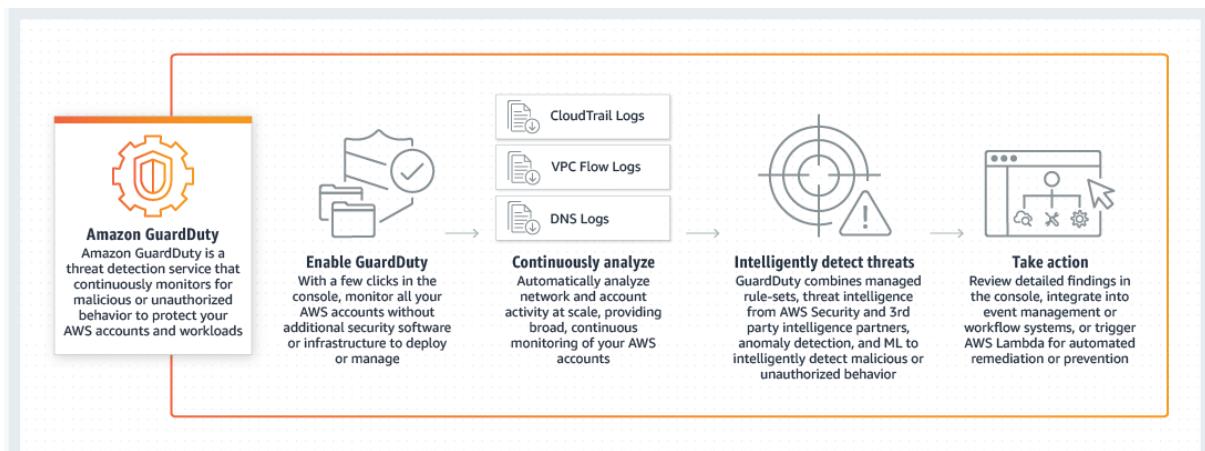
Explanation

Correct option:

GuardDuty

GuardDuty is a threat detection service that monitors malicious activity and unauthorized behavior to protect your AWS account. GuardDuty analyzes billions of events across your AWS accounts from AWS CloudTrail (AWS user and API activity in your accounts), Amazon VPC Flow Logs (network traffic data), and DNS Logs (name query patterns). Security findings are retained and made available through the Amazon GuardDuty console and APIs for 90-days. After 90-days, the findings are discarded. To retain findings for longer than 90-days, you can enable AWS CloudWatch Events to automatically push findings to an Amazon S3 bucket in your account or another data store for long-term retention.

How GuardDuty Works:



via - <https://aws.amazon.com/guardduty/>

Incorrect options:

CloudTrail - AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. Think account-specific activity and audit; think CloudTrail. CloudTrail cannot detect threats to your AWS account.

CloudWatch - Amazon CloudWatch is a monitoring and observability service built for DevOps engineers, developers, site reliability engineers (SREs), and IT managers. CloudWatch provides data and actionable insights to monitor your applications, respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health. Think resource performance monitoring, events, and alerts; think CloudWatch. CloudWatch cannot detect threats to your AWS account.

Trusted Advisor - AWS Trusted Advisor is an online tool that provides you real-time guidance to help you provision your resources following AWS best practices. Whether establishing new workflows, developing applications, or as part of ongoing improvement, recommendations provided by Trusted Advisor regularly help keep your solutions provisioned optimally. Trusted Advisor cannot detect threats to your AWS account.

Reference:

<https://aws.amazon.com/guardduty/>

Question 53: **Correct**

A startup wants to set up its IT infrastructure on AWS Cloud. The CTO would like to receive detailed reports that break down the startup's AWS costs by the hour in an S3 bucket. As a Cloud Practitioner, which AWS service would you recommend for this use-case?

-

AWS Cost and Usage Reports

(Correct)

-

AWS Cost Explorer

-

AWS Pricing Calculator

-

AWS Budgets

Explanation

Correct option:

AWS Cost and 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 updates the report in your bucket once a day in comma-separated value (CSV) format.

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 Pricing Calculator - AWS Pricing Calculator lets you explore AWS services and create an estimate for the cost of your use cases on AWS. You can model your solutions before building them, explore the price points and calculations behind your estimate, and find the available instance types and contract terms that meet your needs. This enables you to make informed decisions about using AWS. You can plan your AWS costs and usage or price out setting up a new set of instances and services.

AWS 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 a detailed report of your AWS costs by the hour into an S3 bucket.

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 the estimate of the monthly AWS bill based on the list of AWS services. AWS Budgets cannot provide a detailed break down of your AWS costs by the hour.

Exam Alert:

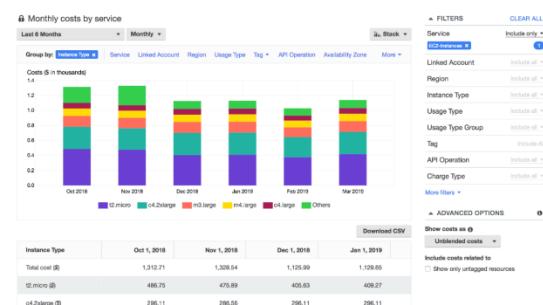
Please review the differences between "AWS Cost and Usage Reports" and "AWS Cost Explorer". Think of "AWS Cost and Usage Reports" as a cost management tool providing the most detailed cost and usage data for your AWS account. It can provide reports that break down your costs by the hour into your S3 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.

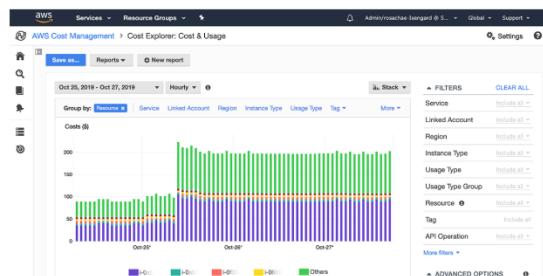
[Launch the Monthly Costs by AWS Service report »](#)



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 54: **Correct**

Which of the following is a part of the AWS Global Infrastructure?

-

Virtual Private Network (VPN)

- 1

Virtual Private Cloud (VPC)

- 1

Subnets

- 1

Region

(Correct)

Explanation

Correct option:

Region

AWS Region is a physical location around the world where AWS builds its data centers. Each group of logical data centers is called an Availability Zone (AZ). Each AWS Region consists of multiple, isolated, and physically separate AZ's within a geographic area.

Please see this illustration for AWS regions in the US:



Map Key		US East (Ohio) Region	GovCloud (US-West) Region
	Regions	Availability Zones: 3 <i>Launched 2016</i>	Availability Zones: 3 <i>Launched 2011</i>
	Edge locations	US West (Oregon) Region Availability Zones: 4 <i>Launched 2011</i> Local Zone: 1 <i>Launched 2019</i>	GovCloud (US-East) Region Availability Zones: 3 <i>Launched 2018</i>
US East (Northern Virginia) Region		US West (Northern California) Region Availability Zones: 3* <i>Launched 2009</i>	Canada (Central) Region** Availability Zones: 3 <i>Launched 2016</i>
Availability Zones: 6 <i>Launched 2006</i>			Learn more at AWS Canada
			See detailed offerings at all AWS locations >>

via - https://aws.amazon.com/about-aws/global-infrastructure/regions_az/

Incorrect options:

Virtual Private Cloud (VPC) - Amazon Virtual Private Cloud (Amazon VPC) is a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including the selection of your IP address range, creation of subnets, and configuration of route tables and network gateways. A VPC spans all of the Availability Zones in the Region.

Virtual Private Network (VPN) - AWS Virtual Private Network (AWS VPN) lets you establish a secure and private encrypted tunnel from your on-premises network to the AWS global network. AWS VPN is comprised of two services: AWS Site-to-Site VPN and AWS Client VPN.

Subnets - A subnet is a range of IP addresses within your VPC. A subnet spans only one Availability Zone in the Region.

These three options are not a part of the AWS Global Infrastructure.

Reference:

https://aws.amazon.com/about-aws/global-infrastructure/regions_az/

Question 55: **Incorrect**

An IT company is on a cost-optimization spree and wants to identify all EC2 instances that are under-utilized. Which AWS services can be used off-the-shelf to address this use-case without needing any manual configurations? (Select two)

-

AWS Cost and Usage Reports

-

Amazon CloudWatch

-

AWS Cost Explorer

(Correct)

-

AWS Trusted Advisor

(Correct)

-

AWS Budgets

Explanation

Correct option:

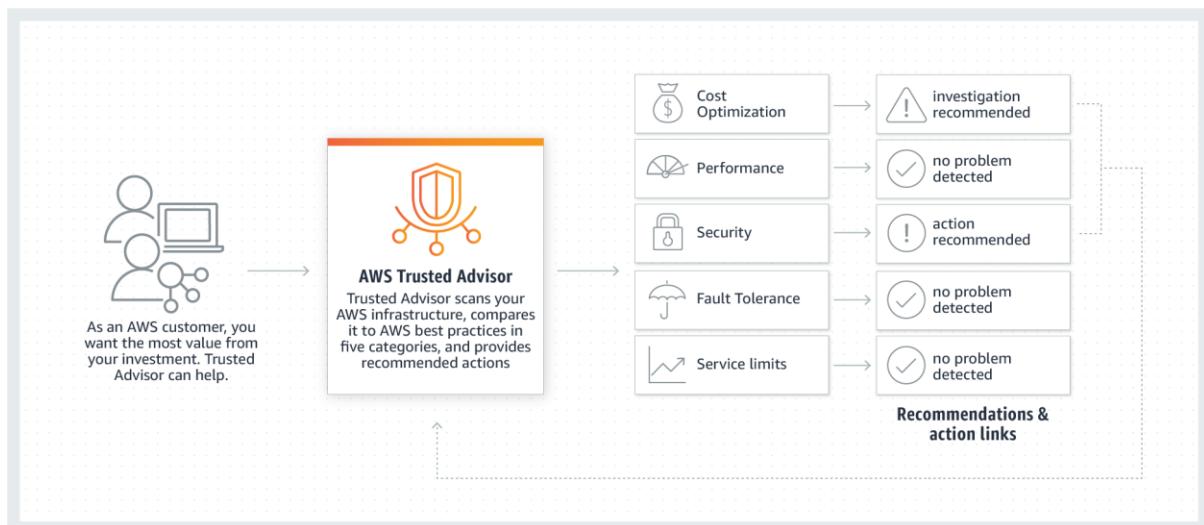
AWS Trusted Advisor

AWS Trusted Advisor is an online tool that provides real-time guidance to help provision your resources following AWS best practices. Whether establishing new workflows, developing applications, or as part of ongoing improvement, recommendations provided by Trusted Advisor regularly help keep your solutions provisioned optimally. AWS Trusted Advisor analyzes your AWS environment and provides best practice recommendations in five categories: Cost Optimization, Performance, Security, Fault Tolerance, Service Limits.

AWS Trusted Advisor checks the Amazon Elastic Compute Cloud (Amazon EC2) instances that were running at any time during the last 14 days and alerts you if the daily CPU utilization was 10% or less and network I/O was 5 MB or less on 4 or more days.

How Trusted Advisor

Works:



via - <https://aws.amazon.com/premiumsupport/technology/trusted-advisor/>

How AWS Trusted Advisor identifies low utilization Amazon EC2 instances:

Low utilization Amazon EC2 instances

Checks the Amazon Elastic Compute Cloud (Amazon EC2) instances that were running at any time during the last 14 days and alerts you if the daily CPU utilization was 10% or less and network I/O was 5 MB or less on 4 or more days. Running instances generate hourly usage charges. Although some scenarios can result in low utilization by design, you can often lower your costs by managing the number and size of your instances.

Estimated monthly savings are calculated by using the current usage rate for On-Demand Instances and the estimated number of days the instance might be underutilized. Actual savings will vary if you are using Reserved Instances or Spot Instances, or if the instance is not running for a full day. To get daily utilization data, download the report for this check.

via - https://aws.amazon.com/premiumsupport/technology/trusted-advisor/best-practice-checklist/#Cost_Optimization

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.

The rightsizing recommendations feature in Cost Explorer helps you identify cost-saving opportunities by downsizing or terminating EC2 instances. You can see all of your underutilized EC2 instances across member accounts in a single view to immediately identify how much you can save.

Incorrect options:

AWS Cost and 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. Cost and Usage Reports cannot be used to identify under-utilized EC2 instances.

Amazon CloudWatch - Amazon CloudWatch can be used to create alarm to monitor your estimated charges. When you enable the monitoring of estimated charges for your AWS account, the estimated charges are calculated and sent several times daily to CloudWatch as metric data. You can choose to receive alerts by email when charges have exceeded a certain threshold. Think resource performance monitoring, events, and alerts; think CloudWatch. CloudWatch cannot be used to identify under-utilized EC2 instances without manually configuring an alarm with the appropriate threshold to track the EC2 utilization, so this option is incorrect.

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 be used to identify under-utilized EC2 instances without manually configuring coverage targets, so this option is incorrect.

References:

https://aws.amazon.com/premiumsupport/technology/trusted-advisor/best-practice-checklist/#Cost_Optimization

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/ce-rightsizing.html>

Question 56: **Correct**

Which AWS service can be used to execute code triggered by new files being uploaded to S3?

-
- SQS**
-
- EC2**
-
- ECS**
-
- Lambda**

(Correct)

Explanation

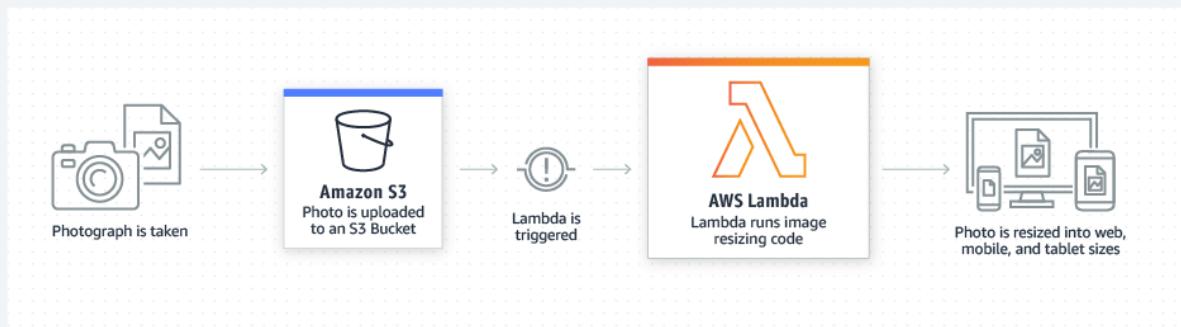
Correct option:

Lambda - AWS Lambda lets you run code without provisioning or managing servers. You pay only for the compute time you consume. 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 use Amazon S3 to trigger AWS Lambda to process data immediately after an upload. For example, you can use Lambda to thumbnail images, transcode videos, index files, process logs, validate content, and aggregate and filter data in real-time.

How Lambda executes code in response to a trigger from S3:



via - <https://aws.amazon.com/lambda/>

Incorrect options:

EC2 - Amazon EC2 is a web service that provides secure, resizable compute capacity in the AWS cloud. You can use EC2 to provision virtual servers on AWS Cloud. EC2 cannot execute code via a trigger from S3.

ECS - Amazon Elastic Container Service (Amazon ECS) is a highly scalable, fast, container management service that makes it easy to run, stop, and manage Docker containers on a cluster. ECS cannot execute code via a trigger from S3.

SQS - Amazon Simple Queue Service (SQS) is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. 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.

Although SQS can be triggered from an S3 event, but SQS cannot execute code as its a message queuing service.

Reference:

<https://aws.amazon.com/lambda/>

Question 57: **Correct**

Under the AWS Shared Responsibility Model, which of the following is the responsibility of a customer regarding lambda functions?

-

Maintain versions of a lambda function

(Correct)

-

Patch underlying OS for the lambda function infrastructure

-

Maintain all runtime environments for lambda functions

-

Configure networking infrastructure for the lambda functions

Explanation

Correct option:

Maintain versions of a lambda function

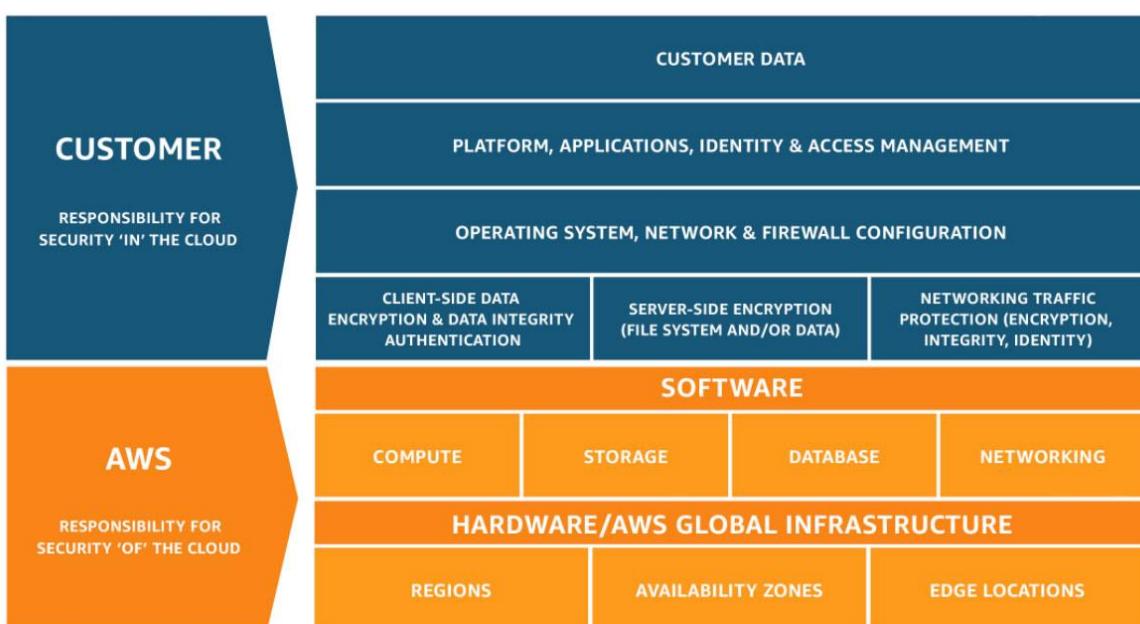
Under the Shared Responsibility Model, AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services.

Under the Shared Responsibility Model, Customer's responsibility is determined by the AWS Cloud services that a customer selects. For abstracted services, such as Amazon S3 and Amazon DynamoDB, AWS operates the infrastructure layer, the operating system, and platforms, and customers access the endpoints to store and retrieve data. Customers are responsible for managing their data (including encryption options), classifying their assets, and using IAM tools to apply the appropriate permissions.

For the given use-case, the customer is responsible for maintaining the versions of a lambda function.

Shared Responsibility Model

Overview:



via - <https://aws.amazon.com/compliance/shared-responsibility-model/>

Incorrect options:

Patch underlying OS for the lambda function infrastructure

Maintain all runtime environments for lambda functions

Configure networking infrastructure for the lambda functions

As mentioned earlier, all these options fall under the ambit of AWS as far as the Shared Responsibility Model is concerned.

Reference:

<https://aws.amazon.com/compliance/shared-responsibility-model/>

Question 58: **Incorrect**

A customer is running a comparative study of pricing models of Amazon EFS and Amazon EBS that are used with the Amazon EC2 instances that host the application. Which of the following statements are correct regarding this use-case? (Select two)

-

With AWS Backup, you pay only for the amount of EFS backup storage you use in a month, you need not pay for restoring this data

-

Amazon EBS Snapshots are stored incrementally, which means you are billed only for the changed blocks stored

(Correct)

-

Amazon EBS Snapshot storage pricing is based on the amount of space your data consumes in EBS

(Incorrect)

-

You will pay a fee each time you read from or write data stored on the EFS - Infrequent Access storage class

(Correct)

-

Amazon EC2 data transfer charges will apply for all EBS direct APIs for Snapshots

Explanation

Correct options:

You will pay a fee each time you read from or write data stored on the EFS - Infrequent Access storage class - The Infrequent Access storage class is cost-optimized for files accessed less frequently. Data stored on the Infrequent Access storage class costs less than Standard and you will pay a fee each time you read from or write to a file.

Amazon EBS Snapshots are stored incrementally, which means you are billed only for the changed blocks stored - Amazon EBS Snapshots are a point in time copy of your block data. For the first snapshot of a volume, Amazon EBS saves a full copy of your data to Amazon S3. EBS Snapshots are stored incrementally, which means you are billed only for the changed blocks stored.

Incorrect options:

Amazon EC2 data transfer charges will apply for all EBS direct APIs for Snapshots - When using EBS direct APIs for Snapshots, additional EC2 data transfer charges will apply only when you use external or cross-region data transfers.

Amazon EBS Snapshot storage pricing is based on the amount of space your data consumes in EBS - Snapshot storage is based on the amount of space your data consumes in Amazon S3. Because Amazon EBS does not save empty blocks, it is likely that the snapshot size will be considerably less than your volume size. Copying EBS snapshots is charged for the data transferred across regions. After the snapshot is copied, standard EBS snapshot charges apply for storage in the destination region.

With AWS Backup, you pay only for the amount of EFS backup storage you use in a month, you need not pay for restoring this data - To back up your Amazon EFS file data you can use AWS Backup, a fully-managed backup service that makes it easy to centralize and automate the back up of data across AWS services. With AWS Backup, you pay only for the amount of backup storage you use and the amount of backup data you restore in the month. There is no minimum fee and there are no set-up charges.

References:

<https://aws.amazon.com/efs/pricing/>

<https://aws.amazon.com/ebs/pricing/>

Question 59: **Correct**

Which budget types can be created under AWS Budgets (Select three)?

-

Hardware budget

-

Reservation budget

(Correct)

-

Software budget

-

Cost budget

(Correct)

-

Resource budget

-

Usage budget

(Correct)

Explanation

Correct options:

AWS Budgets enable you to plan your service usage, service costs, and instance reservations. AWS Budgets information is updated up to three times a day. Updates typically occur between 8 to 12 hours after the previous update. Budgets track your unblended costs, subscriptions, refunds, and RIs. There are four different budget types you can create under AWS Budgets - Cost budget, Usage budget, Reservation budget and Savings Plans budget.

Cost budget - Helps you plan how much you want to spend on a service.

Usage budget - Helps you plan how much you want to use one or more services.

Reservation budget - This helps you track the usage of your Reserved Instances (RI). Two ways of doing it - RI utilization budgets (This lets you see if your RIs are unused or under-utilized), RI coverage budgets (This lets you see how much of your instance usage is covered by a reservation).

Incorrect options:

Resource budget - This is a made-up option and has been added as a distractor

Software budget - This is a made-up option and has been added as a distractor

Hardware budget - This is a made-up option and has been added as a distractor

Reference:

[This is a made-up option and has been added as a distractor](#)

Question 60: **Incorrect**

Which of the following AWS services specialize in data migration from on-premises to AWS Cloud?
(Select two)

-

Site-to-Site VPN

-

Snowball

(Correct)

-

Database Migration Service

(Correct)

-

Direct Connect

(Incorrect)

-

Transit Gateway

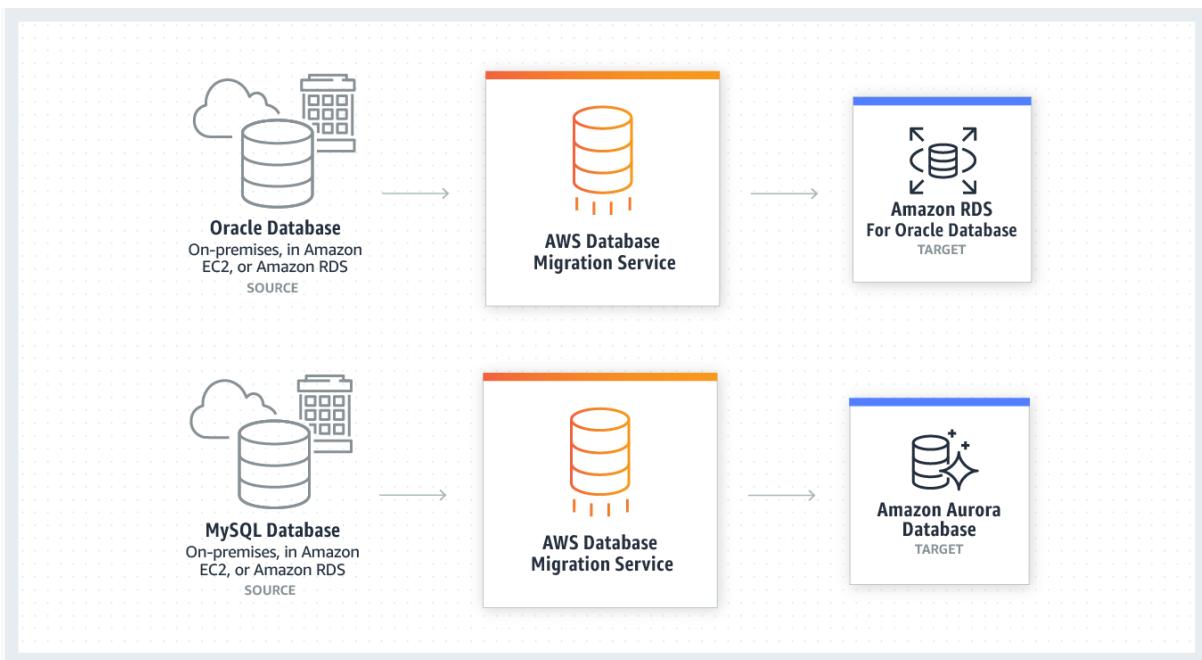
Explanation

Correct options:

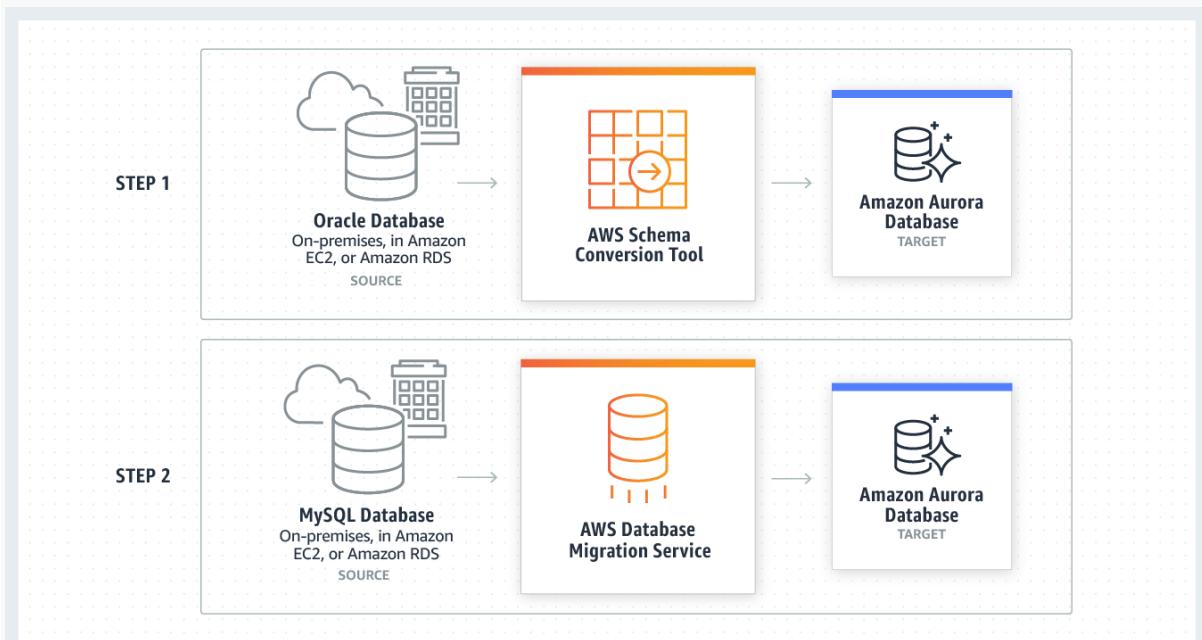
Snowball - AWS Snowball is a data transport solution that accelerates moving terabytes to petabytes of data into and out of AWS services using storage devices designed to be secure for physical transport.

Database Migration Service - AWS Database Migration Service helps you migrate databases from on-premises to AWS quickly and securely. The source database remains fully operational during the migration, minimizing downtime to applications that rely on the database. The AWS Database Migration Service can migrate your data to and from the most widely used commercial and open-source databases.

You can do both homogeneous and heterogeneous database migration using Database Migration Service:



via - <https://aws.amazon.com/dms/>



via - <https://aws.amazon.com/dms/>

Incorrect options:

Site to Site VPN - AWS Site-to-Site VPN creates a secure connection between your data center or branch office and your AWS cloud resources. This connection goes over the public internet. Site to Site VPN is a connectivity service and it does not specialize in data migration.

Direct Connect - AWS Direct Connect creates a dedicated private connection from a remote network to your VPC. This is a private connection and does not use the public internet. Takes at least a month to establish this connection. Direct Connect is a connectivity service and it does not specialize in data migration.

Transit Gateway - AWS Transit Gateway connects VPCs and on-premises networks through a central hub. This simplifies your network and puts an end to complex peering relationships. It acts as a cloud router – each new connection is only made once. As you expand globally, inter-Region peering connects AWS Transit Gateways using the AWS global network. Your data is automatically encrypted and never travels over the public internet. Transit Gateway is a connectivity service and it does not specialize in data migration.

References:

<https://aws.amazon.com/getting-started/projects/migrate-petabyte-scale-data/services-costs/>

<https://aws.amazon.com/dms/>

<https://aws.amazon.com/vpn/>

<https://aws.amazon.com/directconnect/>

Question 61: **Correct**

As a Cloud Practitioner, which S3 storage class would you recommend for data archival?



S3 Standard



S3 One Zone-IA



S3 Intelligent-Tiering



S3 Glacier

(Correct)

Explanation

Correct option:

S3 Glacier

Amazon S3 Glacier is a secure, durable, and extremely low-cost Amazon S3 cloud storage class for data archiving and long-term backup. It is designed to deliver 99.99999999% durability, and provide comprehensive security and compliance capabilities that can help meet even the most stringent regulatory requirements.

You can further review the use-cases for S3 Glacier:

MEDIA ASSET WORKFLOWS	HEALTHCARE INFORMATION ARCHIVING	REGULATORY AND COMPLIANCE ARCHIVING
<p>Media assets such as video and news footage require durable storage and can grow to many petabytes over time. The Amazon S3 Glacier and S3 Glacier Deep Archive storage classes allow you to archive older media content affordably then move it to Amazon S3 for distribution when needed.</p>	<p>Hospital systems need to retain petabytes of patient records (LIS, PACS, EHR, etc.) for decades to meet regulatory requirements. The Amazon S3 Glacier and S3 Glacier Deep Archive storage classes help you reliably archive patient record data securely at a very low cost.</p>	<p>Many enterprises like Financial Services and Healthcare must retain regulatory and compliance archives for extended durations. Amazon S3 Object Lock helps you set compliance controls to meet your objectives, such as SEC Rule 17a-4(f).</p>
SCIENTIFIC DATA STORAGE	DIGITAL PRESERVATION	MAGNETIC TAPE REPLACEMENT
<p>Research organizations generate, analyze, and archive vast amounts of data. With the Amazon S3 Glacier and S3 Glacier Deep Archive storage classes, you avoid the complexities of hardware and facility management and capacity planning.</p>	<p>Libraries and government agencies face data-integrity challenges in their digital preservation efforts. Unlike traditional systems, which can require laborious data verification and manual repair, Amazon S3 performs regular, systematic data integrity checks and is built to be automatically self-healing.</p>	<p>On-premises or offsite tape libraries can lower storage costs but require large upfront investments and specialized maintenance. The Amazon S3 Glacier and S3 Glacier Deep Archive storage classes have no upfront cost and eliminate the cost and burden of maintenance.</p>

via - <https://aws.amazon.com/glacier/>

S3 Storage Classes

Overview:

Performance across the S3 Storage Classes

	S3 Standard	S3 Intelligent-Tiering*	S3 Standard-IA	S3 One Zone-IA†	S3 Glacier Instant Retrieval	S3 Glacier Flexible Retrieval	S3 Glacier Deep Archive
Designed for durability	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)
Designed for availability	99.99%	99.9%	99.9%	99.5%	99.9%	99.99%	99.99%
Availability SLA	99.9%	99%	99%	99%	99%	99.%	99.9%
Availability Zones	≥3	≥3	≥3	1	≥3	≥3	≥3
Minimum capacity charge per object	N/A	N/A	128 KB	128 KB	128 KB	40 KB	40 KB
Minimum storage duration charge	N/A	N/A	30 days	30 days	90 days	90 days	180 days
Retrieval charge	N/A	N/A	per GB retrieved	per GB retrieved	per GB retrieved	per GB retrieved	per GB retrieved
First byte latency	milliseconds	milliseconds	milliseconds	milliseconds	milliseconds	minutes or hours	hours
Storage type	Object	Object	Object	Object	Object	Object	Object
Lifecycle transitions	Yes	Yes	Yes	Yes	Yes	Yes	Yes

via - <https://aws.amazon.com/s3/storage-classes/>

Incorrect options:

S3 Standard - S3 Standard offers high durability, availability, and performance object storage for frequently accessed data. It is not suitable for data archival.

S3 Intelligent-Tiering - The S3 Intelligent-Tiering storage class is designed to optimize costs by automatically moving data to the most cost-effective access tier, without performance impact or operational overhead. It works by storing objects in two access tiers: one tier that is optimized for frequent access and another lower-cost tier that is optimized for infrequent access. It is not suitable for data archival.

S3 One Zone-IA - 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. It is not suitable for data archival.

References:

<https://aws.amazon.com/glacier/>

<https://aws.amazon.com/s3/storage-classes/>

Question 62: **Correct**

An e-commerce company uses AWS Cloud and would like to receive separate invoices for development and production environments. As a Cloud Practitioner, which of the following solutions would you recommend for this use-case?

-
-

Use AWS Cost Explorer to create separate invoices for development and production environments

-
-

Use AWS Organizations to create separate invoices for development and production environments

-
-

Create separate AWS accounts for development and production environments to receive separate invoices

(Correct)

-
-

Tag all resources in the AWS account as either "development" or "production". Then use the tags to create separate invoices

Explanation

Correct option:

"Create separate AWS accounts for development and production environments to receive separate invoices"

Every AWS account provides its own invoice end of the month. You can get separate invoices for development and production environments by setting up separate AWS accounts for each environment.

Incorrect options:

Use AWS Organizations to create separate invoices for development and production environments - AWS Organizations helps you to centrally manage billing; control access, compliance, and security; and share resources across your AWS accounts. Using AWS Organizations, you can automate account creation, create groups of accounts to reflect your business needs, and apply policies for these groups for governance. You can also simplify billing by setting up a single payment method for all of your AWS accounts. AWS Organizations is available to all AWS customers at no additional charge.

AWS Organizations cannot create separate invoices for development and production environments, rather, AWS Organizations helps you to centrally manage billing.

Tag all resources in the AWS account as either "development" or "production". Then use the tags to create separate invoices - You cannot create separate invoices based on tags.

"Use AWS Cost Explorer to create separate invoices for development and production environments" - 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). AWS Cost Explorer cannot create separate invoices for development and production environments.

Reference:

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/billing-what-is.html>

Question 63: **Correct**

A startup runs its proprietary application on docker containers. As a Cloud Practitioner, which AWS service would you recommend so that the startup can run containers and still have access to the underlying servers?

-

Amazon Elastic Container Service (Amazon ECS)

(Correct)

-

Amazon Elastic Container Registry (ECR)

-

AWS Lambda

-

AWS Fargate

Explanation

Correct option:

Amazon Elastic Container Service (Amazon ECS) - Amazon Elastic Container Service (Amazon ECS) is a highly scalable, fast, container management service that makes it easy to run, stop, and manage Docker containers on a cluster. This is not a fully managed service and you can manage the underlying servers yourself.

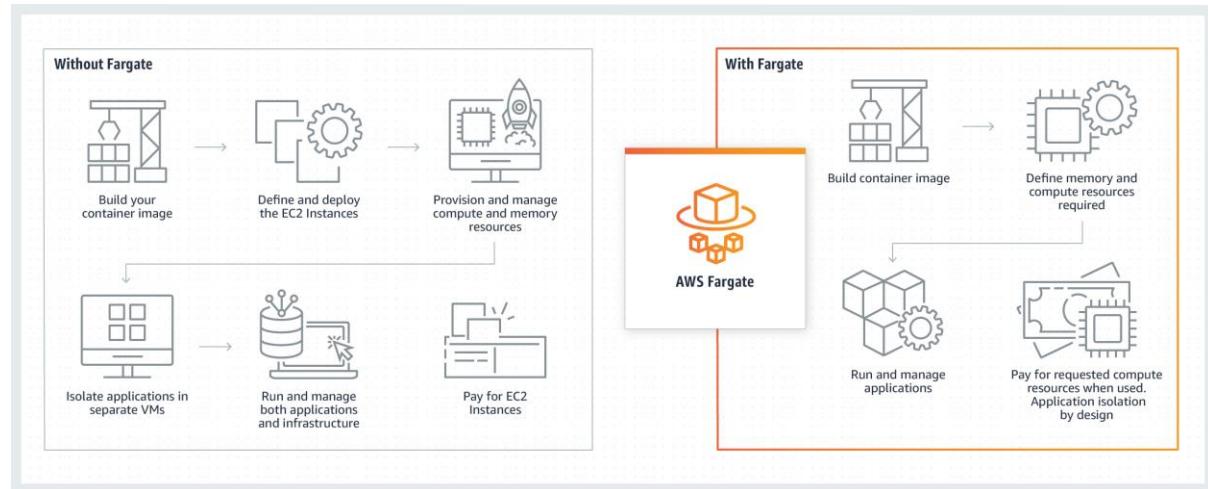
Incorrect options:

AWS Fargate - AWS Fargate is a serverless compute engine for containers. It works with both Amazon Elastic Container Service (ECS) and Amazon Elastic Kubernetes Service (EKS). Fargate makes it easy for you to focus on building your applications. Fargate removes the need to provision and

manage servers, lets you specify and pay for resources per application, and improves security through application isolation by design. With Fargate, you do not have access to the underlying servers, so this option is incorrect.

How Fargate

Works:



via - <https://aws.amazon.com/fargate/>

AWS Lambda - AWS Lambda is a compute service that lets you run code without provisioning or managing servers. AWS Lambda executes your code only when needed and scales automatically, from a few requests per day to thousands per second. Lambda does not support running container applications.

Amazon Elastic Container Registry (ECR) - Amazon Elastic Container Registry (ECR) can be used to store, manage, and deploy Docker container images. Amazon ECR eliminates the need to operate your container repositories. ECR does not support running container applications.

Reference:

<https://aws.amazon.com/fargate/>

Question 64: **Correct**

Which of the following AWS entities provides the information required to launch an EC2 instance?

EBS

EFS

AMI

(Correct)

Lambda

EBS

Explanation

Correct option:

AMI

An Amazon Machine Image (AMI) provides the information required to launch an instance. You must specify an AMI when you launch an instance.

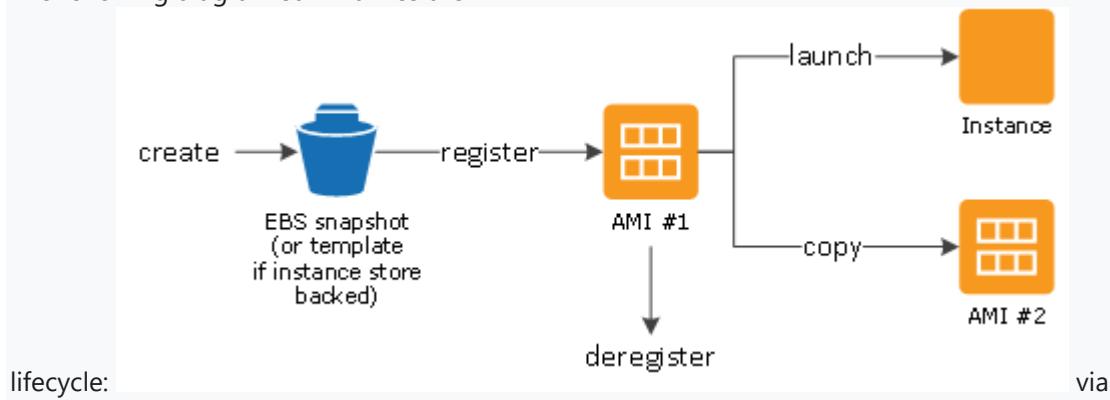
An AMI includes the following:

One or more EBS snapshots, or, for instance-store-backed AMIs, a template for the root volume of the instance (for example, an operating system, an application server, and applications).

Launch permissions that control which AWS accounts can use the AMI to launch instances.

A block device mapping that specifies the volumes to attach to the instance when it's launched.

The following diagram summarizes the AMI



lifecycle:

- <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html>

Incorrect options:

Lambda - AWS Lambda lets you run code without provisioning or managing servers. You pay only for the compute time you consume.

EFS - Amazon Elastic File System (Amazon EFS) provides a simple, scalable, fully managed elastic NFS file system for use with AWS Cloud services and on-premises resources. It is built to scale on-demand to petabytes without disrupting applications, growing and shrinking automatically as you add and remove files, eliminating the need to provision and manage capacity to accommodate growth.

EBS - Amazon Elastic Block Store (EBS) is an easy to use, high-performance block storage service designed for use with Amazon Elastic Compute Cloud (EC2) for both throughput and transaction-intensive workloads at any scale.

Reference:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html>

Question 65: **Correct**

Which of the following are components of an AWS Site-to-Site VPN? (Select two)

-
- **Storage Gateway**
-
- **NAT Gateway**
- **Customer Gateway**
- **(Correct)**
- **Virtual Private Gateway**
- **(Correct)**
-
- **Internet Gateway**

Explanation

Correct option:

Virtual Private Gateway

Customer Gateway

AWS Site-to-Site VPN enables you to securely connect your on-premises network or branch office site to your Amazon Virtual Private Cloud (Amazon VPC). VPN Connections are a good solution if you have an immediate need, and have low to modest bandwidth requirements. This connection goes over the public internet. Virtual Private Gateway (or a Transit Gateway) and Customer Gateway are the components of a VPC.

A virtual private gateway is the VPN concentrator on the Amazon side of the Site-to-Site VPN connection. A customer gateway is a resource in AWS that provides information to AWS about your Customer gateway device.

Components of an AWS Site-to-Site VPN:

Components of your Site-to-Site VPN

A Site-to-Site VPN connection offers two VPN tunnels between a virtual private gateway or a transit gateway on the AWS side, and a customer gateway on the remote (on-premises) side.

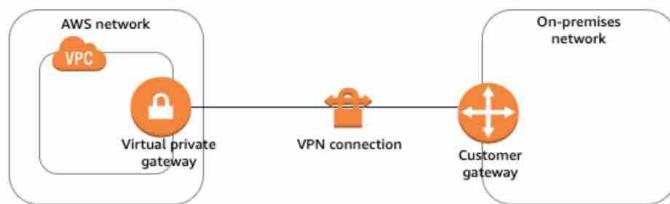
A Site-to-Site VPN connection consists of the following components. For more information about Site-to-Site VPN quotas, see [Site-to-Site VPN quotas](#).

Contents

- [Virtual private gateway](#)
- [Transit gateway](#)
- [Customer gateway](#)
- [Customer gateway device](#)

Virtual private gateway

A *virtual private gateway* is the VPN concentrator on the Amazon side of the Site-to-Site VPN connection. You create a virtual private gateway and attach it to the VPC from which you want to create the Site-to-Site VPN connection.



via - https://docs.aws.amazon.com/vpn/latest/s2svpn/how_it_works.html

Incorrect options:

Storage Gateway - AWS Storage Gateway is a hybrid cloud storage service that connects your existing on-premises environments with the AWS Cloud. Customers use Storage Gateway to simplify storage management and reduce costs for key hybrid cloud storage use cases.

NAT Gateway - A NAT Gateway or a NAT Instance can be used in a public subnet in your VPC to enable instances in the private subnet to initiate outbound IPv4 traffic to the Internet. NAT Gateway is managed by AWS but NAT Instance is managed by you.

Internet Gateway - An internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the internet. It, therefore, imposes no availability risks or bandwidth constraints on your network traffic.

Reference:

https://docs.aws.amazon.com/vpn/latest/s2svpn/how_it_works.html

Practice Test #4 - AWS Certified Cloud Practitioner - Results

[Return to review](#)

Chart

Pie chart with 3 slices.

End of interactive chart.

Attempt 1

All knowledge areas

All questions

Question 1: **Correct**

Which AWS Route 53 routing policy would you use to route traffic to a single resource such as a web server for your website?

-
-

Weighted routing policy

-
-

Failover routing policy

-
-

Latency routing policy

-
-

Simple routing policy

(Correct)

Explanation

Correct option:

Simple routing policy

Amazon Route 53 is a highly available and scalable cloud Domain Name System (DNS) web service. It is designed to give developers and businesses an extremely reliable and cost-effective way to route end users to Internet applications by translating names like `www.example.com` into the numeric IP addresses like `192.0.2.1` that computers use to connect to each other.

Simple routing lets you configure standard DNS records, with no special Route 53 routing such as weighted or latency. With simple routing, you typically route traffic to a single resource, for example, to a web server for your website.

Route 53 Routing Policy

Overview:

Choosing a routing policy

[PDF](#) | [Kindle](#) | [RSS](#)

When you create a record, you choose a routing policy, which determines how Amazon Route 53 responds to queries:

- **Simple routing policy** – Use for a single resource that performs a given function for your domain, for example, a web server that serves content for the example.com website.
- **Failover routing policy** – Use when you want to configure active-passive failover.
- **Geolocation routing policy** – Use when you want to route traffic based on the location of your users.
- **Geoproximity routing policy** – Use when you want to route traffic based on the location of your resources and, optionally, shift traffic from resources in one location to resources in another.
- **Latency routing policy** – Use when you have resources in multiple AWS Regions and you want to route traffic to the region that provides the best latency.
- **Multivalue answer routing policy** – Use when you want Route 53 to respond to DNS queries with up to eight healthy records selected at random.
- **Weighted routing policy** – Use to route traffic to multiple resources in proportions that you specify.

via - <https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html>

Incorrect options:

Failover routing policy - This routing policy is used when you want to configure active-passive failover.

Weighted routing policy - This routing policy is used to route traffic to multiple resources in proportions that you specify.

Latency routing policy - This routing policy is used when you have resources in multiple AWS Regions and you want to route traffic to the region that provides the best latency.

Reference:

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html>

Question 2: **Correct**

Which of the following AWS services can be used to forecast your AWS account usage and costs?



AWS Cost Explorer

(Correct)

AWS Cost and Usage Reports

AWS Pricing Calculator

AWS Budgets

Explanation

Correct options:

AWS Cost Explorer

AWS Cost Explorer has an easy-to-use interface that lets you visualize, understand, and manage your AWS costs and usage over time. AWS Cost Explorer includes a default report that helps you visualize the costs and usage associated with your top five cost-accruing AWS services, and gives you a detailed breakdown of all services in the table view. The reports let you adjust the time range to view historical data going back up to twelve months to gain an understanding of your cost trends. AWS Cost Explorer also supports forecasting to get a better idea of what your costs and usage may look like in the future so that you can plan.

AWS Cost Explorer

Features:

AWS Cost Explorer Features

Get started quickly

A set of default reports are included to help you quickly gain insight into your cost drivers and usage trends.

Set time interval and granularity

Set a custom time period, and determine whether you would like to view your data at a monthly or daily level of granularity.

Filter/Group your data

Dig deeper into your data by taking advantage of filtering and grouping functionality, using a variety of available dimensions.

Forecast future costs and usage

Use forecasting to get a better idea of what your costs and usage may look like in the future, so that you can plan ahead.

Save your progress

Once you arrive at a helpful view, save your progress as a new report that you can refer back to in the future.

Build custom applications

Directly access the interactive, ad-hoc analytics engine that powers AWS Cost Explorer.

via - <https://aws.amazon.com/aws-cost-management/aws-cost-explorer/>

Incorrect options:

AWS Cost and 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 updates the report in your bucket once a day in a comma-separated value (CSV) format. AWS Cost and Usage Reports cannot forecast your AWS account cost and usage.

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 forecast your AWS account cost and usage.

AWS Pricing Calculator - AWS Pricing Calculator lets you explore AWS services and create an estimate for the cost of your use cases on AWS. You can model your solutions before building them, explore the price points and calculations behind your estimate, and find the available instance types and contract terms that meet your needs. This enables you to make informed decisions about using AWS. You can plan your AWS costs and usage or price out setting up a new set of instances and services. You cannot use this service to forecast your AWS account cost and usage.

Reference:

<https://aws.amazon.com/aws-cost-management/aws-cost-explorer/>

Question 3: **Incorrect**

The DevOps team at an IT company wants to centrally manage its servers on AWS Cloud as well as on-premise data center so that it can collect software inventory, run commands, configure and patch servers at scale. As a Cloud Practitioner, which AWS service would you recommend for this use-case?

-

Config

(Incorrect)

-

CloudFormation

-

OpsWorks

-

Systems Manager

(Correct)

Explanation

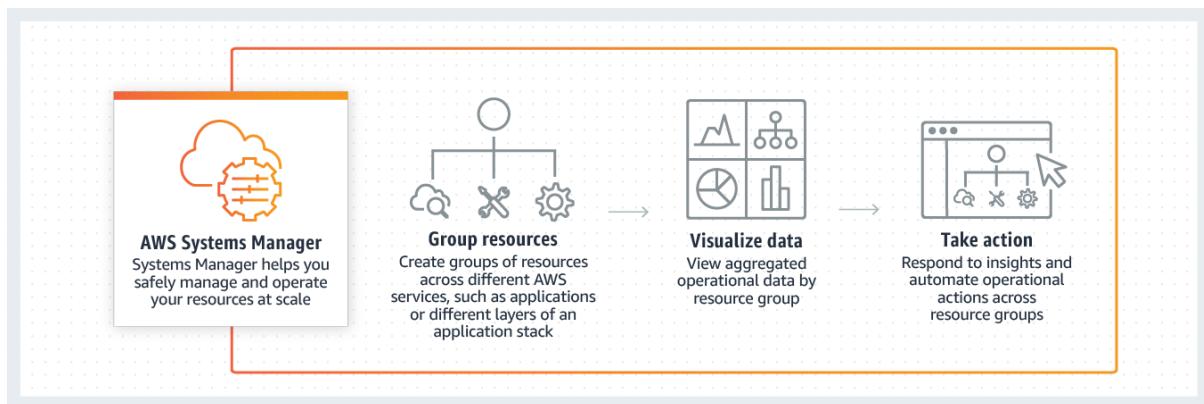
Correct option:

Systems Manager

AWS Systems Manager gives you visibility and control of your infrastructure on AWS. Systems Manager provides a unified user interface so you can view operational data from multiple AWS services and allows you to automate operational tasks such as collecting software inventory, running commands, managing patches, and configuring servers across AWS Cloud as well as on-premises infrastructure.

AWS Systems Manager offers utilities for running commands, patch-management and configuration

compliance: via - <https://aws.amazon.com/systems-manager/faq/>



via - <https://aws.amazon.com/systems-manager/>

Incorrect options:

OpsWorks - AWS OpsWorks is a configuration management service that provides managed instances of Chef and Puppet. OpsWorks lets you use Chef and Puppet to automate how servers are configured, deployed and managed across your Amazon EC2 instances or on-premises compute environments. You cannot use OpsWorks for collecting software inventory and viewing operational data from multiple AWS services.

CloudFormation - AWS CloudFormation allows you to use programming languages or a simple text file to model and provision, in an automated and secure manner, all the resources needed for your applications across all Regions and accounts. Think infrastructure as code; think CloudFormation. You cannot use CloudFormation for running commands or managing patches on servers.

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. You cannot use Config for running commands or managing patches on servers.

References:

<https://aws.amazon.com/systems-manager/>

<https://aws.amazon.com/systems-manager/faq/>

Question 4: **Incorrect**

Which of the following S3 storage classes do not charge any data retrieval fee? (Select two)

-

S3 Glacier

-

S3 Standard

(Correct)

-

S3 Standard-IA

(Incorrect)

-

S3 Intelligent-Tiering

(Correct)

-

S3 One Zone-IA

Explanation

Correct options:

S3 Standard - S3 Standard offers high durability, availability, and performance object storage for frequently accessed data. S3 Standard offers low latency and high throughput performance, It is designed for durability of 99.999999999% of objects across multiple Availability Zones. S3 Standard does not charge any data retrieval fee.

S3 Intelligent-Tiering - The S3 Intelligent-Tiering storage class is designed to optimize costs by automatically moving data to the most cost-effective access tier, without performance impact or operational overhead. It works by storing objects in two access tiers: one tier that is optimized for frequent access and another lower-cost tier that is optimized for infrequent access. S3 Intelligent-Tiering does not charge any data retrieval fee.

Please review this illustration for the S3 Storage Classes retrieval fee. You don't need to memorize the actual numbers, just remember that S3 Standard and S3 Intelligent-Tiering do not charge any retrieval fee:

Performance across the S3 Storage Classes

	S3 Standard	S3 Intelligent-Tiering*	S3 Standard-IA	S3 One Zone-IA†	S3 Glacier Instant Retrieval	S3 Glacier Flexible Retrieval	S3 Glacier Deep Archive
Designed for durability	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)
Designed for availability	99.99%	99.9%	99.9%	99.5%	99.9%	99.99%	99.99%
Availability SLA	99.9%	99%	99%	99%	99%	99.%	99.9%
Availability Zones	≥3	≥3	≥3	1	≥3	≥3	≥3
Minimum capacity charge per object	N/A	N/A	128 KB	128 KB	128 KB	40 KB	40 KB
Minimum storage duration charge	N/A	N/A	30 days	30 days	90 days	90 days	180 days
Retrieval charge	N/A	N/A	per GB retrieved	per GB retrieved	per GB retrieved	per GB retrieved	per GB retrieved
First byte latency	milliseconds	milliseconds	milliseconds	milliseconds	milliseconds	minutes or hours	hours
Storage type	Object	Object	Object	Object	Object	Object	Object
Lifecycle transitions	Yes	Yes	Yes	Yes	Yes	Yes	Yes

via - <https://aws.amazon.com/s3/storage-classes/>

Incorrect options:

S3 Glacier - Amazon S3 Glacier is a secure, durable, and extremely low-cost Amazon S3 cloud storage class for data archiving and long-term backup. It is designed to deliver 99.999999999% durability, and

provide comprehensive security and compliance capabilities that can help meet even the most stringent regulatory requirements. S3 Glacier has a data retrieval fee.

S3 One Zone-IA - 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. It is not suitable for data archival. S3 One Zone-IA has a data retrieval fee.

S3 Standard-IA - S3 Standard-IA is for data that is accessed less frequently, but requires rapid access when needed. S3 Standard-IA offers 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. S3 Standard-IA has a data retrieval fee.

Reference:

<https://aws.amazon.com/s3/storage-classes/>

Question 5: **Incorrect**

AWS Organizations provides which of the following benefits? (Select two)

- **Volume discounts for Amazon EC2 and Amazon S3 aggregated across the member AWS accounts**
(Correct)
- **Provision EC2 Spot instances across the member AWS accounts**
- **Check vulnerabilities on EC2 instances across the member AWS accounts**
(Incorrect)
- **Deploy patches on EC2 instances across the member AWS accounts**
(Incorrect)
- **Share the reserved EC2 instances amongst the member AWS accounts**
(Correct)

Explanation

Correct option:

Volume discounts for Amazon EC2 and Amazon S3 aggregated across the member AWS accounts

Share the reserved EC2 instances amongst the member AWS accounts

AWS Organizations helps you to centrally manage billing; control access, compliance, and security; and share resources such as reserved EC2 instances across your AWS accounts.

Using AWS Organizations, you can automate account creation, create groups of accounts to reflect your business needs, and apply policies for these groups for governance. You can also simplify billing by setting up a single payment method for all of your AWS accounts. AWS Organizations is available to all AWS customers at no additional charge.

You can use AWS Organizations to set up a single payment method for all the AWS accounts in your organization through consolidated billing. With consolidated billing, you can see a combined view of charges incurred by all your accounts, as well as take advantage of pricing benefits from aggregated usage, such as volume discounts for Amazon EC2 and Amazon S3.

Key benefits of AWS Organizations:

CENTRALLY MANAGE POLICIES ACROSS MULTIPLE AWS ACCOUNTS To improve control over your AWS environment, you can use AWS Organizations to create groups of accounts, and then attach policies to a group to ensure the correct policies are applied across the accounts without requiring custom scripts and manual processes.	GOVERN ACCESS TO AWS SERVICES, RESOURCES, AND REGIONS AWS Organizations allows you to restrict what services and actions are allowed in your accounts. You can use Service Control Policies (SCPs) to apply permission guardrails on AWS Identity and Access Management (IAM) users and roles. For example, you can apply an SCP that restricts users in accounts in your organization from launching any resources in regions that you do not explicitly allow.
AUTOMATE AWS ACCOUNT CREATION AND MANAGEMENT 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. For example, you can automate the creation of new accounts for workload or application isolation and grant entities in those accounts access only to the necessary AWS services.	CONFIGURE AWS SERVICES ACROSS MULTIPLE ACCOUNTS AWS Organizations helps you configure AWS services and share resources across accounts in your organization. For example, Organizations integrates with AWS Single Sign-on to enable you to easily provision access for all of your developers to accounts in your organization from a single place. You can make central changes to access permissions and have them automatically updated on accounts in your organization.
CONSOLIDATE BILLING ACROSS MULTIPLE AWS ACCOUNTS You can use AWS Organizations to set up a single payment method for all the AWS accounts in your organization through consolidated billing. With consolidated billing, you can see a combined view of charges incurred by all your accounts, as well as take advantage of pricing benefits from aggregated usage, such as volume discounts for Amazon EC2 and Amazon S3.	

via - <https://aws.amazon.com/organizations/>

Incorrect options:

Check vulnerabilities on EC2 instances across the member AWS accounts

Deploy patches on EC2 instances across the member AWS accounts

Provision EC2 Spot instances across the member AWS accounts

These three options contradict the details provided earlier in the explanation, so these options are incorrect.

Reference:

<https://aws.amazon.com/organizations/>

Question 6: **Correct**

An e-commerce company would like to receive alerts when the Reserved EC2 Instances utilization drops below a certain threshold. Which AWS service can be used to address this use-case?



AWS Trusted Advisor



AWS Cost Explorer



AWS Systems Manager



AWS Budgets

(Correct)

Explanation

Correct option:

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 reservation utilization or coverage targets and receive alerts when your utilization drops below the threshold you define. You can define a utilization threshold and receive alerts when your RI usage falls below that threshold. This lets you see if your RIs are unused or under-utilized. Reservation alerts are supported for Amazon EC2, Amazon RDS, Amazon Redshift, Amazon ElastiCache, and Amazon Elasticsearch reservations.

AWS Budgets

Overview:

Managing your costs with AWS Budgets

[PDF](#) | [Kindle](#) | [RSS](#)

AWS Budgets enable you to plan your service usage, service costs, and instance reservations. Budgets provide you with a way to see the following information:

- How close your plan is to your budgeted amount or to the free tier limits
- Your usage to date, including how much you have used of your Reserved Instances (RIs)
- Your current estimated charges from AWS and how much your predicted usage will incur in charges by the end of the month
- How much of your budget has been used

AWS Budgets information is updated up to three times a day. Updates typically occur between 8 to 12 hours after the previous update. Budgets track your unblended costs, subscriptions, refunds, and RIs. You can create the following types of budgets:

- **Cost budgets** – Plan how much you want to spend on a service.
- **Usage budgets** – Plan how much you want to use one or more services.
- **RI utilization budgets** – Define a utilization threshold and receive alerts when your RI usage falls below that threshold. This lets you see if your RIs are unused or under-utilized.
- **RI coverage budgets** – Define a coverage threshold and receive alerts when the number of your instance hours that are covered by RIs fall below that threshold. This lets you see how much of your instance usage is covered by a reservation.
- **Savings Plans utilization budgets** – Define a utilization threshold and receive alerts when the usage of your Savings Plans falls below that threshold. This lets you see if your Savings Plans are unused or under-utilized.
- **Savings Plans coverage budgets** – Define a coverage threshold and receive alerts when your Savings Plans eligible usage that is covered by Savings Plans fall below that threshold. This lets you see how much of your instance usage is covered by Savings Plans.

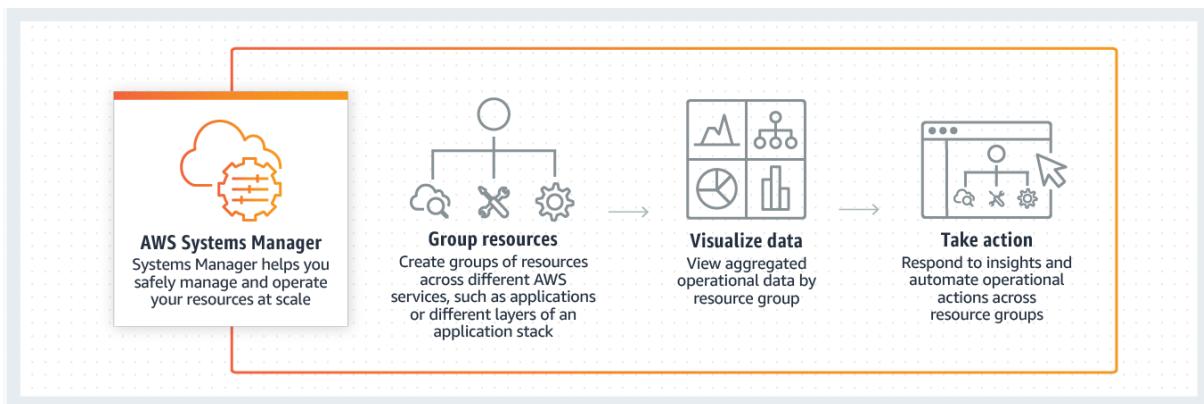
via - <https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/budgets-managing-costs.html>

Incorrect options:

AWS Trusted Advisor - AWS Trusted Advisor is an online tool that provides real-time guidance to help provision your resources following AWS best practices. Whether establishing new workflows, developing applications, or as part of ongoing improvement, recommendations provided by Trusted Advisor regularly help keep your solutions provisioned optimally. AWS Trusted Advisor analyzes your AWS environment and provides best practice recommendations in five categories: Cost Optimization, Performance, Security, Fault Tolerance, Service Limits.

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. Cost Explorer cannot be used to identify under-utilized EC2 instances.

AWS Systems Manager - AWS Systems Manager gives you visibility and control of your infrastructure on AWS. Systems Manager provides a unified user interface so you can view operational data from multiple AWS services and allows you to automate operational tasks such as running commands, managing patches, and configuring servers across AWS Cloud as well as on-premises infrastructure.



via - <https://aws.amazon.com/systems-manager/>

Reference:

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/budgets-managing-costs.html>

Question 7: **Correct**

Amazon EC2 Spot instances are a best-fit for which of the following scenarios?

- **To run batch processes for critical workloads**
- **To run any containerized workload with Elastic Container Service (ECS) that can be interrupted**
- **(Correct)**
- **To install cost-effective RDS database**
- **To run scheduled jobs (jobs that run at the same time every day)**

Explanation

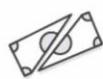
Correct option:

To run any containerized workload with Elastic Container Service (ECS) that can be interrupted

Amazon EC2 Spot Instances let you take advantage of unused EC2 capacity in the AWS cloud. Spot Instances are available at up to a 90% discount compared to On-Demand prices.

Containers are stateless, fault-tolerant and a great fit for Spot Instances. Spot Instances can be used with Elastic Container Service (ECS) or Elastic Container Service for Kubernetes (EKS) to run any containerized workload, from distributed parallel test systems to applications that map millions of miles a day. Spot instances provide the flexibility of ad-hoc provisioning for multiple instance types in different Availability Zones, with an option to hibernate, stop or terminate instances when EC2 needs the capacity back and Spot Instances are reclaimed.

Benefits of Using Spot Instances to Run Containers



LOWER COSTS

Significant price savings of up to 90% over On-Demand EC2 Instances. Simply mix Spot Instances with On-Demand and/or Reserved Instances or run on 100% Spot Instances to optimize cost and performance.



FASTER RESULTS

Easily run multiple projects simultaneously and speed up job flows to generate business results faster and innovate faster without breaking the bank. Run and scale to large numbers of parallel tasks via Spot Fleet or Spot Instance pool.



RESOURCE FLEXIBILITY

Flexibility of ad-hoc provisioning for multiple instance types in different Availability Zones, with an option to hibernate, stop or terminate instances when EC2 needs the capacity back and Spot Instances are reclaimed.



EASE OF USE

Easily launch a Spot Instance via an API call, EC2 Fleet and the AWS Management Console. EC2 Spot is also integrated with other AWS services such as ECS, EKS, EC2 Auto Scaling groups and CloudFormation.

via - <https://aws.amazon.com/ec2/spot/containers-for-less/>

Incorrect options:

To install cost-effective RDS database - Spot instance capacity allocated to you can be taken back anytime without notice if AWS needs them. Hence, Spot instances can only be used as additional compute capacity and not for hosting or installing any software or database.

To run batch processes for critical workloads - Business-critical workloads cannot be run on Spot instances.

To run scheduled jobs (jobs that run at the same time every day) - There is no guarantee that a Spot instance will be available at a specific time every day. For a scheduled requirement, Scheduled Reserved instances should be used.

Reference:

<https://aws.amazon.com/ec2/spot/containers-for-less/>

Question 8: **Correct**

Which of the following is a container service of AWS?



AWS Elastic Beanstalk



Amazon Simple Notification Service



AWS Fargate

(Correct)



Amazon SageMaker

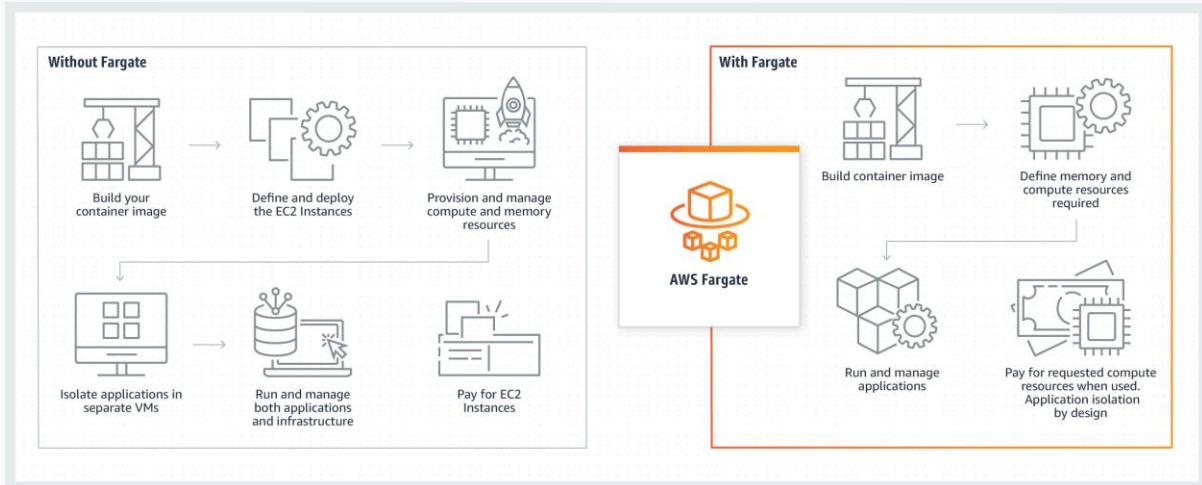
Explanation

Correct option:

AWS Fargate

AWS Fargate is a serverless compute engine for containers that works with both Amazon Elastic Container Service (ECS) and Amazon Elastic Kubernetes Service (EKS). Fargate makes it easy for you to focus on building your applications. Fargate removes the need to provision and manage servers, lets you specify and pay for resources per application, and improves security through application isolation by design.

How Fargate Works:



via - <https://aws.amazon.com/fargate/>

Incorrect options:

AWS Elastic Beanstalk - AWS Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services. You simply upload your code and Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring. Beanstalk provisions servers so it is not a serverless service.

Amazon Simple Notification Service - Amazon Simple Notification Service (SNS) is a highly available, durable, secure, fully managed pub/sub messaging service that enables you to decouple microservices, distributed systems, and serverless applications.

Amazon SageMaker - Amazon SageMaker is a fully managed service that provides every developer and data scientist with the ability to build, train, and deploy machine learning (ML) models quickly. SageMaker removes the heavy lifting from each step of the machine learning process to make it easier to develop high-quality models.

Reference:

<https://aws.amazon.com/fargate/>

Question 9: **Incorrect**

Which of the following statements are true regarding Amazon Simple Storage Service (S3) (Select two)?

-

You can install databases on S3

(Incorrect)

- **S3 is a fully managed, elastic file system storage service used as database backup**
- **S3 is a block storage service designed for a broad range of workloads**
- **S3 is a key value based object storage service**

(Correct)

- **S3 stores data in a flat non-hierarchical structure**

(Correct)

Explanation

Correct options:

S3 is a key value based object storage service

S3 stores data in a flat non-hierarchical structure

Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. S3 stores data in a flat non-hierarchical structure. All objects are stored in S3 buckets and can be organized with shared names called prefixes. You can also append up to 10 key-value pairs called S3 object tags to each object, which can be created, updated, and deleted throughout an object's lifecycle.

Incorrect options:

S3 is a block storage service designed for a broad range of workloads - Block storage service is provided by Amazon Elastic Block Store (EBS) to provide persistent block-level storage volumes for use with Amazon EC2 instances. S3 is an object storage service.

S3 is a fully managed, elastic file system storage service used as database backup - Amazon Elastic File System (Amazon EFS) provides a simple, scalable, fully managed elastic NFS file system for use with AWS Cloud services and on-premises resources. S3 is an object storage service.

You can install databases on S3 - S3 is an object storage service. You cannot install databases on S3.

Reference:

<https://aws.amazon.com/s3/features/>

Question 10: **Incorrect**

Which AWS service will help you install application code automatically to an Amazon EC2 instance?



AWS CloudFormation



AWS CodeDeploy

(Correct)



AWS Elastic Beanstalk

(Incorrect)



AWS CodeBuild

Explanation

Correct option:

AWS CodeDeploy

AWS CodeDeploy is a service that automates application deployments to a variety of compute services including Amazon EC2, AWS Fargate, AWS Lambda, and on-premises instances. CodeDeploy fully automates your application deployments eliminating the need for manual operations. CodeDeploy protects your application from downtime during deployments through rolling updates and deployment health tracking.

Incorrect options:

AWS Elastic Beanstalk - AWS Elastic Beanstalk is the fastest and simplest way to get web applications up and running on AWS. Developers simply upload their application code and the service automatically handles all the details such as resource provisioning, load balancing, auto-scaling, and monitoring. Elastic Beanstalk is an end-to-end application platform, unlike CodeDeploy, which is targeted at code deployment automation for any environment (Development, Testing, Production). It cannot be used to automatically deploy code to an Amazon EC2 instance.

AWS CloudFormation - AWS CloudFormation provides a common language for you to model and provision AWS and third-party application resources in your cloud environment. AWS CloudFormation allows you to use programming languages or a simple text file to model and provision, in an automated and secure manner, all the resources needed for your applications across all regions and accounts. It cannot be used to automatically deploy code to an Amazon EC2 instance.

AWS CodeBuild - AWS CodeBuild is a fully managed continuous integration service that compiles source code, runs tests, and produces software packages that are ready to deploy. With CodeBuild, you don't need to provision, manage, and scale your own build servers. CodeBuild scales continuously and processes multiple builds concurrently, so your builds are not left waiting in a queue. It cannot be used to automatically deploy code to an Amazon EC2 instance.

Reference:

<https://aws.amazon.com/codedeploy/>

Question 11: **Incorrect**

Which of the following is the best practice for application architecture on AWS Cloud?

-

Build monolithic applications

(Incorrect)

-

Build loosely coupled components

(Correct)

-

Build tightly coupled components

-

Use synchronous communication between components

Explanation

Correct option:

Build loosely coupled components

AWS Cloud recommends microservices as an architectural and organizational approach to software development where software is composed of small independent services that communicate over well-defined APIs. These services are owned by small, self-contained teams.

Microservices architectures make applications easier to scale and faster to develop, enabling innovation and accelerating time-to-market for new features. Each service can be considered as a loosely coupled component of a bigger system. You can use services like SNS or SQS to decouple and scale microservices.

Microservices

Overview:

What are Microservices?

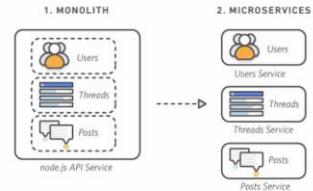
Microservices are an architectural and organizational approach to software development where software is composed of small independent services that communicate over well-defined APIs. These services are owned by small, self-contained teams.

Microservices architectures make applications easier to scale and faster to develop, enabling innovation and accelerating time-to-market for new features.

Monolithic vs. Microservices Architecture

With monolithic architectures, all processes are tightly coupled and run as a single service. This means that if one process of the application experiences a spike in demand, the entire architecture must be scaled. Adding or improving a monolithic application's features becomes more complex as the code base grows. This complexity limits experimentation and makes it difficult to implement new ideas. Monolithic architectures add risk for application availability because many dependent and tightly coupled processes increase the impact of a single process failure.

With a microservices architecture, an application is built as independent components that run each application process as a service. These services communicate via a well-defined interface using lightweight APIs. Services are built for business capabilities and each service performs a single function. Because they are independently run, each service can be updated, deployed, and scaled to meet demand for specific functions of an application.



Breaking a monolithic application into microservices

via - <https://aws.amazon.com/blogs/compute/understanding-asynchronous-messaging-for-microservices/>

Incorrect options:

Build tightly coupled components

Build monolithic applications

With monolithic architectures, all processes are tightly coupled and run as a single service. This means that if one process of the application experiences a spike in demand, the entire architecture must be scaled. Monolithic architectures add risk for application availability because many dependent and tightly coupled processes increase the impact of a single process failure. So both these options are incorrect.

Use synchronous communication between components - Synchronous between applications can be problematic if there are sudden spikes of traffic. You should use SNS or SQS to decouple your application components.

Reference:

<https://aws.amazon.com/blogs/compute/understanding-asynchronous-messaging-for-microservices/>

Question 12: **Correct**

Which of the following AWS services offer LifeCycle Management for cost-optimal storage?

-
-

Amazon Instance Store

-
-

Amazon S3

(Correct)



Amazon EBS



AWS Storage Gateway

Explanation

Correct options:

Amazon S3

You can manage your objects on S3 so that they are stored cost-effectively throughout their lifecycle by configuring 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. For example, you might choose to transition objects to the S3 Standard-IA storage class 30 days after you created them, or archive objects to the S3 Glacier storage class one year after creating them.

Expiration actions – Define when objects expire. Amazon S3 deletes expired objects on your behalf.

Incorrect options:

Amazon Instance Store - An Instance Store provides temporary block-level storage for your EC2 instance. This storage is located on disks that are physically attached to the host computer. Instance store is ideal for the temporary storage of information that changes frequently, such as buffers, caches, scratch data, and other temporary content, or for data that is replicated across a fleet of instances, such as a load-balanced pool of web servers. Instance storage is temporary, data is lost if instance experiences failure or is terminated. Instance Store does not offer Lifecycle Management or Infrequent Access storage class.

Amazon EBS - Amazon Elastic Block Store (EBS) is an easy to use, high-performance block storage service designed for use with Amazon Elastic Compute Cloud (EC2) for both throughput and transaction-intensive workloads at any scale. A broad range of workloads, such as relational and non-relational databases, enterprise applications, containerized applications, big data analytics engines, file systems, and media workflows are widely deployed on Amazon EBS. It does not offer Lifecycle Management or Infrequent Access storage class.

AWS Storage Gateway - AWS Storage Gateway is a hybrid cloud storage service that gives you on-premises access to virtually unlimited cloud storage. All data transferred between the gateway and AWS storage is encrypted using SSL (for all three types of gateways - File, Volume and Tape Gateways). Storage Gateway does not offer Lifecycle Management or Infrequent Access storage class.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html>

Question 13: **Correct**

The DevOps team at a Big Data consultancy has set up EC2 instances across two AWS Regions for its flagship application. Which of the following characterizes this application architecture?



Deploying the application across two AWS Regions improves security



Deploying the application across two AWS Regions improves agility



Deploying the application across two AWS Regions improves availability

(Correct)



Deploying the application across two AWS Regions improves scalability

Explanation

Correct option:

Deploying the application across two AWS Regions improves availability - Highly available systems are those that can withstand some measure of degradation while remaining available. Each AWS Region is fully isolated and comprised of multiple Availability Zones (AZ's), which are fully isolated partitions of AWS infrastructure. To better isolate any issues and achieve high availability, you can partition applications across multiple AZ's in the same AWS Region or even across multiple AWS Regions.

Key Benefits of AWS Global Infrastructure:

Security	Availability	Performance
Security at AWS starts with our core infrastructure. Custom-built for the cloud and designed to meet the most stringent security requirements in the world, our infrastructure is monitored 24/7 to help ensure the confidentiality, integrity, and availability of your data. All data flowing across the AWS global network that interconnects our datacenters and Regions is automatically encrypted at the physical layer before it leaves our secured facilities. You can build on the most secure global infrastructure, knowing you always control your data, including the ability to encrypt it, move it, and manage retention at any time.	AWS delivers the highest network availability of any cloud provider, with 7x fewer down time hours than the next largest cloud provider.* Each region is fully isolated and comprised of multiple AZ's, which are fully isolated partitions of our infrastructure. To better isolate any issues and achieve high availability, you can partition applications across multiple AZ's in the same region. In addition, AWS control planes and the AWS management console are distributed across regions, and include regional API endpoints, which are designed to operate securely for at least 24 hours if isolated from the global control plane functions without requiring customers to access the region or its API endpoints via external networks during any isolation.	The AWS Global Infrastructure is built for performance. AWS Regions offer low latency, low packet loss, and high overall network quality. This is achieved with a fully redundant 100 GbE fiber network backbone, often providing many terabits of capacity between Regions. AWS Local Zones and AWS Wavelength, with our telco providers, provide performance for applications that require single-digit millisecond latencies by delivering AWS infrastructure and services closer to end-users and 5G connected devices. Whatever your application needs, you can quickly spin up resources as you need them, deploying hundreds or even thousands of servers in minutes.
Global Footprint	Scalability	Flexibility
AWS has the largest global infrastructure footprint of any provider, and this footprint is constantly increasing at a significant rate. When deploying your applications and workloads to the cloud, you have the flexibility in selecting a technology infrastructure that is closest to your primary target of users. You can run your workloads on the cloud that delivers the best support for the broadest set of applications, even those with the highest throughput and lowest latency requirements. And if your data lives off this planet, you can use AWS Ground Station , which provides satellite antennas in close proximity to AWS infrastructure Regions.	The AWS Global Infrastructure enables companies to be extremely flexible and take advantage of the conceptually infinite scalability of the cloud. Customers used to over provision to ensure they had enough capacity to handle their business operations at the peak level of activity. Now, they can provision the amount of resources that they actually need, knowing they can instantly scale up or down along with the needs of their business, which also reduces cost and improves the customer's ability to meet their user's demands. Companies can quickly spin up resources as they need them, deploying hundreds or even thousands of servers in minutes.	The AWS Global Infrastructure gives you the flexibility of choosing how and where you want to run your workloads, and when you do you are using the same network, control plane, API's, and AWS services. If you would like to run your applications globally you can choose from any of the AWS Regions and AZ's. If you need to run your applications with single-digit millisecond latencies to mobile devices and end-users you can choose AWS Local Zones or AWS Wavelength . Or if you would like to run your applications on-premises you can choose AWS Outposts .

via - <https://aws.amazon.com/about-aws/global-infrastructure/>

Incorrect options:

Deploying the application across two AWS Regions improves agility - Agility refers to the ability of the cloud to give you easy access to a broad range of technologies so that you can innovate faster and build nearly anything that you can imagine. You can quickly spin up resources as you need them – from infrastructure services, such as compute, storage, and databases, to Internet of Things, machine learning, data lakes and analytics, and much more. Deploying the application across two AWS Regions does not improve agility.

Deploying the application across two AWS Regions improves security - The application security is dependent on multiple factors such as data encryption, IAM policies, IAM roles, VPC security configurations, Security Groups, NACLs, etc. Deploying the application across two AWS Regions directly impacts availability. So this option is not the best fit for the given use-case.

Deploying the application across two AWS Regions improves scalability - For the given use-case, you can improve the scalability of the application by using an Application Load Balancer with an Auto Scaling group. Deploying the application across two AWS Regions directly impacts availability. So this option is not the best fit for the given use-case.

Reference:

<https://aws.amazon.com/about-aws/global-infrastructure/>

Question 14: **Correct**

Which of the following AWS Support plans provide programmatic access to AWS Support Center features to create, manage and close your support cases? (Select two)

-

Business

(Correct)

-

Corporate

-

Enterprise

(Correct)

-

Basic

-

Developer

Explanation

Correct options:

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. You get programmatic access (API Access) to AWS Support Center features to create, manage, and close your support cases, and operationally manage your Trusted Advisor check requests and status.

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. You get programmatic access (API Access) to AWS Support Center features to create, manage, and close your support cases, and operationally manage your Trusted Advisor check requests and status.

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 down: < 1 hour	General guidance: < 24 hours System impaired: < 12 hours Production system impaired: < 4 hours Production system down: < 1 hour Business-critical system down: < 15 minutes
Architectural Guidance	General	Contextual to your use-cases	Consultative review and guidance based on your applications
Programmatic Case Management		AWS Support API	AWS Support API
Third-Party Software Support		Interoperability & configuration guidance and troubleshooting	Interoperability & configuration guidance and troubleshooting

	Developer	Business	Enterprise
Proactive Programs	Access to Infrastructure Event Management for additional fee.	Infrastructure Event Management Well-Architected Reviews Operations Reviews Technical Account Manager (TAM) coordinates access to programs and other AWS experts as needed.	
Technical Account Management		Designated Technical Account Manager (TAM) to proactively monitor your environment and assist with optimization.	
Training		Access to online self-paced labs	
Account Assistance		Concierge Support Team	
Pricing	Greater of \$29 / month*** - or - 3% of monthly AWS usage See pricing detail and example.	Greater of \$100 / month*** - or - 10% of monthly AWS usage for the first \$0-\$10K 7% of monthly AWS usage from \$10K-\$80K 5% of monthly AWS usage from \$80K-\$250K 3% of monthly AWS usage over \$250K See pricing detail and example.	Greater of \$15,000 - or - 10% of monthly AWS usage for the first \$0-\$150K 7% of monthly AWS usage from \$150K-\$500K 5% of monthly AWS usage from \$500K-\$1M 3% of monthly AWS usage over \$1M See pricing detail and example.

via - <https://aws.amazon.com/premiumsupport/plans/>

Incorrect options:

Basic - The basic plan only provides access to the following:

Customer Service & Communities - 24x7 access to customer service, documentation, whitepapers, and support forums. AWS Trusted Advisor - Access to the 7 core Trusted Advisor checks and guidance to provision your resources following best practices to increase performance and improve security. AWS Personal Health Dashboard - A personalized view of the health of AWS services, and alerts when your resources are impacted.

Developer - AWS recommends the Developer Support plan if you are testing or doing early development on AWS and want the ability to get email-based technical support during business hours. This plan also supports general guidance on how services can be used for various use cases, workloads, or applications. You do not get access to Infrastructure Event Management with this plan.

Both these plans do not support programmatic access (API Access) to AWS Support Center.

Corporate - This is a made-up option and has been added as a distractor.

Reference:

<https://aws.amazon.com/premiumsupport/plans/>

Question 15: **Correct**

A social media analytics company wants to migrate to a serverless stack on AWS. Which of the following scenarios can be handled by AWS Lambda? (Select two)

-

You can install low latency databases on Lambda

-

Lambda can be used to execute code in response to events such as updates to DynamoDB tables

(Correct)

-

You can install Container Services on Lambda

-

Lambda can be used for preprocessing of data before it is stored in Amazon S3 buckets

(Correct)

-

Lambda can be used to store sensitive environment variables

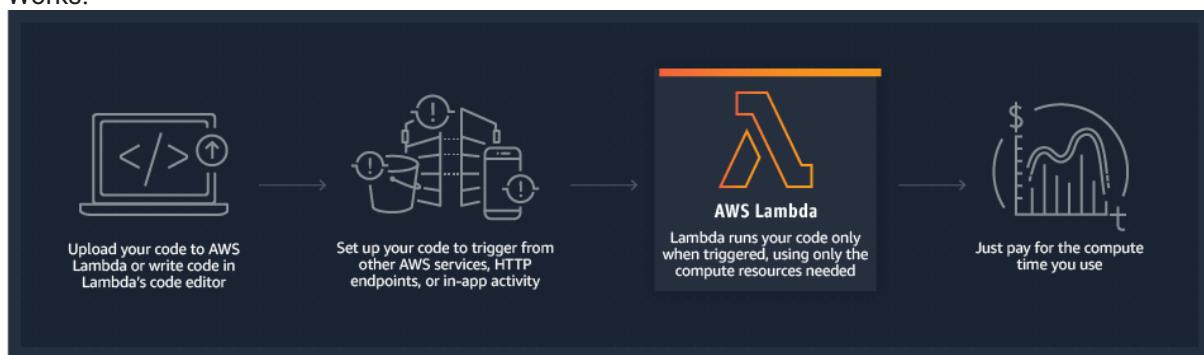
Explanation

Correct options:

AWS Lambda lets you run code without provisioning or managing servers (Lambda is serverless). 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. This functionality makes it an extremely useful service capable of being a serverless backend for websites, data preprocessing, real-time data transformations when used with streaming data, etc.

How Lambda

Works:



via - <https://aws.amazon.com/lambda/>

Lambda can be used to execute code in response to events such as updates to DynamoDB tables - Lambda can be configured to execute code in response to events, such as changes to Amazon S3 buckets, updates to an Amazon DynamoDB table, or custom events generated by your applications or devices.

Lambda can be used for preprocessing of data before it is stored in Amazon S3 buckets - Lambda can be used to run preprocessing scripts to filter, sort or transform data before sending it to downstream applications/services.

Incorrect options:

You can install low latency databases on Lambda - Lambda is serverless, so the underlying hardware and its working is not exposed to the customer. Installing software is not possible since we do not have access to the actual physical server on which Lambda executes the code.

You can install Container Services on Lambda - As discussed above, Lambda cannot be used for installing any software, since the underlying hardware/software might change for each request. But, it is possible to set an environment with necessary libraries when running scripts on Lambda.

Lambda can be used to store sensitive environment variables - Lambda is not a storage service and does not offer capabilities to store data. However, it is possible to read and decrypt/encrypt data using scripts in Lambda.

Reference:

<https://aws.amazon.com/lambda/>

Question 16: **Correct**

AWS Trusted Advisor can provide alerts on which of the following common security misconfigurations? (Select two)?

-

When you share IAM user credentials with others

-

When you don't tag objects in S3 buckets

-

When you don't enable data encryption on S3 Glacier

-

When you don't turn on user activity logging (AWS CloudTrail)

(Correct)

-

When you allow public access to Amazon S3 buckets

(Correct)

Explanation

Correct options:

When you allow public access to Amazon S3 buckets

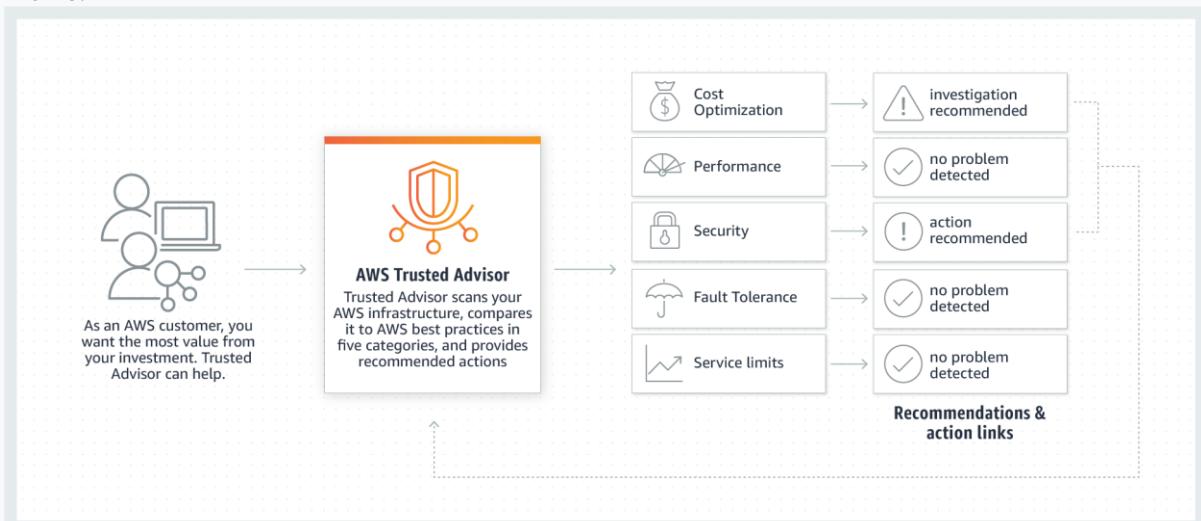
When you don't turn on user activity logging (AWS CloudTrail)

AWS Trusted Advisor is an online tool that provides real-time guidance to help provision your resources following AWS best practices. Whether establishing new workflows, developing

applications, or as part of ongoing improvement, recommendations provided by Trusted Advisor regularly help keep your solutions provisioned optimally. AWS Trusted Advisor analyzes your AWS environment and provides best practice recommendations in five categories: Cost Optimization, Performance, Security, Fault Tolerance, Service Limits.

Trusted Advisor inspects your AWS environment and makes recommendations when opportunities may exist to save money, improve system performance, or close security gaps. It provides alerts on several of the most common security misconfigurations that can occur, including leaving certain ports open that make you vulnerable to hacking and unauthorized access, neglecting to create IAM accounts for your internal users, allowing public access to Amazon S3 buckets, not turning on user activity logging (AWS CloudTrail), or not using MFA on your root AWS Account.

How Trusted Advisor Works:



via - <https://aws.amazon.com/premiumsupport/technology/trusted-advisor/>

Incorrect options:

When you don't tag objects in S3 buckets - Tagging objects (or any resource) in S3 is not mandatory and it's not a security threat.

"When you share IAM user credentials with others" - It is the customer's responsibility to adhere to the IAM security best practices and never share the IAM user credentials with others. Trusted Advisor cannot send an alert for such use-cases.

When you don't enable data encryption on S3 Glacier - By default, data on S3 Glacier is encrypted. So, this option has been added as a distractor.

Reference:

<https://aws.amazon.com/premiumsupport/technology/trusted-advisor/best-practice-checklist/>

Question 17: **Correct**

According to the AWS Shared Responsibility Model, which of the following are responsibilities of the customer for IAM? (Select two)

-

Enable MFA on all accounts

(Correct)

- **Compliance validation for the underlying software infrastructure**
- **Configuration and vulnerability analysis for the underlying software infrastructure**
- **Manage global network security infrastructure**
- **Analyze user access patterns and review IAM permissions**

(Correct)

Explanation

Correct options:

Security and Compliance is a shared responsibility between AWS and the customer. This shared model can help relieve the customer's operational burden as AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates.

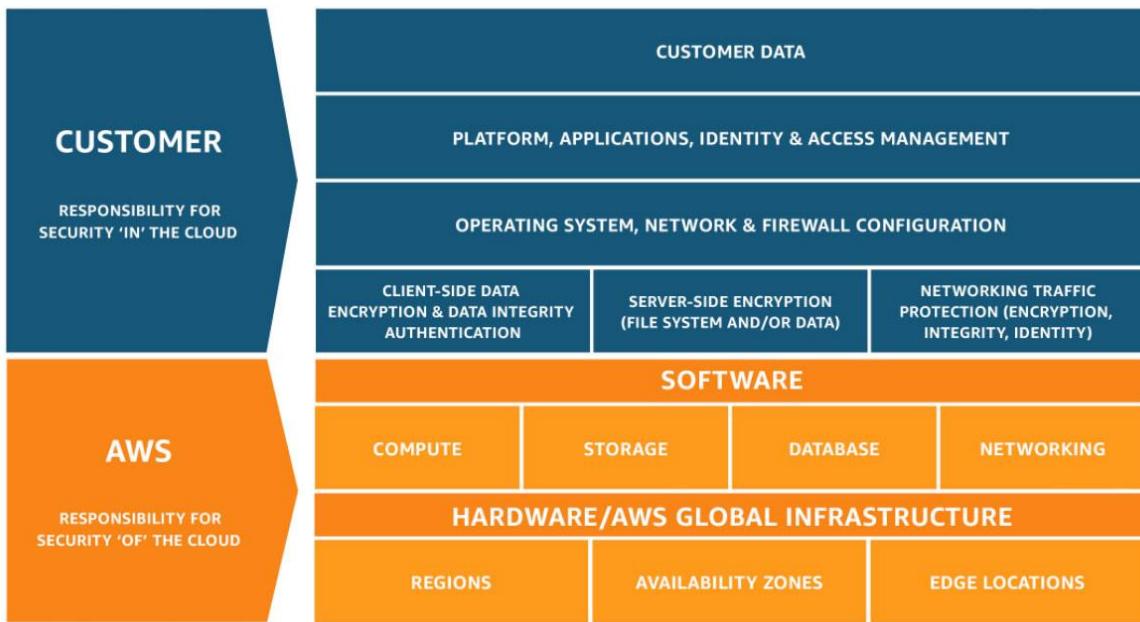
Enable MFA on all accounts

Analyze user access patterns and review IAM permissions

Under the AWS Shared Responsibility Model, customers are responsible for enabling MFA on all accounts, analyzing access patterns and reviewing permissions.

Shared Responsibility Model

Overview:



via - <https://aws.amazon.com/compliance/shared-responsibility-model/>

Incorrect options:

Manage global network security infrastructure

Configuration and vulnerability analysis for the underlying software infrastructure

Compliance validation for the underlying software infrastructure

According to the AWS Shared Responsibility Model, AWS is responsible for "Security of the Cloud". This includes protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services. Therefore these three options fall under the responsibility of AWS.

Reference:

<https://aws.amazon.com/compliance/shared-responsibility-model/>

Question 18: **Correct**

A media company uploads its media (audio and video) files to a centralized S3 bucket from geographically dispersed locations. Which of the following solutions can the company use to optimize transfer speeds?



S3 Transfer Acceleration

(Correct)



Amazon CloudFront



AWS Global Accelerator



AWS Direct Connect

Explanation

Correct option:

S3 Transfer Acceleration

Amazon S3 Transfer Acceleration (S3TA) enables fast, easy, and secure transfers of files over long distances between your client and your Amazon S3 bucket. S3 Transfer Acceleration leverages Amazon CloudFront's globally distributed AWS Edge Locations. As data arrives at an AWS Edge Location, data is routed to your Amazon S3 bucket over an optimized network path. S3 Transfer Acceleration is designed to optimize transfer speeds from across the world into S3 buckets. If you are uploading to a centralized bucket from geographically dispersed locations, or if you regularly transfer GBs or TBs of data across continents, you may save hours or days of data transfer time with S3 Transfer Acceleration.

Benefits of S3 Transfer Acceleration (S3TA):

Move data faster over long distances	Reduce network variability	Shorten the distance to S3	Maximize bandwidth utilization
S3TA can accelerate long-distance transfers to and from your Amazon S3 buckets. The longer the distance between your client application (mobile, web application, or upload tool) and the target S3 bucket, the more S3TA can help. And if S3TA would not accelerate a transfer, you are not charged.	For applications interacting with your S3 buckets through the S3 API from outside of your bucket's region, S3TA helps avoid the variability in Internet routing and congestion. It does this by routing your uploads and downloads over the AWS global network infrastructure, so you get the benefit of our network optimizations.	S3TA shortens the distance between client applications and AWS servers that acknowledge PUTS and GETS to Amazon S3 using our global network of hundreds of CloudFront Edge Locations. We automatically route your uploads and downloads through the closest Edge Locations to your application.	S3TA on average fully utilizes your bandwidth for transfers, and minimizes the effect of distance on throughput. This helps to ensure consistently fast performance to Amazon S3 regardless of your client's location.

via - <https://aws.amazon.com/s3/transfer-acceleration/>

Incorrect options:

Amazon CloudFront - Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a developer-friendly environment. CloudFront is used for content delivery than for data uploads. CloudFront caches data and a subsequent request for a webpage will not go to the origin server, but will be served from the cache. S3 Transfer Acceleration is a better option for the given use-case.

AWS Direct Connect - AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS. You can use AWS Direct Connect to establish a private virtual interface from your on-premise network directly to your Amazon VPC. This private connection takes at least one month for completion. You cannot use Direct Connect to optimize media uploads into S3.

AWS Global Accelerator - AWS Global Accelerator is a service that improves the availability and performance of your applications with local or global users. It provides static IP addresses that act as a fixed entry point to your application endpoints in a single or multiple AWS Regions, such as your Application Load Balancers, Network Load Balancers or Amazon EC2 instances. Similar to CloudFront it uses AWS Global network and edge locations for enhanced performance. It's an overall performance enhancer than an upload speed accelerator. You cannot use Global Accelerator to optimize media uploads into S3.

Reference:

<https://aws.amazon.com/s3/transfer-acceleration/>

Question 19: **Incorrect**

Which of the following entities should be used for an Amazon EC2 Instance to access a DynamoDB table?



IAM role

(Correct)



Amazon Cognito



AWS IAM user access keys



AWS Key Management Service

(Incorrect)

Explanation

Correct option:

IAM Role

An IAM Role is an IAM identity that you can create in your account that has specific permissions. An IAM role is similar to an IAM user in that it is an AWS identity with permissions policies that determine what the identity can and cannot do in AWS. When you assume a role, it provides you with temporary security credentials for your role session.

Incorrect options:

AWS IAM user access keys - Access keys are long-term credentials for an IAM user or the AWS account root user. You can use access keys to sign programmatic requests to the AWS CLI or AWS API (directly or using the AWS SDK). Access keys consist of two parts: an access key ID and a secret access key. As a user name and password, you must use both the access key ID and secret access key together to authenticate your requests. As a best practice, AWS suggests the use of temporary security credentials (IAM roles) instead of access keys.

Amazon Cognito - Amazon Cognito lets you add user sign-up, sign-in, and access control to your web and mobile apps quickly and easily. Amazon Cognito scales to millions of users and supports sign-in with social identity providers, such as Facebook, Google, and Amazon, and enterprise identity providers via SAML 2.0. Amazon Cognito cannot be used to facilitate an Amazon EC2 Instance to access a DynamoDB table.

AWS Key Management Service - AWS Key Management Service (KMS) makes it easy for you to create and manage cryptographic keys and control their use across a wide range of AWS services and in your applications. AWS KMS is a secure and resilient service that uses hardware security modules that have been validated under FIPS 140-2, or are in the process of being validated, to protect your keys. AWS KMS cannot be used to facilitate an Amazon EC2 Instance to access a DynamoDB table.

Reference:

https://docs.amazonaws.cn/en_us/amazondynamodb/latest/developerguide/authentication-and-access-control.html

Question 20: **Incorrect**

Which AWS service will you use to provision the same AWS infrastructure across multiple AWS accounts and regions?



AWS Systems Manager



AWS CloudFormation

(Correct)



AWS OpsWorks

(Incorrect)



AWS CodeDeploy

Explanation

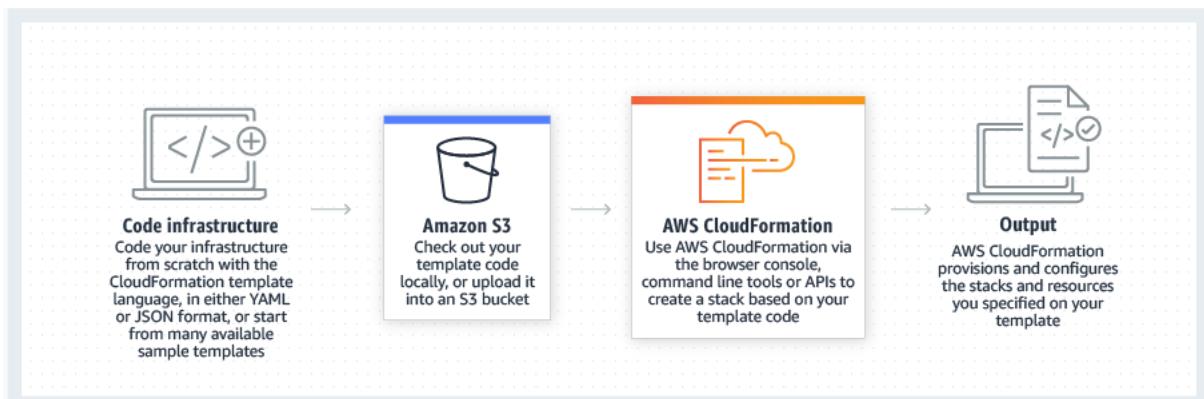
Correct option:

AWS CloudFormation

AWS CloudFormation allows you to use programming languages or a simple text file to model and provision, in an automated and secure manner, all the resources needed for your applications across all Regions and accounts. A stack is a collection of AWS resources that you can manage as a single unit. In other words, you can create, update, or delete a collection of resources by creating, updating, or deleting stacks.

AWS CloudFormation StackSets extends the functionality of stacks by enabling you to create, update, or delete stacks across multiple accounts and regions with a single operation. Using an administrator account, you define and manage an AWS CloudFormation template, and use the template as the basis for provisioning stacks into selected target accounts across specified regions.

How CloudFormation Works:



via - <https://aws.amazon.com/cloudformation/>

Incorrect options:

AWS CodeDeploy - AWS CodeDeploy is a fully managed deployment service that automates software deployments to a variety of compute services such as Amazon EC2, AWS Fargate, AWS Lambda, and your on-premises servers. AWS CodeDeploy makes it easier for you to rapidly release new features, helps you avoid downtime during application deployment, and handles the complexity of updating your applications. You cannot use this service to provision AWS infrastructure.

AWS OpsWorks - AWS OpsWorks is a configuration management service that provides managed instances of Chef and Puppet. OpsWorks lets you use Chef and Puppet to automate how servers are configured, deployed and managed across your Amazon EC2 instances or on-premises compute environments. You cannot use OpsWorks for running commands or managing patches on servers. You cannot use this service to provision AWS infrastructure.

AWS Systems Manager - AWS Systems Manager gives you visibility and control of your infrastructure on AWS. Systems Manager provides a unified user interface so you can view operational data from multiple AWS services and allows you to automate operational tasks across your AWS resources. With Systems Manager, you can group resources, like Amazon EC2 instances, Amazon S3 buckets, or Amazon RDS instances, by application, view operational data for monitoring and troubleshooting, and take action on your groups of resources. You cannot use this service to provision AWS infrastructure.

Reference:

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/what-is-cfnstacksets.html>

Question 21: **Correct**

As per the AWS Shared Responsibility Model, which of the following is a responsibility of AWS from a security and compliance point of view?

-
- Service and Communications Protection**
-
- Identity and Access Management**
-
- Patching networking infrastructure**

(Correct)

-

Patching guest OS and applications

Explanation

Correct option:

Patching networking infrastructure

According to the AWS Shared Responsibility Model, AWS is responsible for "Security of the Cloud". This includes protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services. Therefore, patching networking infrastructure is the responsibility of AWS.

Incorrect options:

Service and Communications Protection

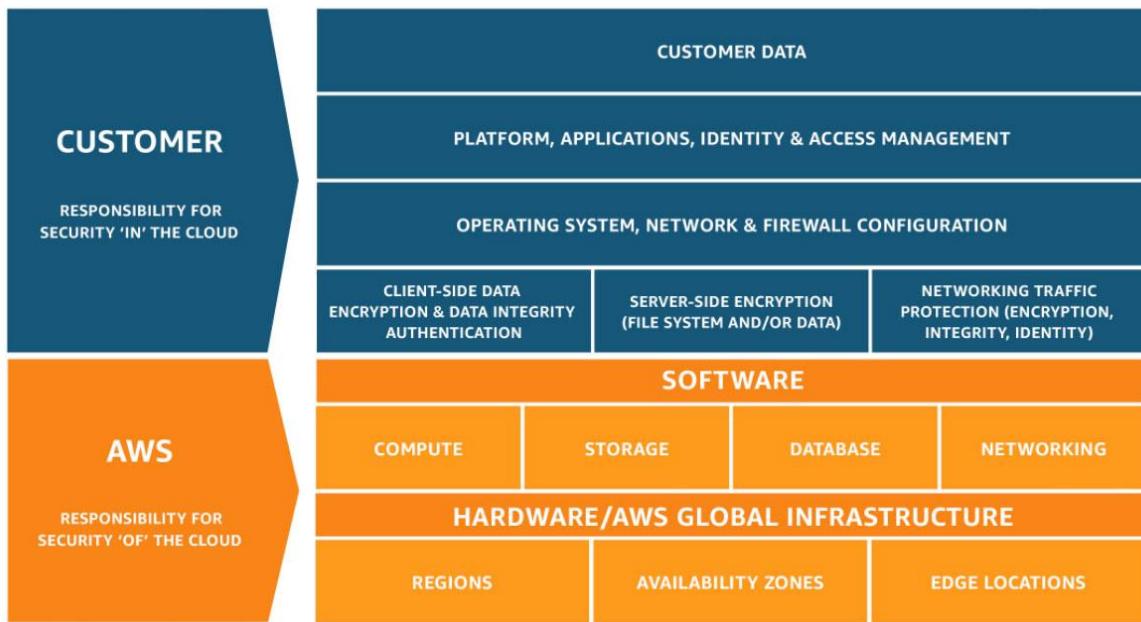
Identity and Access Management

Patching guest OS and applications

The customer is responsible for security "in" the cloud. This covers things such as services and communications protection; Identity and Access Management; and patching guest OS and applications. Customers are responsible for managing their data including encryption options and using Identity and Access Management tools for implementing appropriate access control policies as per their organization requirements. Therefore, these three options fall under the responsibility of the customer according to the AWS shared responsibility model.

Exam Alert:

Please review the Shared Responsibility Model in detail as you can expect multiple questions on the shared responsibility model in the exam:



via - <https://aws.amazon.com/compliance/shared-responsibility-model/>

Reference:

<https://aws.amazon.com/compliance/shared-responsibility-model/>

Question 22: **Incorrect**

Which of the following AWS storage services can be directly used with on-premises systems?

-

Amazon Simple Storage Service (Amazon S3)

-

Amazon Elastic Block Store (EBS)

-

Amazon Elastic File System (Amazon EFS)

(Correct)

-

Amazon EC2 Instance Store

(Incorrect)

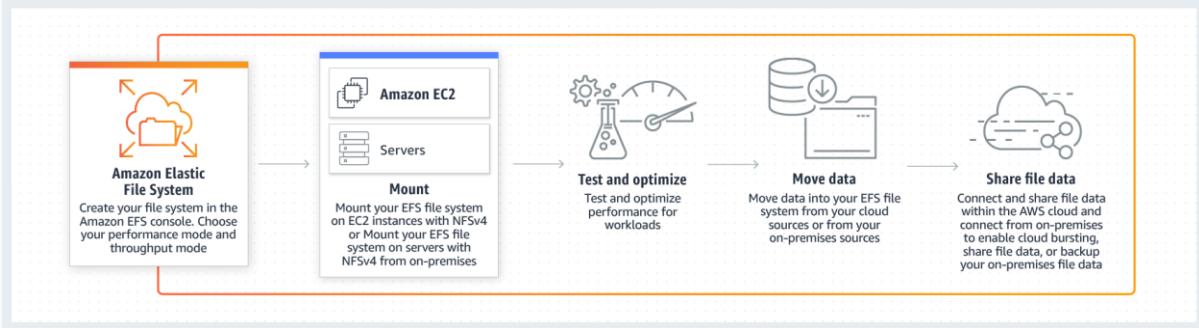
Explanation

Correct option: **Amazon Elastic File System (Amazon EFS)**

Amazon Elastic File System (Amazon EFS) provides a simple, scalable, fully managed elastic NFS file system for use with AWS Cloud services and on-premises resources.

To access EFS file systems from on-premises, you must have an AWS Direct Connect or AWS VPN connection between your on-premises datacenter and your Amazon VPC. You mount an EFS file system on your on-premises Linux server using the standard Linux mount command for mounting a file system

How EFS Works:



via - <https://aws.amazon.com/efs/faq/>

Incorrect options:

Amazon Elastic Block Store (EBS) - Amazon Elastic Block Store (EBS) is an easy to use, high-performance block storage service designed for use with Amazon Elastic Compute Cloud (EC2) for both throughput and transaction-intensive workloads at any scale. EBS volumes can only be mounted with Amazon EC2.

Amazon EC2 Instance Store - An instance store provides temporary block-level storage for your Amazon EC2 instance. This storage is located on disks that are physically attached to the host computer. It is not possible to use this storage from on-premises systems.

Amazon Simple Storage Service (Amazon S3) - Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. Amazon S3 can be accessed from on-premises only via AWS Storage Gateway. It is not possible to access S3 directly from on-premises systems.

Reference:

<https://aws.amazon.com/efs/faq/>

Question 23: **Correct**

Which of the following is correct regarding the AWS RDS service?

-
-

You can use Read Replicas for both improved read performance as well as Disaster Recovery

(Correct)

-
-

You can use both Read Replicas and Multi-AZ for improved read performance

- You can use Read Replicas for improved read performance and Multi-AZ for Disaster Recovery
- You can use Read Replicas for Disaster Recovery and Multi-AZ for improved read performance

Explanation

Correct option:

You can use Read Replicas for both improved read performance as well as Disaster Recovery

Amazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and scale a relational database in the cloud. Read Replicas allow you to create read-only copies that are synchronized with your master database. Read Replicas are used for improved read performance. You can also place your read replica in a different AWS Region closer to your users for better performance. Using a cross-Region Read Replica can also help ensure that you get back up and running if you experience a regional availability issue in case of a disaster. Read Replicas are an example of horizontal scaling of resources.

Read Replica

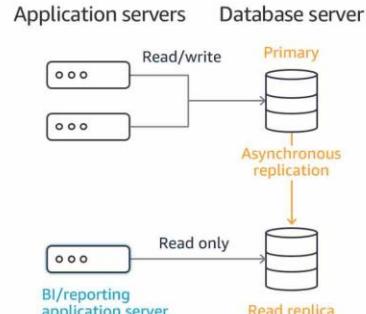
Overview:

Amazon RDS Read Replicas provide enhanced performance and durability for RDS database (DB) instances. They make it easy to elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads. You can create one or more replicas of a given source DB Instance and serve high-volume application read traffic from multiple copies of your data, thereby increasing aggregate read throughput. Read replicas can also be promoted when needed to become standalone DB instances. Read replicas are available in Amazon RDS for MySQL, MariaDB, PostgreSQL, Oracle, and SQL Server as well as Amazon Aurora.

For the MySQL, MariaDB, PostgreSQL, Oracle, and SQL Server database engines, Amazon RDS creates a second DB instance using a snapshot of the source DB instance. It then uses the engines' native asynchronous replication to update the read replica whenever there is a change to the source DB instance. The read replica operates as a DB instance that allows only read-only connections; applications can connect to a read replica just as they would to any DB instance. Amazon RDS replicates all databases in the source DB instance.

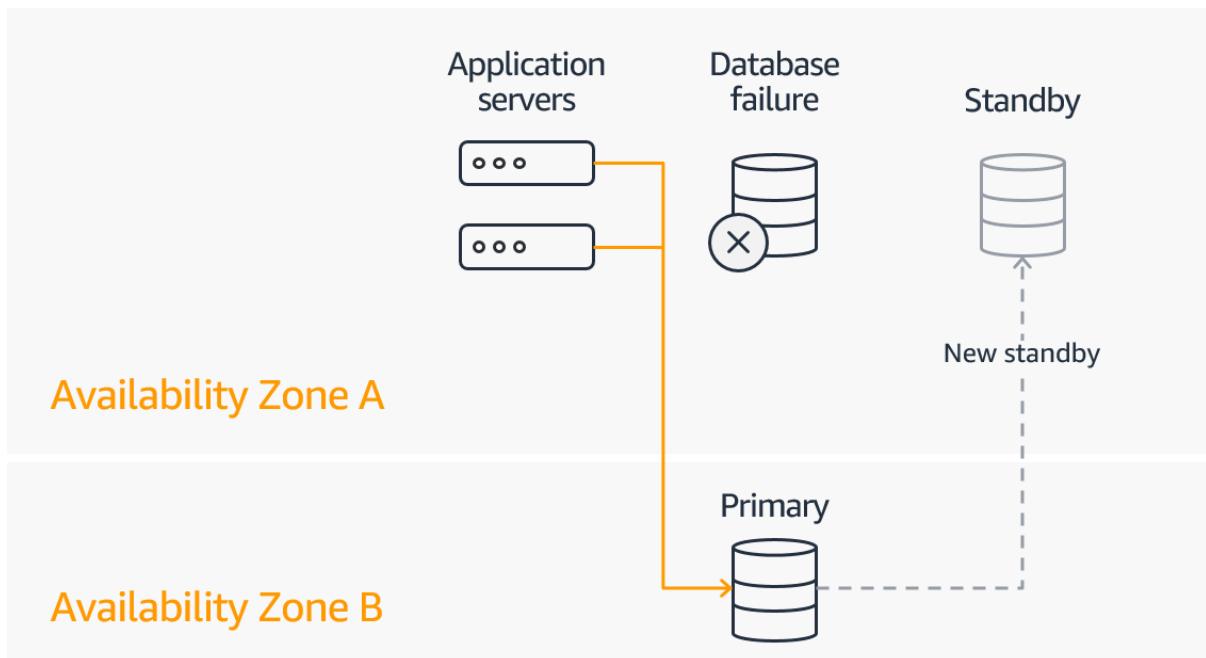
Amazon Aurora further extends the benefits of read replicas by employing an SSD-backed virtualized storage layer purpose-built for database workloads. Amazon Aurora replicas share the same underlying storage as the source instance, lowering costs and avoiding the need to copy data to the replica nodes. For more information about replication with Amazon Aurora, see the [online documentation](#).

via - <https://aws.amazon.com/rds/features/multi-az/>



Amazon RDS Multi-AZ deployments provide enhanced availability and durability for RDS database (DB) instances, making them a natural fit for production database workloads. When you provision a Multi-AZ DB Instance, Amazon RDS automatically creates a primary DB Instance and synchronously replicates the data to a standby instance in a different Availability Zone (AZ). Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. Since the endpoint for your DB Instance remains the same after a failover, your application can resume database operation without the need for manual administrative intervention. Think of multi-AZ as enhancing the availability and reliability of your system, however, by itself, multi-AZ cannot be used for disaster recovery.

How Multi-AZ Works:



via - <https://aws.amazon.com/rds/features/multi-az/>

To understand the RDS disaster recovery capabilities in more detail, you can refer to this excellent AWS blog: <https://aws.amazon.com/blogs/database/implementing-a-disaster-recovery-strategy-with-amazon-rds/>

Incorrect options:

You can use Read Replicas for improved read performance and Multi-AZ for Disaster Recovery

You can use both Read Replicas and Multi-AZ for improved read performance

You can use Read Replicas for Disaster Recovery and Multi-AZ for improved read performance

These three options contradict the details provided earlier in the explanation, so these options are incorrect.

References:

<https://aws.amazon.com/blogs/database/implementing-a-disaster-recovery-strategy-with-amazon-rds/>

<https://aws.amazon.com/rds/features/multi-az/>

Question 24: **Correct**

Which of the following is best-suited for load-balancing HTTP and HTTPS traffic?

-

Network Load Balancer

-

System Load Balancer

Application Load Balancer

(Correct)

AWS Auto Scaling

Explanation

Correct option:

Application Load Balancer

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. 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.

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/elasticloadbalancing/>

Application Load Balancer is used for load balancing of HTTP and HTTPS traffic and provides advanced request routing targeted at the delivery of modern application architectures, including microservices and containers.

Incorrect options:

Network Load Balancer - Network Load Balancer is best suited for load balancing of Transmission Control Protocol (TCP), User Datagram Protocol (UDP) and Transport Layer Security (TLS) traffic where extreme performance is required.

AWS Auto Scaling - AWS Auto Scaling monitors your applications and automatically adjusts the capacity to maintain steady, predictable performance at the lowest possible cost. Using AWS Auto Scaling, it's easy to setup application scaling for multiple resources across multiple services in minutes. The service provides a simple, powerful user interface that lets you build scaling plans for resources including Amazon EC2 instances and Spot Fleets, Amazon ECS tasks, Amazon DynamoDB tables and indexes, and Amazon Aurora Replicas. Auto Scaling cannot be used for load-balancing HTTP and HTTPS traffic.

System Load Balancer - This is a made-up option and has been added as a distractor.

Reference:

<https://aws.amazon.com/elasticloadbalancing/>

Question 25: **Incorrect**

AWS Shield Advanced provides expanded DDoS attack protection for web applications running on which of the following resources? (Select two)

- **AWS Identity and Access Management (IAM)**
- **Amazon CloudFront**
(Correct)
- **AWS Elastic Beanstalk**
(Incorrect)
- **Amazon Elastic Compute Cloud**
(Correct)
- **Amazon Simple Storage Service (Amazon S3)**
(Incorrect)

Explanation

Correct options:

Amazon CloudFront

Amazon Elastic Compute Cloud

AWS Shield Standard is activated for all AWS customers, by default. For higher levels of protection against attacks, you can subscribe to AWS Shield Advanced. With Shield Advanced, you also have exclusive access to advanced, real-time metrics and reports for extensive visibility into attacks on your AWS resources. With the assistance of the DRT (DDoS response team), AWS Shield Advanced includes intelligent DDoS attack detection and mitigation for not only for network layer (layer 3) and transport layer (layer 4) attacks but also for application layer (layer 7) attacks.

AWS Shield Advanced provides expanded DDoS attack protection for web applications running on the following resources: Amazon Elastic Compute Cloud, Elastic Load Balancing (ELB), Amazon CloudFront, Amazon Route 53, AWS Global Accelerator.

Incorrect options:

Amazon Simple Storage Service (Amazon S3)

AWS Elastic Beanstalk

AWS Identity and Access Management (IAM)

These three resource types are not supported by AWS Shield Advanced.

Reference:

<https://docs.aws.amazon.com/waf/latest/developerguide/ddos-overview.html>

Question 26: **Correct**

A streaming media company wants to convert English language subtitles into Spanish language subtitles. As a Cloud Practitioner, which AWS service would you recommend for this use-case?



Amazon Transcribe



Amazon Translate

(Correct)



Amazon Polly



Amazon Rekognition

Explanation

Correct option:

Amazon Translate

Amazon Translate is a neural machine translation service that delivers fast, high-quality, and affordable language translation. Amazon Translate allows you to localize content - such as websites and applications - for international users, and to easily translate large volumes of text efficiently.

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 Transcribe - You can use Amazon Transcribe to add speech-to-text capability to your applications. Amazon Transcribe uses a deep learning process called automatic speech recognition (ASR) to convert speech to text quickly and accurately. Amazon Transcribe can be used to transcribe customer service calls, to automate closed captioning and subtitling, and to generate metadata for media assets.

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.

Reference:

<https://aws.amazon.com/translate/>

Question 27: **Correct**

AWS Marketplace facilitates which of the following use-cases? (Select two)

- **Buy Amazon EC2 Standard Reserved Instances**
 - **AWS customer can buy software that has been bundled into customized AMIs by the AWS Marketplace sellers**
- (Correct)**
- **Raise request for purchasing AWS Direct Connect connection**
 - **Sell Software as a Service (SaaS) solutions to AWS customers**
- (Correct)**
- **Purchase compliance documents from third-party vendors**

Explanation

Correct option:

Sell Software as a Service (SaaS) solutions to AWS customers

AWS customer can buy software that has been bundled into customized AMIs by the AWS Marketplace sellers

AWS Marketplace is a digital catalog with thousands of software listings from independent software vendors that make it easy to find, test, buy, and deploy software that runs on AWS. The AWS Marketplace enables qualified partners to market and sell their software to AWS Customers.

AWS Marketplace offers two ways for sellers to deliver software to customers: Amazon Machine Image (AMI) and Software as a Service (SaaS).

Amazon Machine Image (AMI): Offering an AMI is the preferred option for listing products in AWS Marketplace. Partners have the option for free or paid products. Partners can offer paid products charged by the hour or month. Bring Your Own License (BYOL) is also available and enables customers with existing software licenses to easily migrate to AWS.

Software as a Service (SaaS): If you offer a SaaS solution running on AWS (and are unable to build your product into an AMI) the SaaS listing offers our partners a way to market their software to customers.

Incorrect options:

Purchase compliance documents from third-party vendors - There is no third party vendor for providing compliance documents. 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.

Buy Amazon EC2 Standard Reserved Instances - Amazon EC2 Standard Reserved Instances can be bought from the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>

Raise request for purchasing AWS Direct Connect connection - AWS Direct Connect connection can be raised from the AWS management console at <https://console.aws.amazon.com/directconnect/v2/home>

References:

<https://aws.amazon.com/partners/aws-marketplace/>

<https://aws.amazon.com/artifact/>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ri-market-concepts-buying.html#ri-queued-purchase>

Question 28: **Incorrect**

Which of the following AWS entities lists all users in your account and the status of their various account aspects such as passwords, access keys, and MFA devices?



AWS Cost and Usage Reports

- AWS Trusted Advisor
- Credential Reports
(Correct)
- Amazon Inspector
(Incorrect)

Explanation

Correct option:

Credential Reports

You can generate and download a credential report that lists all users in your account and the status of their various credentials, including passwords, access keys, and MFA devices. You can use credential reports to assist in your auditing and compliance efforts. You can use the report to audit the effects of credential lifecycle requirements, such as password and access key rotation. You can provide the report to an external auditor, or grant permissions to an auditor so that he or she can download the report directly.

Incorrect options:

AWS Trusted Advisor - AWS Trusted Advisor is an online tool that provides real-time guidance to help provision your resources following AWS best practices. Whether establishing new workflows, developing applications, or as part of ongoing improvement, recommendations provided by Trusted Advisor regularly help keep your solutions provisioned optimally. AWS Trusted Advisor analyzes your AWS environment and provides best practice recommendations in five categories: Cost Optimization, Performance, Security, Fault Tolerance, Service Limits.

AWS Cost and 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. Cost and Usage Reports cannot be used to identify under-utilized EC2 instances.

Amazon Inspector - Amazon Inspector is an automated, security assessment service that helps you check for unintended network accessibility of your Amazon EC2 instances and for vulnerabilities on those EC2 instances. Amazon Inspector assessments are offered to you as pre-defined rules packages mapped to common security best practices and vulnerability definitions.

Reference:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_getting-report.html

Question 29: **Incorrect**

Which pillar of AWS Well-Architected Framework is responsible for making sure that you select the right resource types and sizes based on your workload requirements?

-
- **Reliability**
-
- **Operational Excellence**
- **(Incorrect)**
-
- **Performance Efficiency**
- **(Correct)**
-
- **Cost Optimization**

Explanation

Correct option:

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 six pillars – Operational Excellence, Security, Reliability, Performance Efficiency, Cost Optimization and Sustainability.

Overview of the six pillars of the Well-Architected Framework:

AWS Well-Architected and the Six Pillars

Framework Overview

The AWS Well-Architected Framework describes key concepts, design principles, and architectural best practices for designing and running workloads in the cloud. By answering a few foundational questions, learn how well your architecture aligns with cloud best practices and gain guidance for making improvements.

[HTML](#) | [Kindle](#) | [Labs](#)



Operational Excellence Pillar

The operational excellence pillar focuses on running and monitoring systems, and continually improving processes and procedures. Key topics include automating changes, responding to events, and defining standards to manage daily operations.

[HTML](#) | [Kindle](#) | [Labs](#)

Security Pillar

The security pillar focuses on protecting information and systems. Key topics include confidentiality and integrity of data, managing user permissions, and establishing controls to detect security events.

[HTML](#) | [Kindle](#) | [Labs](#)

Reliability Pillar

The reliability pillar focuses on workloads performing their intended functions and how to recover quickly from failure to meet demands. Key topics include distributed system design, recovery planning, and adapting to changing requirements.

[HTML](#) | [Kindle](#) | [Labs](#)

Performance Efficiency Pillar

The performance efficiency pillar focuses on structured and streamlined allocation of IT and computing resources. Key topics include selecting resource types and sizes optimized for workload requirements, monitoring performance, and maintaining efficiency as business needs evolve.

via - <https://aws.amazon.com/architecture/well-architected/>

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.

Incorrect options:

Cost Optimization - Cost Optimization focuses on avoiding un-needed costs. Key topics include understanding and controlling where the 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.

Reliability - This refers to the ability of a system to recover from infrastructure or service disruptions, dynamically acquire computing resources to meet demand, and mitigate disruptions such as misconfigurations or transient network issues.

Operational Excellence - The Operational Excellence pillar includes the ability to run and monitor systems to deliver business value and to continually improve supporting processes and procedures. In the cloud, you can apply the same engineering discipline that you use for application code to your entire environment. You can define your entire workload (applications, infrastructure) as code and update it with code. You can implement your operations procedures as code and automate their execution by triggering them in response to events.

Reference:

<https://aws.amazon.com/architecture/well-architected/>

Question 30: **Incorrect**

Which of the following AWS authentication mechanisms supports a Multi-Factor Authentication (MFA) device that you can plug into a USB port on your computer?

- SMS text message-based MFA
 - Virtual MFA device
 - U2F security key
- (Correct)**
- Hardware MFA device
- (Incorrect)**

Explanation

Correct option:

U2F security key - Universal 2nd Factor (U2F) Security Key is a device that you can plug into a USB port on your computer. U2F is an open authentication standard hosted by the FIDO Alliance. When you enable a U2F security key, you sign in by entering your credentials and then tapping the device instead of manually entering a code.

How to enable the U2F Security Key for your own IAM user:

To enable a U2F security key for your own IAM user (console)

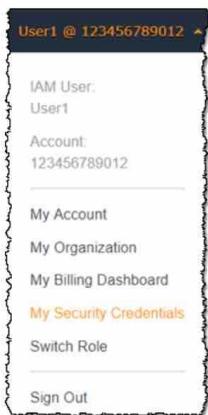
1. Use your AWS account ID or account alias, your IAM user name, and your password to sign in to the [IAM console](#).

Note

For your convenience, the AWS sign-in page uses a browser cookie to remember your IAM user name and account information. If you previously signed in as a different user, choose **Sign in to a different account** near the bottom of the page to return to the main sign-in page. From there, you can type your AWS account ID or account alias to be redirected to the IAM user sign-in page for your account.

To get your AWS account ID, contact your administrator.

2. In the navigation bar on the upper right, choose your user name, and then choose **My Security Credentials**.



3. On the **AWS IAM credentials** tab, in the **Multi-factor authentication** section, choose **Manage MFA device**.
4. In the **Manage MFA device** wizard, choose **U2F security key**, and then choose **Continue**.
5. Insert the U2F security key into your computer's USB port.



6. Tap the U2F security key, and then choose **Close** when U2F setup is complete.

via - https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_enable_u2f.html

Incorrect options:

Virtual MFA device - This is a software app that runs on a phone or other device and emulates a physical device. The device generates a six-digit numeric code based upon a time-synchronized one-time password algorithm. The user must type a valid code from the device on a second webpage during sign-in. Each virtual MFA device assigned to a user must be unique.

Hardware MFA device - This is a hardware device that generates a six-digit numeric code based upon a time-synchronized one-time password algorithm. The user must type a valid code from the device on a second webpage during sign-in. Each MFA device assigned to a user must be unique. A user cannot type a code from another user's device to be authenticated.

SMS text message-based MFA - This is a type of MFA in which the IAM user settings include the phone number of the user's SMS-compatible mobile device. When the user signs in, AWS sends a six-digit numeric code by SMS text message to the user's mobile device. The user is required to type that code on a second webpage during sign-in.

References:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa.html

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_enable_u2f.html

Question 31: **Incorrect**

Which AWS service can help you analyze your infrastructure to identify unattached or underutilized EBS volumes?

-
-

Amazon CloudWatch

(Incorrect)

-
-

Amazon Inspector

-
-

AWS Trusted Advisor

(Correct)

-
-

AWS Config

Explanation

Correct option:

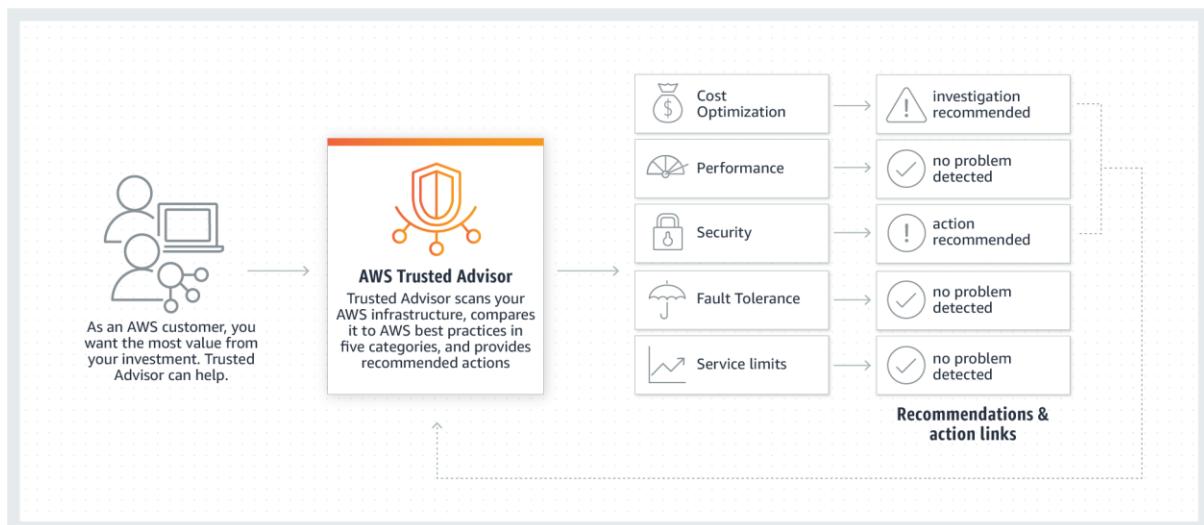
AWS Trusted Advisor

AWS Trusted Advisor is an online tool that provides real-time guidance to help provision your resources following AWS best practices. Whether establishing new workflows, developing applications, or as part of ongoing improvement, recommendations provided by Trusted Advisor regularly help keep your solutions provisioned optimally. AWS Trusted Advisor analyzes your AWS environment and provides best practice recommendations in five categories: Cost Optimization, Performance, Security, Fault Tolerance, Service Limits.

AWS Trusted Advisor can check Amazon Elastic Block Store (Amazon EBS) volume configurations and warns when volumes appear to be underused. Charges begin when a volume is created. If a volume remains unattached or has very low write activity (excluding boot volumes) for a period of time, the volume is probably not being used.

How Trusted Advisor

Works:



via - <https://aws.amazon.com/premiumsupport/technology/trusted-advisor/>

Incorrect options:

AWS Config - AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. Think resource-specific change history, audit, and compliance; think Config. Its a configuration tracking service and not an infrastructure tracking service.

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. Amazon EBS emits notifications based on Amazon CloudWatch Events for a variety of volume, snapshot, and encryption status changes. With CloudWatch Events, you can establish rules that trigger programmatic actions in response to a change in volume, snapshot, or encryption key state (though not for underutilized volume usage).

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. Its a security assessment service and not an infrastructure tracking service.

References:

<https://aws.amazon.com/premiumsupport/technology/trusted-advisor/best-practice-checklist/>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-cloud-watch-events.html>

Question 32: **Incorrect**

Which of the following are the serverless computing services offered by AWS (Select two)

-

Amazon Lightsail

-

AWS Lambda

(Correct)

-

AWS Fargate

(Correct)

-

Amazon Elastic Compute Cloud (EC2)

-

AWS Elastic Beanstalk

(Incorrect)

Explanation

Correct options:

Serverless is the native architecture of the cloud that enables you to shift more of your operational responsibilities to AWS, increasing your agility and innovation. Serverless allows you to build and run applications and services without thinking about servers. It eliminates infrastructure management tasks such as server or cluster provisioning, patching, operating system maintenance, and capacity provisioning.

The AWS serverless platform overview:

Compute	Storage	Data stores	API Proxy
<p>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.</p> <p>Lambda@Edge allows you to run Lambda functions at AWS Edge locations in response to Amazon CloudFront events.</p> <p>AWS Fargate is a purpose-built serverless compute engine for containers. Fargate scales and manages the infrastructure required to run your containers.</p>	<p>Amazon Simple Storage Service (Amazon S3) provides developers and IT teams with secure, durable, highly-scalable object storage. Amazon S3 is easy to use, with a simple web service interface to store and retrieve any amount of data from anywhere on the web.</p> <p>Amazon Elastic File System (Amazon EFS) provides simple, scalable, elastic file storage. It is built to elastically scale on demand, growing and shrinking automatically as you add and remove files.</p>	<p>Amazon DynamoDB is a fast and flexible NoSQL database service for all applications that need consistent, single-digit millisecond latency at any scale.</p> <p>Amazon Aurora Serverless is an on-demand, auto-scaling configuration for Amazon Aurora (MySQL-compatible edition), where the database will automatically start up, shut down, and scale capacity up or down based on your application's needs.</p> <p>Amazon RDS Proxy is a highly available database proxy that manages thousands of concurrent connections to relational databases, allowing you to build highly scalable,</p>	<p>Amazon API Gateway is a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale. It offers a comprehensive platform for API management. API Gateway allows you to process hundreds of thousands of concurrent API calls and handles traffic management, authorization and access control, monitoring, and API version management.</p>
Application integration	Orchestration	Analytics	Developer tooling
<p>Amazon SNS is a fully managed pub/sub messaging service that makes it easy to decouple and scale microservices, distributed systems, and serverless applications.</p> <p>Amazon SQS is a fully managed message queuing service that makes it easy to decouple and scale microservices, distributed systems, and serverless applications.</p> <p>AWS AppSync simplifies application development by letting you create a flexible GraphQL API to securely access, manipulate, and combine data from one or more data sources.</p>	<p>AWS Step Functions makes it easy to coordinate the components of distributed applications and microservices using visual workflows. Building applications from individual components that each perform a discrete function lets you scale and change applications quickly. Step Functions is a reliable way to coordinate components and step through the functions of your application.</p>	<p>Amazon Kinesis is a platform for streaming data on AWS, offering powerful services to make it easy to load and analyze streaming data, and also providing the ability for you to build custom streaming data applications for specialized needs.</p> <p>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.</p>	<p>AWS provides tools and services that aid developers in the serverless application development process. AWS and its partner ecosystem offer tools for continuous integration and delivery, testing, deployments, monitoring and diagnostics, SDKs, frameworks, and integrated development environment (IDE) plugins.</p>

via - <https://aws.amazon.com/serverless/>

AWS Lambda - 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 call it directly from any web or mobile app.

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.

AWS Fargate - AWS Fargate is a serverless compute engine for containers that works with both Amazon Elastic Container Service (ECS) and Amazon Elastic Kubernetes Service (EKS). Fargate makes it easy for you to focus on building your applications. Fargate removes the need to provision and manage servers, lets you specify and pay for resources per application, and improves security through application isolation by design.

AWS Fargate is a purpose-built serverless compute engine for containers. Fargate scales and manages the infrastructure required to run your containers.

Incorrect options:

Amazon Elastic Compute Cloud (EC2) - Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud with support for per-second billing. It is the easiest way to provision servers on AWS Cloud and access the underlying OS. Amazon EC2 reduces the time required to obtain and boot new server instances to minutes, allowing you to quickly scale capacity, both up and down, as your computing requirements change.

AWS Elastic Beanstalk - AWS Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services. You simply upload your code and Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring. Beanstalk provisions servers so it is not a serverless service.

Amazon Lightsail - Lightsail is an easy-to-use cloud platform that offers you everything needed to build an application or website, plus a cost-effective, monthly plan. Lightsail offers several preconfigured, one-click-to-launch operating systems, development stacks, and web applications, including Linux, Windows OS, and WordPress.

References:

<https://aws.amazon.com/serverless/>

<https://aws.amazon.com/fargate/>

Question 33: **Correct**

Which AWS service would you use to create a logically isolated section of the AWS Cloud where you can launch AWS resources in your virtual network?

-
- Subnet**
-
- Virtual Private Cloud (VPC)**
- (Correct)**
-
- Network Access Control List (NACL)**
-
- Virtual Private Network (VPN)**

Explanation

Correct option:

Virtual Private Cloud (VPC)

Amazon Virtual Private Cloud (Amazon VPC) is a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including the selection of your IP address range, creation of subnets, and configuration of route tables and network gateways. You can easily customize the network configuration of your Amazon VPC using public and private subnets.

Incorrect options:

Virtual Private Network (VPN) - AWS Virtual Private Network (AWS VPN) lets you establish a secure and private encrypted tunnel from your on-premises network to the AWS global network. AWS VPN is

comprised of two services: AWS Site-to-Site VPN and AWS Client VPN. You cannot use VPN to create a logically isolated section of the AWS Cloud.

Subnet - A subnet is a range of IP addresses within your VPC. A subnet is not an AWS service, so this option is ruled out.

Network Access Control List (NACL) - 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. A NACL is not an AWS service, so this option is ruled out.

Reference:

<https://aws.amazon.com/vpc/>

Question 34: **Correct**

Which AWS service can be used to host a static website with the LEAST effort?



Amazon S3 Glacier



AWS Storage Gateway



Amazon Simple Storage Service (Amazon S3)

(Correct)



Amazon Elastic File System (Amazon EFS)

Explanation

Correct option:

Amazon Simple Storage Service (Amazon S3)

Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance. Amazon S3's flat, non-hierarchical structure and various management features are helping customers of all sizes and industries organize their data in ways that are valuable to their businesses and teams.

To host a static website on Amazon S3, you configure an Amazon S3 bucket for website hosting and then upload your website content to the bucket. When you configure a bucket as a static website, you must enable website hosting, set permissions, and create and add an index document.

Hosting a static website on Amazon S3:

Hosting a static website on Amazon S3

[PDF](#) | [Kindle](#) | [RSS](#)

You can use Amazon S3 to host a static website. On a *static* website, individual webpages include static content. They might also contain client-side scripts.

By contrast, a *dynamic* website relies on server-side processing, including server-side scripts such as PHP, JSP, or ASP.NET. Amazon S3 does not support server-side scripting, but AWS has other resources for hosting dynamic websites. To learn more about website hosting on AWS, see [Web Hosting](#).

 **Note**

You can use the AWS Amplify Console to host a single page web app. The AWS Amplify Console supports single page apps built with single page app frameworks (for example, React JS, Vue JS, Angular JS, and Nuxt) and static site generators (for example, Gatsby JS, React-static, Jekyll, and Hugo). For more information, see [Getting Started](#) in the *AWS Amplify Console User Guide*.

To configure your bucket for static website hosting, you can use the AWS Management Console without writing any code. You can also create, update, and delete the website configuration *programmatically* by using the AWS SDKs. The SDKs provide wrapper classes around the Amazon S3 REST API. If your application requires it, you can send REST API requests directly from your application.

To host a static website on Amazon S3, you configure an Amazon S3 bucket for website hosting and then upload your website content to the bucket. When you configure a bucket as a static website, you must [enable website hosting](#), [set permissions](#), and [create and add an index document](#). Depending on your website requirements, you can also [configure redirects](#), [web traffic logging](#), and a [custom error document](#).

After you configure your bucket as a static website, you can access the bucket through the AWS Region-specific Amazon S3 website endpoints for your bucket. Website endpoints are different from the endpoints where you send REST API requests. For more information, see [Website endpoints](#).

via - <https://docs.aws.amazon.com/AmazonS3/latest/dev/WebsiteHosting.html>

Incorrect options:

AWS Storage Gateway - AWS Storage Gateway is a hybrid cloud storage service that gives you on-premises access to virtually unlimited cloud storage. Customers use Storage Gateway to simplify storage management and reduce costs for key hybrid cloud storage use cases. It helps on-premises applications to access data on AWS Cloud. It cannot be used to host a website.

Amazon Elastic File System (Amazon EFS) - Amazon Elastic File System (Amazon EFS) provides a simple, scalable, fully managed elastic NFS file system for use with AWS Cloud services and on-premises resources. EFS storage option cannot directly be used to host a website, EFS needs to be mounted on Amazon EC2 to work as a static website.

Amazon S3 Glacier - Amazon S3 Glacier is a secure, durable, and extremely low-cost Amazon S3 cloud storage class for data archiving and long-term backup. As you see, this cannot be used for hosting a website.

Reference:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/WebsiteHosting.html>

Question 35: **Correct**

A social media company wants to have the MOST cost-optimal strategy for deploying EC2 instances. As a Cloud Practitioner, which of the following options would you recommend? (Select two)

-

Use Reserved Instances to run applications with a predictable usage over the next one year

(Correct)

-

Use Reserved Instances for ad-hoc jobs that can be interrupted

- - **Use On-Demand Instances to run applications with a predictable usage over the next one year**
 -
 - **Use On-Demand Instances for ad-hoc jobs that can be interrupted**
 -
 - **Use Spot Instances for ad-hoc jobs that can be interrupted**
- (Correct)**

Explanation

Correct options:

Use Spot Instances for ad-hoc jobs that can be interrupted

A Spot Instance is an unused EC2 instance that is available for less than the On-Demand price. Because Spot Instances enable you to request unused EC2 instances at steep discounts (up to 90%), you can lower your Amazon EC2 costs significantly. Spot Instances are well-suited for data analysis, batch jobs, background processing, and optional tasks. These can be terminated at short notice, so these are not suitable for critical workloads that need to run at a specific point in time.

Use Reserved Instances to run applications with a predictable usage over the next one year

Reserved Instances provide you with significant savings (up to 75%) on your Amazon EC2 costs compared to On-Demand Instance pricing. Reserved Instances are not physical instances, but rather a billing discount applied to the use of On-Demand Instances in your account. You can purchase a Reserved Instance for a one-year or three-year commitment, with the three-year commitment offering a bigger discount. Reserved instances are a great fit for application with a steady-state usage. Reserved instances cannot be interrupted.

EC2 Pricing Options

Overview:

On-Demand

With On-Demand instances, you pay for compute capacity by the hour or the second depending on which instances you run. No longer-term commitments or upfront payments are needed. You can increase or decrease your compute capacity depending on the demands of your application and only pay the specified per hourly rates for the instance you use.

On-Demand instances are recommended for:

- Users that prefer the low cost and flexibility of Amazon EC2 without any up-front payment or long-term commitment
- Applications with short-term, spiky, or unpredictable workloads that cannot be interrupted
- Applications being developed or tested on Amazon EC2 for the first time

[See On-Demand pricing »](#)

Spot instances

Amazon EC2 Spot instances allow you to request spare Amazon EC2 computing capacity for up to 90% off the On-Demand price. [Learn More](#).

Spot instances are recommended for:

- Applications that have flexible start and end times
- Applications that are only feasible at very low compute prices
- Users with urgent computing needs for large amounts of additional capacity

[See Spot pricing »](#)

Savings Plans

Savings Plans are a flexible pricing model that offer low prices on EC2 and Fargate usage, in exchange for a commitment to a consistent amount of usage (measured in \$/hour) for a 1 or 3 year term.

Dedicated Hosts

A Dedicated Host is a physical EC2 server dedicated for your use. Dedicated Hosts can help you reduce costs by allowing you to use your existing server-bound software licenses, including Windows Server, SQL Server, and SUSE Linux Enterprise Server (subject to your license terms), and can also help you meet compliance requirements. [Learn more](#).

- Can be purchased On-Demand (hourly).
- Can be purchased as a Reservation for up to 70% off the On-Demand price.

[See Dedicated pricing »](#)

Reserved Instances

Reserved Instances provide you with a significant discount (up to 75%) compared to On-Demand Instance pricing. In addition, when Reserved Instances are assigned to a specific Availability Zone, they provide a capacity reservation, giving you additional confidence in your ability to launch instances when you need them.

For applications that have steady state or predictable usage, Reserved Instances can provide significant savings compared to using On-Demand instances. See [How to Purchase Reserved Instances](#) for more information.

Reserved Instances are recommended for:

- Applications with steady state usage
- Applications that may require reserved capacity
- Customers that can commit to using EC2 over a 1 or 3 year term to reduce their total computing costs

via - <https://aws.amazon.com/ec2/pricing/>

Incorrect options:

Use On-Demand Instances to run applications with a predictable usage over the next one year

Use On-Demand Instances for ad-hoc jobs that can be interrupted

An On-Demand Instance is an instance that you use on-demand. You have full control over its lifecycle – you decide when to launch, stop, hibernate, start, reboot, or terminate it. There is no long-term commitment required when you purchase On-Demand Instances. There is no upfront payment and you pay only for the seconds that your On-Demand Instances are running. The price per second for running an On-Demand Instance is fixed. On-demand instances cannot be interrupted. However, On-demand instances are not as cost-effective as Spot instances or Reserved instances, so both these options are not correct.

Use Reserved Instances for ad-hoc jobs that can be interrupted - Spot instances are more cost-effective than Reserved instances for running ad-hoc jobs that can be interrupted, so this option is not correct.

Reference:

<https://aws.amazon.com/ec2/pricing/>

Question 36: **Incorrect**

Which AWS services can be used together to send alerts whenever the AWS account root user signs in? (Select two)

•

SNS

(Correct)

-

Lambda

-

Step Function

-

CloudWatch

(Correct)

-

SQS

(Incorrect)

Explanation

Correct options:

SNS

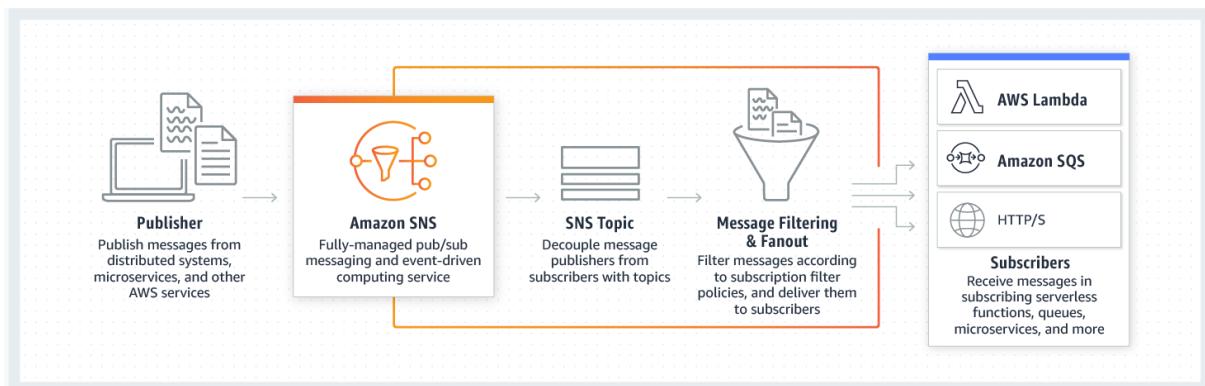
CloudWatch

Amazon CloudWatch Events delivers a near real-time stream of system events that describe changes in Amazon Web Services (AWS) resources. Using simple rules that you can quickly set up, you can match events and route them to one or more target functions or streams. CloudWatch Events becomes aware of operational changes as they occur. CloudWatch Events responds to these operational changes and takes corrective action as necessary, by sending messages to respond to the environment, activating functions, making changes, and capturing state information.

Amazon Simple Notification Service (SNS) is a highly available, durable, secure, fully managed pub/sub messaging service that enables you to decouple microservices, distributed systems, and serverless applications. Additionally, SNS can be used to fan out notifications to end users using mobile push, SMS, and email.

How SNS

Works:



via - <https://aws.amazon.com/sns/>

To send alerts whenever the AWS account root user signs in, you can create an Amazon Simple Notification Service (Amazon SNS) topic. Then, create an Amazon CloudWatch event rule to monitor userIdentity root logins from the AWS Management Console and send an email via SNS when the event triggers.

Incorrect options:

SQS - Amazon Simple Queue Service (SQS) is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. 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.

Lambda - AWS Lambda is a compute service that lets you run code without provisioning or managing servers.

Step Function - AWS Step Function lets you coordinate multiple AWS services into serverless workflows. You can design and run workflows that stitch together services such as AWS Lambda, AWS Glue and Amazon SageMaker.

References:

<https://aws.amazon.com/premiumsupport/knowledge-center/root-user-account-cloudwatch-rule/>

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/events/WhatIsCloudWatchEvents.html>

Question 37: **Incorrect**

An e-commerce company has migrated its IT infrastructure from the on-premises data center to AWS Cloud. Which of the following costs is the company responsible for?

-

Application software license costs

(Correct)

-

Costs for powering servers on AWS Cloud

(Incorrect)

-

AWS Data Center physical security costs

-

Costs for hardware infrastructure on AWS Cloud

Explanation

Correct option:

Application software license costs

Cloud computing is the on-demand delivery of compute power, database storage, applications, and other IT resources through a cloud services platform via the Internet with pay-as-you-go pricing. With cloud computing, you don't need to make large upfront investments in hardware and spend a lot of time on the heavy lifting of managing that hardware. Therefore, all costs for hardware infrastructure, powering servers and physical security for the Data Center fall under the ambit of AWS.

The customer needs to take care of software licensing costs and human resources costs.

Incorrect options:

AWS Data Center physical security costs

Costs for hardware infrastructure on AWS Cloud

Costs for powering servers on AWS Cloud

As per the details mentioned in the explanation above, these three options are not correct for the given use-case.

Reference:

<https://docs.aws.amazon.com/whitepapers/latest/aws-overview/what-is-cloud-computing.html>

Question 38: **Incorrect**

Which of the following S3 storage classes has NO constraint of a minimum storage duration charge for objects?

-

S3 Glacier

(Incorrect)

-

S3 One Zone-IA

-

S3 Standard-IA

S3 Standard

(Correct)

Explanation

Correct option:

Correct options:

S3 Standard - S3 Standard offers high durability, availability, and performance object storage for frequently accessed data. S3 Standard offers low latency and high throughput performance, It is designed for durability of 99.999999999% of objects across multiple Availability Zones. S3 Standard has no constraint of a minimum storage duration for objects.

Please review this illustration for S3 Storage Classes retrieval fee. You don't need to memorize the actual numbers, just remember that S3 Standard and S3 Intelligent-Tiering do not charge any retrieval fee:

Performance across the S3 Storage Classes

	S3 Standard	S3 Intelligent-Tiering*	S3 Standard-IA	S3 One Zone-IA†	S3 Glacier Instant Retrieval	S3 Glacier Flexible Retrieval	S3 Glacier Deep Archive
Designed for durability	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)				
Designed for availability	99.99%	99.9%	99.9%	99.5%	99.9%	99.99%	99.99%
Availability SLA	99.9%	99%	99%	99%	99%	99.9%	99.9%
Availability Zones	≥3	≥3	≥3	1	≥3	≥3	≥3
Minimum capacity charge per object	N/A	N/A	128 KB	128 KB	128 KB	40 KB	40 KB
Minimum storage duration charge	N/A	N/A	30 days	30 days	90 days	90 days	180 days
Retrieval charge	N/A	N/A	per GB retrieved	per GB retrieved	per GB retrieved	per GB retrieved	per GB retrieved
First byte latency	milliseconds	milliseconds	milliseconds	milliseconds	milliseconds	minutes or hours	hours
Storage type	Object	Object	Object	Object	Object	Object	Object
Lifecycle transitions	Yes	Yes	Yes	Yes	Yes	Yes	Yes

via - <https://aws.amazon.com/s3/storage-classes/>

Incorrect options:

S3 Glacier - Amazon S3 Glacier is a secure, durable, and extremely low-cost Amazon S3 cloud storage class for data archiving and long-term backup. It is designed to deliver 99.99999999% durability, and provide comprehensive security and compliance capabilities that can help meet even the most stringent regulatory requirements. S3 Glacier mandates a minimum storage duration charge for 90 days.

S3 One Zone-IA - 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. It is not suitable for data archival. S3 One Zone-IA mandates a minimum storage duration charge for 30 days.

S3 Standard-IA - S3 Standard-IA is for data that is accessed less frequently, but requires rapid access when needed. S3 Standard-IA offers 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. S3 Standard-IA mandates a minimum storage duration charge for 30 days.

Reference:

<https://aws.amazon.com/s3/storage-classes/>

Question 39: **Correct**

An organization maintains a separate Virtual Private Cloud (VPC) for each of its business units. Two units need to privately share data. Which is the most optimal way of privately sharing data between the two VPCs?

-

VPC Peering

(Correct)

-

Site to Site VPN

-

AWS Direct Connect

-

VPC Endpoint

Explanation

Correct option:

VPC Peering

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them privately. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your VPCs, with a VPC in another AWS account, or with a VPC in a different AWS Region.

VPC Peering

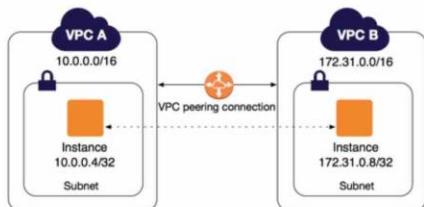
Overview:

What is VPC peering?

PDF

Amazon Virtual Private Cloud (Amazon VPC) enables you to launch AWS resources into a virtual network that you've defined.

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. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account. The VPCs can be in different regions (also known as an inter-region VPC peering connection).



AWS uses the existing infrastructure of a VPC to create a VPC peering connection; it is neither a gateway nor a VPN connection, and does not rely on a separate piece of physical hardware. There is no single point of failure for communication or a bandwidth bottleneck.

A VPC peering connection helps you to facilitate the transfer of data. For example, if you have more than one AWS account, you can peer the VPCs across those accounts to create a file sharing network. You can also use a VPC peering connection to allow other VPCs to access resources you have in one of your VPCs.

via - <https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html>

Incorrect options:

Site to Site VPN - AWS Site-to-Site VPN creates a secure connection between your data center or branch office and your AWS cloud resources. This connection goes over the public internet. Site to Site VPN cannot be used to interconnect VPCs.

AWS Direct Connect - AWS Direct Connect creates a dedicated private connection from a remote network to your VPC. This is a private connection and does not use the public internet. Takes at least a month to establish this connection. Direct Connect cannot be used to interconnect VPCs.

VPC Endpoint - 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. You cannot connect two VPCs using a VPC endpoint.

Reference:

<https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html>

Question 40: **Correct**

Which of the following are recommended security best practices for the AWS account root user?
(Select two)

-

Enable MFA for the AWS account root user

(Correct)

-

Set up an IAM user with administrator permissions and do not use AWS account root user for administrative tasks

(Correct)

-

Share AWS account root user access keys with other administrators

-

Disable MFA for the AWS account root user as it can lock the entire AWS account if the MFA device is lost

-

Keep your AWS account root user access keys in an encrypted file on S3

Explanation

Correct options:

Enable MFA for the AWS account root user

Set up an IAM user with administrator permissions and do not use AWS account root user for administrative tasks

When you create an AWS account, you create an AWS account root user identity, which you use to sign in to AWS. You can sign in to the AWS Management Console using this root user identity—that is, the email address and password that you provided when creating the account. This combination of your email address and password is also called your root user credentials.

Some of the AWS account root user security best practices are as follows:

Do not use the AWS account root user for any task where it's not required. Instead, create a new IAM user for each person that requires administrator access. Then make those users administrators by placing the users into an "Administrators" group to which you attach the AdministratorAccess managed policy.

If you don't already have an access key for your AWS account root user, don't create one unless you need to. If you do have an access key for your AWS account root user, delete it.

Never share your AWS account root user password or access keys with anyone. Use a strong password to help protect account-level access to the AWS Management Console.

Enable AWS multi-factor authentication (MFA) on your AWS account root user account.

Lock Away Your AWS Account Root User Access Keys

You use an access key (an access key ID and secret access key) to make programmatic requests to AWS. However, do not use your AWS account root user access key. The access key for your AWS account root user gives full access to all your resources for all AWS services, including your billing information. You cannot reduce the permissions associated with your AWS account root user access key.

Therefore, protect your root user access key like you would your credit card numbers or any other sensitive secret. Here are some ways to do that:

- If you don't already have an access key for your AWS account root user, don't create one unless you absolutely need to. Instead, use your account email address and password to sign in to the AWS Management Console and [create an IAM user for yourself](#) that has administrative permissions.
- If you do have an access key for your AWS account root user, delete it. If you must keep it, rotate (change) the access key regularly. To delete or rotate your root user access keys, go to the [My Security Credentials page](#) in the AWS Management Console and sign in with your account's email address and password. You can manage your access keys in the **Access keys** section. For more information about rotating access keys, see [Rotating Access Keys](#).
- [Never share your AWS account root user password or access keys with anyone.](#) The remaining sections of this document discuss various ways to avoid having to share your AWS account root user credentials with other users. They also explain how to avoid having to embed them in an application.
- Use a strong password to help protect account-level access to the AWS Management Console. For information about managing your AWS account root user password, see [Changing the AWS Account Root User Password](#).
- Enable AWS multi-factor authentication (MFA) on your AWS account root user account. For more information, see [Using Multi-Factor Authentication \(MFA\) in AWS](#).

via - <https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#lock-away-credentials>

Incorrect options:

Disable MFA for the AWS account root user as it can lock the entire AWS account if the MFA device is lost - AWS recommends that you enable AWS multi-factor authentication (MFA) on your AWS account root user account.

Keep your AWS account root user access keys in an encrypted file on S3 - AWS recommends that if you do have an access key for your AWS account root user, delete it.

Share AWS account root user access keys with other administrators - The access key for your AWS account root user gives full access to all your resources for all AWS services, including your billing information. You cannot reduce the permissions associated with your AWS account root user access key. You should never share these access keys with any other users, not even the administrators.

References:

<https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#lock-away-credentials>

https://docs.aws.amazon.com/IAM/latest/UserGuide/getting-started_create-admin-group.html

Question 41: **Incorrect**

A cargo shipping company runs its server-fleet on Amazon EC2 instances. Some of these instances host the CRM (Customer Relationship Management) applications that need to be accessible 24*7. These applications are not mission-critical. In case of a disaster, these applications can be managed on a lesser number of instances for some time.

Which disaster recovery strategy is well-suited as well as cost-effective for this requirement?

-
- **Pilot Light strategy**
-
- **Warm Standby strategy**
- **(Correct)**
-
- **Multi-site active-active strategy**
-
- **Backup & Restore strategy**
- **(Incorrect)**

Explanation

Correct option:

Warm Standby strategy

When selecting your DR strategy, you must weigh the benefits of lower RTO (recovery time objective) and RPO (recovery point objective) vs the costs of implementing and operating a strategy. The pilot light and warm standby strategies both offer a good balance of benefits and cost.

This strategy replicates data from the primary Region to data resources in the recovery Region, such as Amazon Relational Database Service (Amazon RDS) DB instances or Amazon DynamoDB tables. These data resources are ready to serve requests. In addition to replication, this strategy requires you to create a continuous backup in the recovery Region. This is because when "human action" type disasters occur, data can be deleted or corrupted, and replication will replicate the bad data. Backups are necessary to enable you to get back to the last known good state.

The warm standby strategy deploys a functional stack, but at reduced capacity. The DR endpoint can handle requests, but cannot handle production levels of traffic. It may be more, but is always less than the full production deployment for cost savings. If the passive stack is deployed to the recovery Region at full capacity, however, then this strategy is known as "hot standby." Because warm standby deploys a functional stack to the recovery Region, this makes it easier to test Region readiness using synthetic transactions.

DR
strategies:

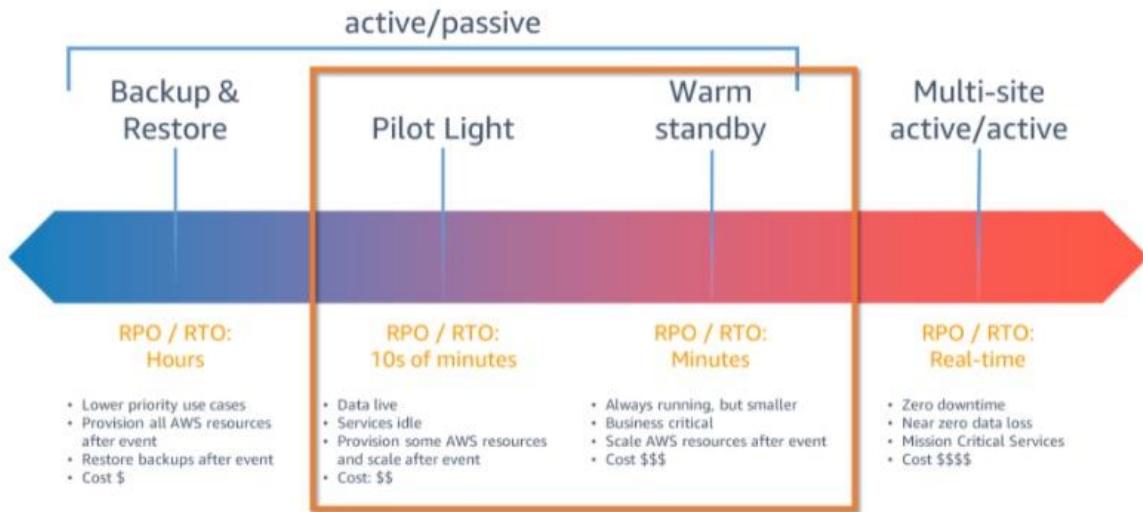


Figure 1. DR strategies

via - <https://aws.amazon.com/blogs/architecture/disaster-recovery-dr-architecture-on-aws-part-iii-pilot-light-and-warm-standby/>

Incorrect options:

Multi-site active-active strategy - This strategy uses AWS Regions as your active sites, creating a multi-Region active/active architecture. Generally, two Regions are used. Each Region hosts a highly available, multi-Availability Zone (AZ) workload stack. In each Region, data is replicated live between the data stores and also backed up. This protects against disasters that include data deletion or corruption since the data backup can be restored to the last known good state. Each regional stack serves production traffic effectively. But, this strategy is cost involving and should only be used for mission-critical applications.

Pilot Light strategy - Pilot Light, like Warm Standby strategy, replicates data from the primary Region to data resources in the recovery Region, such as Amazon Relational Database Service (Amazon RDS) DB instances or Amazon DynamoDB tables. But, the DR Region in a pilot light strategy (unlike warm standby) cannot serve requests until additional steps are taken. A pilot light in a home furnace does not provide heat to the home. It provides a quick way to light the furnace burners that then provide heat.

Warm standby can handle traffic at reduced levels immediately. Pilot light requires you to first deploy infrastructure and then scale out resources before the workload can handle requests.

Backup & Restore strategy - Backup and Restore is associated with higher RTO (recovery time objective) and RPO (recovery point objective). This results in longer downtimes and greater loss of data between when the disaster event occurs and recovery. However, backup and restore can still be the right strategy for workloads because it is the easiest and least expensive strategy to implement.

Reference:

<https://aws.amazon.com/blogs/architecture/disaster-recovery-dr-architecture-on-aws-part-iii-pilot-light-and-warm-standby/>

Question 42: **Correct**

A financial services company wants to migrate from its on-premises data center to AWS Cloud. As a Cloud Practitioner, which AWS service would you recommend so that the company can compare the cost of running their IT infrastructure on-premises vs AWS Cloud?

- AWS Cost Explorer
- AWS Budgets
- AWS Trusted Advisor
- AWS Pricing Calculator

AWS Pricing Calculator

(Correct)

Explanation

Correct option:

AWS Pricing Calculator

AWS Pricing Calculator lets you explore AWS services and create an estimate for the cost of your use cases on AWS. You can model your solutions before building them, explore the price points and calculations behind your estimate, and find the available instance types and contract terms that meet your needs. This enables you to make informed decisions about using AWS. You can plan your AWS costs and usage or price out setting up a new set of instances and services. AWS Pricing Calculator can be accessed at <https://calculator.aws/#/>.

AWS also offers a complimentary service called Migration Evaluator (Formerly TSO Logic) to create data-driven business cases for AWS Cloud planning and migration.

Incorrect options:

AWS Trusted Advisor - AWS Trusted Advisor provides recommendations that help you follow AWS best practices. Trusted Advisor evaluates your account by using checks. These checks identify ways to optimize your AWS infrastructure, improve security and performance, reduce costs, and monitor service quotas. This service cannot be used to compare the cost of running the IT infrastructure on-premises vs AWS Cloud.

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 be used to compare the cost of running the IT infrastructure on-premises vs AWS Cloud.

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 be used to compare the cost of running the IT infrastructure on-premises vs AWS Cloud.

Reference:

<https://calculator.aws/#/>

<https://docs.aws.amazon.com/whitepapers/latest/how-aws-pricing-works/aws-pricingtco-tools.html>

<https://aws.amazon.com/migration-evaluator/>

Question 43: **Correct**

A firm wants to maintain the same data on S3 between its production account and multiple test accounts. Which technique should you choose to copy data into multiple test accounts while retaining object metadata?

-
- **Amazon S3 Storage Classes**
-
- **Amazon S3 Bucket Policy**
-
- **Amazon S3 Transfer Acceleration**
-
- **Amazon S3 Replication**

(Correct)

Explanation

Correct option:

Amazon S3 Replication

Replication enables automatic, asynchronous copying of objects across Amazon S3 buckets. Buckets that are configured for object replication can be owned by the same AWS account or by different accounts. You can copy objects between different AWS Regions or within the same Region. You can use replication to make copies of your objects that retain all metadata, such as the original object creation time and version IDs. This capability is important if you need to ensure that your replica is identical to the source object.

Exam Alert:

Amazon S3 supports two types of replication: Cross Region Replication vs Same Region Replication. Please review the differences between SRR and CRR:

When to Use CRR

Cross-Region replication can help you do the following:

- **Meet compliance requirements** — Although Amazon S3 stores your data across multiple geographically distant Availability Zones by default, compliance requirements might dictate that you store data at even greater distances. Cross-Region replication allows you to replicate data between distant AWS Regions to satisfy these requirements.
 - **Minimize latency** — If your customers are in two geographic locations, you can minimize latency in accessing objects by maintaining object copies in AWS Regions that are geographically closer to your users.
 - **Increase operational efficiency** — If you have compute clusters in two different AWS Regions that analyze the same set of objects, you might choose to maintain object copies in those Regions.
-

When to Use SRR

Same-Region replication can help you do the following:

- **Aggregate logs into a single bucket** — If you store logs in multiple buckets or across multiple accounts, you can easily replicate logs into a single, in-Region bucket. This allows for simpler processing of logs in a single location.
- **Configure live replication between production and test accounts** — If you or your customers have production and test accounts that use the same data, you can replicate objects between those multiple accounts, while maintaining object metadata, by implementing SRR rules.
- **Abide by data sovereignty laws** — You might be required to store multiple copies of your data in separate AWS accounts within a certain Region. Same-Region replication can help you automatically replicate critical data when compliance regulations don't allow the data to leave your country.

via - <https://docs.aws.amazon.com/AmazonS3/latest/dev/replication.html>

Incorrect options:

Amazon S3 Bucket Policy - 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. You cannot replicate data using a bucket policy.

Amazon 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. Transfer Acceleration takes advantage of Amazon CloudFront's globally distributed edge locations. This facility speeds up access between end-user and S3, this is not for replicating data.

Amazon S3 Storage Classes - Amazon S3 offers a range of storage classes designed for different use cases. Each storage class has a defined set of rules to store, encrypt data at a certain price. Based on the use case, customers can choose the storage class that best suits their business requirements.

These include S3 Standard for general-purpose storage of frequently accessed data; S3 Intelligent-Tiering for data with unknown or changing access patterns; S3 Standard-Infrequent Access (S3 Standard-IA) and S3 One Zone-Infrequent Access (S3 One Zone-IA) for long-lived, but less frequently accessed data; and Amazon S3 Glacier (S3 Glacier) and Amazon S3 Glacier Deep Archive (S3 Glacier

Deep Archive) for long-term archive and digital preservation. You cannot replicate data using storage classes.

Reference:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/replication.html>

Question 44: **Incorrect**

Bob and Susan each have an AWS account in AWS Organizations. Susan has five Reserved Instances (RIs) of the same type and Bob has none. During one particular hour, Susan uses three instances and Bob uses six for a total of nine instances on the organization's consolidated bill.

Which of the following statements are correct about consolidated billing in AWS Organizations? (Select two)

-

AWS bills five instances as Reserved Instances, and the remaining four instances as regular instances

(Correct)

-

Bob does not receive any cost-benefit since he hasn't purchased any RIs. If his account has even one RI, then the cost-benefit from Susan's account is also added to his account

(Incorrect)

-

Bob receives the cost-benefit from Susan's Reserved Instances only if he launches his instances in the same Region where Susan purchased her Reserved Instances

-

AWS bills three instances as Reserved Instances, and the remaining six instances as regular instances

-

Bob receives the cost-benefit from Susan's Reserved Instances only if he launches his instances in the same Availability Zone where Susan purchased her Reserved Instances

(Correct)

Explanation

Correct options:

Bob receives the cost-benefit from Susan's Reserved Instances only if he launches his instances in the same Availability Zone where Susan purchased her Reserved Instances - Bob receives the cost-benefit from Susan's Reserved Instances only if he launches his instances in the same Availability Zone where Susan purchased her Reserved Instances. For example, if Susan specifies us-west-2a

when she purchases her Reserved Instances, Bob must specify us-west-2a when he launches his instances to get the cost-benefit on the organization's consolidated bill. However, the actual locations of Availability Zones are independent of one account to another. For example, the us-west-2a Availability Zone for Bob's account might be in a different location than the location for Susan's account.

AWS bills five instances as Reserved Instances, and the remaining four instances as regular instances - Since Susan has five Reserved Instances (RIs), AWS bills five instances as Reserved Instances, and the remaining four instances as regular instances.

Incorrect options:

AWS bills three instances as Reserved Instances, and the remaining six instances as regular instances - This option contradicts the explanation provided above, so it's incorrect.

Bob does not receive any cost-benefit since he hasn't purchased any RIs. If his account has even one RI, then the cost-benefit from Susan's account is also added to his account - For billing purposes, the consolidated billing feature of AWS Organizations treats all the accounts in the organization as one account. This means that all accounts in the organization can receive the hourly cost-benefit of Reserved Instances that are purchased by any other account.

Bob receives the cost-benefit from Susan's Reserved Instances only if he launches his instances in the same Region where Susan purchased her Reserved Instances - As discussed above, this statement is incorrect. Bob receives the cost-benefit from Susan's Reserved Instances only if he launches his instances in the same Availability Zone where Susan purchased her Reserved Instances.

Reference:

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/consolidatedbilling-other.html>

Question 45: **Incorrect**

Which of the following can you use to run a bootstrap script while launching an EC2 instance?

- **EC2 instance AMI data**
- **EC2 instance user data**
(Correct)
- **EC2 instance configuration data**
- **EC2 instance metadata**
(Incorrect)

Explanation

Correct option:

EC2 instance user data

EC2 instance user data is the data that you specified in the form of a bootstrap script or configuration parameters while launching your instance.

EC2 instance metadata and user data:

Instance metadata and user data

[PDF](#) | [Kindle](#) | [RSS](#)

Instance metadata is data about your instance that you can use to configure or manage the running instance. Instance metadata is divided into categories, for example, host name, events, and security groups.

You can also use instance metadata to access *user data* that you specified when launching your instance. For example, you can specify parameters for configuring your instance, or include a simple script. You can build generic AMIs and use user data to modify the configuration files supplied at launch time.

For example, if you run web servers for various small businesses, they can all use the same generic AMI and retrieve their content from the Amazon S3 bucket that you specify in the user data at launch. To add a new customer at any time, create a bucket for the customer, add their content, and launch your AMI with the unique bucket name provided to your code in the user data. If you launch more than one instance at the same time, the user data is available to all instances in that reservation. Each instance that is part of the same reservation has a unique `ami-launch-index` number, allowing you to write code that controls what to do. For example, the first host might elect itself as an initial master node in a cluster. For a detailed AMI launch example, see [Example: AMI launch index value](#).

Incorrect options:

EC2 instance metadata - EC2 instance metadata is data about your instance that you can use to manage the instance. You can get instance items such as ami-id, public-hostname, local-hostname, hostname, public-ipv4, local-ipv4, public-keys, instance-id by using instance metadata. You cannot use EC2 instance metadata to run a bootstrap script while launching an EC2 instance. So this option is incorrect.

EC2 instance configuration data

EC2 instance AMI data

There is no such thing as EC2 instance configuration data or EC2 instance AMI data. These options have been added as distractors.

Reference:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html>

Question 46: **Incorrect**

Which benefit of Cloud Computing allows AWS to offer lower pay-as-you-go prices as usage from hundreds of thousands of customers is aggregated in the cloud?



Trade capital expense for variable expense

(Incorrect)



Increased speed and agility

-
-

Go global in minutes

-
-

Massive economies of scale

(Correct)

Explanation

Correct option:

Massive economies of scale

Cloud computing is the on-demand delivery of IT resources over the Internet with pay-as-you-go pricing. Instead of buying, owning, and maintaining physical data centers and servers, you can access technology services, such as computing power, storage, and databases, on an as-needed basis.

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.

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:

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.

Increased 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.

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.

Although these three options are also benefits of Cloud Computing, it is the massive economies of scale that allow AWS to offer lower pay-as-you-go prices as usage from hundreds of thousands of customers is aggregated in the cloud.

References:

<https://aws.amazon.com/what-is-cloud-computing/>

<https://docs.aws.amazon.com/whitepapers/latest/aws-overview/six-advantages-of-cloud-computing.html>

Question 47: **Correct**

A financial services company wants to ensure that all customer data uploaded on its data lake on Amazon S3 always stays private. Which of the following is the MOST efficient solution to address this compliance requirement?

-

Use Amazon S3 Block Public Access to ensure that all S3 resources stay private

(Correct)

-

Use CloudWatch to ensure that all S3 resources stay private

-

Trigger a lambda function every time an object is uploaded on S3. The lambda function should change the object settings to make sure it stays private

-

Set up a high-level advisory committee to review the privacy settings of each object uploaded into S3

Explanation

Correct option:

Use Amazon S3 Block Public Access to ensure that all S3 resources stay private

The Amazon S3 Block Public Access feature provides settings for access points, buckets, and accounts to help you manage public access to Amazon S3 resources. By default, new buckets, access points, and objects don't allow public access. However, users can modify bucket policies,

access point policies, or object permissions to allow public access. S3 Block Public Access settings override these policies and permissions so that you can limit public access to these resources.

When Amazon S3 receives a request to access a bucket or an object, it determines whether the bucket or the bucket owner's account has a block public access setting applied. If the request was made through an access point, Amazon S3 also checks for block public access settings for the access point. If there is an existing block public access setting that prohibits the requested access, Amazon S3 rejects the request.

Amazon S3 Block Public Access
Overview:

Using Amazon S3 block public access

[PDF](#) | [Kindle](#) | [RSS](#)

The Amazon S3 Block Public Access feature provides settings for access points, buckets, and accounts to help you manage public access to Amazon S3 resources. By default, new buckets, access points, and objects don't allow public access. However, users can modify bucket policies, access point policies, or object permissions to allow public access. S3 Block Public Access settings override these policies and permissions so that you can limit public access to these resources.

With S3 Block Public Access, account administrators and bucket owners can easily set up centralized controls to limit public access to their Amazon S3 resources that are enforced regardless of how the resources are created.

When Amazon S3 receives a request to access a bucket or an object, it determines whether the bucket or the bucket owner's account has a block public access setting applied. If the request was made through an access point, Amazon S3 also checks for block public access settings for the access point. If there is an existing block public access setting that prohibits the requested access, Amazon S3 rejects the request.

Amazon S3 Block Public Access provides four settings. These settings are independent and can be used in any combination. Each setting can be applied to an access point, a bucket, or an entire AWS account. If the block public access settings for the access point, bucket, or account differ, then Amazon S3 applies the most restrictive combination of the access point, bucket, and account settings.

When Amazon S3 evaluates whether an operation is prohibited by a block public access setting, it rejects any request that violates an access point, bucket, or account setting.

⚠️ Warning

Public access is granted to buckets and objects through access control lists (ACLs), access point policies, bucket policies, or all. To help ensure that all of your Amazon S3 access points, buckets, and objects have their public access blocked, we recommend that you turn on all four settings for block public access for your account. These settings block public access for all current and future buckets and access points.

Before applying these settings, verify that your applications will work correctly without public access. If you require some level of public access to your buckets or objects, for example to host a static website as described at [Hosting a static website on Amazon S3](#), you can customize the individual settings to suit your storage use cases.

via - <https://docs.aws.amazon.com/AmazonS3/latest/dev/access-control-block-public-access.html>

Incorrect options:

Trigger a lambda function every time an object is uploaded on S3. The lambda function should change the object settings to make sure it stays private - Although it's possible to implement this solution, but it is more efficient to use the "Amazon S3 Block Public Access" feature as its available off-the-shelf.

Use CloudWatch to ensure that all S3 resources stay private - Amazon CloudWatch is a monitoring and observability service built for DevOps engineers, developers, site reliability engineers (SREs), and IT managers. CloudWatch provides data and actionable insights to monitor applications, respond to

system-wide performance changes, optimize resource utilization, and get a unified view of operational health. This is an excellent service for building Resilient systems. Think resource performance monitoring, events, and alerts; think CloudWatch. CloudWatch cannot be used to ensure data privacy on S3.

Set up a high-level advisory committee to review the privacy settings of each object uploaded into S3 - This option has been added as a distractor.

Reference:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/access-control-block-public-access.html>

Question 48: **Correct**

How is Amazon EC2 different from traditional hosting systems? (Select two)

-

Amazon EC2 provides a pre-configured instance for a fixed monthly cost

-

With Amazon EC2, developers can launch and terminate the instances anytime they need to

(Correct)

-

Amazon EC2 can scale with changing computing requirements

(Correct)

-

With Amazon EC2, users risk overbuying resources

-

Amazon EC2 caters more towards groups of users with similar system requirements so that the server resources are shared across multiple users and the cost is reduced

Explanation

Correct options:

Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud with support for per-second billing. It is the easiest way to provision servers on AWS Cloud and access the underlying OS.

Amazon EC2 differs fundamentally with the traditional on-premises hosting systems in the flexibility, control and significant cost savings it offers developers, allowing them to treat Amazon EC2 instance as their own customized server backed by the robust infrastructure of AWS Cloud.

Amazon EC2 can scale with changing computing requirements - When computing requirements unexpectedly change, Amazon EC2 can be scaled to match the requirements. Developers can control how many EC2 instances are in use at any given point in time.

With Amazon EC2, developers can launch and terminate the instances anytime they need to - Using Amazon EC2, developers can choose not only to launch, terminate, start or shut down instances at any time, but they can also completely customize the configuration of their instances to suit their needs.

Incorrect options:

Amazon EC2 provides a pre-configured instance for a fixed monthly cost - This is an incorrect option. EC2 developers enjoy the benefit of paying only for their actual resource consumption with no monthly or upfront costs. Developers can customize their EC2 instances for their application stack.

With Amazon EC2, users risk overbuying resources - This is an incorrect statement. Users risk overbuying in traditional hosting services where users pay a fixed, up-front fee irrespective of their actual computing power used. With EC2, users pay only for the actual resources consumed.

Amazon EC2 caters more towards groups of users with similar system requirements so that the server resources are shared amongst multiple users and the cost is reduced - This is an incorrect statement. Resources are not shared between users in EC2, which is why the users have the flexibility to start or shutdown the instances as per their requirement. This is not possible for the traditional hosting systems where the resources are shared across users.

Reference:

<https://aws.amazon.com/ec2/faqs/>

Question 49: **Incorrect**

Which of the following statements are CORRECT regarding AWS Global Accelerator? (Select two)

- **Global Accelerator provides static IP addresses that act as a fixed entry point to your applications**
(Correct)
- **Global Accelerator can be used to host static websites**
- **Global Accelerator uses the AWS global network and its edge locations. But the edge locations used by Global Accelerator are different from Amazon CloudFront edge locations**
- **Global Accelerator is a good fit for non-HTTP use cases**
(Correct)
- **Global Accelerator cannot be configured with an Elastic Load Balancer (ELB)**

(Incorrect)

Explanation

Correct options:

AWS Global Accelerator is a networking service that helps you improve the availability and performance of the applications that you offer to your global users. Global Accelerator improves performance for a wide range of applications over TCP or UDP by proxying packets at the edge to applications running in one or more AWS Regions.

How Global Accelerator

Works:



via - <https://aws.amazon.com/global-accelerator/>

Global Accelerator is a good fit for non-HTTP use cases - Global Accelerator is a good fit for non-HTTP use cases, such as gaming (UDP), IoT (MQTT), or Voice over IP, as well as for HTTP use cases that specifically require static IP addresses or deterministic, fast regional failover.

Global Accelerator provides static IP addresses that act as a fixed entry point to your applications - It provides static IP addresses that provide a fixed entry point to your applications and eliminate the complexity of managing specific IP addresses for different AWS Regions and Availability Zones.

Incorrect options:

Global Accelerator uses the AWS global network and its edge locations. But the edge locations used by Global Accelerator are different from Amazon CloudFront edge locations - AWS Global Accelerator and Amazon CloudFront use the same edge locations.

Global Accelerator cannot be configured with an Elastic Load Balancer (ELB) - A regional ELB load balancer is an ideal target for AWS Global Accelerator. AWS Global Accelerator complements ELB by extending these capabilities beyond a single AWS Region, allowing you to provide a global interface for your applications in any number of Regions.

Global Accelerator can be used to host static websites - Amazon S3 can host static websites. So this option is incorrect.

Reference:

<https://aws.amazon.com/global-accelerator/>

Question 50: **Correct**

Which of the following is the MOST cost-effective EC2 instance purchasing option for short-term, spiky and critical workloads on AWS Cloud?

-

On-Demand Instance

(Correct)

-

Reserved Instance

-

Spot Instance

-

Dedicated Host

Explanation

Correct option:

On-Demand Instance

An On-Demand Instance is an instance that you use on-demand. You have full control over its lifecycle – you decide when to launch, stop, hibernate, start, reboot, or terminate it. There is no long-term commitment required when you purchase On-Demand Instances. There is no upfront payment and you pay only for the seconds that your On-Demand Instances are running. There is no need for a long-term purchasing commitment. The price per second for running an On-Demand Instance is fixed. On-demand instances cannot be interrupted. Therefore On-Demand instances are the best fit for short-term, spiky and critical workloads.

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 »](#)

via - <https://aws.amazon.com/ec2/pricing/>

Incorrect options:

Spot Instance - A Spot Instance is an unused EC2 instance that is available for less than the On-Demand price. Because Spot Instances enable you to request unused EC2 instances at steep discounts (up to 90%), you can lower your Amazon EC2 costs significantly. Spot Instances are well-suited for data analysis, batch jobs, background processing, and other flexible tasks that can be interrupted. These can be terminated at short notice, so these are not suitable for critical workloads that need to run at a specific point in time.

Reserved Instance - Reserved Instances provide you with significant savings (up to 75%) on your Amazon EC2 costs compared to On-Demand Instance pricing. Reserved Instances are not physical instances, but rather a billing discount applied to the use of On-Demand Instances in your account. You can purchase a Reserved Instance for a one-year or three-year commitment, with the three-year commitment offering a bigger discount. Reserved instances cannot be interrupted. Reserved instances are not the right choice for short-term workloads.

Dedicated Host - Amazon EC2 Dedicated Hosts allow you to use your eligible software licenses from vendors such as Microsoft and Oracle on Amazon EC2 so that you get the flexibility and cost-effectiveness of using your licenses, but with the resiliency, simplicity, and elasticity of AWS. An Amazon EC2 Dedicated Host is a physical server fully dedicated for your use, so you can help address corporate compliance requirement. They're not cost-efficient compared to On-Demand instances. So this option is not correct.

Reference:

<https://aws.amazon.com/ec2/pricing/>

Question 51: **Correct**

Which AWS entity enables you to privately connect your VPC to an Amazon SQS queue?

-
- AWS Direct Connect**
-
- VPC Interface Endpoint**
- (Correct)**
-
- VPC Gateway Endpoint**
-
- Internet Gateway**

Explanation

Correct option:

VPC Interface Endpoint

An interface endpoint is an elastic network interface with a private IP address from the IP address range of your subnet that serves as an entry point for traffic destined to a supported service. Interface endpoints are powered by AWS PrivateLink, a technology that enables you to privately access services by using private IP addresses. AWS PrivateLink restricts all network traffic between your VPC and services to the Amazon network. You do not need an internet gateway, a NAT device, or a virtual private gateway.

Exam Alert:

You may see a question around this concept in the exam. Just remember that only S3 and DynamoDB support VPC Endpoint Gateway. All other services that support VPC Endpoints use a VPC Endpoint Interface.

Incorrect options:

VPC Gateway Endpoint - A Gateway Endpoint is a gateway that you specify as a target for a route in your route table for traffic destined to a supported AWS service. The following AWS services are supported: Amazon S3, DynamoDB. You cannot use VPC Gateway Endpoint to privately connect your VPC to an Amazon SQS queue.

AWS Direct Connect - AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS. You can use AWS Direct Connect to establish a private virtual interface from your on-premise network directly to your Amazon VPC. This private connection takes at least one month for completion. You cannot use AWS Direct Connect to privately connect your VPC to an Amazon SQS queue.

Internet Gateway - An Internet Gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between your VPC and the internet. An internet gateway serves two purposes: to provide a target in your VPC route tables for internet-routable traffic, and to perform network address translation (NAT) for instances that have been assigned public IPv4

addresses. You cannot use an Internet Gateway to privately connect your VPC to an Amazon SQS queue.

Reference:

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints.html>

Question 52: **Incorrect**

An e-commerce company wants to review the Payment Card Industry (PCI) reports on AWS Cloud. Which AWS resource can be used to address this use-case?



AWS Trusted Advisor



AWS Secrets Manager



AWS Cost and Usage Reports

(Incorrect)



AWS Artifact

(Correct)

Explanation

Correct option:

AWS Artifact

AWS Artifact is your go-to, central resource for compliance-related information that matters to your organization. It provides on-demand access to AWS' security and compliance reports and select online agreements. Reports available in AWS Artifact include our Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, and certifications from accreditation bodies across geographies and compliance verticals that validate the implementation and operating effectiveness of AWS security controls. It is not a service, it's a no-cost, self-service portal for on-demand access to AWS' compliance reports.

Incorrect options:

AWS Trusted Advisor - AWS Trusted Advisor is an online tool that provides you real-time guidance to help you provision your resources following AWS best practices. Whether establishing new workflows, developing applications, or as part of ongoing improvement, recommendations provided by Trusted Advisor regularly help keep your solutions provisioned optimally.

AWS Secrets Manager - AWS Secrets Manager helps you protect secrets needed to access your applications, services, and IT resources. The service enables you to easily rotate, manage, and

retrieve database credentials, API keys, and other secrets throughout their lifecycle. Users and applications retrieve secrets with a call to Secrets Manager APIs, eliminating the need to hardcode sensitive information in plain text.

AWS Cost and 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 updates the report in your bucket once a day in comma-separated value (CSV) format.

Reference:

<https://aws.amazon.com/artifact/>

Question 53: **Incorrect**

As per the Shared Responsibility Model, Security and Compliance is a shared responsibility between AWS and the customer. Which of the following security services falls under the purview of AWS under the Shared Responsibility Model?

-
- **AWS Web Application Firewall (WAF)**
-
- **Security Groups for Amazon EC2**
- **(Incorrect)**
-
- **AWS Shield Advanced**
-
- **AWS Shield Standard**
- **(Correct)**

Explanation

Correct option:

AWS Shield Standard

AWS Shield is a managed service that protects against Distributed Denial of Service (DDoS) attacks for applications running on AWS. AWS Shield Standard is enabled for all AWS customers at no additional cost. AWS Shield Standard automatically protects your web applications running on AWS against the most common, frequently occurring DDoS attacks. You can get the full benefits of AWS Shield Standard by following the best practices of DDoS resiliency on AWS. As Shield Standard is automatically activated for all AWS customers with no options for any customizations, therefore AWS needs to manage the maintenance and configurations for this service. Hence this service falls under the purview of AWS.

Incorrect options:

AWS Web Application Firewall (WAF) - AWS WAF is a web application firewall that lets you monitor the HTTP and HTTPS requests that are forwarded to an Amazon API Gateway API, Amazon CloudFront or an Application Load Balancer. AWS WAF also lets you control access to your content. AWS WAF has to be enabled by the customer and comes under the customer's responsibility.

AWS Shield Advanced - For higher levels of protection against attacks, you can subscribe to AWS Shield Advanced. As an AWS Shield Advanced customer, you can contact a 24x7 DDoS response team (DRT) for assistance during a DDoS attack. You also have exclusive access to advanced, real-time metrics and reports for extensive visibility into attacks on your AWS resources. Customers need to subscribe to Shield Advanced and need to pay for this service. It falls under customer responsibility per the AWS Shared Responsibility Model.

Security Groups for Amazon EC2 - A Security Group acts as a virtual firewall for the EC2 instance to control incoming and outgoing traffic. Inbound rules control the incoming traffic to your instance, and outbound rules control the outgoing traffic from your instance. Security groups are the responsibility of the customer.

Reference:

<https://aws.amazon.com/compliance/shared-responsibility-model/>

Question 54: **Incorrect**

The QA team at a company wants a tool/service that can provide access to different mobile devices with variations in firmware and Operating System versions.

Which AWS service can address this use case?



AWS Device Farm

(Correct)



AWS Elastic Beanstalk

(Incorrect)



AWS CodePipeline



AWS Mobile Farm

Explanation

Correct option:

AWS Device Farm - AWS Device Farm is an application testing service that lets you improve the quality of your web and mobile apps by testing them across an extensive range of desktop browsers

and real mobile devices; without having to provision and manage any testing infrastructure. The service enables you to run your tests concurrently on multiple desktop browsers or real devices to speed up the execution of your test suite, and generates videos and logs to help you quickly identify issues with your app.

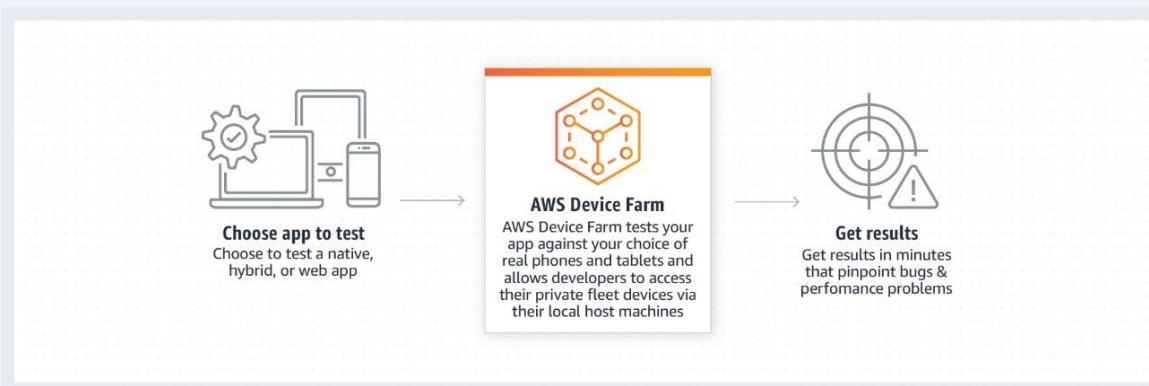
AWS Device Farm is designed for developers, QA teams, and customer support representatives who are building, testing, and supporting mobile apps to increase the quality of their apps. Application quality is increasingly important, and also getting complex due to the number of device models, variations in firmware and OS versions, carrier and manufacturer customizations, and dependencies on remote services and other apps. AWS Device Farm accelerates the development process by executing tests on multiple devices, giving developers, QA and support professionals the ability to perform automated tests and manual tasks like reproducing customer issues, exploratory testing of new functionality, and executing manual test plans. AWS Device Farm also offers significant savings by eliminating the need for internal device labs, lab managers, and automation infrastructure development.

How it
works:

Testing on real mobile devices

Automated Testing

Test your app in parallel against a massive collection of physical devices in the AWS Cloud. Use one of our built-in frameworks, to test your applications without having to write or maintain test scripts, or use one of our supported automation testing frameworks.



via - <https://aws.amazon.com/device-farm/>

Incorrect options:

AWS CodePipeline - AWS CodePipeline is a fully managed continuous delivery service that helps you automate your release pipelines for fast and reliable application and infrastructure updates. CodePipeline automates the build, test, and deploy phases of your release process every time there is a code change, based on the release model you define. This enables you to rapidly and reliably deliver features and updates.

AWS Elastic Beanstalk - AWS Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services developed with Java, .NET, PHP, Node.js, Python, etc.

You can simply upload your code and Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring. At the same time, you retain full control over the AWS resources powering your application and can access the underlying resources at any time.

AWS Mobile Farm - This is an invalid option, given only as a distractor.

Reference:

<https://aws.amazon.com/device-farm/>

Question 55: **Incorrect**

Which of the following describes an Availability Zone in the AWS Cloud?

-
- One or more server racks in the same location**
-
- One or more data centers in the same location**
- (Correct)**
-
- One or more server racks in multiple locations**
-
- One or more data centers in multiple locations**
- (Incorrect)**

Explanation

Correct option:

"One or more data centers in the same location"

An Availability Zone (AZ) is one or more discrete data centers with redundant power, networking, and connectivity in an AWS Region. An AWS Region refers to a physical location around the world where AWS clusters data centers. 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.

AWS Regions and Availability Zones

Explained:

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/

Incorrect options:

"One or more data centers in multiple locations"

"One or more server racks in the same location"

"One or more server racks in multiple locations"

These three options contradict the details provided earlier in the explanation, so these options are incorrect.

Reference:

https://aws.amazon.com/about-aws/global-infrastructure/regions_az/

Question 56: **Correct**

Which of the following entities are part of a VPC in the AWS Cloud? (Select two)

-

Subnet

(Correct)

-

Internet Gateway

(Correct)

-

Storage Gateway

-

Object

-

API Gateway

Explanation

Correct option:

Subnet

Internet Gateway

Amazon Virtual Private Cloud (Amazon VPC) enables you to launch AWS resources into a virtual network that you've defined.

The following are the key concepts for VPCs:

Virtual private cloud (VPC) – A virtual network dedicated to your AWS account.

Subnet – A range of IP addresses in your VPC.

Route table – A set of rules, called routes, that are used to determine where network traffic is directed.

Internet Gateway – A gateway that you attach to your VPC to enable communication between resources in your VPC and the internet.

VPC endpoint – Enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection.

Incorrect options:

Storage Gateway - AWS Storage Gateway is a hybrid cloud storage service that gives you on-premises access to virtually unlimited cloud storage. Customers use Storage Gateway to simplify storage management and reduce costs for key hybrid cloud storage use cases. Storage Gateway is not part of VPC.

API Gateway - Amazon API Gateway is a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale. APIs act as the "front door" for applications to access data, business logic, or functionality from your backend services. API Gateway is not part of a VPC.

Object - Buckets and objects are part of Amazon S3. Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance.

Reference:

https://docs.amazonaws.cn/en_us/vpc/latest/userguide/what-is-amazon-vpc.html

Question 57:

Skipped

Which entity ensures that your application on Amazon EC2 always has the right amount of capacity to handle the current traffic demand?

-
- **Network Load Balancer**
-
- **Application Load Balancer**
-
- **Auto Scaling**
- **(Correct)**
-
- **Multi AZ deployment**

Explanation

Correct option:

Auto Scaling

Auto Scaling helps you ensure that you have the correct number of Amazon EC2 instances available to handle the load for your application. You create collections of EC2 instances, called Auto Scaling groups. You can specify the minimum number of instances in each Auto Scaling group, and Amazon EC2 Auto Scaling ensures that your group never goes below this size.

EC2 Auto Scaling

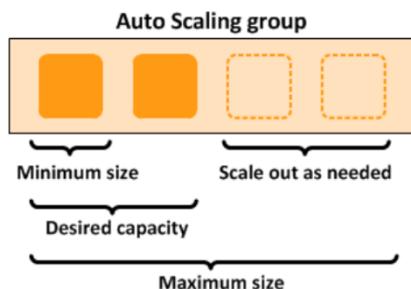
Overview:

What Is Amazon EC2 Auto Scaling?

[PDF](#) | [Kindle](#) | [RSS](#)

Amazon EC2 Auto Scaling helps you ensure that you have the correct number of Amazon EC2 instances available to handle the load for your application. You create collections of EC2 instances, called *Auto Scaling groups*. You can specify the minimum number of instances in each Auto Scaling group, and Amazon EC2 Auto Scaling ensures that your group never goes below this size. You can specify the maximum number of instances in each Auto Scaling group, and Amazon EC2 Auto Scaling ensures that your group never goes above this size. If you specify the desired capacity, either when you create the group or at any time thereafter, Amazon EC2 Auto Scaling ensures that your group has this many instances. If you specify scaling policies, then Amazon EC2 Auto Scaling can launch or terminate instances as demand on your application increases or decreases.

For example, the following Auto Scaling group has a minimum size of one instance, a desired capacity of two instances, and a maximum size of four instances. The scaling policies that you define adjust the number of instances, within your minimum and maximum number of instances, based on the criteria that you specify.



via - <https://docs.aws.amazon.com/autoscaling/ec2/userguide/what-is-amazon-ec2-auto-scaling.html>

Incorrect options:

Multi AZ deployment - With Availability Zones, you can design and operate applications and databases that automatically failover between zones without interruption. Multi AZ deployment of EC2 instances provided high availability, it does not help in scaling resources.

Network Load Balancer - Network Load Balancer is best suited for load balancing of Transmission Control Protocol (TCP), User Datagram Protocol (UDP) and Transport Layer Security (TLS) traffic where extreme performance is required. It distributes traffic, does not scale resources.

Application Load Balancer - An Application Load Balancer serves as the single point of contact for clients. The load balancer distributes incoming application traffic across multiple targets, such as EC2 instances, in multiple Availability Zones. It distributes traffic, does not scale resources.

Reference:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/what-is-amazon-ec2-auto-scaling.html>

Question 58: **Correct**

Which AWS service can be used to set up billing alarms to monitor estimated charges on your AWS account?



Amazon CloudWatch

(Correct)

-

AWS CloudTrail

-

AWS Cost Explorer

-

AWS Organizations

Explanation

Correct option:

Amazon CloudWatch

Amazon CloudWatch can be used to create an alarm to monitor your estimated charges. When you enable the monitoring of estimated charges for your AWS account, the estimated charges are calculated and sent several times daily to CloudWatch as metric data. You can choose to receive alerts by email when charges have exceeded a certain threshold. These alerts are triggered by CloudWatch and messages are sent using Amazon Simple Notification Service (Amazon SNS). Billing metric data is stored in the US East (N. Virginia) Region and reflects worldwide charges.

The alarm triggers when your account billing exceeds the threshold you specify. It triggers only when actual billing exceeds the threshold. It doesn't use projections based on your usage so far in the month.

CloudWatch Billing Alarms

Overview:

Creating a Billing Alarm to Monitor Your Estimated AWS Charges

[PDF](#) | [Kindle](#) | [RSS](#)

You can monitor your estimated AWS charges by using Amazon CloudWatch. When you enable the monitoring of estimated charges for your AWS account, the estimated charges are calculated and sent several times daily to CloudWatch as metric data.

Billing metric data is stored in the US East (N. Virginia) Region and represents worldwide charges. This data includes the estimated charges for every service in AWS that you use, in addition to the estimated overall total of your AWS charges.

The alarm triggers when your account billing exceeds the threshold you specify. It triggers only when actual billing exceeds the threshold. It doesn't use projections based on your usage so far in the month.

If you create a billing alarm at a time when your charges have already exceeded the threshold, the alarm goes to the ALARM state immediately.

via

- https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/monitor_estimated_charges_with_cloudwatch.html

Exam Alert:

It is useful to note the difference between CloudWatch Billing vs Budgets:

CloudWatch Billing Alarms: Sends an alarm when the actual cost exceeds a certain threshold.

Budgets: Sends an alarm when the actual cost exceeds the budgeted amount or even when the cost forecast exceeds the budgeted amount.

Incorrect options:

AWS CloudTrail - AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. Billing alarms cannot be triggered via CloudTrail.

AWS Organizations - AWS Organizations is an account management service that enables you to consolidate multiple AWS accounts into an organization that you create and centrally manage. Consolidated billing is a feature of AWS Organizations. You can use the master account of your organization to consolidate and pay for all member accounts. Billing alarms cannot, however, be triggered using Consolidated Billing.

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. Cost Explorer will help analyze your data at a high level or dive deeper into your cost and usage data using various reports (Monthly costs by AWS service, hourly and resource Level cost). Billing alarms cannot be triggered via Cost Explorer.

Reference:

https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/monitor_estimated_charges_with_cloudwatch.html

Question 59: **Correct**

Which of the following entities can be used to connect to an EC2 server from a Mac OS, Windows or Linux based computer via a browser-based client?

-
- Putty**
-
- EC2 Instance Connect**
- (Correct)**
-
- SSH**
-
- AWS Direct Connect**

Explanation

Correct option:

EC2 Instance Connect

Amazon EC2 Instance Connect provides a simple and secure way to connect to your instances using Secure Shell (SSH). With EC2 Instance Connect, you use AWS Identity and Access Management (IAM) policies and principals to control SSH access to your instances, removing the need to share and manage SSH keys. All connection requests using EC2 Instance Connect are logged to AWS CloudTrail so that you can audit connection requests.

You can use Instance Connect to connect to your Linux instances using a browser-based client, the Amazon EC2 Instance Connect CLI, or the SSH client of your choice. EC2 Instance Connect can be used to connect to an EC2 instance from a Mac OS, Windows or Linux based computer.

Incorrect options:

SSH - SSH can be used from a Mac OS, Windows or Linux based computer, but it's not a browser-based client.

Putty - Putty can be used only from Windows based computers.

AWS Direct Connect - AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS. You can use AWS Direct Connect to establish a private virtual interface from your on-premise network directly to your Amazon VPC. This private connection takes at least one month for completion. Direct Connect cannot be used to connect to an EC2 instance from a Mac OS, Windows or Linux based computer.

Reference:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Connect-using-EC2-Instance-Connect.html>

Question 60: **Incorrect**

Which AWS service would you choose for a data processing project that needs a schemaless database?

- Amazon Aurora**
(Incorrect)
- Amazon RedShift**
- Amazon DynamoDB**
(Correct)
- Amazon RDS**

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. DynamoDB is schemaless. DynamoDB can manage structured or semistructured data, including JSON documents.

Incorrect options:

Amazon RedShift - Amazon Redshift is a fully-managed petabyte-scale cloud-based data warehouse product designed for large scale data set storage and analysis. Amazon Redshift requires a well-defined schema.

Amazon Aurora - Amazon Aurora is an AWS service for relational databases. Aurora requires a well-defined schema.

Amazon RDS - Amazon RDS is an AWS service for relational databases. RDS requires a well-defined schema.

References:

<https://aws.amazon.com/dynamodb/features/>

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/SQLtoNoSQL.WhyDynamoDB.html>

Question 61: **Incorrect**

Which of the following are benefits of the AWS Web Application Firewall (WAF)? (Select two)

-

WAF offers dedicated support from the DDoS Response Team (DRT) and advanced reporting
(Incorrect)

-

WAF offers protection against all known infrastructure (Layer 3 and 4) attacks

-

AWS WAF lets you monitor the HTTP and HTTPS requests that are forwarded to Amazon Route 53

(Incorrect)

-

WAF can check for the presence of SQL code that is likely to be malicious (known as SQL injection)

(Correct)

-

WAF can block all requests except the ones that you allow

(Correct)

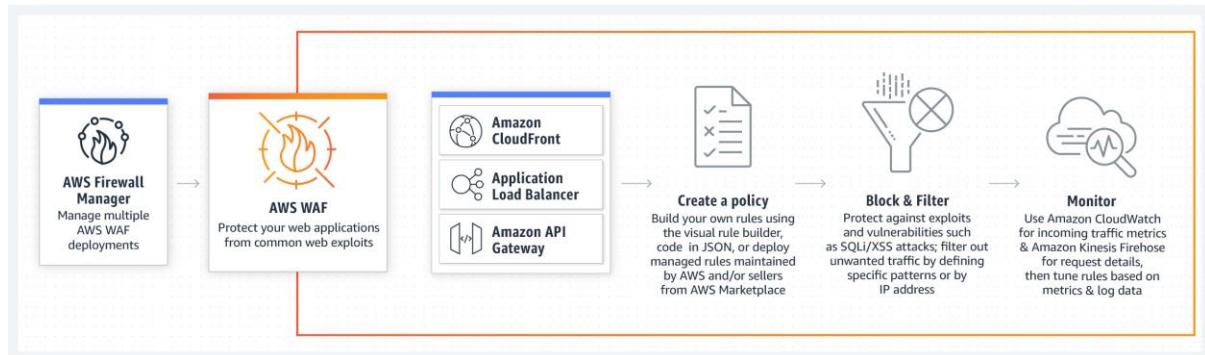
Explanation

Correct options:

AWS WAF is a web application firewall that helps protect your web applications or APIs against common web exploits that may affect availability, compromise security, or consume excessive resources. AWS WAF gives you control over how traffic reaches your applications by enabling you to create security rules that block common attack patterns such as SQL injection or cross-site scripting. You can also use rate-based rules to mitigate the Web layer DDoS attack.

How WAF

Works:



via - <https://aws.amazon.com/waf/>

WAF can block all requests except the ones that you allow - WAF can block all requests except the ones that you allow. This is useful when you want to serve content for a restricted website whose users are readily identifiable by properties in web requests, such as the IP addresses that they use to browse to the website.

WAF can check for the presence of SQL code that is likely to be malicious (known as SQL injection) - WAF offers additional protection against web attacks using conditions that you specify. You can define conditions by using characteristics of web requests such as - IP addresses that requests originate from, presence of a script that is likely to be malicious (known as cross-site scripting), presence of SQL code that is likely to be malicious (known as SQL injection) and many more.

Incorrect options:

WAF offers protection against all known infrastructure (Layer 3 and 4) attacks - WAF lets you monitor the HTTP and HTTPS requests to your application, it only works at the application layer (layer 7).

WAF offers dedicated support from the DDoS Response Team (DRT) and advanced reporting - As AWS Shield Advanced customer can contact a 24x7 DDoS response team (DRT) for assistance during a DDoS attack, it is a feature of Shield Advanced, and not of WAF.

AWS WAF lets you monitor the HTTP and HTTPS requests that are forwarded to Amazon Route 53 -
AWS WAF is a web application firewall that lets you monitor the HTTP and HTTPS requests that are forwarded to an Amazon API Gateway API, Amazon CloudFront or an Application Load Balancer. It does not cover Amazon Route 53, which is a Domain Name System (DNS) web service.

Reference:

<https://docs.aws.amazon.com/waf/latest/developerguide/what-is-aws-waf.html>

Question 62: **Incorrect**

Which of the following types are free under the Amazon S3 pricing model? (Select two)

-

Data storage fee for objects stored in S3 Glacier

-

Data transferred in from the internet

(Correct)

-

Data transferred out to an Amazon Elastic Compute Cloud (Amazon EC2) instance, when the instance is in the same AWS Region as the S3 bucket

(Correct)

-

Data storage fee for objects stored in S3 Standard

-

Data transferred out to an Amazon Elastic Compute Cloud (Amazon EC2) instance in any AWS Region

(Incorrect)

Explanation

Correct options:

Data transferred in from the internet

Data transferred out to an Amazon Elastic Compute Cloud (Amazon EC2) instance, when the instance is in the same AWS Region as the S3 bucket

There are four cost components to consider for S3 pricing – storage pricing; request and data retrieval pricing; data transfer and transfer acceleration pricing; and data management features pricing. Under "Data Transfer", You pay for all bandwidth into and out of Amazon S3, except for the following: (1) Data transferred in from the internet, (2) Data transferred out to an Amazon Elastic

Compute Cloud (Amazon EC2) instance, when the instance is in the same AWS Region as the S3 bucket, (3) Data transferred out to Amazon CloudFront (CloudFront).

Incorrect options:

Data transferred out to an Amazon Elastic Compute Cloud (Amazon EC2) instance in any AWS Region - This is incorrect. Data transfer charges apply when the instance is not in the same AWS Region as the S3 bucket.

Data storage fee for objects stored in S3 Standard - S3 Standard charges a storage fee for objects.

Data storage fee for objects stored in S3 Glacier - S3 Glacier charges a storage fee for objects.

Reference:

<https://aws.amazon.com/s3/pricing/>

Question 63: **Correct**

Reserved Instance pricing is available for which of the following AWS services? (Select two)

- **Amazon CloudFront**
- **AWS Identity & Access Management (IAM)**
- **Amazon Relational Database Service (Amazon RDS)**
(Correct)
- **Amazon Simple Storage Service (Amazon S3)**
- **Amazon Elastic Compute Cloud (Amazon EC2)**
(Correct)

Explanation

Correct options:

Amazon Elastic Compute Cloud (Amazon EC2)

Amazon Relational Database Service (Amazon RDS)

A Reserved Instance is a reservation that provides a discounted hourly rate in exchange for an upfront fee and term contract. Services such as Amazon Elastic Compute Cloud (Amazon EC2) and Amazon Relational Database Service (Amazon RDS) use this approach to sell reserved capacity for hourly use of Reserved Instances. It is not a virtual machine. It is a commitment to pay in advance for specific Amazon EC2 or Amazon RDS instances.

Incorrect options:

Amazon CloudFront - Amazon CloudFront is a content delivery network (CDN) service. CloudFront does not offer "Reserved Capacity" pricing.

Amazon Simple Storage Service (Amazon S3) - Amazon S3 infrastructure is managed by AWS. So, Reserved Instance does not make sense here. But, S3 offers volume discounts for its storage classes.

AWS Identity & Access Management (IAM) - AWS Identity and Access Management (IAM) enables you to manage access to AWS services and resources securely. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources. This is a free service to every AWS customer.

Reference:

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/con-bill-blended-rates.html>

Question 64: **Correct**

Which of the following is available across all AWS Support plans?

-

AWS Personal Health Dashboard

(Correct)

-

Third-Party Software Support

-

Enhanced Technical Support with unlimited cases and unlimited contacts

-

Full set of AWS Trusted Advisor best practice checks

Explanation

Correct option:

"AWS Personal Health Dashboard"

Full set of AWS Trusted Advisor best practice checks, enhanced Technical Support with unlimited cases, and unlimited contacts and third-party Software Support are available only for Business and Enterprise Support plans.

AWS Personal Health Dashboard is available for all Support plans.

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:

"Full set of AWS Trusted Advisor best practice checks"

"Enhanced Technical Support with unlimited cases and unlimited contacts"

"Third-Party Software Support"

As mentioned in the explanation above, these options are available only for Business and Enterprise Support plans.

Reference:

<https://aws.amazon.com/premiumsupport/plans/>

Question 65: **Incorrect**

A multi-national organization has separate VPCs for each of its business units on the AWS Cloud. The organization also wants to connect its on-premises data center with all VPCs for better organization-wide collaboration. Which AWS services can be combined to build the MOST efficient solution for this use-case? (Select two)

-

AWS Transit Gateway

(Correct)

-

AWS Storage Gateway

-

AWS Internet Gateway

-

AWS Direct Connect

(Correct)

-

VPC Peering

(Incorrect)

Explanation

Correct option:

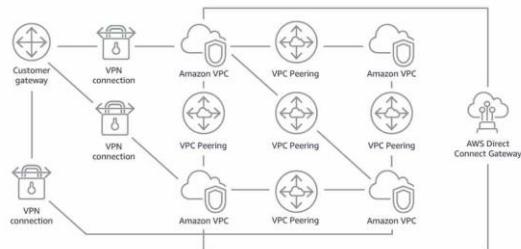
AWS Transit Gateway

AWS Transit Gateway connects VPCs and on-premises networks through a central hub. This simplifies your network and puts an end to complex peering relationships. It acts as a cloud router –

each new connection is only made once. As you expand globally, inter-Region peering connects AWS Transit Gateways using the AWS global network. Your data is automatically encrypted and never travels over the public internet.

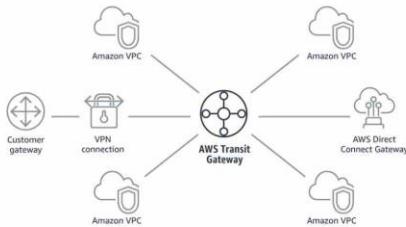
How Transit Gateway can simplify your network:

Without AWS Transit Gateway



Complexity increases with scale. You must maintain routing tables within each VPC and connect to each onsite location using separate network gateways.

With AWS Transit Gateway



Your network is streamlined and scalable. AWS Transit Gateway routes all traffic to and from each VPC or VPN, and you have one place to manage and monitor it all.

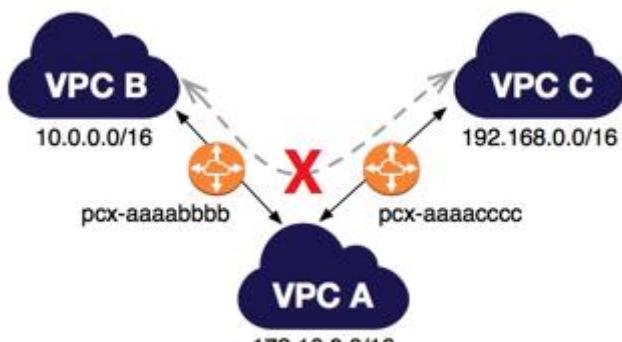
via - <https://aws.amazon.com/transit-gateway/>

AWS Direct Connect

AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect, you can establish private connectivity between AWS and your datacenter, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.

Incorrect options:

VPC Peering - A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them privately. VPC peering is not transitive, a separate VPC peering connection has to be made between two VPCs that need to talk to each other. With growing VPCs, this gets difficult to manage.



Transitive VPC Peering is not allowed:

- <https://docs.aws.amazon.com/vpc/latest/peering/invalid-peering-configurations.html>

via

Internet Gateway - An internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the internet. It, therefore, imposes no availability risks or bandwidth constraints on your network traffic. You cannot use Internet Gateway to connect your on-premises data center with multiple VPCs within your AWS network.

AWS Storage Gateway - AWS Storage Gateway is a hybrid cloud storage service that gives you on-premises access to virtually unlimited cloud storage. All data transferred between the gateway and AWS storage is encrypted using SSL (for all three types of gateways - File, Volume and Tape Gateways). You cannot use Storage Gateway to connect your on-premises data center with multiple VPCs within your AWS network.

Reference:

<https://aws.amazon.com/transit-gateway/>

Practice Test #5 - AWS Certified Cloud Practitioner - Results

Return to review

Chart

Pie chart with 3 slices.

End of interactive chart.

Attempt 1

All knowledge areas

All questions

Question 1: **Correct**

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?

-

Create an IAM user for each user in each region

-

There is nothing to do, IAM is a global service

(Correct)

-

Create 'global' permissions so users can access resources from all around the world

-

As employees travel, they can use other employees' 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 2: **Incorrect**

A company would like to separate cost for AWS services by the department for cost allocation. Which of the following is the simplest way to achieve this task?

-
-

Create tags for each department

(Correct)

-
-

Create one account for all departments and share this account

(Incorrect)

-
-

Create different accounts for different departments

-
-

Create different VPCs for different departments

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. Also, it is much simpler to set up tags for tracking costs for each department.

Create one account for all departments 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 3: **Incorrect**

Which AWS serverless service allows you to prepare data for analytics?



Amazon Redshift



Amazon EMR



AWS Glue

(Correct)



Amazon Athena

(Incorrect)

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: 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 4: Correct

A company using a hybrid cloud would like to store secondary backup copies of the on-premises data. Which S3 Storage Class would you use for a cost-optimal yet rapid access solution?

S3 Glacier

S3 Standard - General Purposes

S3 One Zone - Infrequent Access

(Correct)

S3 Standard - Infrequent Access

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:

Performance across the S3 Storage Classes

	S3 Standard	S3 Intelligent-Tiering*	S3 Standard-IA	S3 One Zone-IA†	S3 Glacier Instant Retrieval	S3 Glacier Flexible Retrieval	S3 Glacier Deep Archive
Designed for durability	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)				
Designed for availability	99.99%	99.9%	99.9%	99.5%	99.9%	99.99%	99.99%
Availability SLA	99.9%	99%	99%	99%	99%	99%	99.9%
Availability Zones	≥3	≥3	≥3	1	≥3	≥3	≥3
Minimum capacity charge per object	N/A	N/A	128 KB	128 KB	128 KB	40 KB	40 KB
Minimum storage duration charge	N/A	N/A	30 days	30 days	90 days	90 days	180 days
Retrieval charge	N/A	N/A	per GB retrieved	per GB retrieved	per GB retrieved	per GB retrieved	per GB retrieved
First byte latency	milliseconds	milliseconds	milliseconds	milliseconds	milliseconds	minutes or hours	hours
Storage type	Object	Object	Object	Object	Object	Object	Object
Lifecycle transitions	Yes	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 5: **Incorrect**

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)

-

Server administration

(Correct)

-

Application advertising

-

Power/Cooling

(Correct)

-

Number of end-users

(Incorrect)

-

Electronic equipment at office

Explanation

Correct option:

Server administration

Power/Cooling

AWS Pricing Calculator lets you explore AWS services and create an estimate for the cost of your use cases on AWS. You can model your solutions before building them, explore the price points and calculations behind your estimate, and find the available instance types and contract terms that meet your needs. This enables you to make informed decisions about using AWS. You can plan your AWS

costs and usage or price out setting up a new set of instances and services. AWS Pricing Calculator can be accessed at <https://calculator.aws/#/>.

AWS Pricing 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.

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://calculator.aws/#/>

<https://aws.amazon.com/blogs/aws/new-cloud-tco-comparison-calculator-for-web-applications/>

Question 6: **Incorrect**

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?



Amazon EC2

(Incorrect)



Amazon LightSail

(Correct)



AWS CloudFormation



Amazon ECS

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 7: **Incorrect**

According to the Shared Responsibility Model, which of the following is a responsibility of the customer?

-

Managing DynamoDB

(Incorrect)

-

Protecting hardware infrastructure

-

Edge locations security

-

Firewall & networking configuration in EC2

(Correct)

Explanation

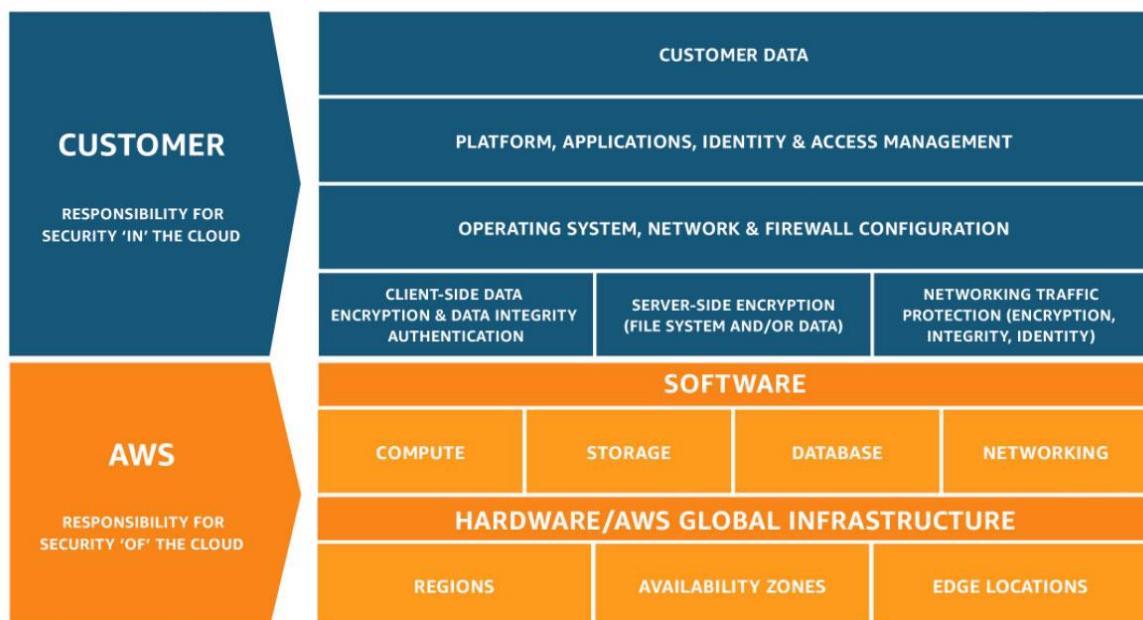
Correct option:

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 8: **Correct**

Which of the following options are the benefits of using AWS Elastic Load Balancing (ELB)? (Select TWO)

-

Fault tolerance

(Correct)

-

Agility

-

Less costly

-

Storage

-

High availability

(Correct)

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 9: **Incorrect**

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?

-
- S3 Versioning**
-
- S3 Cross-Region Replication (CRR)**
-
- S3 Bucket Policies**
(Incorrect)
-
- S3 Access Logs**
(Correct)

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 10: **Incorrect**

Which AWS service can be used to send, store, and receive messages between software components at any volume to decouple application tiers?



AWS Organizations



AWS Elastic Beanstalk



Amazon SQS

(Correct)



Amazon SNS

(Incorrect)

Explanation

Correct option:

Amazon SQS

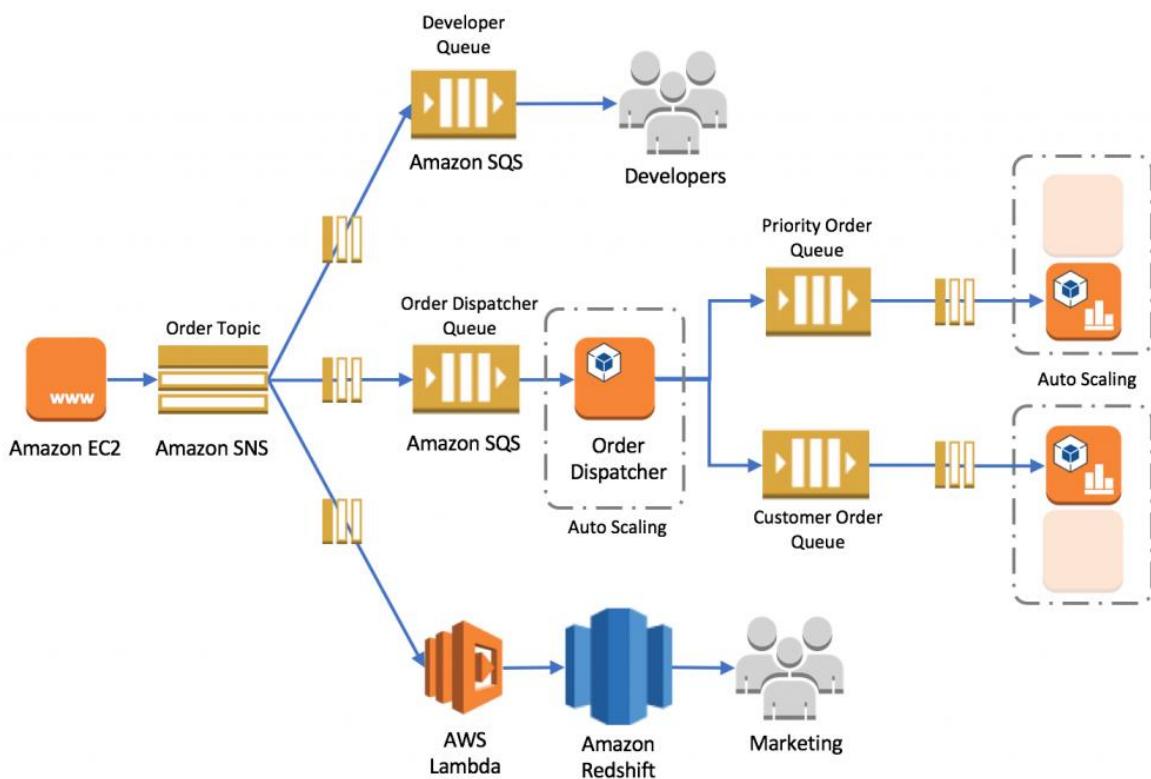
Amazon Simple Queue Service (Amazon SQS) is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SQS eliminates the complexity and overhead associated with managing and operating message-oriented middleware, and 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-c-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 11: **Correct**

Which of the following are advantages of using the AWS Cloud? (Select TWO)

-

AWS is responsible for security in the cloud

-

Increase speed and agility

(Correct)

-
- **Limited scaling**
-
- **Trade operational expense for capital expense**
-
- **Stop guessing about capacity**

(Correct)

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 12: **Incorrect**

An organization would like to copy data across different Availability Zones (AZs) using EBS snapshots. Where are EBS snapshots stored in the AWS Cloud?



Amazon S3

(Correct)



Amazon EC2

(Incorrect)



Amazon EFS



Amazon RDS

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 13: **Correct**

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)

-

1 year

(Correct)

-

2 years

-

3 years

(Correct)

-

6 months

-

5 years

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 14: **Incorrect**

Which Amazon EC2 Auto Scaling feature can help with fault tolerance?



Distributing load to EC2 instances

(Incorrect)

- Having the right amount of computing capacity
- Lower cost by adjusting the number of EC2 instances
- Replacing unhealthy EC2 instances

(Correct)

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 15: **Incorrect**

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?

- AWS Cost Explorer**
- (Correct)**
-
- AWS Cost and Usage Reports**
- (Incorrect)**
-
- AWS Pricing Calculator**
-
- AWS Budgets**

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-accreting 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.

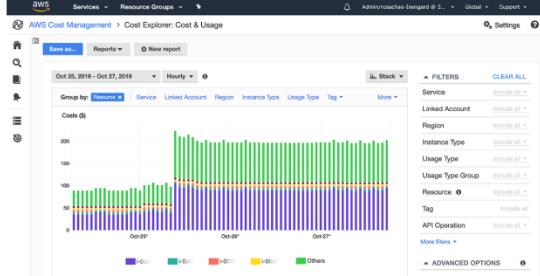
[Launch the Monthly Costs by AWS Service report »](#)



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://assets-pt.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 16: Correct

A company would like to optimize Amazon EC2 costs. Which of the following actions can help with this task? (Select TWO)

-

Purchase EC2 Reserved instances

(Correct)

-

Vertically scale the EC2 instances

-

Opt for a higher AWS Support plan

- -
- Build its own servers**
- Set up Auto Scaling groups to align the number of instances with demand**
- (Correct)**

Explanation

Correct option:

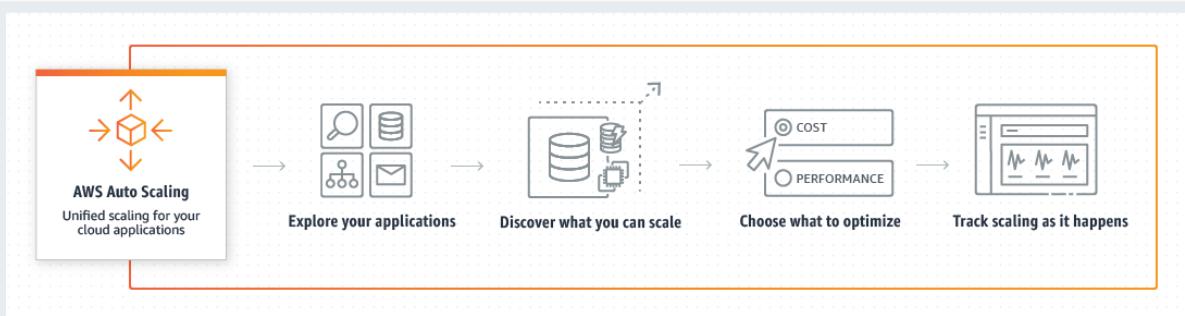
Set up Auto Scaling groups to align the number of instances with demand

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 »](#)

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 17: **Correct**

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?



S3 Bucket policies

-

S3 Lifecycle management

(Correct)

-

S3 Transfer Acceleration

-

S3 Cross-Region Replication (CRR)

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 18: **Incorrect**

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?

- **Amazon Inspector**
- **AWS Systems Manager**
(Correct)
- **AWS Trusted Advisor**
- **AWS Personal Health Dashboard**
(Incorrect)

Explanation

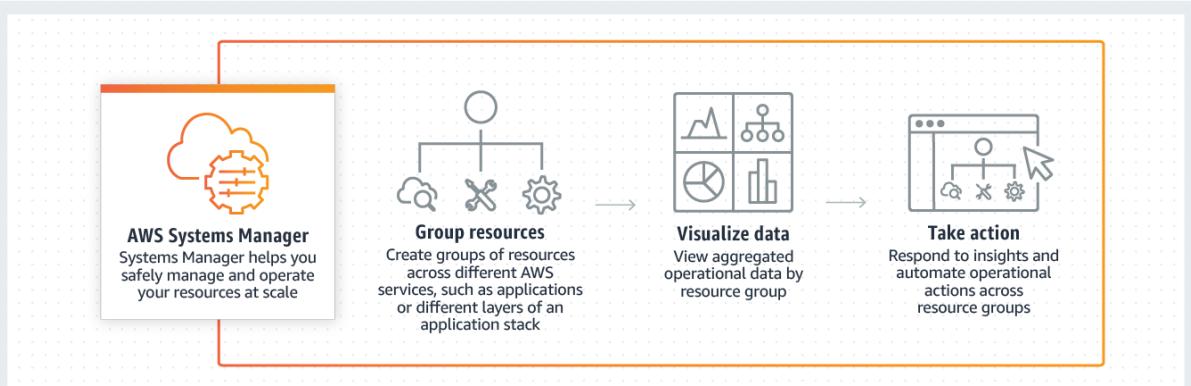
Correct option:

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 19: **Correct**

Adding more CPU/RAM to an Amazon EC2 instance represents which of the following?

- Vertical scaling**
(Correct)
- Managing increasing volumes of data**
- Horizontal scaling**
- 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 20: **Incorrect**

A company is planning to implement Chaos Engineering to expose any blind spots that can disrupt the resiliency of the application.

Which AWS service will help implement this requirement with the least effort?

-

AWS Fault Injection Simulator

(Correct)

-

AWS GuardDuty

(Incorrect)

-

AWS Trusted Advisor

-

Amazon Inspector

Explanation

Correct option:

AWS Fault Injection Simulator

AWS Fault Injection Simulator is a fully managed service for running fault injection experiments on AWS that makes it easier to improve an application's performance, observability, and resiliency. Fault injection experiments are used in chaos engineering, which is the practice of stressing an application in testing or production environments by creating disruptive events, such as a sudden increase in CPU or memory consumption, observing how the system responds, and implementing improvements. Fault injection experiment helps teams create the real-world conditions needed to uncover the hidden bugs, monitoring blind spots, and performance bottlenecks that are difficult to find in distributed systems.

Fault Injection Simulator simplifies the process of setting up and running controlled fault injection experiments across a range of AWS services so teams can build confidence in their application behavior. With Fault Injection Simulator, teams can quickly set up experiments using pre-built templates that generate the desired disruptions. Fault Injection Simulator provides the controls and guardrails that teams need to run experiments in production, such as automatically rolling back or stopping the experiment if specific conditions are met. With a few clicks in the console, teams can run complex scenarios with common distributed system failures happening in parallel or building sequentially over time, enabling them to create the real-world conditions necessary to find hidden weaknesses.

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. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity.

AWS Trusted Advisor - AWS Trusted Advisors provides recommendations that help you follow AWS best practices. Trusted Advisor evaluates your account by using checks. These checks identify ways to optimize your AWS infrastructure, improve security and performance, reduce costs, and monitor service quotas. You can then follow the check recommendations to optimize your services and resources.

AWS GuardDuty - Amazon GuardDuty is a threat detection service that continuously monitors your AWS accounts and workloads for malicious activity and delivers detailed security findings for visibility and remediation.

Reference:

<https://aws.amazon.com/fis/features/>

Question 21: **Incorrect**

The development team at a company manages 300 microservices and it is now trying to automate the code reviews to improve the code quality. Which tool/service is the right fit for this requirement?



AWS X-Ray



Amazon CodeGuru

(Correct)



AWS Trusted Advisor



AWS CodeBuild

(Incorrect)

Explanation

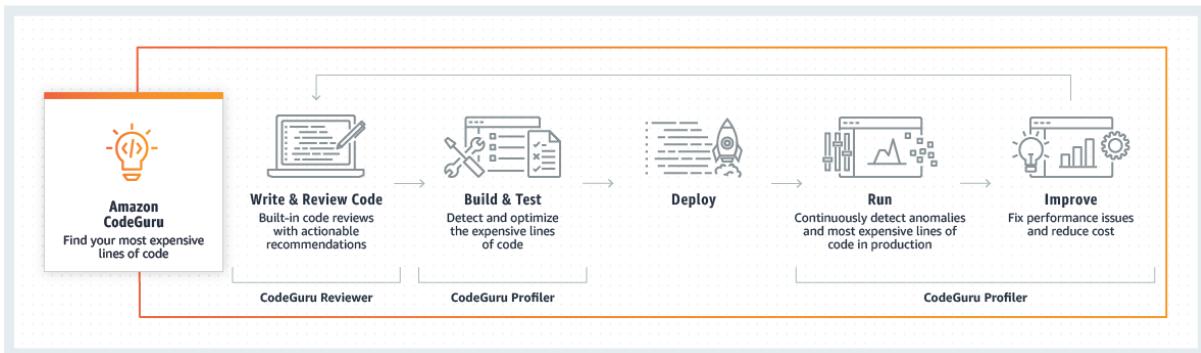
Correct option:

Amazon CodeGuru - Amazon CodeGuru is a developer tool that provides intelligent recommendations to improve code quality and identify an application's most expensive lines of code. Integrate CodeGuru into your existing software development workflow to automate code reviews during application development, continuously monitor application performance in production, provide recommendations and visual clues for improving code quality and application performance, and reduce overall cost.

CodeGuru Reviewer uses machine learning and automated reasoning to identify critical issues, security vulnerabilities, and hard-to-find bugs during application development and provides recommendations to improve code quality.

CodeGuru Profiler pinpoints an application's most expensive lines of code by helping developers understand the runtime behavior of their applications, identify and remove code inefficiencies, improve performance, and significantly decrease compute costs.

How CodeGuru works:



via - <https://aws.amazon.com/codeguru/>

Incorrect options:

AWS X-Ray - AWS X-Ray helps developers analyze and debug production, distributed applications, such as those built using a microservices architecture. With X-Ray, you can understand how your application and its underlying services are performing to identify and troubleshoot the root cause of performance issues and errors. X-Ray provides an end-to-end view of requests as they travel through your application, and shows a map of your application's underlying components.

AWS CodeBuild - AWS CodeBuild is a fully managed continuous integration service that compiles source code, runs tests, and produces software packages that are ready to deploy. With CodeBuild, you don't need to provision, manage, and scale your own build servers. CodeBuild scales continuously and processes multiple builds concurrently, so your builds are not left waiting in a queue.

AWS Trusted Advisor - AWS Trusted Advisors provides recommendations that help you follow AWS best practices. Trusted Advisor evaluates your account by using checks. These checks identify ways to optimize your AWS infrastructure, improve security and performance, reduce costs, and monitor service quotas.

Reference:

<https://aws.amazon.com/codeguru/>

Question 22: **Incorrect**

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?



AWS Quick Starts references

(Correct)



AWS Forums



AWS CodeDeploy

(Incorrect)



AWS Whitepapers

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 23: **Incorrect**

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?

- Elastic Load Balancing (ELB)**
- (Incorrect)**
-
- AWS Lambda**
-
- EBS snapshots**
-
- Amazon Machine Image (AMI)**

(Correct)

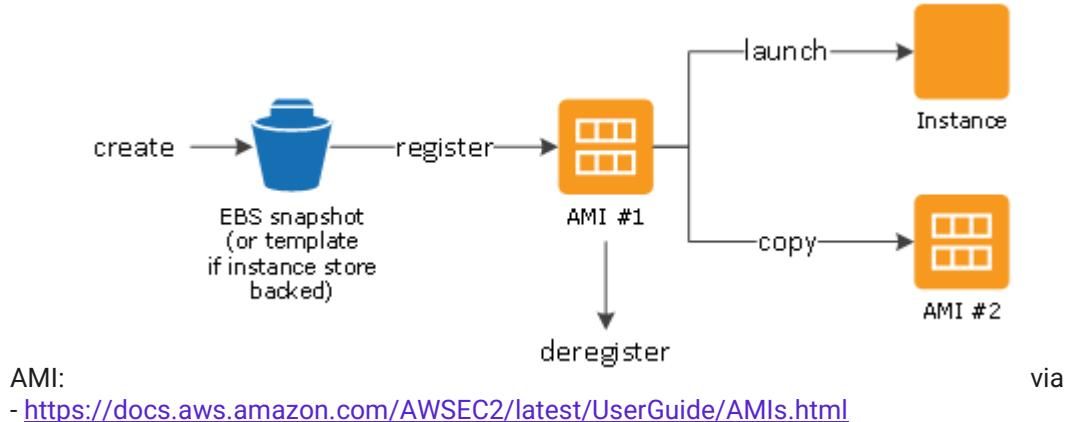
Explanation

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



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 24: **Correct**

Which security control tool can be used to deny traffic from a specific IP address?



Network ACL

(Correct)



VPC Flow Logs



Security Group



AWS GuardDuty

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 25: **Incorrect**

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 Comprehend

(Incorrect)

- ○

Amazon Lex

(Correct)

- ○

Amazon Rekognition

- ○

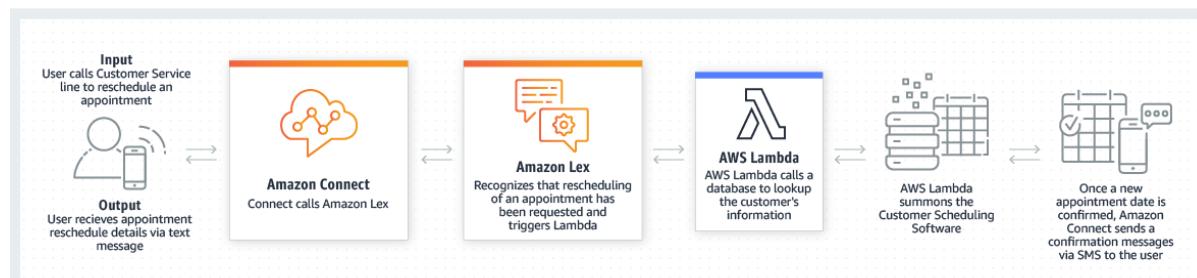
Amazon SageMaker

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 26: **Incorrect**

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?

-

AWS Storage Gateway

-

AWS Snowball

(Incorrect)

-

AWS Snowmobile

(Correct)

-

AWS Snowball Edge

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 27: **Incorrect**

Which of the following AWS services can be used to generate, use, and manage encryption keys on the AWS Cloud?

-

AWS Secrets Manager

(Incorrect)

-

AWS GuardDuty

-

Amazon Inspector

-

AWS CloudHSM

(Correct)

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: 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/cloudhsm/>

Question 28: **Incorrect**

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?

-
-

Standard Reserved Instances

-
-

Scheduled Reserved Instances

(Incorrect)

-
-

Adaptable Reserved Instances

-
-

Convertible Reserved Instances

(Correct)

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 »](#)

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 - AWS does not support Scheduled Reserved Instances, so this option is ruled out.

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 29: **Correct**

Which of the following statements is CORRECT regarding the scope of an Amazon Virtual Private Cloud (VPC)?

-
-
- A VPC spans all Availability Zones (AZs) within a region**
(Correct)
-
- A VPC spans all regions within an Availability Zone (AZ)**
-
- A VPC spans all Availability Zones (AZs) in all regions**
-
- A VPC spans all subnets in all regions**

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 30: **Correct**

Which of the following statements is the MOST accurate when describing AWS Elastic Beanstalk?

-
-

It is a Platform as a Service (PaaS) which allows you to deploy and scale web applications and services

(Correct)

-
-

It is an Infrastructure as a Service (IaaS) which allows you to deploy and scale web applications and services

-
-

It is a Platform as a Service (PaaS) which allows you to model and provision resources needed for an application

-
-

It is an Infrastructure as Code which allows you to model and provision resources needed for an application

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 31: **Incorrect**

Which types of monitoring can be provided by Amazon CloudWatch? (Select TWO)

- **API access**
- **Application performance**
(Correct)
- **Account management**
- **Resource utilization**
(Correct)
- **Performance and availability of AWS services**
(Incorrect)

Explanation

Correct option:

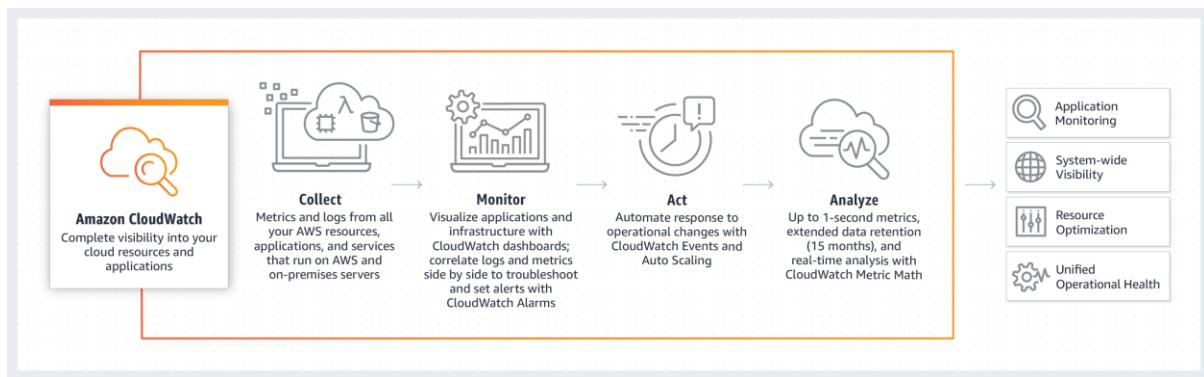
Application performance

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 32: **Incorrect**

Which service/tool will you use to create and provide trusted users with temporary security credentials that can control access to your AWS resources?



Amazon Cognito



AWS Single Sign-On (SSO)



AWS Web Application Firewall (AWS WAF)

(Incorrect)



AWS Security Token Service (AWS STS)

(Correct)

Explanation

Correct option:

AWS Security Token Service (AWS STS) - AWS Security Token Service (AWS STS) is a web service that enables you to request temporary, limited-privilege credentials for AWS Identity and Access Management (IAM) users or for users that you authenticate (federated users).

You can use the AWS Security Token Service (AWS STS) to create and provide trusted users with temporary security credentials that can control access to your AWS resources. Temporary security credentials work almost identically to the long-term access key credentials that your IAM users can use, with the following differences:

1. Temporary security credentials are short-term, as the name implies. They can be configured to last for anywhere from a few minutes to several hours. After the credentials expire, AWS no longer recognizes them or allows any kind of access from API requests made with them.
2. Temporary security credentials are not stored with the user but are generated dynamically and provided to the user when requested. When (or even before) the temporary security credentials expire, the user can request new credentials, as long as the user requesting them still has permissions to do so.

Temporary security credentials are generated by AWS STS. By default, AWS STS is a global service with a single endpoint at <https://sts.amazonaws.com>. However, you can also choose to make AWS STS API calls to endpoints in any other supported Region.

Incorrect options:

Amazon Cognito - Amazon Cognito is a higher level of abstraction than STS. Amazon Cognito supports the same identity providers as AWS STS, and also supports unauthenticated (guest) access, and lets you migrate user data when a user signs in. Amazon Cognito also provides API operations for synchronizing user data so that it is preserved as users move between devices. Cognito helps create the user database, which is not possible with STS.

AWS Single Sign-On (SSO) - AWS Single Sign-On (SSO) makes 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 access and user permissions to all of your accounts in AWS Organizations centrally. AWS SSO configures and maintains all the necessary permissions for your accounts automatically, without requiring any additional setup in the individual accounts.

AWS Web Application Firewall (AWS WAF) - AWS WAF is a web application firewall that helps protect your web applications or APIs against common web exploits and bots that may affect availability, compromise security, or consume excessive resources. AWS WAF gives you control over how traffic reaches your applications by enabling you to create security rules that control bot traffic and block common attack patterns, such as SQL injection or cross-site scripting.

Reference:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp.html

Question 33: **Incorrect**

Which of the following options is NOT a feature of Amazon Inspector?

-

Automate security assessments

-

Inspect running operating systems (OS) against known vulnerabilities

(Incorrect)

-

Analyze against unintended network accessibility

-

Track configuration changes

(Correct)

Explanation

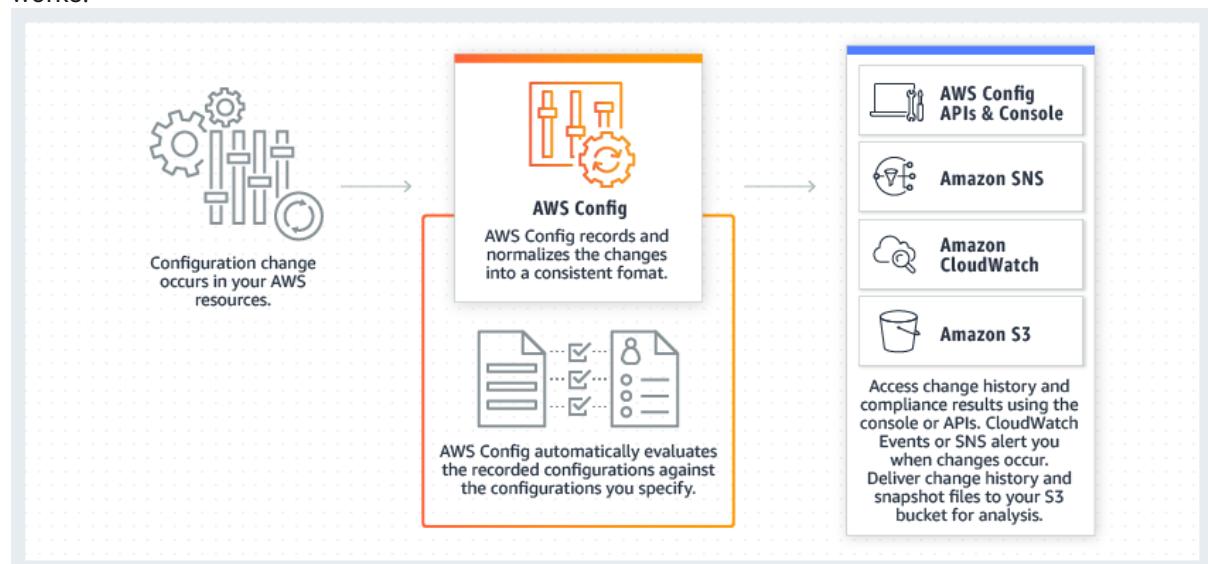
Correct option:

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 34: **Incorrect**

A company needs to use a secure online data transfer tool/service that can automate the ongoing transfers from on-premises systems into AWS while providing support for incremental data backups.

Which AWS tool/service is an optimal fit for this requirement?



AWS Snowcone



AWS Snowmobile

(Incorrect)



AWS DataSync

(Correct)



AWS Storage Gateway

Explanation

Correct option:

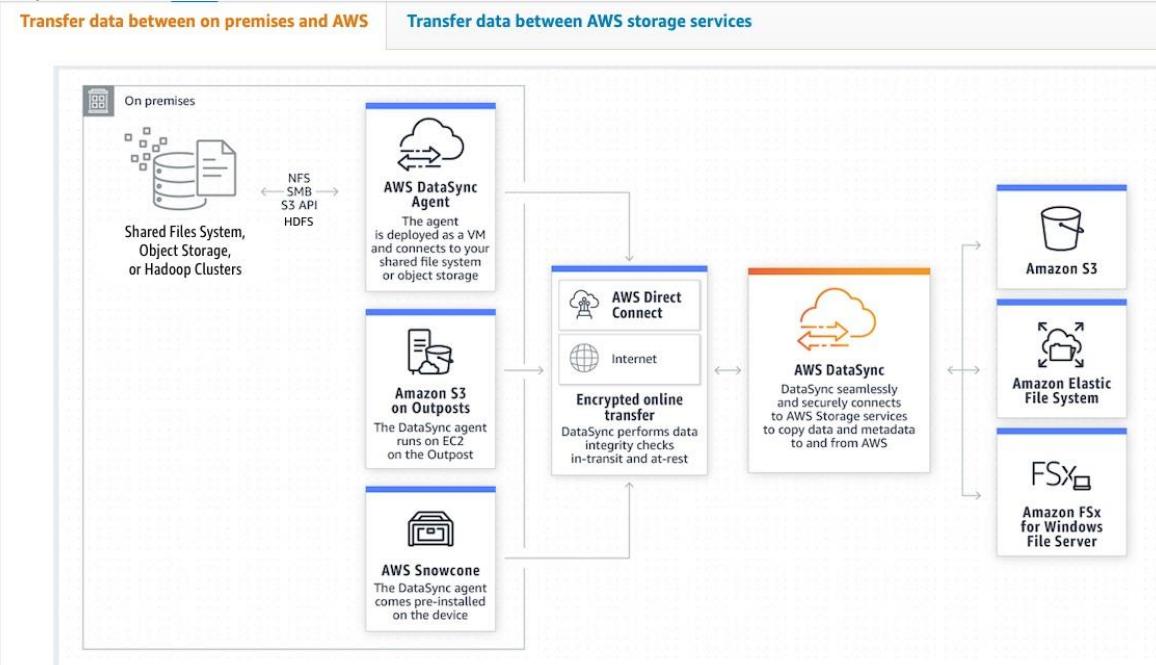
AWS DataSync

AWS DataSync is a secure online data transfer service that simplifies, automates, and accelerates copying terabytes of data to and from AWS storage services. Easily migrate or replicate large data sets without having to build custom solutions or oversee repetitive tasks. DataSync can copy data between Network File System (NFS) shares, or Server Message Block (SMB) shares, self-managed object storage, AWS Snowcone, Amazon Simple Storage Service (Amazon S3) buckets, Amazon Elastic File System (Amazon EFS) file systems, and Amazon FSx for Windows File Server file systems.

You can use AWS DataSync for ongoing transfers from on-premises systems into or out of AWS for processing. DataSync can help speed up your critical hybrid cloud storage workflows in industries that need to move active files into AWS quickly. This includes machine learning in life sciences, video production in media and entertainment, and big data analytics in financial services. DataSync provides timely delivery to ensure dependent processes are not delayed. You can specify exclude filters, include filters, or both, to determine which files, folders or objects get transferred each time your task runs.

AWS DataSync employs an AWS-designed transfer protocol—decoupled from the storage protocol—to accelerate data movement. The protocol performs optimizations on how, when, and what data is sent over the network. Network optimizations performed by DataSync include incremental transfers, in-line compression, and sparse file detection, as well as in-line data validation and encryption.

Data Transfer between on-premises and AWS using DataSync:



via - <https://aws.amazon.com/datasync/>

Incorrect options:

AWS Storage Gateway - AWS Storage Gateway is a set of hybrid cloud services that give you on-premises access to virtually unlimited cloud storage. Customers use Storage Gateway to integrate AWS Cloud storage with existing on-site workloads so they can simplify storage management and reduce costs for key hybrid cloud storage use cases. These include moving backups to the cloud, using on-premises file shares backed by cloud storage, and providing low latency access to data in AWS for on-premises applications.

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.

AWS Snowcone - AWS Snowcone is the smallest member of the AWS Snow Family of edge computing, edge storage, and data transfer devices. Weighing in at 4.5 pounds (2.1 kg), AWS Snowcone is equipped with 8 terabytes of usable storage, while AWS Snowcone Solid State Drive (SSD) supports 14 terabytes of usable storage. Both referred to as Snowcone, the device is ruggedized, secure, and purpose-built for use outside of a traditional data center. Its small form factor makes it a perfect fit for tight spaces or where portability is a necessity and network connectivity is unreliable. You can use Snowcone in backpacks on first responders, or for IoT, vehicular, and drone use cases. You can execute compute applications at the edge, and you can ship the device with data to AWS for offline data transfer, or you can transfer data online with AWS DataSync from edge locations.

References:

<https://aws.amazon.com/datasync/>

<https://aws.amazon.com/datasync/features/>

Question 35: **Incorrect**

Which of the following criteria are used to charge for Elastic Block Store (EBS) volumes? (Select TWO)

-

Provisioned IOPS

(Correct)

-

Data type

-

The EC2 instance type the EBS volume is attached to

(Incorrect)

-

Volume type

(Correct)

-

Data transfer IN

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 36: **Incorrect**

A data science team would like to build Machine Learning models for its projects. Which AWS service can it use?

-
-

Amazon Comprehend

-
-

Amazon Connect

-
-

Amazon Polly

(Incorrect)

-
-

Amazon SageMaker

(Correct)

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 37: **Incorrect**

A growing start-up has trouble identifying and protecting sensitive data at scale. Which AWS fully managed service can assist with this task?

-
-

AWS Secrets Manager

(Incorrect)

-
-

AWS KMS

-
-

AWS Artifact

-
-

Amazon Macie

(Correct)

Explanation

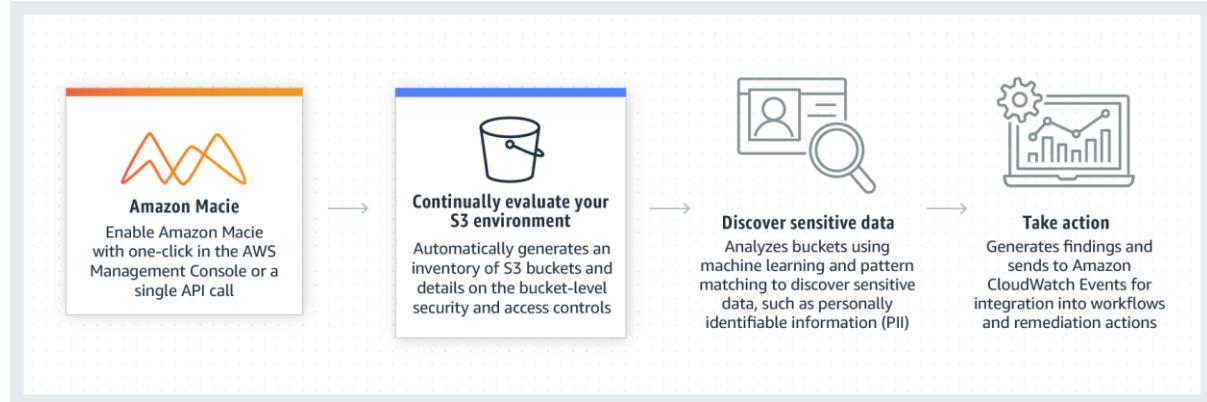
Correct option:

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 38: **Correct**

According to the Shared Responsibility Model, which of the following are responsibilities of AWS? (Select two)

-

Encrypting application data

-

Configuring IAM Roles

- -
- Installing security patches of the guest operating system (OS)**
-
- Network operability**
- (Correct)**
-

Data center security

(Correct)

Explanation

Correct option:

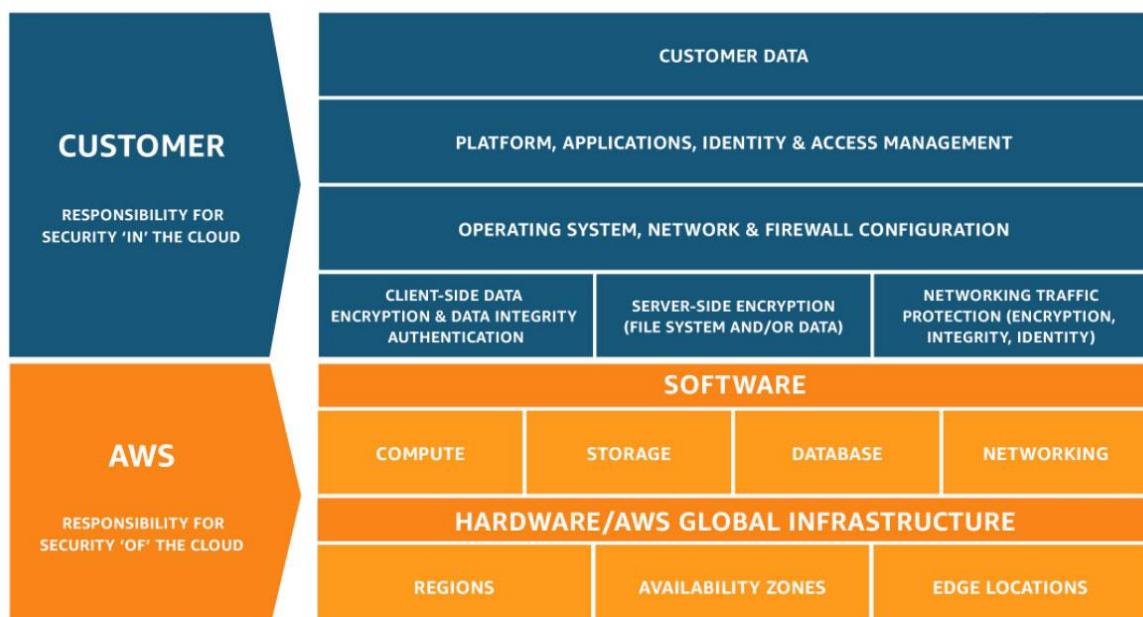
Data center security

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 39: **Incorrect**

Which AWS tool/service will help you define your cloud infrastructure using popular programming languages such as Python and JavaScript?



AWS Cloud Development Kit (CDK)

(Correct)



AWS CodeBuild



AWS CloudFormation



AWS Elastic Beanstalk

(Incorrect)

Explanation

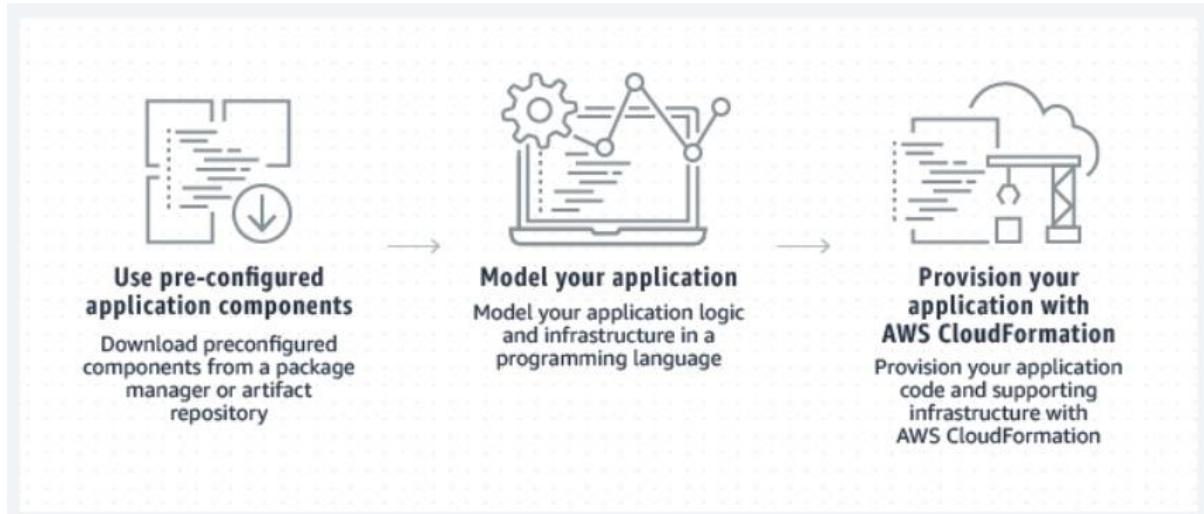
Correct option:

AWS Cloud Development Kit (CDK) - The AWS Cloud Development Kit (AWS CDK) is an open-source software development framework to define your cloud application resources using familiar programming languages.

AWS CDK uses the familiarity and expressive power of programming languages for modeling your applications. It provides you with high-level components called constructs that preconfigure cloud resources with proven defaults, so you can build cloud applications without needing to be an expert. AWS CDK provisions your resources in a safe, repeatable manner through AWS CloudFormation. It also enables you to compose and share your own custom constructs that incorporate your organization's requirements, helping you start new projects faster.

In short, you use the AWS CDK framework to author AWS CDK projects which are executed to generate CloudFormation templates.

How CDK works:



via - <https://aws.amazon.com/cdk/>

Incorrect options:

AWS Elastic Beanstalk - AWS Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services developed with Java, .NET, PHP, Node.js, Python etc. You can simply upload your code in a programming language of your choice and Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring.

AWS CloudFormation - AWS CloudFormation is a service that gives developers and businesses an easy way to create a collection of related AWS and third-party resources, and provision and manage them in an orderly and predictable fashion. AWS CloudFormation is designed to allow resource lifecycles to be managed repeatably, predictable, and safely, while allowing for automatic rollbacks, automated state management, and management of resources across accounts and regions. AWS CDK helps code the same in higher-level languages and converts them into CloudFormation templates.

AWS CodeBuild - AWS CodeBuild is a fully managed continuous integration service that compiles source code, runs tests, and produces software packages that are ready to deploy. With CodeBuild, you don't need to provision, manage, and scale your own build servers. CodeBuild scales continuously and processes multiple builds concurrently, so your builds are not left waiting in a queue.

Reference:

<https://aws.amazon.com/cdk/>

Question 40: **Incorrect**

A media company wants to enable customized content suggestions for the users of its movies streaming platform. Which AWS service can provide these personalized recommendations based on the historic data?



Amazon SageMaker



Amazon Customize

(Incorrect)



Amazon Personalize

(Correct)



Amazon Comprehend

Explanation

Correct option:

Amazon Personalize - Amazon Personalize enables developers to build applications with the same machine learning (ML) technology used by Amazon.com for real-time personalized recommendations. Amazon Personalize can be used to personalize the end-user experience over any digital channel. Examples include product recommendations for e-commerce, news articles and content recommendation for publishing, media and social networks, hotel recommendations for travel websites, credit card recommendations for banks, and match recommendations for dating sites. These recommendations and personalized experiences can be delivered over websites, mobile apps, or email/messaging. Amazon Personalize can also be used to customize the user experience when user interaction is over a physical channel, e.g., a meal delivery company could personalize weekly meals to users in a subscription plan.

Amazon Personalize supports the following key use cases:

1. Personalized recommendations
2. Similar items
3. Personalized reranking i.e. rerank a list of items for a user
4. Personalized promotions/notifications

Incorrect options:

Amazon SageMaker - Amazon SageMaker is a fully managed service that provides every developer and data scientist with the ability to build, train, and deploy machine learning (ML) models quickly.

SageMaker removes the heavy lifting from each step of the machine learning process to make it easier to develop high-quality models.

Amazon Customize - There is no such service as Amazon Customize. This option has been added as a distractor.

Amazon Comprehend - Amazon Comprehend is a natural-language processing (NLP) service that uses machine learning to uncover information in unstructured data. Instead of combing through documents, the process is simplified and unseen information is easier to understand.

The service can identify critical elements in data, including references to language, people, and places, and the text files can be categorized by relevant topics. In real-time, you can automatically and accurately detect customer sentiment in your content.

Reference:

<https://aws.amazon.com/personalize/>

Question 41: **Incorrect**

Which AWS tool can provide best practice recommendations for performance, service limits, and cost optimization?

-
- Amazon Inspector**
-
- AWS Trusted Advisor**
- (Correct)**
-
- Amazon CloudWatch**
-
- AWS Service Health Dashboard**
- (Incorrect)**

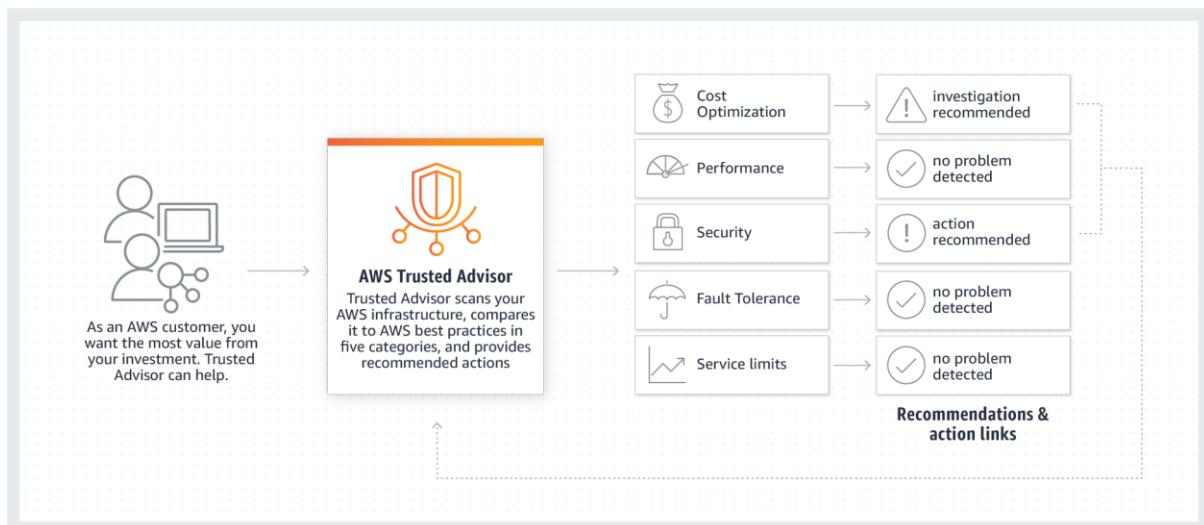
Explanation

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 42: **Incorrect**

According to the Shared Responsibility Model, which of the following is both the responsibility of AWS and the customer? (Select two)

-

Configuration management

(Correct)

-

Operating system (OS) configuration

(Correct)

-

Customer data

(Incorrect)

-

Disposal of disk drives

-

Data center security

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.

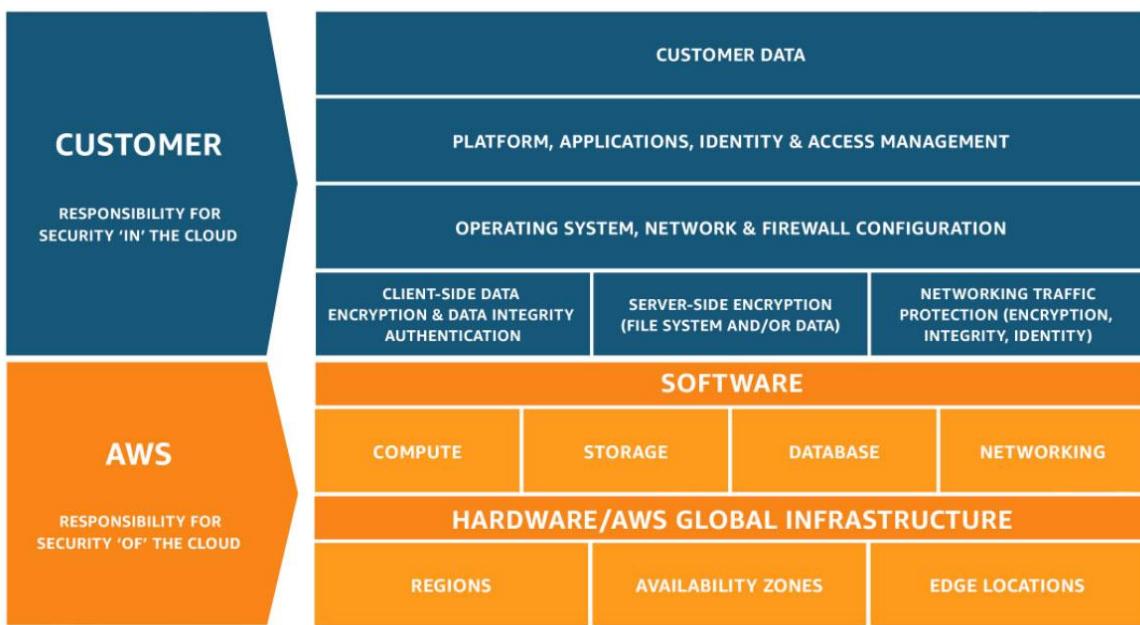
Operating system (OS) configuration

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.

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

Data center security

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 as well as data center security.

Reference:

<https://aws.amazon.com/compliance/shared-responsibility-model/>

Question 43: **Correct**

According to the Well-Architected Framework, which of the following action is recommended in the Security pillar?

-
- Use Amazon CloudWatch to measure overall efficiency**
-
- Use AWS Cost Explorer to view and track your usage in detail**
-
- Use AWS CloudFormation to automate security best practices**



Use AWS KMS to encrypt data

(Correct)

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 six pillars – Operational Excellence, Security, Reliability, Performance Efficiency, Cost Optimization and Sustainability.

Overview of the six pillars of the Well-Architected Framework:

AWS Well-Architected and the Six Pillars

Framework Overview

The AWS Well-Architected Framework describes key concepts, design principles, and architectural best practices for designing and running workloads in the cloud. By answering a few foundational questions, learn how well your architecture aligns with cloud best practices and gain guidance for making improvements.

[HTML](#) | [Kindle](#) | [Labs](#)



Operational Excellence Pillar The operational excellence pillar focuses on running and monitoring systems, and continually improving processes and procedures. Key topics include automating changes, responding to events, and defining standards to manage daily operations. HTML Kindle Labs	Security Pillar The security pillar focuses on protecting information and systems. Key topics include confidentiality and integrity of data, managing user permissions, and establishing controls to detect security events. HTML Kindle Labs	Reliability Pillar The reliability pillar focuses on workloads performing their intended functions and how to recover quickly from failure to meet demands. Key topics include distributed system design, recovery planning, and adapting to changing requirements. HTML Kindle Labs
Performance Efficiency Pillar The performance efficiency pillar focuses on structured and streamlined allocation of IT and computing resources. Key topics include selecting resource types and sizes optimized for workload requirements, monitoring performance, and maintaining efficiency as business needs evolve. HTML Kindle Labs	Cost Optimization Pillar The cost optimization pillar focuses on avoiding unnecessary costs. Key topics include understanding spending over time and controlling fund allocation, selecting resources of the right type and quantity, and scaling to meet business needs without overspending. HTML Kindle Labs	Sustainability Pillar The sustainability pillar focuses on minimizing the environmental impacts of running cloud workloads. Key topics include a shared responsibility model for sustainability, understanding impact, and maximizing utilization to minimize required resources and reduce downstream impacts. HTML Kindle Labs

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 44: **Correct**

Which of the following billing timeframes is applied when running a Windows EC2 on-demand instance?



Pay per day



Pay per minute



Pay per hour



Pay per second

(Correct)

Explanation

Correct option:

Pay per second

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 second pricing is applied.

Incorrect options:

Pay per hour - When running a Windows EC2 on-demand instance, pay per second pricing is applied. Windows based EC2 instances used to follow pay-per-hour pricing earlier.

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 45: **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?

-
- AWS Batch**
-
- AWS OpsWorks**
-
- AWS CodeDeploy**
-
- AWS CloudFormation**

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 46: **Incorrect**

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?



Platform as a Service (PaaS)

(Correct)



Software as a Service (SaaS)



On-premises



Infrastructure as a Service (IaaS)

(Incorrect)

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 47: **Correct**

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?

-
-

AWS Single Sign-On (SSO)

(Correct)

-
-

AWS Cognito

- ○ **AWS Command Line Interface (CLI)**
- ○ **AWS Identity and Access Management (IAM)**

Explanation

Correct option:

AWS Single Sign-On (SSO)

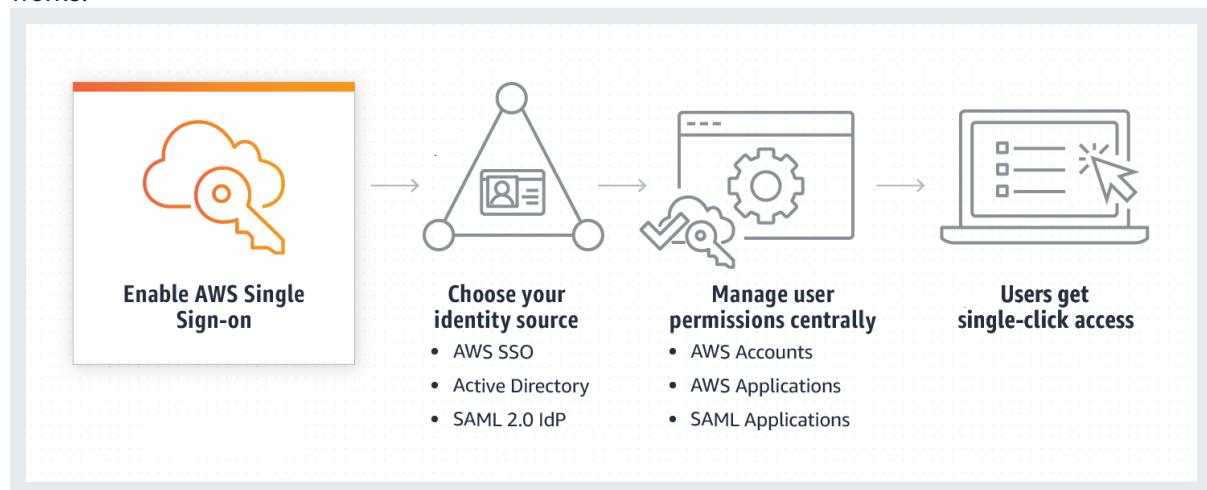
AWS SSO is an AWS service that enables you to make it easy to centrally manage access to multiple AWS accounts and business applications and provide users with single sign-on access to all their assigned accounts and applications from one place.

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 48: **Incorrect**

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?



AWS CloudFormation

(Correct)



AWS CodeDeploy

(Incorrect)



AWS Directory Service



Amazon LightSail

Explanation

Correct option:

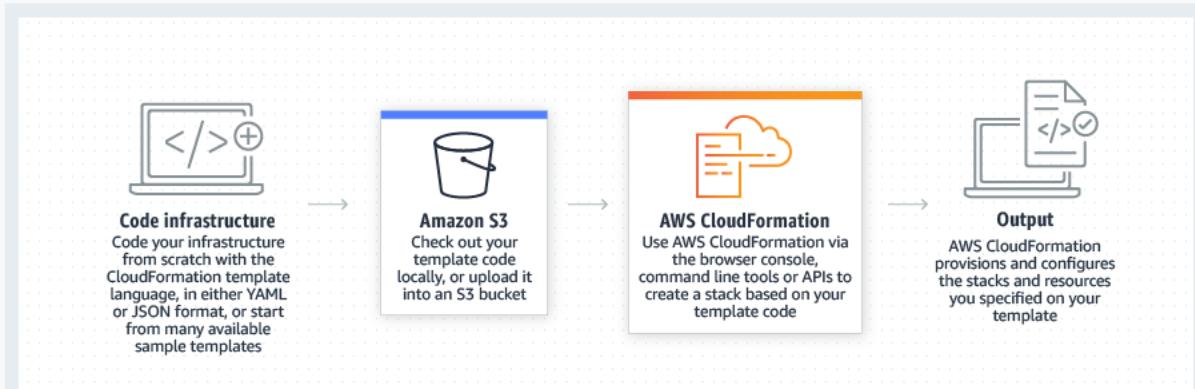
AWS CloudFormation

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 49: **Incorrect**

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?

-

Amazon Inspector

(Incorrect)

-

AWS Config

(Correct)

-

AWS Secrets Manager



AWS Trusted Advisor

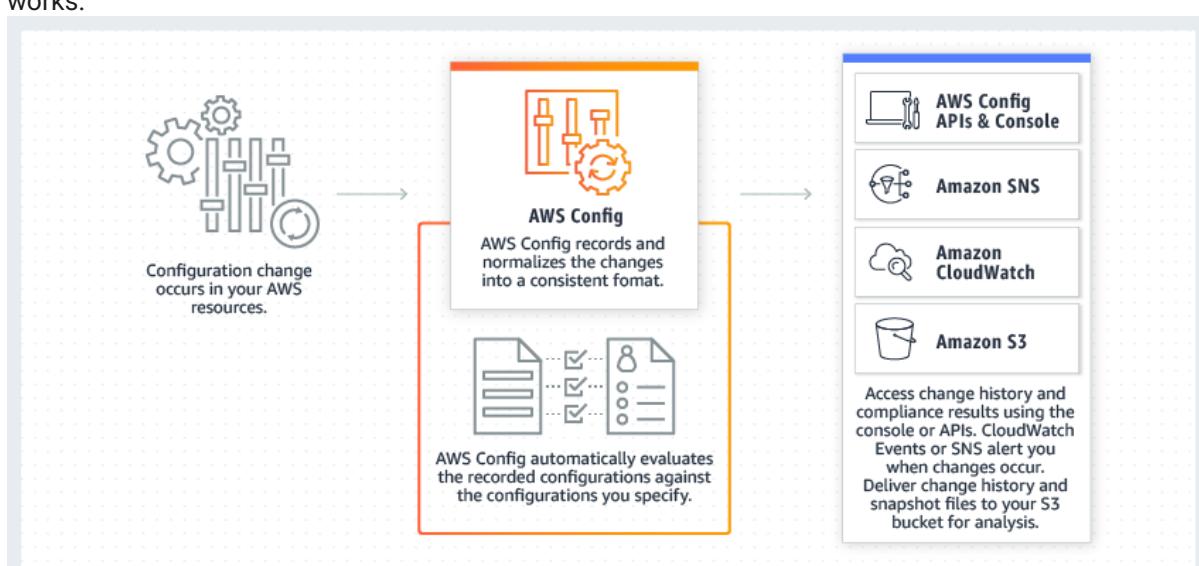
Explanation

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 50: **Correct**

Which of the following are the best practices when using AWS Organizations? (Select TWO)

-

Do not use AWS Organizations to automate AWS account creation

-

Create accounts per department

(Correct)

-

Disable CloudTrail on several accounts

-

Restrict account privileges using Service Control Policies (SCP)

(Correct)

-

Never use tags for billing

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 51: **Incorrect**

Which of the following AWS Support plans is the MOST cost-effective when getting enhanced technical support by Cloud Support Engineers?

-
-

Developer

(Incorrect)

-
-

Enterprise

-
-

Business

(Correct)

-
-

Basic

Explanation

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:

	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	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

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
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*** Greater of \$29 / month*** - or - 3% of monthly AWS usage See pricing detail and example.	Greater of \$100 / month*** 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 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 52: **Correct**

Which AWS service can be used to subscribe to an RSS feed to be notified of the status of all AWS service interruptions?

AWS Service Health Dashboard

(Correct)

AWS Personal Health Dashboard

AWS Lambda

Amazon SNS

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:

The screenshot shows the AWS Service Health Dashboard interface. At the top, there's a navigation bar with the AWS logo and the text "SERVICE HEALTH DASHBOARD". Below the navigation bar, a breadcrumb trail says "Amazon Web Services » Service Health Dashboard". A sub-header reads "Get a personalized view of AWS service health". A prominent orange button labeled "Open the Personal Health Dashboard" is visible. The main content area is titled "Current Status - Jun 2, 2020 PDT". It includes a note about staying updated on service availability and submitting issues via "Contact Us". Below this, there's a table with tabs for "North America", "South America", "Europe", "Africa", "Asia Pacific", and "Middle East". The "North America" tab is selected. The table has three columns: "Recent Events", "Details", and "RSS". Under "Recent Events", it says "No recent events." Under "Remaining Services", there's a list of services with their status and RSS feeds:

Region	Service	Status	RSS
North America	Alexa for Business (N. Virginia)	Service is operating normally	
North America	Amazon API Gateway (Montreal)	Service is operating normally	
North America	Amazon API Gateway (N. California)	Service is operating normally	
North America	Amazon API Gateway (N. Virginia)	Service is operating normally	
North America	Amazon API Gateway (Ohio)	Service is operating normally	
North America	Amazon API Gateway (Oregon)	Service is operating normally	
North America	Amazon AppStream 2.0 (N. Virginia)	Service is operating normally	
North America	Amazon AppStream 2.0 (Oregon)	Service is operating normally	
North America	Amazon Athena (Montreal)	Service is operating normally	
North America	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.

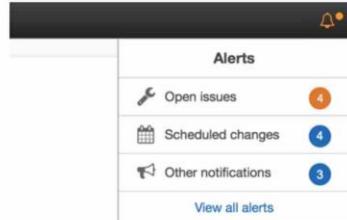
AWS Personal Health Dashboard - AWS Personal Health Dashboard provides alerts and remediation guidance when AWS is experiencing events that may impact you. It does not provide updates about the general status for all AWS services.

AWS Personal Health Dashboard Overview:

Technology & Tools To Monitor, Manage, and Optimize Your AWS Environment

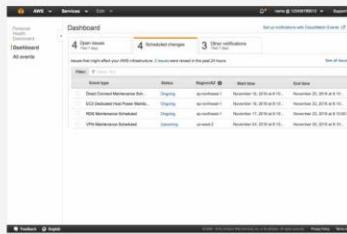
AWS Personal Health Dashboard provides alerts and remediation guidance when AWS is experiencing events that may impact you. While the Service Health Dashboard displays the general status of AWS services, Personal Health Dashboard gives you a personalized view into the performance and availability of 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 all AWS services' status.

Reference:

<https://status.aws.amazon.com/>

Question 53: **Incorrect**

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?

-

Amazon EMR

(Incorrect)

-

Amazon Relational Database Service (RDS)

-

Amazon ElastiCache

(Correct)



AWS Glue

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 54: **Correct**

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?



AWS Batch

(Correct)



Amazon Lightsail



AWS Lambda



AWS Fargate

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.

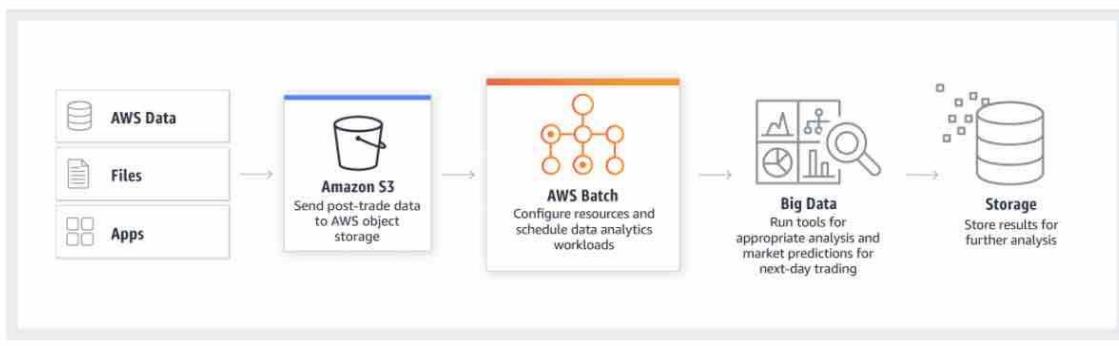
You can use AWS Batch to plan, schedule, and execute your batch computing workloads across the full range of AWS compute services. AWS Batch dynamically provisions the optimal quantity and type of compute resources (e.g., CPU or memory optimized instances) based on the volume and specific resource requirements 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

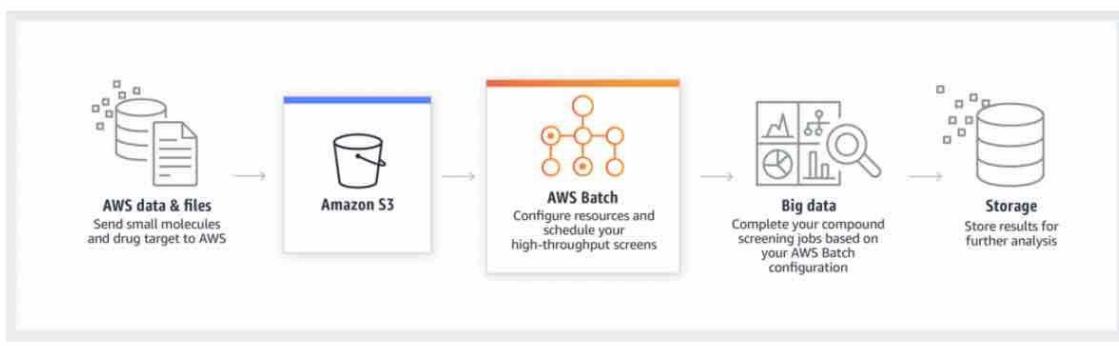
Financial services: Post-trade analytics

Automate the analysis of the day's transaction costs, execution reporting, and market performance.



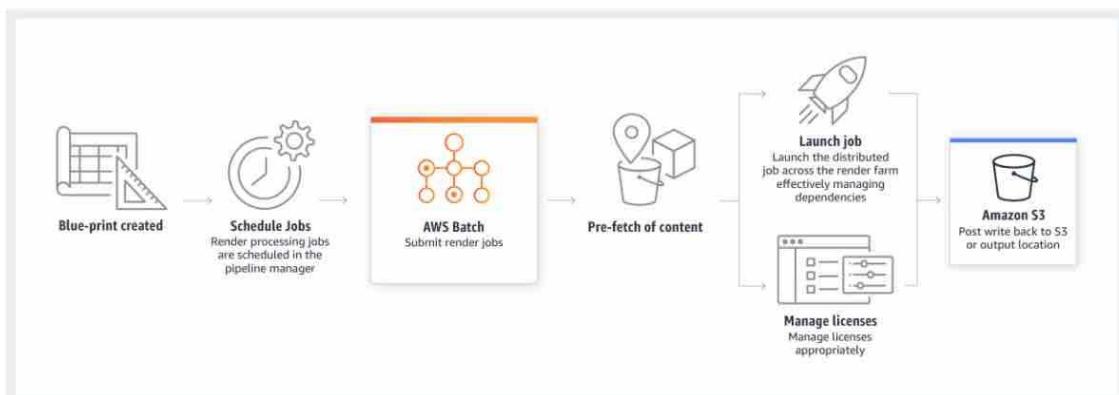
Life sciences: Drug screening for biopharma

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 55: **Incorrect**

Which of the following statements is INCORRECT regarding EBS Volumes?

-

EBS Volumes can persist data after their termination

-

EBS Volumes can be bound to several Availability Zones (AZs)

(Correct)

-

EBS Volumes are bound to a specific Availability Zone (AZ)

-

EBS Volumes can be mounted to one instance at a time

(Incorrect)

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 56: **Incorrect**

Which AWS service allows you to quickly and easily add user sign-up, sign-in, and access control to web and mobile applications?



AWS Single Sign-On (SSO)

(Incorrect)



AWS Organizations



AWS Identity and Access Management (IAM)



Amazon Cognito

(Correct)

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 57: **Incorrect**

Which AWS service can inspect CloudFront distributions running on any HTTP web-server?



AWS WAF

(Correct)



Amazon Inspector



AWS GuardDuty

(Incorrect)



AWS Elastic Load Balancer

Explanation

Correct option:

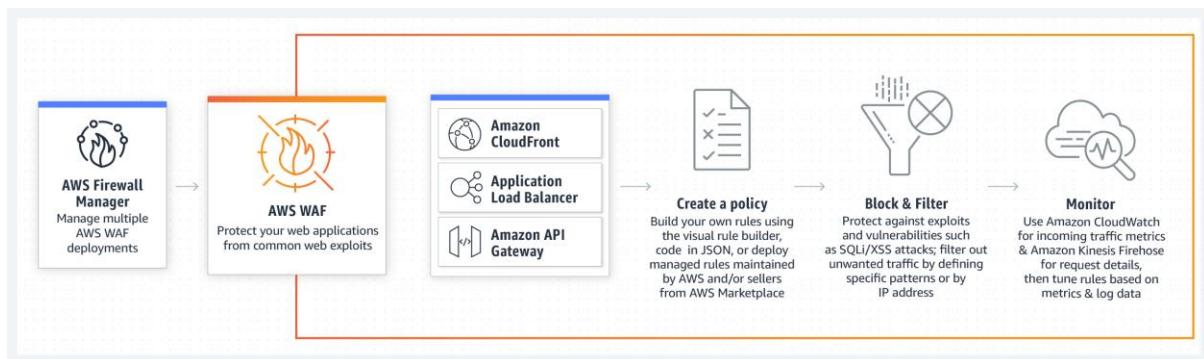
AWS WAF

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.

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.

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 58: **Incorrect**

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?



On-premises



Private Cloud

(Incorrect)



Hybrid Cloud

(Correct)



Public Cloud

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 59: **Incorrect**

Which of the following IAM Security Tools allows you to review permissions granted to a user?

- IAM access advisor**
(Correct)
-
- IAM policies**
- Multi-Factor Authentication (MFA)**
(Incorrect)
-

IAM credentials report

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. To summarize, you can identify unnecessary permissions so that you can revise your IAM policies accordingly.

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 60: **Correct**

Which of the following statements is an AWS best practice when architecting for the Cloud?

-

Security comes last

-

Servers, not services

-

Automation

(Correct)

-

Close coupling

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 61: **Incorrect**

Which AWS service can be used to view the most comprehensive billing details for the past month?

-

AWS Budgets

-

AWS Cost Explorer

-

AWS Pricing Calculator

(Incorrect)

-

AWS Cost and Usage Reports

(Correct)

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 granular billing details for the past month.

AWS Pricing Calculator - AWS Pricing Calculator lets you explore AWS services and create an estimate for the cost of your use cases on AWS. You can model your solutions before building them, explore the price points and calculations behind your estimate, and find the available instance types and contract terms that meet your needs. This enables you to make informed decisions about using AWS. You can plan your AWS costs and usage or price out setting up a new set of instances and services. AWS Pricing Calculator cannot provide billing details for the past month.

Exam Alert:

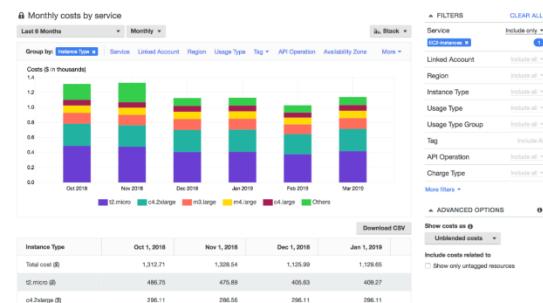
Please review the differences between "AWS Cost and Usage Reports" and "AWS Cost Explorer". Think of "AWS Cost and Usage Reports" as a cost management tool providing the most detailed cost and usage data for your AWS account. It can provide reports that break down your costs by the hour into your S3 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.

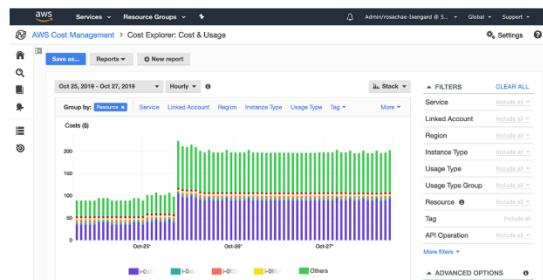
[Launch the Monthly Costs by AWS Service report »](#)



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 62: Incorrect

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?

- A security group
 - A virtual private gateway
 - A customer gateway
 - (Correct)
 - A VPC endpoint interface
 - (Incorrect)

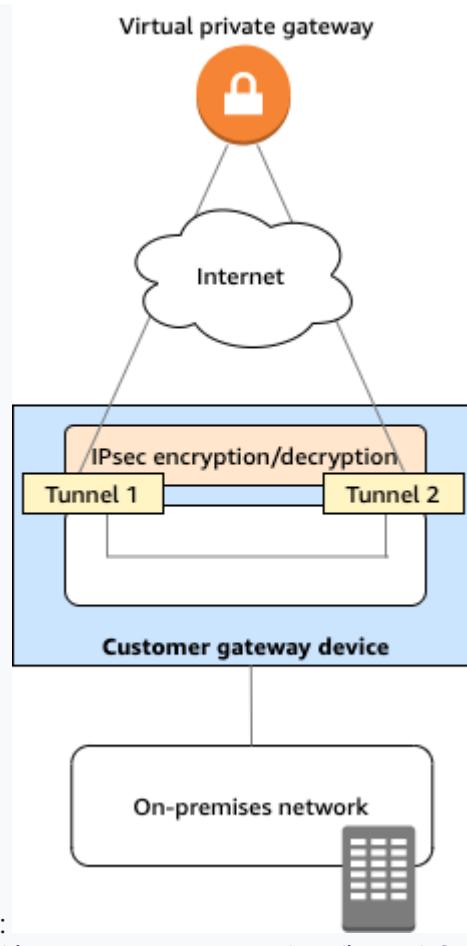
Explanation

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

Question 63:

Skipped

According to the Well-Architected Framework, which of the following statements are recommendations in the Operational Excellence pillar? (Select two)

- **Enable traceability**
- **Automatically recover from failure**
- **Use serverless architectures**
- **Anticipate failure**
(Correct)
- **Make frequent, small, reversible changes**
(Correct)

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 six pillars – Operational Excellence, Security, Reliability, Performance Efficiency, Cost Optimization and Sustainability.

Overview of the six pillars of the Well-Architected Framework:

AWS Well-Architected and the Six Pillars

Framework Overview

The AWS Well-Architected Framework describes key concepts, design principles, and architectural best practices for designing and running workloads in the cloud. By answering a few foundational questions, learn how well your architecture aligns with cloud best practices and gain guidance for making improvements.

[HTML](#) | [Kindle](#) | [Labs](#)



Operational Excellence Pillar	Security Pillar	Reliability Pillar
<p>The operational excellence pillar focuses on running and monitoring systems, and continually improving processes and procedures. Key topics include automating changes, responding to events, and defining standards to manage daily operations.</p> <p>HTML Kindle Labs</p>	<p>The security pillar focuses on protecting information and systems. Key topics include confidentiality and integrity of data, managing user permissions, and establishing controls to detect security events.</p> <p>HTML Kindle Labs</p>	<p>The reliability pillar focuses on workloads performing their intended functions and how to recover quickly from failure to meet demands. Key topics include distributed system design, recovery planning, and adapting to changing requirements.</p> <p>HTML Kindle Labs</p>
Performance Efficiency Pillar	Cost Optimization Pillar	Sustainability Pillar
<p>The performance efficiency pillar focuses on structured and streamlined allocation of IT and computing resources. Key topics include selecting resource types and sizes optimized for workload requirements, monitoring performance, and maintaining efficiency as business needs evolve.</p>	<p>The cost optimization pillar focuses on avoiding unnecessary costs. Key topics include understanding spending over time and controlling fund allocation, selecting resources of the right type and quantity, and scaling to meet business needs without overspending.</p>	<p>The sustainability pillar focuses on minimizing the environmental impacts of running cloud workloads. Key topics include a shared responsibility model for sustainability, understanding impact, and maximizing utilization to minimize required resources and reduce downstream impacts.</p>

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 64: **Incorrect**

Which of the following services are provided by Amazon Route 53? (Select TWO)

-

Health checks and monitoring

(Correct)

-

IP routing

(Incorrect)

-

Domain registration

(Correct)

-

Transfer acceleration

-

Load balancing

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 65: **Correct**

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?

-
-

Site-to-Site VPN

-
-

Direct Connect

(Correct)

-
-

VPC Endpoints

-
-

VPC Peering

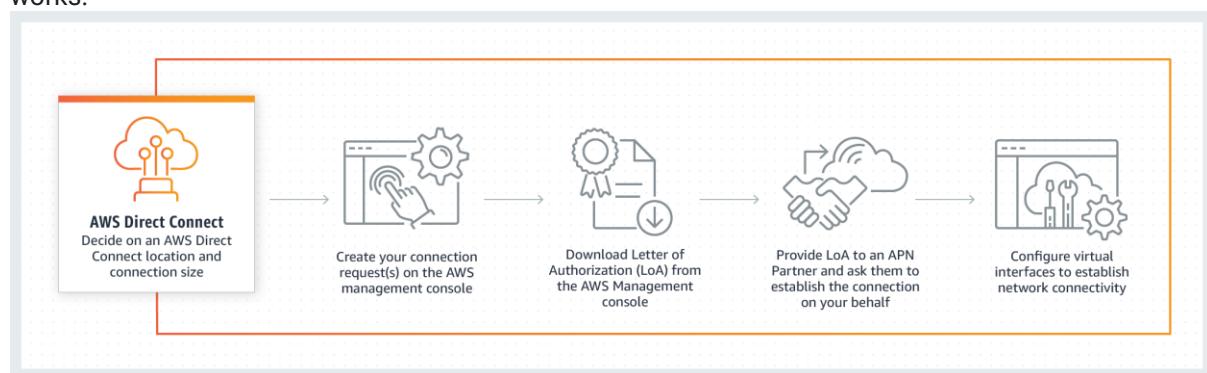
Explanation

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/>

Practice Test #6 - AWS Certified Cloud Practitioner - Results

Return to review

Chart

Pie chart with 3 slices.

End of interactive chart.

Attempt 1

All knowledge areas

All questions

Question 1: **Incorrect**

A healthcare company wants to implement a continuous replication based disaster recovery mechanism and provide fast, reliable recovery of physical, virtual, and cloud-based servers into AWS Cloud. Which of the following represents the best-fit solution for this use case?

-

AWS Storage Gateway

(Incorrect)

-

AWS Snowball Edge

-

CloudCover Disaster Recovery

-

CloudEndure Disaster Recovery

(Correct)

Explanation

Correct option:

CloudEndure Disaster Recovery - CloudEndure Disaster Recovery, available from the AWS Marketplace, continuously replicates server-hosted applications and server-hosted databases from any source into AWS using block-level replication of the underlying server. CloudEndure Disaster Recovery enables you to use AWS Cloud as a disaster recovery Region for an on-premises workload and its environment. It can also be used for disaster recovery of AWS hosted workloads if they consist only of applications and databases hosted on EC2 (i.e. not RDS).

Features of CloudEndure Disaster Recovery:

1. Continuous replication: CloudEndure Disaster Recovery provides continuous, asynchronous, block-level replication of your source machines into a staging area. This allows you to achieve sub-second Recovery Point Objectives (RPOs), since up-to-date applications are always ready to be spun up on AWS if a disaster strikes.
2. Low-cost staging area: Data is continually kept in sync in a lightweight staging area in your target AWS Region. The staging area contains low-cost resources that are automatically provisioned and managed by CloudEndure Disaster Recovery. This eliminates the need for duplicate resources and significantly reduces your disaster recovery total cost of ownership (TCO).
3. Automated machine conversion and orchestration: In the event of a disaster or drill, CloudEndure Disaster Recovery triggers a highly automated machine conversion process and a scalable orchestration engine that quickly spins up thousands of machines in your target AWS Region in parallel. This enables Recovery Time Objectives (RTOs) of minutes. Unlike application-level solutions, CloudEndure Disaster Recovery replicates entire machines, including OS, system state configuration, system disks, databases, applications, and files.
4. Point-in-time recovery: Granular point-in-time recovery allows you to recover applications and IT environments that have been corrupted as a result of accidental system changes, ransomware, or other malicious attacks. In such cases, you can launch applications from a previous consistent point in time rather than launching applications in their most up-to-date state. During the recovery, you can select either the latest state or an earlier state from a list of points in time.
5. Easy, non-disruptive drills: With CloudEndure Disaster Recovery, you can conduct disaster recovery drills without disrupting your source environment or risking data loss. During drills, CloudEndure Disaster Recovery spins up machines in your target AWS Region in complete isolation to avoid network conflicts and performance impact.
6. Wide application and infrastructure support: Because CloudEndure Disaster Recovery replicates data at the block level, you can use it for all applications and databases that run on supported versions of Windows and Linux OS.

CloudEndure Disaster

Recovery:

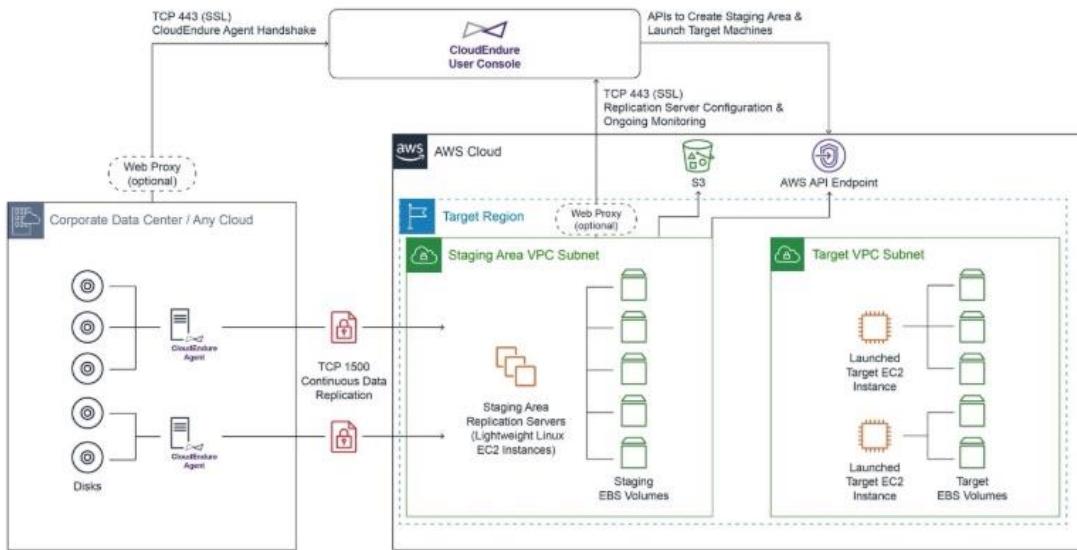


Figure 10 - CloudEndure Disaster Recovery architecture

via - <https://docs.aws.amazon.com/whitepapers/latest/disaster-recovery-workloads-on-aws/disaster-recovery-options-in-the-cloud.html>

Incorrect options:

AWS Snowball Edge - AWS Snowball Edge is a type of Snowball device with on-board storage and compute power for select AWS capabilities. Snowball Edge can do local processing and edge-computing workloads in addition to transferring data between your local environment and the AWS Cloud. Snowball edge cannot be used to optimize connections through mobile networks. It cannot be used for continuous replication based disaster recovery.

AWS Storage Gateway - AWS Storage Gateway is a hybrid cloud storage service that gives you on-premises access to virtually unlimited cloud storage. Storage Gateway provides a standard set of storage protocols such as iSCSI, SMB, and NFS, which allow you to use AWS storage without rewriting your existing applications. You can take point-in-time snapshots of your Volume Gateway volumes in the form of Amazon EBS snapshots. Using this approach, you can easily supply data from your on-premises applications to your applications running on Amazon EC2 if you require additional on-demand compute capacity for data processing or replacement capacity for disaster recovery purposes. However, Storage Gateways cannot be used for continuous replication based disaster recovery.

CloudCover Disaster Recovery - This is a made-up option and has been added as a distractor.

References:

<https://docs.aws.amazon.com/whitepapers/latest/disaster-recovery-workloads-on-aws/disaster-recovery-options-in-the-cloud.html>

Question 2: **Incorrect**

Which of the following are NoSQL database services from AWS? (Select two)

-
-

Amazon RDS

(Incorrect)

-

Amazon Aurora

(Incorrect)

-

Amazon DocumentDB

(Correct)

-

AWS Storage Gateway

-

Amazon Neptune

(Correct)

Explanation

Correct options:

Amazon Neptune - A graph database's purpose is to make it easy to build and run applications that work with highly connected datasets. Typical use cases for a graph database include social networking, recommendation engines, fraud detection, and knowledge graphs. Amazon Neptune is a fully-managed graph database service and it's also considered as a type of NoSQL database.

Amazon DocumentDB - In application code, data is represented often as an object or JSON-like document because it is an efficient and intuitive data model for developers. Document databases make it easier for developers to store and query data in a database by using the same document model format that they use in their application code. Amazon DocumentDB (with MongoDB compatibility) and MongoDB are popular document databases that provide powerful and intuitive APIs for flexible and iterative development.

Incorrect options:

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.

Amazon Aurora - Amazon Aurora is a MySQL and PostgreSQL-compatible relational database built for the cloud, that combines the performance and availability of traditional enterprise databases with the simplicity and cost-effectiveness of open source databases. Amazon Aurora is fully managed by Amazon Relational Database Service (RDS), which automates time-consuming administration tasks like hardware provisioning, database setup, patching, and backups.

AWS Storage Gateway - AWS Storage Gateway is a hybrid cloud storage service that gives you on-premises access to virtually unlimited cloud storage. Customers use Storage Gateway to simplify storage management and reduce costs for key hybrid cloud storage use cases. These include moving backups to the cloud, using on-premises file shares backed by cloud storage, and providing low latency access to data in AWS for on-premises applications. It is not a database service.

Reference:

<https://aws.amazon.com/nosql/>

Question 3: **Incorrect**

Which of the following are security best practices suggested by AWS for Identity and Access Management (IAM)? (Select two)

-

Do not change passwords and access keys once created. This results in failure of connectivity in the application logic

-

Enable AWS multi-factor authentication (MFA) on your AWS root user account. MFA helps give root access to multiple users without actually sharing the root user login credentials

(Incorrect)

-

When you create IAM policies, grant the least privileges required to perform a task

(Correct)

-

Share your AWS account root user credentials only if absolutely necessary for performing an important billing operation

-

Don't share security credentials between accounts, use IAM roles instead

(Correct)

Explanation

Correct options:

When you create IAM policies, grant the least privileges required to perform a task - When you create IAM policies, follow the standard security advice of granting the least privileges, or granting only the permissions required to perform a task. Determine what users (and roles) need to do and then craft policies that allow them to perform only those tasks.

Start with a minimum set of permissions and grant additional permissions as necessary. Doing so is more secure than starting with permissions that are too lenient and then trying to tighten them later.

Don't share security credentials between accounts, use IAM roles instead - Don't share security credentials between accounts to allow users from another AWS account to access resources in your AWS account. Instead, use IAM roles. You can define a role that specifies what permissions the IAM users in the other account are allowed. You can also designate which AWS accounts have the IAM users that are allowed to assume the role.

Incorrect options:

Share your AWS account root user credentials only if absolutely necessary for performing an important billing operation - Never share your AWS account root user password or access keys with anyone. Don't use your AWS account root user credentials to access AWS, and don't give your credentials to anyone else. Instead, create individual users for anyone who needs access to your AWS account. Create an IAM user for yourself as well, give that user administrative permissions, and use that IAM user for all your work.

Enable AWS multi-factor authentication (MFA) on your AWS root user account. MFA helps give root access to multiple users without actually sharing the root user login credentials - The given option just acts as a distractor. For extra security, AWS recommends that you use multi-factor authentication (MFA) for the root user in your account. With MFA, users have a device that generates a response to an authentication challenge. Both the user's credentials and the device-generated response are required to complete the sign-in process. If a user's password or access keys are compromised, your account resources are still secure because of the additional authentication requirement.

Do not change passwords and access keys once created. This results in failure of connectivity in the application logic - The given option just acts as a distractor. You should change your own passwords and access keys regularly, and make sure that all IAM users in your account do as well. That way, if a password or access key is compromised without your knowledge, you limit how long the credentials can be used to access your resources. You can apply a custom password policy to your account to require all your IAM users to rotate their AWS Management Console passwords. You can also choose how often they must do so.

Reference:

<https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html>

Question 4: **Incorrect**

Which of the following statements are true about AWS Regions and Availability Zones (AZs)? (Select two)

-

AWS calls each group of logical data centers as AWS Regions

-

Each AWS Region consists of multiple, isolated, and physically separate AZ's within a geographic area

(Correct)

-

Traffic between AZ's is not encrypted by default, but can be configured from AWS console

- All traffic between AZ's is encrypted
(Correct)
- An Availability Zone is a physical location where AWS clusters the data centers
(Incorrect)

Explanation

Correct options:

Each AWS Region consists of multiple, isolated, and physically separate AZ's within a geographic area - AWS has the concept of a Region, which is a physical location around the world where we cluster data centers. AWS calls 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.

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.

All traffic between AZ's is encrypted - 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.

Incorrect options:

Traffic between AZ's is not encrypted by default, but can be configured from AWS console - All traffic between AZ's is encrypted.

An Availability Zone is a physical location where AWS clusters the data centers - AWS has the concept of a Region, which is a physical location around the world where AWS clusters the data centers.

AWS calls each group of logical data centers as AWS Regions - AWS has the concept of a Region, which is a physical location around the world where AWS clusters the data centers. AWS calls each group of logical data centers as an Availability Zone.

Reference:

https://aws.amazon.com/about-aws/global-infrastructure/regions_az/

Question 5: **Correct**

A team manager needs data about the changes that have taken place for AWS resources in his account during the past two weeks. Which AWS service can help get this data?

- Amazon Inspector



AWS Config

(Correct)



AWS CloudTrail



Amazon CloudWatch

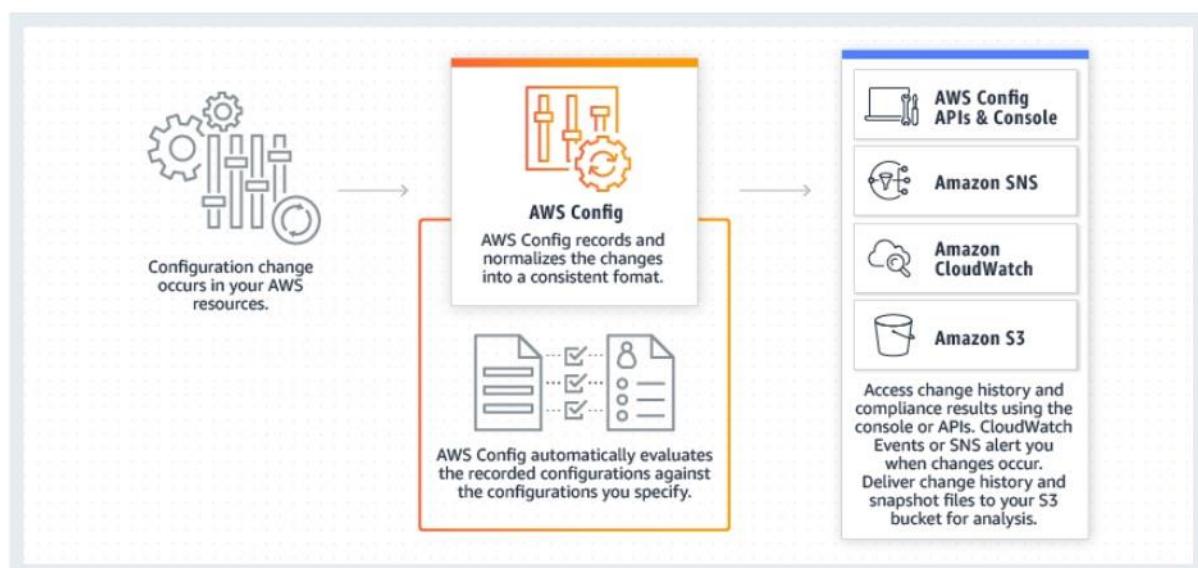
Explanation

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.

While AWS Config helps you answer questions like - "What did my AWS resource look like?" at a point in time. You can use AWS CloudTrail to answer "Who made an API call to modify this resource?"

Diagrammatic representation of how AWS Config works:



via - <https://aws.amazon.com/config/>

Incorrect options:

Amazon CloudWatch - 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. CloudWatch cannot however tell if the configuration of the resource has changed and what exactly changed.

Amazon Inspector - Amazon Inspector is an automated security assessment service that helps you test the network accessibility of your Amazon EC2 instances and the security state of your applications running on the instances. Amazon Inspector allows you to automate security vulnerability assessments throughout your development and deployment pipeline or against static production systems. This allows you to make security testing a more regular occurrence as part of the development and IT operations.

AWS CloudTrail - AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command-line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting. In addition, you can use CloudTrail to detect unusual activity in your AWS accounts. These capabilities help simplify operational analysis and troubleshooting.

Reference:

<https://aws.amazon.com/config/>

Question 6: **Incorrect**

As part of log analysis, you have realized that one or more AWS-owned IP addresses are being used for port scanning your on-premises server. Which service/team should you connect to resolve this issue?

-
-

Contact AWS Abuse team

(Correct)

-
-

Reach out to Werner Vogels, the CTO of Amazon, with the details of the incident

-
-

Contact AWS Support

-
-

Use AWS Trusted Advisor to log a complaint with AWS

(Incorrect)

Explanation

Correct option:

Contact AWS Abuse team - If you suspect that AWS resources are being used for abusive purposes, you need to contact the AWS Abuse team using the Report Amazon AWS abuse form, or by contacting abuse@amazonaws.com.

The AWS Abuse team can assist you when AWS resources are used to engage in the following types of abusive behavior: spam from AWS-owned IP addresses or AWS resources, port scanning, Denial-of-service (DoS) or DDoS from AWS-owned IP addresses, intrusion attempts, hosting objectionable or copyrighted content, distributing malware.

List of activities that fall under abusive behavior:

The AWS Abuse team can assist you when AWS resources are used to engage in the following types of abusive behavior:

- **Spam:** You are receiving unwanted emails from an AWS-owned IP address, or AWS resources are used to spam websites or forums.
- **Port scanning:** Your logs show that one or more AWS-owned IP addresses are sending packets to multiple ports on your server, and you believe this is an attempt to discover unsecured ports.
- **Denial-of-service (DoS) attacks:** Your logs show that one or more AWS-owned IP addresses are used to flood ports on your resources with packets, and you believe that this is an attempt to overwhelm or crash your server or the software running on your server.
- **Intrusion attempts:** Your logs show that one or more AWS-owned IP addresses are used to attempt to log in to your resources.
- **Hosting objectionable or copyrighted content:** You have evidence that AWS resources are used to host or distribute illegal content or distribute copyrighted content without the consent of the copyright holder.
- **Distributing malware:** You have evidence that AWS resources are used to distribute software that was knowingly created to compromise or cause harm to computers or machines on which it is installed.

via - <https://aws.amazon.com/premiumsupport/knowledge-center/report-aws-abuse/>

Incorrect options:

Contact AWS Support - AWS Support can't assist with reports of abuse or questions about notifications from the AWS Abuse team. AWS Abuse team is the right contact point for raising voice on abusive behavior using AWS resources.

Use AWS Trusted Advisor to log a complaint with AWS - AWS Trusted Advisor is an online tool that provides you real-time guidance to help you provision your resources following AWS best practices. Trusted Advisor checks help optimize your AWS infrastructure, increase security and performance, reduce your overall costs, and monitor service limits. Whether establishing new workflows, developing applications, or as part of ongoing improvement, take advantage of the recommendations provided by Trusted Advisor on a regular basis to help keep your solutions provisioned optimally.

Reach out to Werner Vogels, the CTO of Amazon, with the details of the incident - This has been added as a distractor. For the record, please let us know if you do get a shout out from Mr. Vogels.

Reference:

<https://aws.amazon.com/premiumsupport/knowledge-center/report-aws-abuse/>

Question 7: **Incorrect**

A media company uses Amazon Simple Storage Service (Amazon S3) for storing all its data. Which storage class should it consider for cost-optimal storage of the data that has random access patterns?

-

Amazon S3 Standard (S3 Standard)

(Incorrect)

-

Amazon S3 Random Access (S3 Random-Access)

-

Amazon S3 Intelligent-Tiering (S3 Intelligent-Tiering)

(Correct)

-

Amazon S3 Standard-Infrequent Access (S3 Standard-IA)

Explanation

Correct option:

Amazon S3 Intelligent-Tiering (S3 Intelligent-Tiering) - Amazon S3 Intelligent-Tiering (S3 Intelligent-Tiering) is the only cloud storage class that delivers automatic cost savings by moving objects between four access tiers when access patterns change. The S3 Intelligent-Tiering storage class is designed to optimize costs by automatically moving data to the most cost-effective access tier, without operational overhead. It works by storing objects in four access tiers: two low latency access tiers optimized for frequent and infrequent access, and two optional archive access tiers designed for asynchronous access that are optimized for rare access.

S3 Intelligent-Tiering works by storing objects in four access tiers: two low latency access tiers optimized for frequent and infrequent access, and two opt-in archive access tiers designed for asynchronous access that are optimized for rare access. Objects uploaded or transitioned to S3 Intelligent-Tiering are automatically stored in the Frequent Access tier. S3 Intelligent-Tiering works by monitoring access patterns and then moving the objects that have not been accessed in 30 consecutive days to the Infrequent Access tier. Once you have activated one or both of the archive access tiers, S3 Intelligent-Tiering will automatically move objects that haven't been accessed for 90 consecutive days to the Archive Access tier and then after 180 consecutive days of no access to the Deep Archive Access tier. If the objects are accessed later, S3 Intelligent-Tiering moves the objects back to the Frequent Access tier.

There are no retrieval fees when using the S3 Intelligent-Tiering storage class, and no additional tiering fees when objects are moved between access tiers within S3 Intelligent-Tiering. It is the ideal storage class for data sets with unknown storage access patterns, like new applications, or unpredictable access patterns, like data lakes.

Incorrect options:

Amazon S3 Standard (S3 Standard) - 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.

Amazon S3 Standard-Infrequent Access (S3 Standard-IA) - 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.

Amazon S3 Random Access (S3 Random-Access) - This is a made-up option, given only as a distractor.

Reference:

<https://aws.amazon.com/s3/storage-classes/>

Question 8: **Correct**

A company wants to establish a private, dedicated connection between AWS and its on-premises datacenter. Which AWS service is the right choice for this requirement?



Amazon API Gateway



AWS Direct Connect

(Correct)



Amazon CloudFront



AWS Site to Site Virtual Private Network (VPN)

Explanation

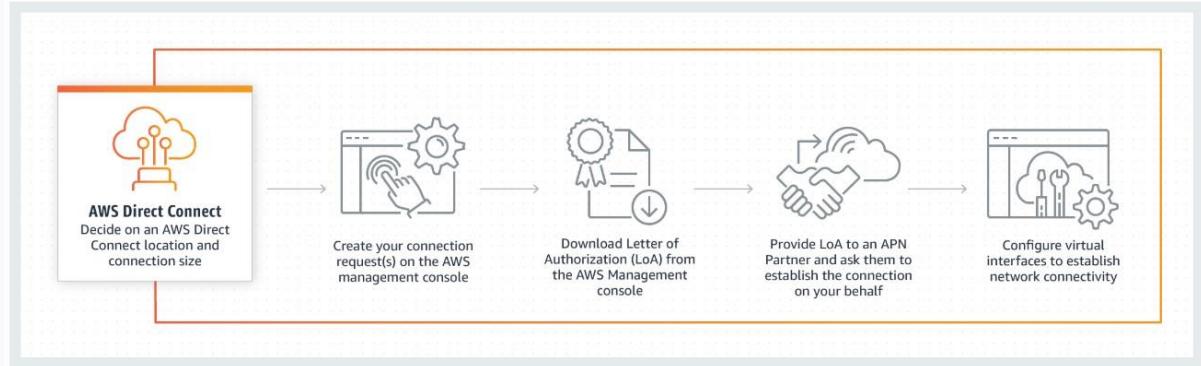
Correct option:

AWS Direct Connect - AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect, you can establish private connectivity between AWS and your datacenter, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections. AWS Direct Connect does not encrypt your traffic that is in transit.

AWS Direct Connect lets you establish a dedicated network connection between your network and one of the AWS Direct Connect locations. Using industry-standard 802.1q VLANs, this dedicated connection can be partitioned into multiple virtual interfaces. This allows you to use the same connection to access public resources such as objects stored in Amazon S3 using public IP address space, and private resources such as Amazon EC2 instances running within an Amazon Virtual Private Cloud (VPC) using private IP space while maintaining network separation between the public

and private environments. Virtual interfaces can be reconfigured at any time to meet your changing needs.

How Direct Connect works:



via - <https://aws.amazon.com/directconnect/>

Incorrect options:

AWS Site to Site Virtual Private Network (VPN) - AWS Virtual Private Network solutions establish secure connections between your on-premises networks, remote offices, client devices, and the AWS global network. AWS VPN is comprised of two services: AWS Site-to-Site VPN and AWS Client VPN. AWS Site-to-Site VPN creates encrypted tunnels between your network and your Amazon Virtual Private Clouds or AWS Transit Gateways.

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 offers the most advanced security capabilities, including field-level encryption and HTTPS support, seamlessly integrated with AWS Shield, AWS Web Application Firewall, and Route 53 to protect against multiple types of attacks including network and application layer DDoS attacks.

Amazon API Gateway - Amazon API Gateway is a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale. APIs act as the "front door" for applications to access data, business logic, or functionality from your backend services. Using API Gateway, you can create RESTful APIs and WebSocket APIs that enable real-time two-way communication applications. API Gateway supports containerized and serverless workloads, as well as web applications.

References:

<https://aws.amazon.com/directconnect/>

<https://aws.amazon.com/vpn/>

Question 9: **Correct**

Which of the following use-cases can be solved using the Amazon Forecast service?

-

To recommend personalized products for users based on their previous purchases

-

Document search service that can extract answers from text within documents

-

To develop and test fully functional machine learning models

-

Predict the web traffic of a website for the next few weeks

(Correct)

Explanation

Correct option:

Predict the web traffic of a website for the next few weeks - Amazon Forecast is a fully managed service that uses machine learning to deliver highly accurate forecasts. Based on the same technology used at Amazon.com, Amazon Forecast uses machine learning to combine time series data with additional variables to build forecasts. Amazon Forecast requires no machine learning experience to get started. You only need to provide historical data, plus any additional data that you believe may impact your forecasts.

Amazon Forecast can be used to forecast any time-series data, such as retail demand, manufacturing demand, travel demand, revenue, IT capacity, logistics, and web traffic.

Incorrect options:

To develop and test fully functional machine learning models - Amazon SageMaker is the correct service for this requirement. Amazon SageMaker is a fully managed service that provides every developer and data scientist with the ability to build, train, and deploy machine learning (ML) models quickly. SageMaker removes the heavy lifting from each step of the machine learning process to make it easier to develop high-quality models.

Document search service that can extract answers from text within documents - Amazon Kendra is the best fit for this use case. Amazon Kendra is an intelligent search service powered by machine learning. Kendra reimagines enterprise search for your websites and applications so your employees and customers can easily find the content they are looking for, even when it's scattered across multiple locations and content repositories within your organization.

To recommend personalized products for users based on their previous purchases - Amazon Personalize is useful in creating recommendations. Amazon Personalize makes it easy for developers to build applications capable of delivering a wide array of personalization experiences, including specific product recommendations, personalized product re-ranking, and customized direct marketing.

Reference:

<https://aws.amazon.com/forecast/>

Question 10: **Incorrect**

Which of the following points have to be considered when choosing an AWS Region for a service?
(Select two)

-

The AWS Region should have 5G networks, to seamlessly access the breadth of AWS services in the region

-

The AWS Region with high availability index should be considered for your business

(Incorrect)

-

Compliance and Data Residency guidelines of the AWS Region should match your business requirements

(Correct)

-

AWS Region chosen should be geographically closer to the user base that utilizes the hosted AWS services

(Correct)

-

The AWS Region chosen should have all its Availability Zones (AZs) within 100 Kms radius, to keep latency low for hosted applications

Explanation

Correct options:

Compliance and Data Residency guidelines of the AWS Region should match your business requirements

- If you have data residency requirements, you can choose the AWS Region that is in close proximity to your desired location. You retain complete control and ownership over the region in which your data is physically located, making it easy to meet regional compliance and data residency requirements.

AWS Region chosen should be geographically closer to the user base that utilizes the hosted AWS services - When deploying your applications and workloads to the cloud, you have the flexibility in selecting a technology infrastructure and AWS Region that is closest to your primary target of users.

Incorrect options:

The AWS Region with high availability index should be considered for your business - AWS delivers the highest network availability of any cloud provider. Each region is fully isolated and comprised of multiple AZ's, which are fully isolated partitions of our infrastructure. All AWS Regions are designed to be highly available.

The AWS Region should have 5G networks, to seamlessly access the breadth of AWS services in the region - AWS Local Zones and AWS Wavelength, with telco providers, provide performance for applications that require single-digit millisecond latencies by delivering AWS infrastructure and services closer to end-users and 5G connected devices. But, having a 5G network is not a factor for a customer to decide on an AWS Region.

The AWS Region chosen should have all its Availability Zones (AZs) within 100 Kms radius, to keep latency low for hosted applications - An Availability Zone (AZ) is one or more discrete data centers with redundant power, networking, and connectivity in an AWS Region. 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. This applies to all AZs and hence is not a criterion for choosing an AWS Region.

Reference:

https://aws.amazon.com/about-aws/global-infrastructure/regions_az/

Question 11: **Correct**

A company has defined a baseline that mentions the number of AWS resources to be used for different stages of application testing. However, the company realized that employees are not adhering to the guidelines and provisioning additional resources via API calls, resulting in higher testing costs.

Which AWS service will help the company raise alarms whenever the baseline resource numbers are crossed?

-
- AWS Config**
-
- AWS X-Ray**
-
- Amazon Detective**
-
- AWS CloudTrail Insights**

(Correct)

Explanation

Correct option:

AWS CloudTrail Insights - AWS CloudTrail Insights helps AWS users identify and respond to unusual activity associated with write API calls by continuously analyzing CloudTrail management events.

Insights events are logged when CloudTrail detects unusual write management API activity in your account. If you have CloudTrail Insights enabled, and CloudTrail detects unusual activity, Insights events are delivered to the destination S3 bucket for your trail. You can also see the type of insight and the incident time period when you view Insights events on the CloudTrail console. Unlike other types of events captured in a CloudTrail trail, Insights events are logged only when CloudTrail detects changes in your account's API usage that differ significantly from the account's typical usage patterns.

CloudTrail Insights can help you detect unusual API activity in your AWS account by raising Insights events. CloudTrail Insights measures your normal patterns of API call volume, also called the baseline, and generates Insights events when the volume is outside normal patterns.

CloudTrail Insights continuously monitors CloudTrail write management events, and uses mathematical models to determine the normal levels of API and service event activity for an account. CloudTrail Insights identifies behavior that is outside normal patterns, generates Insights events, and delivers those events to a /CloudTrail-Insight folder in the chosen destination S3 bucket for your trail. You can also access and view Insights events in the AWS Management Console for CloudTrail.

Identify and Respond to Unusual API Activity using CloudTrail Insights:

Enabling AWS CloudTrail Insights

CloudTrail tracks user activity and API usage. It provides an event history of AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. With the launch of [AWS CloudTrail Insights](#), you can enable machine learning models that detect unusual activity in these logs with just a few clicks. [AWS CloudTrail Insights](#) will analyze historical API calls, identifying usage patterns and generating Insight Events for unusual activity.

Creating a trail might incur charges. For more information, see [AWS CloudTrail Pricing](#).

Create Trail

Trail name*

Apply trail to all regions Yes No
Creates the same trail in all regions and delivers log files for all regions

Management events

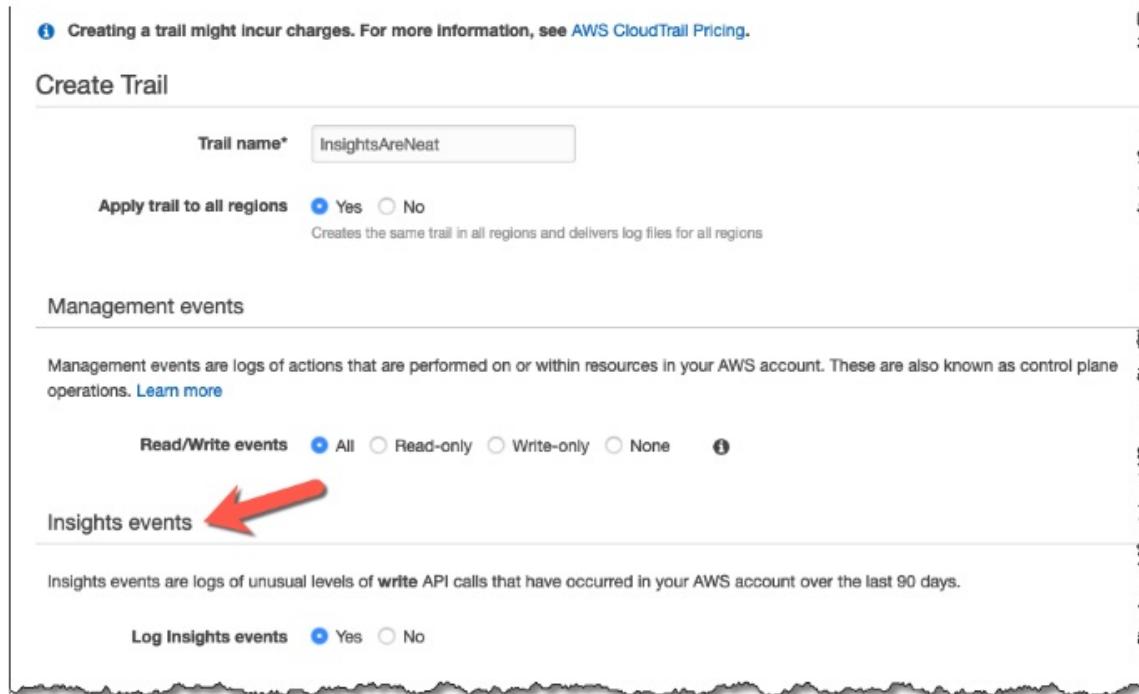
Management events are logs of actions that are performed on or within resources in your AWS account. These are also known as control plane operations. [Learn more](#)

Read/Write events All Read-only Write-only None (i)

Insights events 

Insights events are logs of unusual levels of write API calls that have occurred in your AWS account over the last 90 days.

Log Insights events Yes No



via - <https://aws.amazon.com/blogs/aws/announcing-cloudtrail-insights-identify-and-respond-to-unusual-api-activity/>

Incorrect options:

AWS X-Ray - AWS X-Ray helps developers analyze and debug production, distributed applications, such as those built using a microservices architecture. With X-Ray, you can understand how your application and its underlying services are performing to identify and troubleshoot the root cause of performance issues and errors. X-Ray provides an end-to-end view of requests as they travel through your application, and shows a map of your application's underlying components. X-Ray is not for tracking user actions when interacting with the AWS systems.

Amazon Detective - Amazon Detective simplifies the process of investigating security findings and identifying the root cause. Amazon Detective analyzes trillions of events from multiple data sources

such as VPC Flow Logs, AWS CloudTrail logs, and Amazon GuardDuty findings and automatically creates a graph model that provides you with a unified, interactive view of your resources, users, and the interactions between them over time.

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.

Reference:

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/logging-insights-events-with-cloudtrail.html>

Question 12: **Incorrect**

AWS Web Application Firewall (AWS WAF) can be deployed on which of the following services?

-
-

Amazon CloudFront, Amazon Elastic Compute Cloud (Amazon EC2), Amazon API Gateway, Application Load Balancer

(Incorrect)

-
-

AWS AppSync, Amazon CloudFront, Application Load Balancer, Amazon Elastic Compute Cloud (Amazon EC2)

-
-

Application Load Balancer, Amazon Elastic Compute Cloud (Amazon EC2), Amazon API Gateway

-
-

Amazon CloudFront, Application Load Balancer, Amazon API Gateway, AWS AppSync

(Correct)

Explanation

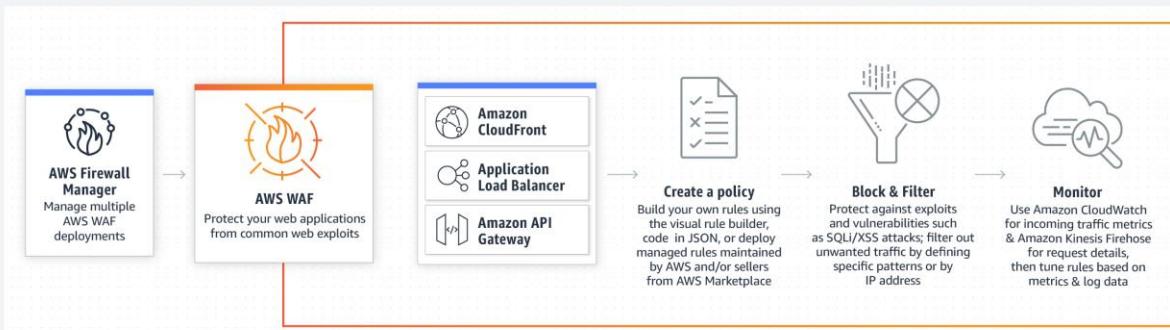
Correct option:

Amazon CloudFront, Application Load Balancer, Amazon API Gateway, AWS AppSync - AWS WAF is a web application firewall that helps protect your web applications or APIs against common web exploits that may affect availability, compromise security, or consume excessive resources. AWS WAF gives you control over how traffic reaches your applications by enabling you to create security rules that block common attack patterns, such as SQL injection or cross-site scripting, and rules that filter out specific traffic patterns you define.

You can deploy AWS WAF on Amazon CloudFront as part of your CDN solution, the Application Load Balancer that fronts your web servers or origin servers running on EC2, Amazon API Gateway for your REST APIs, or AWS AppSync for your GraphQL APIs.

AWS WAF is tightly integrated with Amazon CloudFront, the Application Load Balancer (ALB), Amazon API Gateway, and AWS AppSync – services that AWS customers commonly use to deliver content for their websites and applications. 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. When you use AWS WAF on regional services, such as Application Load Balancer, Amazon API Gateway, and AWS AppSync, your rules run in the region and can be used to protect internet-facing resources as well as internal resources.

How AWS WAF Works:



via - <https://aws.amazon.com/waf/>

Incorrect options:

Amazon CloudFront, Amazon Elastic Compute Cloud (Amazon EC2), Amazon API Gateway, Application Load Balancer

Application Load Balancer, Amazon Elastic Compute Cloud (Amazon EC2), Amazon API Gateway

AWS AppSync, Amazon CloudFront, Application Load Balancer, Amazon Elastic Compute Cloud (Amazon EC2)

AWS WAF cannot be deployed on Amazon EC2 instances directly, so these three options are incorrect. Application Load Balancer should be configured in front of EC2 instances to deploy AWS WAF.

Reference:

<https://aws.amazon.com/waf/>

Question 13:

Skipped

A company is looking at a service/tool to automate and minimize the time spent on keeping the server images up-to-date. These server images are used by EC2 instances as well as the on-premises systems.

Which AWS service will help achieve the company's need?

- **Amazon EC2 Image Builder**
- **(Correct)**
-
- **AWS CloudFormation templates**
-
- **Amazon EC2 AMI**
-

AWS Systems Manager (Amazon Simple Systems Manager (SSM))

Explanation

Correct option:

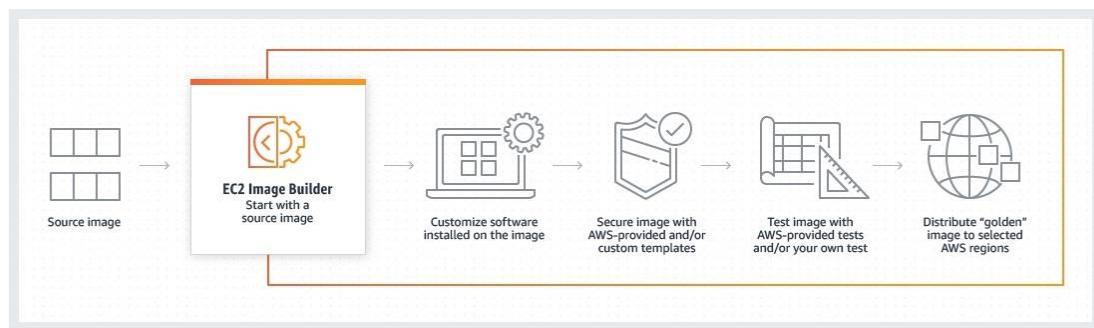
Amazon EC2 Image Builder - EC2 Image Builder simplifies the building, testing, and deployment of Virtual Machine and container images for use on AWS or on-premises.

Keeping Virtual Machine and container images up-to-date can be time-consuming, resource-intensive, and error-prone. Currently, customers either manually update and snapshot VMs or have teams that build automation scripts to maintain images.

Image Builder significantly reduces the effort of keeping images up-to-date and secure by providing a simple graphical interface, built-in automation, and AWS-provided security settings. With Image Builder, there are no manual steps for updating an image nor do you have to build your own automation pipeline.

How to use Image Builder to automate server image creation:

Image Builder provides a one-stop-shop to automate image management processes. Customers can generate an automated pipeline with an intuitive wizard in the AWS console to produce compliant Linux and Windows Server images for use on AWS and on-premises. When software updates become available, Image Builder automatically produces a new image and distributes it to stipulated AWS regions after running tests on it.



Examples of **customize software installed on the image** includes: 1/ Applications (build environments, business productivity tools, and databases) 2/ OS Updates 3/ Security patches.

Examples of **secure image with AWS-provided and/or custom templates** includes: 1/ Ensure security patches are applied, 2/ Enforce strong passwords, 3/ Turn on full disk encryption, 4/ Close all non-essential open ports, 5/ Enable software firewall, 6/ Enable logging/audit controls.

Examples of **test image with AWS-provided test and/or your own test** includes: 1/ Test that AMI can boot, 2/ Test that sample application can be run, 3/ Test specific patch has been applied, 5/ Test security policy.

via - <https://aws.amazon.com/image-builder/>

Incorrect options:

Amazon EC2 AMI - An Amazon Machine Image (AMI) provides the information required to launch an instance. You must specify an AMI when you launch an EC2 instance. An Amazon Machine Image (AMI) is the basic unit of deployment in Amazon EC2 and is one of the types of images you can create with Image Builder.

AWS CloudFormation templates - AWS CloudFormation simplifies provisioning and management on AWS. You can create templates for the service or application architectures you want and have AWS CloudFormation use those templates for quick and reliable provisioning of the services or applications.

AWS Systems Manager (Amazon Simple Systems Manager (SSM)) - AWS Systems Manager (formerly known as SSM) is an AWS service that you can use to view and control your infrastructure on AWS. Using the Systems Manager console, you can view operational data from multiple AWS services and automate operational tasks across your AWS resources.

Instances used to build images and run tests using Image Builder must have access to the Systems Manager service. All build activity is orchestrated by SSM Automation. The SSM Agent will be installed on the source image if it is not already present, and it will be removed before the image is created.

References:

<https://aws.amazon.com/image-builder/>

<https://docs.aws.amazon.com/imagebuilder/latest/userguide/image-builder-setting-up.html>

Question 14:

Skipped

Due to regulatory guidelines, a company needs to encrypt data as it passes through the different layers of its AWS architecture. The company is reviewing the capabilities of the various AWS services and their encryption options.

Which of the below services are encrypted by default and need no user intervention to enable encryption?



AWS Organizations, Amazon EC2, CloudTrail Logs



AWS Storage Gateway, Application Load Balancer (ALB), Amazon CloudFront



CloudTrail Logs, S3 Glacier, AWS Storage Gateway

(Correct)



CloudWatch logs, Application Load Balancer (ALB), S3 Glacier

Explanation

Correct option:

CloudTrail Logs, S3 Glacier, AWS Storage Gateway - By default, all data stored by AWS Storage Gateway in S3 is encrypted server-side with Amazon S3-Managed Encryption Keys (SSE-S3). Also, you can optionally configure different gateway types to encrypt stored data with AWS Key Management Service (KMS) via the Storage Gateway API.

Data at rest stored in S3 Glacier is automatically server-side encrypted using 256-bit Advanced Encryption Standard (AES-256) with keys maintained by AWS. If you prefer to manage your own keys, you can also use client-side encryption before storing data in S3 Glacier.

By default, the log files delivered by CloudTrail to your bucket are encrypted by Amazon server-side encryption with Amazon S3-managed encryption keys (SSE-S3). To provide a security layer that is directly manageable, you can instead use server-side encryption with AWS KMS-managed keys (SSE-KMS) for your CloudTrail log files. To use SSE-KMS with CloudTrail, you create and manage a KMS key, also known as a customer master key (CMK).

Incorrect options:

CloudWatch logs, Application Load Balancer (ALB), S3 Glacier - Encryption at rest and Encryption in transit is a configurable feature in Application Load Balancer.

Data protection in Elastic Load Balancing:

Encryption at rest

If you enable server-side encryption with Amazon S3-managed encryption keys (SSE-S3) for your S3 bucket for Elastic Load Balancing access logs, Elastic Load Balancing automatically encrypts each access log file before it is stored in your S3 bucket. Elastic Load Balancing also decrypts the access log files when you access them. Each log file is encrypted with a unique key, which is itself encrypted with a master key that is regularly rotated.

Encryption in transit

Elastic Load Balancing simplifies the process of building secure web applications by terminating HTTPS and TLS traffic from clients at the load balancer. The load balancer performs the work of encrypting and decrypting the traffic, instead of requiring each EC2 instance to handle the work for TLS termination. When you configure a secure listener, you specify the cipher suites and protocol versions that are supported by your application, and a server certificate to install on your load balancer. You can use AWS Certificate Manager (ACM) or AWS Identity and Access Management (IAM) to manage your server certificates. Application Load Balancers support HTTPS listeners. Network Load Balancers support TLS listeners. Classic Load Balancers support both HTTPS and TLS listeners.

via - <https://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/data-protection.html>

AWS Organizations, Amazon EC2, CloudTrail Logs - AWS Organizations helps you centrally manage and govern your environment as you grow and scale your AWS resources.

Instance storage provides temporary block-level storage for Amazon EC2 instances. This storage is located on disks attached physically to a host computer. By default, files stored on these disks are not encrypted. EBS volumes attached to EC2 instances are not encrypted by default either.

AWS Storage Gateway, Application Load Balancer (ALB), Amazon CloudFront - Amazon CloudFront does not encrypt data by default. But, encryption can be enabled if needed, by configuring encryption in transit and encryption at rest, for your distributions.

More information on data protection in Amazon CloudFront:

Encryption in Transit

To encrypt your data during transit, you configure Amazon CloudFront to require that viewers use HTTPS to request your files, so that connections are encrypted when CloudFront communicates with viewers. You also can configure CloudFront to use HTTPS to get files from your origin, so that connections are encrypted when CloudFront communicates with your origin.

For more information, see [Using HTTPS with CloudFront](#).

Field-level encryption adds an additional layer of security along with HTTPS that lets you protect specific data throughout system processing so that only certain applications can see it. By configuring field-level encryption in CloudFront, you can securely upload user-submitted sensitive information to your web servers. The sensitive information provided by your clients is encrypted at the edge closer to the user. It remains encrypted throughout your entire application stack, ensuring that only applications that need the data—and have the credentials to decrypt it—are able to do so.

For more information, see [Using Field-Level Encryption to Help Protect Sensitive Data](#).

Encryption at Rest

CloudFront uses SSDs which are encrypted for edge location points of presence (POPs), and encrypted EBS volumes for Regional Edge Caches (RECs).

via - <https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/data-protection-summary.html>

References:

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/best-practices-security.html>

<https://docs.aws.amazon.com/amazonglacier/latest/dev/DataEncryption.html>

<https://aws.amazon.com/storagegateway/features/>

Question 15:

Skipped

Which of the following statements are correct regarding the health monitoring and reporting capabilities supported by AWS Elastic Beanstalk? (Select two)

-

AWS Elastic Beanstalk provides only basic health reporting system; Combined with Elastic Load Balancer, they provide advanced health check features

- In a single instance environment, Elastic Beanstalk determines the instance's health by monitoring the Elastic Load Balancing health settings**
 - The Elastic Beanstalk health monitoring can determine that the environment's Auto Scaling group is available and has a minimum of at least one instance**
- (Correct)**
- The basic health reporting system that provides information about the health of instances in an Elastic Beanstalk environment does not use health checks performed by Elastic Load Balancing**
 - With basic health reporting, the Elastic Beanstalk service does not publish any metrics to Amazon CloudWatch**
- (Correct)**

Explanation

Correct options:

The Elastic Beanstalk health monitoring can determine that the environment's Auto Scaling group is available and has a minimum of at least one instance - In addition to Elastic Load Balancing health checks, Elastic Beanstalk monitors resources in your environment and changes health status to red if they fail to deploy, are not configured correctly, or become unavailable. These checks confirm that: 1. The environment's Auto Scaling group is available and has a minimum of at least one instance. 2. The environment's security group is available and is configured to allow incoming traffic on port 80. 3. The environment CNAME exists and is pointing to the right load balancer. 4. In a worker environment, the Amazon Simple Queue Service (Amazon SQS) queue is being polled at least once every three minutes.

With basic health reporting, the Elastic Beanstalk service does not publish any metrics to Amazon CloudWatch - With basic health reporting, the Elastic Beanstalk service does not publish any metrics to Amazon CloudWatch. The CloudWatch metrics used to produce graphs on the Monitoring page of the environment console are published by the resources in your environment.

Incorrect options:

AWS Elastic Beanstalk provides only a basic health reporting system; Combined with Elastic Load Balancer, they provide advanced health check features - This option has been added as a distractor.

In a single instance environment, Elastic Beanstalk determines the instance's health by monitoring the Elastic Load Balancing health settings - In a single instance or worker tier environment, Elastic Beanstalk determines the instance's health by monitoring its Amazon EC2 instance status. Elastic Load Balancing health settings, including HTTP health check URLs cannot be used in these environment types.

The basic health reporting system that provides information about the health of instances in an Elastic Beanstalk environment does not use health checks performed by Elastic Load Balancing -
The basic health reporting system provides information about the health of instances in an Elastic Beanstalk environment based on health checks performed by Elastic Load Balancing for load-balanced environments, or Amazon Elastic Compute Cloud for single-instance environments.

Reference:

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.healthstatus.html#monitoring-basic-additionalchecks>

Question 16:

Skipped

A financial consulting company is looking for automated reference deployments, that will speed up the process of deploying its financial solutions on AWS Cloud. The reference deployment should be able to deploy most of the well-known functions of financial services and leave space for customizations, if necessary.

Which AWS service will help achieve this requirement?

-

AWS Quick Starts

(Correct)

-

AWS Elastic Beanstalk

-

AWS CloudFormation

-

Amazon Quicksight

Explanation

Correct option:

AWS Quick Starts - AWS Quick Starts are automated reference deployments for key workloads on the AWS Cloud. Each Quick Start launches, configures and runs the AWS compute, network, storage, and other services required to deploy a specific workload on AWS, using AWS best practices for security and availability.

Quick Starts are accelerators that condense hundreds of manual procedures into just a few steps. They are fast, low-cost, and customizable. They are fully functional and designed for production.

Quick Starts include: 1. A reference architecture for the deployment 2. AWS CloudFormation templates (JSON or YAML scripts) that automate and configure the deployment 3. A deployment guide, which explains the architecture and implementation in detail, and provides instructions for customizing the deployment.

Quick Starts also include integrations that extend the cloud-based contact center functionality provided by Amazon Connect with key services and solutions from APN Partners—for customer relationship management (CRM), workforce optimization (WFO), analytics, unified communications (UC), and other use cases.

Incorrect options:

AWS CloudFormation - AWS CloudFormation gives you an easy way to model a collection of related AWS and third-party resources, provision them quickly and consistently, and manage them throughout their lifecycles, by treating infrastructure as code. A CloudFormation template describes your desired resources and their dependencies so you can launch and configure them together as a stack.

AWS Elastic Beanstalk - AWS Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services developed with Java, .NET, PHP, Node.js, Python, Ruby, Go, and Docker on familiar servers such as Apache, Nginx, Passenger, and IIS. You can simply upload your code and Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring. At the same time, you retain full control over the AWS resources powering your application and can access the underlying resources at any time.

Amazon Quicksight - Amazon QuickSight is a scalable, serverless, embeddable, machine learning-powered business intelligence (BI) service built for the cloud. QuickSight lets you easily create and publish interactive BI dashboards that include Machine Learning-powered insights. With QuickSight, you can quickly embed interactive dashboards into your applications, websites, and portals.

Reference:

<https://aws.amazon.com/quickstart/faq/>

Question 17:

Skipped

An online retail clothing store is looking for a service/tool to easily create and embed 3D scenes into their existing web pages to enhance user experience and improve sales. Which AWS service will help create these 3D visuals?

-

Amazon SageMaker

-

Amazon Comprehend

-

Amazon Sumerian

(Correct)

-

Amazon Polly

Explanation

Correct option:

Amazon Sumerian - Amazon Sumerian is a managed service that lets you create and run 3D, Augmented Reality (AR) and Virtual Reality (VR) applications. You can build immersive and interactive scenes that run on AR and VR, mobile devices, and your web browser. Whether you are non-technical, a web or mobile developer, or have years of 3D development experience, getting started with Sumerian is easy. You can design scenes directly from your browser and, because Sumerian is a web-based application, you can quickly add connections in your scenes to existing AWS services.

Amazon Sumerian leverages the power of AWS to create smarter and more engaging front-end experiences. Easily embed conversational interfaces into scenes using Amazon Lex and embed scenes in a web application using AWS Amplify. Amazon Sumerian embraces the latest WebGL and WebXR standards to create immersive experiences directly in a web browser, accessible via a simple URL in seconds, and able to run on major hardware platforms for AR/VR. Build your scene once and deploy it anywhere.

Incorrect options:

Amazon SageMaker - Amazon SageMaker is a fully managed service that provides every developer and data scientist with the ability to build, train, and deploy machine learning (ML) models quickly. SageMaker removes the heavy lifting from each step of the machine learning process to make it easier to develop high-quality models. Amazon SageMaker ensures that ML model artifacts and other system artifacts are encrypted in transit and at rest.

Amazon Comprehend - Amazon Comprehend is a natural language processing (NLP) service that uses machine learning to find meaning and insights in text. You can use Amazon Comprehend to identify the language of the text, extract key phrases, places, people, brands, or events, understand sentiment about products or services, and identify the main topics from a library of documents. The source of this text could be web pages, social media feeds, emails, or articles.

Amazon Polly - Amazon Polly is a service that turns text into lifelike speech, allowing you to create applications that talk, and build entirely new categories of speech-enabled products. Polly's Text-to-Speech (TTS) service uses advanced deep learning technologies to synthesize natural sounding human speech. With dozens of lifelike voices across a broad set of languages, you can build speech-enabled applications that work in many different countries.

Reference:

<https://aws.amazon.com/sumerian/>

Question 18:

Skipped

To meet the compliance norms, a consulting company is expected to store its data for three years. The company needs a tamper-proof technology/feature to keep the data protected and prevent any overwriting or data manipulation during the three-year duration.

As a Cloud Practitioner, which service/functionality will you suggest to keep the data safe?

-

Amazon Macie

-

Amazon S3 Object Lock



Amazon S3 Glacier Vault Lock

(Correct)



Amazon S3 Storage Lens

Explanation

Correct option:

Amazon S3 Glacier Vault Lock - S3 Glacier Vault Lock allows you to easily deploy and enforce compliance controls for individual S3 Glacier vaults with a vault lock policy. You can specify controls such as "write once read many" (WORM) in a vault lock policy and lock the policy from future edits. Once locked, the policy can no longer be changed.

A vault lock policy can be locked to prevent future changes, providing strong enforcement for your compliance controls. You can use the vault lock policy to deploy regulatory and compliance controls, which typically require tight controls on data access.

As an example of a Vault Lock policy, suppose that you are required to retain archives for one year before you can delete them. To implement this requirement, you can create a Vault Lock policy that denies users permission to delete an archive until the archive has existed for one year. You can test this policy before locking it down. After you lock the policy, the policy becomes immutable.

Incorrect options:

Amazon S3 Object Lock - You can use S3 Object Lock to store objects using a write-once-read-many (WORM) model. It can help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. You can use S3 Object Lock to meet regulatory requirements that require WORM storage, or add an extra layer of protection against object changes and deletion.

Amazon S3 Glacier Vault Lock is the right choice here, because with S3 Object Lock, users with special permissions can make changes to the Lock policy and delete the data. This is not possible with S3 Glacier Vault Lock.

Amazon S3 Storage Lens - S3 Storage Lens delivers organization-wide visibility into object storage usage, activity trends, and makes actionable recommendations to improve cost-efficiency and apply data protection best practices. S3 Storage Lens is the first cloud storage analytics solution to provide a single view of object storage usage and activity across hundreds, or even thousands, of accounts in an organization, with drill-downs to generate insights at the account, bucket, or even prefix level.

Amazon Macie - You can use Amazon Macie to discover and protect sensitive data stored in Amazon S3. Macie automatically gathers a complete S3 inventory and continually evaluates every bucket to alert on any publicly accessible buckets, unencrypted buckets, or buckets shared or replicated with AWS accounts outside of your organization. Then, Macie applies machine learning and pattern matching techniques to the buckets you select to identify and alert you to sensitive data, such as personally identifiable information (PII).

References:

<https://docs.aws.amazon.com/amazonglacier/latest/dev/vault-lock-policy.html>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lock-overview.html>

<https://aws.amazon.com/s3/features/>

Question 19:

Skipped

Which of the following services/tools offers a user-friendly graphical user interface to manage AWS Snowball devices without a need for command-line interface or REST APIs?

-

AWS Transfer Family

-

AppStream 2.0

-

AWS OpsHub

(Correct)

-

AWS OpsWorks

Explanation

Correct option:

AWS OpsHub - AWS OpsHub is a graphical user interface you can use to manage your AWS Snowball devices, enabling you to rapidly deploy edge computing workloads and simplify data migration to the cloud. With just a few clicks in AWS OpsHub, you have the full functionality of the Snowball devices at your fingertips; you can unlock and configure devices, drag-and-drop data to devices, launch applications, and monitor device metrics.

Previously, customers operated Snowball devices by either entering commands into a command-line interface or by using REST APIs. Now with AWS OpsHub, you have an easier way to deploy and manage even large fleets of Snowball devices, all while operating without an internet connection.

AWS OpsHub takes all the existing operations available in the Snowball API and presents them as a simple graphical user interface. This interface helps you quickly and easily migrate data to the AWS Cloud and deploy edge computing applications on Snow Family Devices.

AWS OpsHub provides a unified view of AWS services that are running on Snow Family Devices and automates operational tasks through AWS Systems Manager. With AWS OpsHub, users with different levels of technical expertise can easily manage a large number of Snow Family Devices. With just a few clicks, you can unlock devices, transfer files, manage Amazon EC2 instances, and monitor device metrics.

When your Snow device arrives at your site, you download, install, and launch the AWS OpsHub application on a client machine, such as a laptop. After installation, you can unlock the device and start managing it and using supported AWS services locally. AWS OpsHub provides a dashboard that summarizes key metrics such as storage capacity and active instances on your device. It also provides a selection of the AWS services that are supported on the Snow Family Devices. Within minutes, you can begin transferring files to the device.

Incorrect options:

Amazon AppStream 2.0 - Amazon AppStream 2.0 is a fully managed non-persistent application and desktop streaming service. You centrally manage your desktop applications on AppStream 2.0 and securely deliver them to any computer. You can easily scale to any number of users across the globe without acquiring, provisioning, and operating hardware or infrastructure. AppStream 2.0 is built on AWS, so you benefit from a data center and network architecture designed for the most security-sensitive organizations. This is not a tool for AWS Snowball devices.

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.

AWS Transfer Family - The AWS Transfer Family is the aggregated name of AWS Transfer for SFTP, AWS Transfer for FTPS, and AWS Transfer for FTP. The AWS Transfer Family offers fully managed support for the transfer of files over SFTP, FTPS, and FTP directly into and out of Amazon S3 or Amazon EFS.

Reference:

<https://docs.aws.amazon.com/snowball/latest/developer-guide/aws-opshub.html>

Question 20:

Skipped

A company is looking at real-time processing of streaming big data for their ad-tech platform. Which of the following AWS services is the right choice for this requirement?

-
- Amazon Simple Queue Service (Amazon SQS)**
-
- Amazon Redshift**
-
- Amazon EMR**
-
- Amazon Kinesis data stream**

(Correct)

Explanation

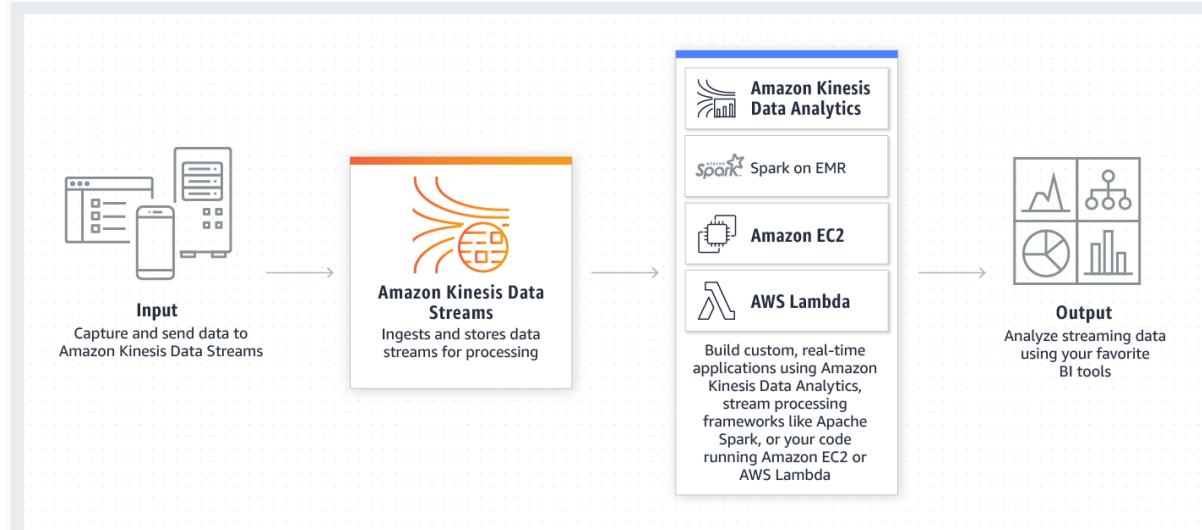
Correct option:

Amazon Kinesis data stream - Amazon Kinesis Data Streams enables you to build custom applications that process or analyze streaming data for specialized needs. You can continuously add various types of data such as clickstreams, application logs, and social media to an Amazon Kinesis

data stream from hundreds of thousands of sources. Within seconds, the data will be available for your Amazon Kinesis Applications to read and process from the stream.

Amazon Kinesis Data Streams is useful to rapidly move the data off data producers and then continuously process the data, be it to transform the data before emitting it to a data store, run real-time metrics and analytics, or derive more complex data streams for further processing. The following are typical scenarios for using Amazon Kinesis Data Streams: accelerated log and data feed intake, real-time metrics and reporting, real-time data analytics, complex stream processing.

How Kinesis Data Streams Work:



via - <https://aws.amazon.com/kinesis/data-streams/>

Incorrect options:

Amazon Simple Queue Service (Amazon SQS) - Amazon Simple Queue Service (Amazon SQS) offers a reliable, highly scalable hosted queue for storing messages as they travel between computers. Amazon SQS lets you easily move data between distributed application components and helps you build applications in which messages are processed independently (with message-level ack/fail semantics), such as automated workflows.

Amazon Redshift - With Redshift, you can query and combine exabytes of structured and semi-structured data across your data warehouse, operational database, and data lake using standard SQL. Redshift lets you easily save the results of your queries back to your S3 data lake using open formats, like Apache Parquet, so that you can do additional analytics from other analytics services like Amazon EMR, Amazon Athena, and Amazon SageMaker. Redshift is a data warehousing solution and not a real-time streaming service.

Amazon EMR - Amazon EMR makes it easy to set up, operate, and scale your big data environments by automating time-consuming tasks like provisioning capacity and tuning clusters. EMR is not suitable as a real-time streaming service.

Reference:

<https://aws.amazon.com/kinesis/data-streams/>

Question 21:

Skipped

Which feature/functionality will help you organize your AWS resources, manage and automate tasks on large numbers of resources at a time?

-
- Tags**
-
- Amazon WorkSpaces**
-
- AWS Resource Groups**
- (Correct)**
-
- AWS Organizations**

Explanation

Correct option:

AWS Resource Groups - In AWS, a resource is an entity that you can work with. Examples include an Amazon EC2 instance, an AWS CloudFormation stack, or an Amazon S3 bucket. If you work with multiple resources, you might find it useful to manage them as a group rather than move from one AWS service to another for each task. If you manage large numbers of related resources, such as EC2 instances that make up an application layer, you likely need to perform bulk actions on these resources at one time.

You can use Resource Groups to organize your AWS resources. Resource groups make it easier to manage and automate tasks on large numbers of resources at a time. Resource Groups feature permissions are at the account level. As long as users who are sharing your account have the correct IAM permissions, they can work with resource groups that you create.

Incorrect options:

AWS Organizations - AWS Organizations helps you centrally manage and govern your environment as you grow and scale your AWS resources. Using AWS Organizations, you can programmatically create new AWS accounts and allocate resources, group accounts to organize your workflows, apply policies to accounts or groups for governance, and simplify billing by using a single payment method for all of your accounts.

Tags - To help you manage your instances, images, and other Amazon EC2 resources, you can assign your own metadata to each resource in the form of tags. Tags enable you to categorize your AWS resources in different ways, for example, by purpose, owner, or environment. Tags are properties of a resource. Resource Groups allow you to easily create, maintain, and view a collection of resources that share common tags.

Amazon WorkSpaces - Amazon WorkSpaces enables you to provision virtual, cloud-based Microsoft Windows or Amazon Linux desktops for your users, known as WorkSpaces. Amazon WorkSpaces eliminates the need to procure and deploy hardware or install complex software. You can quickly add or remove users as your needs change. Users can access their virtual desktops from multiple devices or web browsers.

References:

<https://docs.aws.amazon.com/ARG/latest/userguide/welcome.html>

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html

<https://aws.amazon.com/organizations/>

Question 22:

Skipped

Which of the following data sources are used by Amazon Detective to analyze events and identify potential security issues?



Amazon CloudWatch Logs, AWS CloudTrail logs and S3 Access Logs



Amazon CloudWatch Logs, AWS CloudTrail logs and Amazon Inspector logs



AWS CloudTrail logs, Amazon VPC Flow Logs and Amazon GuardDuty findings

(Correct)



Amazon CloudWatch Logs, Amazon VPC Flow Logs and Amazon GuardDuty findings

Explanation

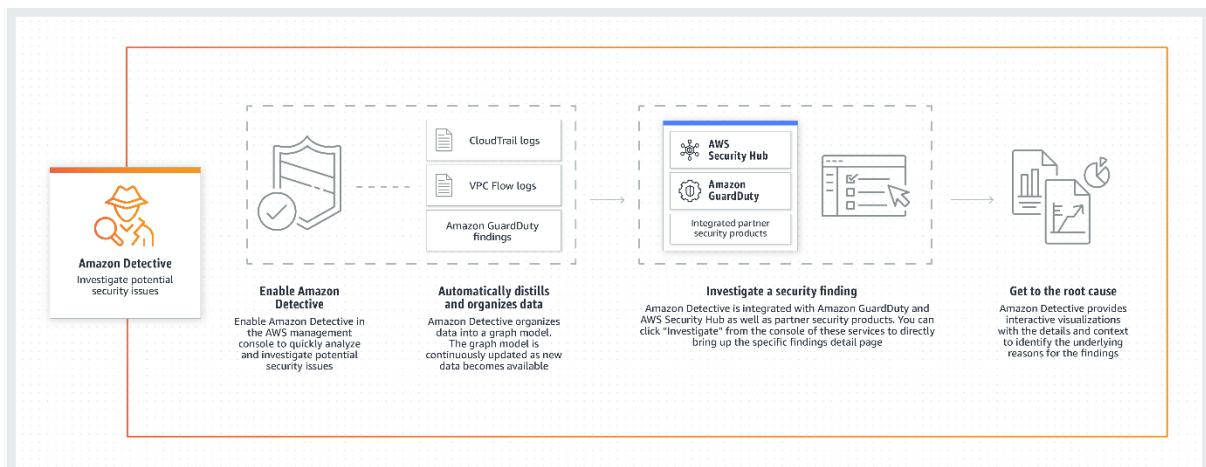
Correct option:

AWS CloudTrail logs, Amazon VPC Flow Logs and Amazon GuardDuty findings - Amazon Detective can analyze trillions of events from multiple data sources such as Virtual Private Cloud (VPC) Flow Logs, AWS CloudTrail, and Amazon GuardDuty, and automatically creates a unified, interactive view of your resources, users, and the interactions between them over time.

Amazon Detective conforms to the AWS shared responsibility model, which includes regulations and guidelines for data protection. Once enabled, Amazon Detective will process data from AWS CloudTrail logs, VPC Flow Logs, and Amazon GuardDuty findings for any accounts where it has been turned on.

Amazon Detective requires that you have Amazon GuardDuty enabled on your accounts for at least 48 hours before you enable Detective on those accounts. However, you can use Detective to investigate more than just your GuardDuty findings. Amazon Detective provides detailed summaries, analysis, and visualizations of the behaviors and interactions amongst your AWS accounts, EC2 instances, AWS users, roles, and IP addresses. This information can be very useful in understanding security issues or operational account activity.

How Amazon Detective Works:



via - <https://aws.amazon.com/detective/>

Incorrect options:

Amazon CloudWatch Logs, Amazon VPC Flow Logs and Amazon GuardDuty findings

Amazon CloudWatch Logs, AWS CloudTrail logs and S3 Access Logs

Amazon CloudWatch Logs, AWS CloudTrail logs and Amazon Inspector logs

These three options contradict the explanation provided above, so these options are incorrect.

Reference:

<https://aws.amazon.com/detective/>

Question 23:

Skipped

A Security Group has been changed in an AWS account and the manager of the account has asked you to find out the details of the user who changed it. As a Cloud Practitioner, which AWS service will you use to fetch the necessary information?

-
- AWS Trusted Advisor**
-
- Amazon Inspector**
-
- AWS CloudTrail**
- (Correct)**
-

AWS X-Ray

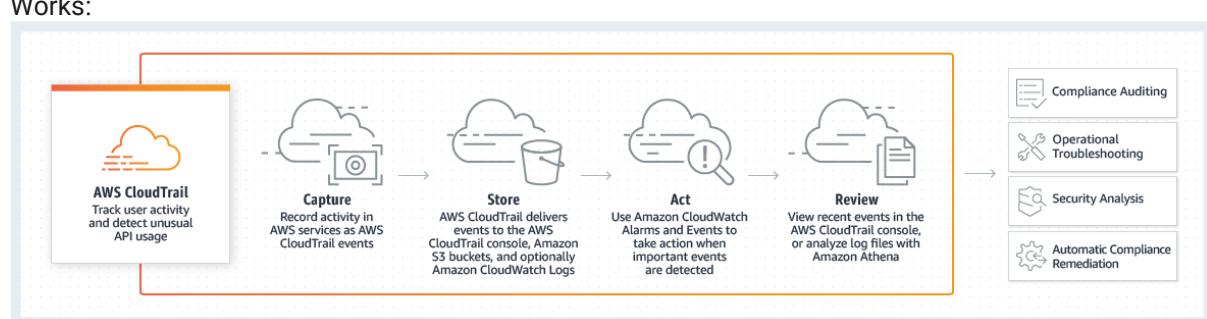
Explanation

Correct option:

AWS CloudTrail - AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command-line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting. In addition, you can use CloudTrail to detect unusual activity in your AWS accounts. These capabilities help simplify operational analysis and troubleshooting.

CloudTrail provides visibility into user activity by recording actions taken on your account. CloudTrail records important information about each action, including who made the request, the services used, the actions performed, parameters for the actions, and the response elements returned by the AWS service. This information helps you to track changes made to your AWS resources and to troubleshoot operational issues. CloudTrail makes it easier to ensure compliance with internal policies and regulatory standards.

How CloudTrail Works:



via - <https://aws.amazon.com/cloudtrail/>

Incorrect options:

AWS X-Ray - AWS X-Ray helps developers analyze and debug production, distributed applications, such as those built using a microservices architecture. With X-Ray, you can understand how your application and its underlying services are performing to identify and troubleshoot the root cause of performance issues and errors. X-Ray provides an end-to-end view of requests as they travel through your application, and shows a map of your application's underlying components. X-Ray is not for tracking user actions when interacting with the AWS systems.

Amazon Inspector - Amazon Inspector is an automated security assessment service that helps you test the network accessibility of your Amazon EC2 instances and the security state of your applications running on the instances. Amazon Inspector allows you to automate security vulnerability assessments throughout your development and deployment pipeline or against static production systems. This allows you to make security testing a more regular occurrence as part of the development and IT operations.

AWS Trusted Advisor - AWS Trusted Advisor is an online tool that provides you real-time guidance to help you provision your resources following AWS best practices. Trusted Advisor checks help optimize your AWS infrastructure, increase security and performance, reduce your overall costs, and monitor service limits. Whether establishing new workflows, developing applications, or as part of ongoing improvement, take advantage of the recommendations provided by Trusted Advisor on a regular basis to help keep your solutions provisioned optimally.

Reference:

<https://aws.amazon.com/cloudtrail/>

Question 24:

Skipped

Which of the following will help you control the incoming traffic to an Amazon EC2 instance?



AWS Resource Group



NACL (Network ACL)



Route Table



Security Group

(Correct)

Explanation

Correct option:

Security Group - A security group acts as a virtual firewall for your EC2 instances to control incoming and outgoing traffic. Inbound rules control the incoming traffic to your instance, and outbound rules control the outgoing traffic from your instance. When you launch an instance, you can specify one or more security groups. If you don't specify a security group, Amazon EC2 uses the default security group. You can add rules to each security group that allows traffic to or from its associated instances. You can modify the rules for a security group at any time. New and modified rules are automatically applied to all instances that are associated with the security group. When Amazon EC2 decides whether to allow traffic to reach an instance, it evaluates all of the rules from all of the security groups that are associated with the instance.

Security is a shared responsibility between AWS and you. AWS provides security groups as one of the tools for securing your instances, and you need to configure them to meet your security needs. If you have requirements that aren't fully met by security groups, you can maintain your own firewall on any of your instances in addition to using security groups.

Incorrect options:

AWS Resource Group - You can use Resource Groups to organize your AWS resources. Resource groups make it easier to manage and automate tasks on large numbers of resources at one time. Resource Groups feature permissions are at the account level. As long as users who are sharing your account have the correct IAM permissions, they can work with resource groups that you create. Resource Groups are for grouping resources for managing the resources. They do not provide access to Amazon EC2 instance.

NACL (Network ACL) - A Network Access Control List (ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC.

Route Table - A Route table contains a set of rules, called routes, that are used to determine where network traffic from your VPC is directed. You can explicitly associate a subnet with a particular route table. Otherwise, the subnet is implicitly associated with the main route table.

Each route in a route table specifies the range of IP addresses where you want the traffic to go (the destination) and the gateway, network interface, or connection through which to send the traffic (the target).

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-security-groups.html>

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html>

Question 25:

Skipped

Which of the following statements are true about AWS Elastic Beanstalk? (Select two)

- **AWS Elastic Beanstalk supports web applications built on different languages. But, Elastic Beanstalk cannot be used for deploying non-web applications**
- **AWS Elastic Beanstalk automates the details of capacity provisioning, load balancing, and application deployment, creating an environment that runs a version of your application. However, auto-scaling functionality cannot be automated using Elastic Beanstalk**
- **With Elastic Beanstalk, you can quickly deploy and manage applications in the AWS Cloud without having to learn about the infrastructure that runs those applications**
(Correct)
- **There is no additional charge for Elastic Beanstalk. You pay only for the underlying AWS resources that your application consumes**
(Correct)
- **AWS Elastic Beanstalk supports Java, .NET, PHP, but does not support Docker web applications**

Explanation

Correct options:

With Elastic Beanstalk, you can quickly deploy and manage applications in the AWS Cloud without having to learn about the infrastructure that runs those applications

There is no additional charge for Elastic Beanstalk. You pay only for the underlying AWS resources that your application consumes

With Elastic Beanstalk, you can quickly deploy and manage applications in the AWS Cloud without having to learn about the infrastructure that runs those applications. Elastic Beanstalk reduces management complexity without restricting choice or control. You simply upload your application, and Elastic Beanstalk automatically handles the details of capacity provisioning, load balancing, scaling, and application health monitoring.

Elastic Beanstalk supports applications developed in Go, Java, .NET, Node.js, PHP, Python, and Ruby. When you deploy your application, Elastic Beanstalk builds the selected supported platform version and provisions one or more AWS resources, such as Amazon EC2 instances, to run your application.

There is no additional charge for Elastic Beanstalk. You pay only for the underlying AWS resources that your application consumes.

Incorrect options:

AWS Elastic Beanstalk supports Java, .NET, PHP, but does not support Docker web applications - AWS Elastic Beanstalk supports Java, .NET, PHP, Node.js, Python, Ruby, Go, and Docker web applications.

AWS Elastic Beanstalk automates the details of capacity provisioning, load balancing, and application deployment, creating an environment that runs a version of your application. However, auto-scaling functionality cannot be automated using Elastic Beanstalk - AWS Elastic Beanstalk automates the details of capacity provisioning, load balancing, auto-scaling, and application deployment, creating an environment that runs a version of your application. You can simply upload your deployable code (e.g., WAR file), and AWS Elastic Beanstalk does the rest.

AWS Elastic Beanstalk supports web applications built on different languages. But, Elastic Beanstalk cannot be used for deploying non-web applications - AWS Elastic Beanstalk supports Java, .NET, PHP, Node.js, Python, Ruby, Go, and Docker, and is ideal for web applications. However, due to Elastic Beanstalk's open architecture, non-web applications can also be deployed using Elastic Beanstalk.

References:

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/Welcome.html>

<https://aws.amazon.com/elasticbeanstalk/faqs/>

Question 26:

Skipped

A financial services company needs to retain its data for 10 years to meet the compliance norms. Which Amazon S3 storage class is the best fit for this use-case considering that the data has to be stored at minimal cost?



Amazon S3 Glacier

-
-

Amazon S3 Glacier Deep Archive

(Correct)

-
-

Amazon S3 Intelligent-Tiering

-
-

Amazon S3 Standard-Infrequent Access

Explanation

Correct option:

Amazon S3 Glacier Deep Archive - S3 Glacier Deep Archive is Amazon S3's lowest-cost storage class and supports long-term retention and digital preservation for data that may be accessed once or twice a year. It is designed for customers – particularly those in highly-regulated industries, such as the Financial Services, Healthcare, and Public Sectors – that retain data sets for 7-10 years or longer to meet regulatory compliance requirements. S3 Glacier Deep Archive can also be used for backup and disaster recovery use cases, and is a cost-effective and easy-to-manage alternative to magnetic tape systems, whether they are on-premises libraries or off-premises services.

S3 Glacier Deep Archive complements Amazon S3 Glacier, which is ideal for archives where data is regularly retrieved and some of the data may be needed in minutes. All objects stored in S3 Glacier Deep Archive are replicated and stored across at least three geographically-dispersed Availability Zones, protected by 99.99999999% of durability, and can be restored within 12 hours.

Incorrect options:

Amazon 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 the on-premises solutions. To keep costs low yet suitable for varying needs, S3 Glacier provides three retrieval options that range from a few minutes to hours. You can upload objects directly to S3 Glacier, or use S3 Lifecycle policies to transfer data between any of the S3 Storage Classes for active data and S3 Glacier.

Amazon 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. S3 Storage Classes can be configured at the object level and a single bucket can contain objects stored across S3 Standard, S3 Intelligent-Tiering, S3 Standard-IA, and S3 One Zone-IA. You can also use S3 Lifecycle policies to automatically transition objects between storage classes without any application changes.

Amazon S3 Intelligent-Tiering - Amazon S3 Intelligent-Tiering (S3 Intelligent-Tiering) is the only cloud storage class that delivers automatic cost savings by moving objects between four access tiers when access patterns change. The S3 Intelligent-Tiering storage class is designed to optimize costs by automatically moving data to the most cost-effective access tier, without operational overhead. It works by storing objects in four access tiers: two low latency access tiers optimized for frequent and

infrequent access, and two optional archive access tiers designed for asynchronous access that are optimized for rare access.

Reference:

<https://aws.amazon.com/s3/storage-classes/>

Question 27:

Skipped

A blogging company is looking at an easy to use solution to host WordPress blogs. The company needs a cost-effective, readily available solution without the need to manage the configurations for servers or the databases.

Which AWS service will help you achieve this functionality?

- Amazon Lightsail**
(Correct)
-
- Host the application directly on Amazon S3**
-
- Amazon Elastic Compute Cloud (EC2) with Amazon S3 for storage**
-

AWS Fargate

Explanation

Correct option:

Amazon Lightsail - Amazon Lightsail is the easiest way to get started with AWS for developers, small businesses, students, and other users who need a solution to build and host their applications on the cloud. Lightsail provides developers with compute, storage, and networking capacity and capabilities to deploy and manage websites and web applications in the cloud. Lightsail includes everything you need to launch your project quickly – virtual machines, containers, databases, CDN, load balancers, DNS management, etc. – for a low, predictable monthly price.

You can get preconfigured virtual private server plans that include everything to easily deploy and manage your application. Lightsail is best suited to projects that require a few virtual private servers and users who prefer a simple management interface. Common use cases for Lightsail include running websites, web applications, blogs, e-commerce sites, simple software, and more.

Also referred to as a bundle, a Lightsail plan includes a virtual server with a fixed amount of memory (RAM) and compute (vCPUs), SSD-based storage (disks), and a free data transfer allowance. Lightsail plans also offer static IP addresses (5 per account) and DNS management (3 domain zones per account). Lightsail plans are charged on an hourly, on-demand basis, so you only pay for a plan when you're using it.

Lightsail offers a number of preconfigured, one-click-to-launch operating systems, development stacks, and web applications, including Linux and Windows OS, WordPress, LAMP, CentOS, and more.

Incorrect options:

AWS Fargate - AWS Fargate is a serverless compute engine for containers that work with both Amazon Elastic Container Service (ECS) and Amazon Elastic Kubernetes Service (EKS). Fargate makes it easy for you to focus on building your applications. Fargate removes the need to provision and manage servers, lets you specify and pay for resources per application, and improves security through application isolation by design. Fargate is meant for container applications that you wish to host without having to manage the servers such as EC2 instances.

Amazon Elastic Compute Cloud (EC2) with Amazon S3 for storage - Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud. It is designed to make web-scale cloud computing easier for developers. Amazon EC2's simple web service interface allows you to obtain and configure capacity with minimal friction. It provides you with complete control of your computing resources and lets you run on Amazon's proven computing environment.

Amazon EC2 instances need to be managed by the customers and hence is the wrong choice for the given scenario.

Host the application directly on Amazon S3 - Amazon S3 does not support compute capacity to generate dynamic content. Only static web applications can be hosted on Amazon S3.

Reference:

<https://aws.amazon.com/lightsail/>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/WebsiteHosting.html>

Question 28:

Skipped

Per the AWS Shared Responsibility Model, management of which of the following AWS services is the responsibility of the customer?

-

Amazon Elastic Compute Cloud (Amazon EC2)

(Correct)

-

Amazon Simple Storage Service (Amazon S3)

-

AWS Elastic Beanstalk

-

Amazon DynamoDB

Explanation

Correct option:

Amazon Elastic Compute Cloud (Amazon EC2) - Security and Compliance is a shared responsibility between AWS and the customer. This shared model can help relieve the customer's operational burden as AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates.

"Security of the Cloud" is the responsibility of AWS - 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.

"Security in the Cloud" is the responsibility of the customer. Customer responsibility will be determined by the AWS Cloud services that a customer selects. This determines the amount of configuration work the customer must perform as part of their security responsibilities. For example, a service such as Amazon Elastic Compute Cloud (Amazon EC2) is categorized as Infrastructure as a Service (IaaS) and, as such, requires the customer to perform all of the necessary security configuration and management tasks. Customers that deploy an Amazon EC2 instance are responsible for the management of the guest operating system (including updates and security patches), any application software or utilities installed by the customer on the instances, and the configuration of the AWS-provided firewall (called a security group) on each instance.

Incorrect options:

Amazon Simple Storage Service (Amazon S3)

Amazon DynamoDB

AWS Elastic Beanstalk

For abstracted services, such as Amazon S3, Amazon DynamoDB and for managed services such as AWS Elastic Beanstalk, AWS operates the infrastructure layer, the operating system, and platforms, and customers access the endpoints to store and retrieve data. Customers are responsible for managing their data (including encryption options), classifying their assets, and using IAM tools to apply the appropriate permissions.

Reference:

<https://aws.amazon.com/compliance/shared-responsibility-model/>

Question 29:

Skipped

Which AWS service is used to store and commit code privately and also offer features for version control?

-

AWS CodeStar

-

AWS CodePipeline

- **AWS CodeBuild**
- **AWS CodeCommit**
(Correct)

Explanation

Correct option:

AWS CodeCommit - AWS CodeCommit is a fully-managed source control service that hosts secure Git-based repositories. It makes it easy for teams to collaborate on code in a secure and highly scalable ecosystem. CodeCommit eliminates the need to operate your own source control system or worry about scaling its infrastructure. You can use CodeCommit to securely store anything from source code to binaries, and it works seamlessly with your existing Git tools.

AWS CodeCommit eliminates the need to host, maintain, back up, and scale your own source control servers. The service automatically scales to meet the growing needs of your project. AWS CodeCommit automatically encrypts your files in transit and at rest. CodeCommit is integrated with AWS Identity and Access Management (IAM) allowing you to customize user-specific access to your repositories.

AWS CodeCommit supports all Git commands and works with your existing Git tools. You can keep using your preferred development environment plugins, continuous integration/continuous delivery systems, and graphical clients with CodeCommit.

Incorrect options:

AWS CodePipeline - AWS CodePipeline is a fully managed continuous delivery service that helps you automate your release pipelines for fast and reliable application and infrastructure updates. CodePipeline automates the build, test, and deploy phases of your release process every time there is a code change, based on the release model you define. This enables you to rapidly and reliably deliver features and updates.

AWS CodeBuild - AWS CodeBuild is a fully managed continuous integration service that compiles source code, runs tests, and produces software packages that are ready to deploy. With CodeBuild, you don't need to provision, manage, and scale your own build servers. CodeBuild scales continuously and processes multiple builds concurrently, so your builds are not left waiting in a queue. You can get started quickly by using prepackaged build environments, or you can create custom build environments that use your own build tools. With CodeBuild, you are charged by the minute for the compute resources you use.

AWS CodeStar - AWS CodeStar is a cloud-based development service that provides the tools you need to quickly develop, build, and deploy applications on AWS. With AWS CodeStar, you can set up your entire continuous delivery toolchain in minutes, allowing you to start releasing code faster. AWS CodeStar makes it easy for your whole team to work together securely, with built-in role-based policies that allow you to easily manage access and add owners, contributors, and viewers to your projects.

Each CodeStar project includes development tools, including AWS CodePipeline, AWS CodeCommit, AWS CodeBuild and AWS CodeDeploy, that can be used on their own and with existing AWS applications.

References:

<https://aws.amazon.com/codecommit/>

<https://aws.amazon.com/codestar/>

Question 30:

Skipped

A team lead is reviewing the AWS services that can be used in the development workflow for his company. Which of the following statements are correct regarding the capabilities of these AWS services? (Select three)

-

CodePipeline uses Amazon CloudWatch Events to detect changes in CodeCommit repositories used as a source for a pipeline

(Correct)

-

Each CodeStar project includes development tools, including AWS CodePipeline, AWS CodeCommit, AWS CodeBuild, and AWS CodeDeploy, that can be used on their own and with existing AWS applications

(Correct)

-

AWS CodeStar is a cloud-based integrated development environment that lets you write, run, and debug your code with just a browser

-

CodeCommit allows you to run builds and tests as part of your CodePipeline

-

You can use AWS CodeStar and AWS Cloud9 to develop, build, and deploy a serverless web application

(Correct)

-

CodeBuild is directly integrated with both CodePipeline and CodeCommit

Explanation

Correct options:

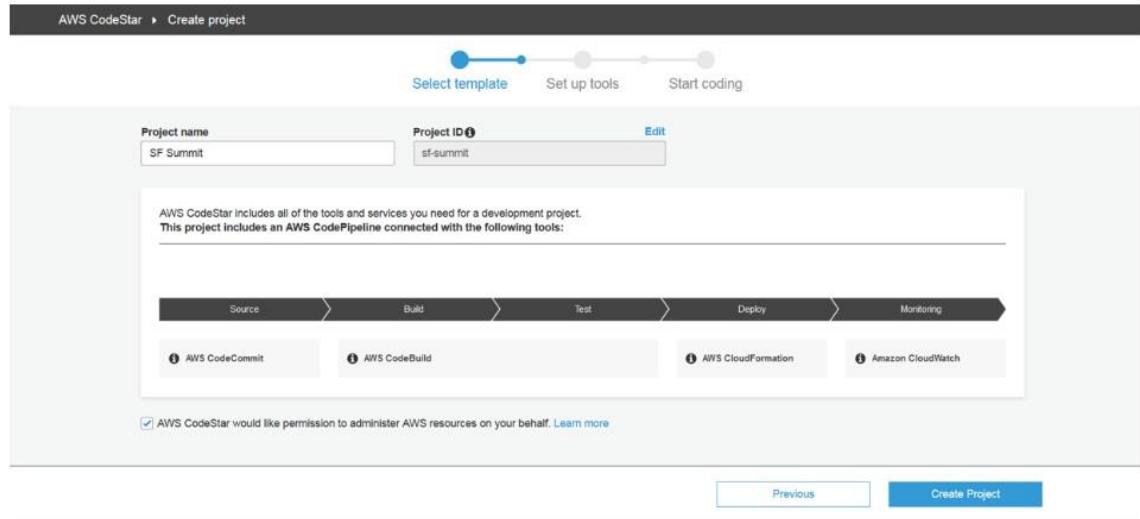
Each CodeStar project includes development tools, including AWS CodePipeline, AWS CodeCommit, AWS CodeBuild, and AWS CodeDeploy, that can be used on their own and with existing AWS applications - AWS CodeStar accelerates software release with the help of AWS CodePipeline, a

continuous integration and continuous delivery (CI/CD) service. Each project comes pre-configured with an automated pipeline that continuously builds, tests, and deploys your code with each commit. AWS CodeStar integrates with AWS CodeDeploy and AWS CloudFormation so that you can easily update your application code and deploy to Amazon EC2 and AWS Lambda.

More information on AWS CodeStar:

Automated continuous delivery pipeline

AWS CodeStar accelerates software release with the help of [AWS CodePipeline](#), a continuous integration and continuous delivery (CI/CD) service. Each project comes pre-configured with an automated pipeline that continuously builds, tests, and deploys your code with each commit.



via - <https://aws.amazon.com/codestar/features/>

CodePipeline uses Amazon CloudWatch Events to detect changes in CodeCommit repositories used as a source for a pipeline - CodePipeline uses Amazon CloudWatch Events to detect changes in CodeCommit repositories used as a source for a pipeline. Each source action has a corresponding event rule. This event rule starts your pipeline when a change occurs in the repository.

CodePipeline integration with CodeCommit:

CodeCommit source actions

CodeCommit	<p>CodeCommit is a version control service that you can use to privately store and manage assets (such as documents, source code, and binary files) in the cloud. You can configure CodePipeline to use a branch in a CodeCommit repository as the source for your code. Create the repository and associate it with a working directory on your local machine. Then you can create a pipeline that uses the branch as part of a source action in a stage. You can connect to the CodeCommit repository by either creating a pipeline or editing an existing one.</p> <p>You can use the Full clone option for this action to reference the repository Git metadata so that downstream actions can perform Git commands directly. This option can only be used by CodeBuild downstream actions.</p> <p>Learn more:</p> <ul style="list-style-type: none">• To view configuration parameters and an example JSON/YAML snippet, see CodeCommit.• Tutorial: Create a simple pipeline (CodeCommit repository)• CodePipeline uses Amazon CloudWatch Events to detect changes in CodeCommit repositories used as a source for a pipeline. Each source action has a corresponding event rule. This event rule starts your pipeline when a change occurs in the repository. See General integrations with CodePipeline.
-------------------	---

via - <https://docs.aws.amazon.com/codepipeline/latest/userguide/integrations-action-type.html>

You can use AWS CodeStar and AWS Cloud9 to develop, build, and deploy a serverless web application - AWS CodeStar is a cloud-based development service that provides the tools you need to quickly develop, build, and deploy applications on AWS. AWS Cloud9 is a cloud-based integrated development environment (IDE) that lets you write, run, and debug your code with just a browser. Together, the two services can be used to build serverless applications in very little time.

Incorrect options:

CodeBuild is directly integrated with both CodePipeline and CodeCommit - CodeCommit can trigger a Lambda function that in turns invokes a CodeBuild job, therefore CodeBuild has an indirect integration with CodeCommit. However, CodePipeline is directly integrated with both CodeBuild and CodeCommit because CodePipeline can use source action integrations with CodeCommit and build action integrations with CodeBuild.

CodeCommit allows you to run builds and tests as part of your CodePipeline - CodeCommit is a version control service that you can use to privately store and manage assets (such as documents, source code, and binary files) in the cloud. AWS CodeBuild is a fully managed continuous integration service that compiles source code, runs tests, and produces software packages that are ready to deploy. CodeBuild allows you to run builds and tests as part of your pipeline.

AWS CodeStar is a cloud-based integrated development environment that lets you write, run, and debug your code with just a browser - AWS CodeStar is a cloud-based development service that provides the tools you need to quickly develop, build, and deploy applications on AWS. AWS Cloud9 is a cloud-based integrated development environment (IDE) that lets you write, run, and debug your code with just a browser.

Here is an example to explain the collaboration between these services - You can use AWS CodeStar to build a new AWS Lambda based Node.js serverless web application. You will use AWS CodeStar to set up a continuous delivery mechanism using AWS CodeCommit for source control and AWS CodePipeline to automate your release process. You can then change some code in the Node.js project using Cloud9 and commit the change to trigger your continuous pipeline and redeploy your project.

Build a Serverless Application using AWS CodeStar and AWS Cloud9:

In this tutorial you will learn how to use AWS CodeStar and AWS Cloud9 to develop, build, and deploy a Node.js serverless web application. As a developer, setting up an automated software development workflow can be a time-intensive, detailed task. AWS CodeStar is a software development tool that enables you to quickly develop, build, and deploy applications on AWS. With CodeStar, you can setup your continuous delivery toolchain in minutes, allowing you to start releasing code faster.

Cloud9 is a cloud IDE for writing, running, and debugging code. Cloud9 comes prepackaged with essential tools for many popular programming languages (JavaScript, Python, PHP, etc.) so you don't have to tinker with installing various compilers and toolchains.

In the next several minutes, you'll use AWS CodeStar to build a new AWS Lambda based Node.js serverless web application. You will use AWS CodeStar to set up a continuous delivery toolchain using AWS CodeCommit for source control and AWS CodePipeline to automate your release process. You will then change some code in the Node.js project using Cloud9 and commit the change to trigger your continuous pipeline and redeploy your project.

via - <https://aws.amazon.com/getting-started/hands-on/build-serverless-app-codestar-cloud9/>

References:

<https://aws.amazon.com/codestar/faqs/>

<https://aws.amazon.com/codebuild/>

<https://aws.amazon.com/cloud9/>

Question 31:

Skipped

A gaming company needs compute and storage services close to edge locations in order to ensure ultra-low latency for end-users and devices that connect through mobile networks. Which AWS service is the best fit for this requirement?

-

AWS Wavelength

(Correct)

-

AWS Snowmobile

-

AWS Outposts

-

AWS Snowball Edge

Explanation

Correct option:

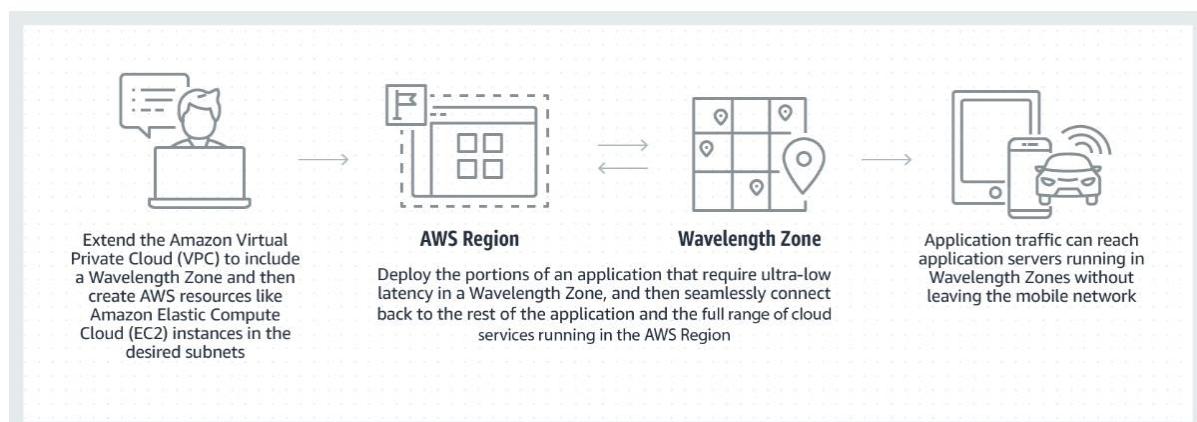
AWS Wavelength - AWS Wavelength is an AWS Infrastructure offering optimized for mobile edge computing applications. Wavelength Zones are AWS infrastructure deployments that embed AWS compute and storage services within communications service providers' (CSP) data centers at the edge of the 5G network, so application traffic from 5G devices can reach application servers running in Wavelength Zones without leaving the telecommunications network. This avoids the latency that would result from application traffic having to traverse multiple hops across the Internet to reach their destination, enabling customers to take full advantage of the latency and bandwidth benefits offered by modern 5G networks.

AWS enterprise customers that build applications to serve their own use-cases such as IoT, live media production, and industrial automation can use Wavelength to deliver low-latency solutions. Customers with edge data processing needs such as image and video recognition, inference, data aggregation, and responsive analytics can use Wavelength to perform low-latency operations and processing right where their data is generated, reducing the need to move large amounts of data to be processed in centralized locations.

How Wavelength works:

How it works

Getting started is easy, you simply log-in to the AWS Management Console and enable the Wavelength Zones you want to use for your account.



via - <https://aws.amazon.com/wavelength/>

Incorrect options:

AWS Outposts - AWS Outposts is designed for workloads that need to remain on-premises due to latency requirements, where customers want that workload to run seamlessly with the rest of their other workloads in AWS. AWS Outposts are fully managed and configurable compute and storage racks built with AWS-designed hardware that allow customers to run compute and storage on-premises, while seamlessly connecting to AWS's broad array of services in the cloud.

You should also note another service called AWS Local Zones, which is a new type of AWS infrastructure designed to run workloads that require single-digit millisecond latency in more locations, like video rendering and graphics intensive, virtual desktop applications. Not every customer wants to operate their own on-premises data center, while others may be interested in getting rid of their local data center entirely. Local Zones allow customers to gain all the benefits of having compute and storage resources closer to end-users, without the need to own and operate their own data center infrastructure.

AWS Snowball Edge - AWS Snowball Edge is a type of Snowball device with on-board storage and compute power for select AWS capabilities. Snowball Edge can do local processing and edge-computing workloads in addition to transferring data between your local environment and the AWS Cloud. Snowball edge cannot be used to optimize connections through mobile networks.

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. Snowmobile cannot be used to optimize connections through mobile networks.

Reference:

<https://aws.amazon.com/wavelength/>

Question 32:

Skipped

Which of the following AWS services can be used to continuously monitor both malicious activities as well as unauthorized behavior to protect your AWS accounts and workloads?



AWS Security Hub



Amazon Detective



Amazon GuardDuty

(Correct)



Amazon Inspector

Explanation

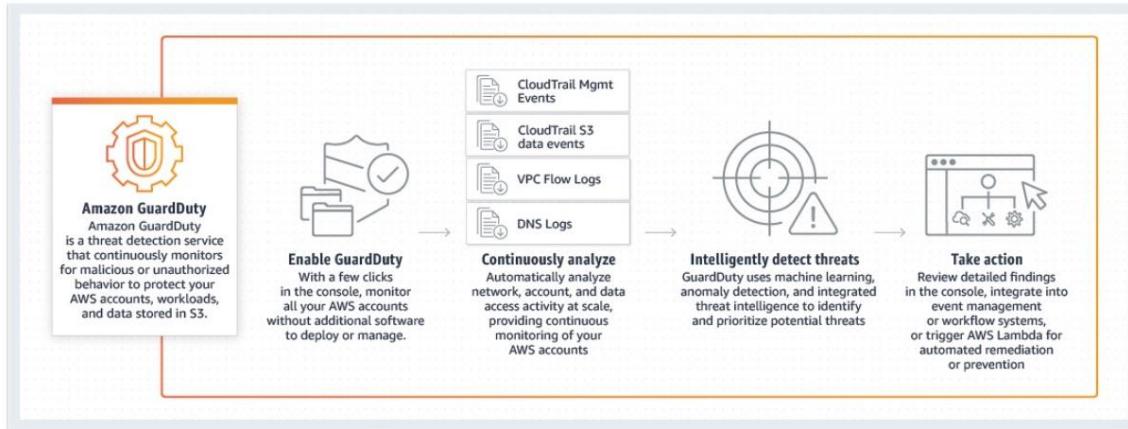
Correct option:

Amazon GuardDuty - Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts, workloads, and data stored in Amazon S3. With the cloud, the collection and aggregation of account and network activities are simplified, but it can be time-consuming for security teams to continuously analyze event log data for potential threats. With GuardDuty, you now have an intelligent and cost-effective option for continuous threat detection in AWS.

The service uses machine learning, anomaly detection, and integrated threat intelligence to identify and prioritize potential threats. GuardDuty analyzes tens of billions of events across multiple AWS data sources, such as AWS CloudTrail event logs, Amazon VPC Flow Logs, and DNS logs. With a few clicks in the AWS Management Console, GuardDuty can be enabled with no software or hardware to deploy or maintain.

Amazon GuardDuty makes it easy for you to enable continuous monitoring of your AWS accounts, workloads, and data stored in Amazon S3. It operates completely independently from your resources so there is no risk of performance or availability impacts to your workloads. It's fully managed with integrated threat intelligence, anomaly detection, and machine learning. Amazon GuardDuty delivers detailed and actionable alerts that are easy to integrate with existing event management and workflow systems. There are no upfront costs and you pay only for the events analyzed, with no additional software to deploy or subscriptions to threat intelligence feeds required.

How GuardDuty Works:



via - <https://aws.amazon.com/guardduty/>

Incorrect options:

AWS Security Hub - AWS Security Hub gives you a comprehensive view of your security alerts and security posture across your AWS accounts. There is a range of powerful security tools at your disposal, from firewalls and endpoint protection to vulnerability and compliance scanners. With Security Hub, you have a single place that aggregates, organizes, and prioritizes your security alerts, or findings, from multiple AWS services, such as Amazon GuardDuty, Amazon Inspector, and Amazon Macie, as well as from AWS Partner solutions.

Amazon Detective - Amazon Detective simplifies the process of investigating security findings and identifying the root cause. Amazon Detective analyzes trillions of events from multiple data sources such as VPC Flow Logs, AWS CloudTrail logs, and Amazon GuardDuty findings and automatically creates a graph model that provides you with a unified, interactive view of your resources, users, and the interactions between them over time.

Amazon Inspector - Amazon Inspector is an automated security assessment service that helps you test the network accessibility of your Amazon EC2 instances and the security state of your applications running on the instances. Amazon Inspector allows you to automate security vulnerability assessments throughout your development and deployment pipeline or against static production systems. This allows you to make security testing a more regular occurrence as part of the development and IT operations.

References:

<https://aws.amazon.com/guardduty/>

<https://aws.amazon.com/detective/faqs/>

Question 33:

Skipped

Which of the following statements are correct regarding the AWS Control Tower and Service Control Policies? (Select two)

-

Service Control Policies (SCPs), by default, effect all the users in the AWS Organization. They have to be configured to effect only the member accounts, if needed

-

Service Control Policies (SCPs) are a type of organization policy that you can use to manage permissions in your organization

(Correct)

-

Control Tower is an AWS native service providing a pre-defined set of blueprints and guardrails to help customers implement a landing zone for new AWS accounts

(Correct)

-

AWS Control Tower helps you deploy a multi-account AWS environment and operate it with day-to-day reminders and recommendations

-

Service Control Policies (SCPs) can help grant permissions to the accounts in your organization

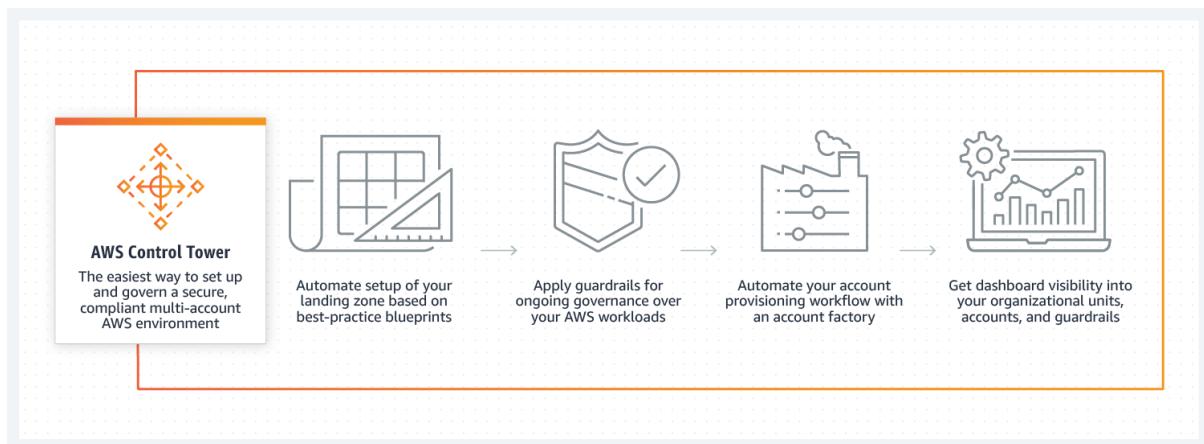
Explanation

Correct options:

Control Tower is an AWS native service providing a pre-defined set of blueprints and guardrails to help customers implement a landing zone for new AWS accounts - Control Tower is an AWS native service providing a pre-defined set of blueprints and guardrails to help customers implement a landing zone for new AWS accounts.

Control Tower is designed to provide an easy, self-service setup experience and an interactive user interface for ongoing governance with guardrails. While Control Tower automates creation of a new landing zone with pre-configured blueprints (e.g., AWS SSO for directory and access), the AWS Landing Zone solution provides a configurable setup of a landing zone with rich customization options through custom add-ons (e.g., Active Directory, Okta Directory) and ongoing modifications through a code deployment and configuration pipeline.

How AWS Control Tower Works:



via - <https://aws.amazon.com/controlltower/>

Service control policies (SCPs) are a type of organization policy that you can use to manage permissions in your organization - Service control policies (SCPs) are a type of organization policy that you can use to manage permissions in your organization. SCPs offer central control over the maximum available permissions for all accounts in your organization. SCPs help you to ensure your accounts stay within your organization's access control guidelines. SCPs are available only in an organization that has all features enabled. SCPs aren't available if your organization has enabled only the consolidated billing features.

Incorrect options:

AWS Control Tower helps you deploy a multi-account AWS environment and operate it with day-to-day reminders and recommendations - AWS Control Tower helps you deploy a multi-account AWS environment based on best practices, however, the customer is still responsible for day-to-day operations and checking compliance status. Enterprises that need help operating regulated infrastructure in the cloud should consider a certified MSP partner or AWS Managed Services (AMS).

Service Control Policies (SCPs) can help grant permissions to the accounts in your organization - SCPs alone are not sufficient to grant permissions to the accounts in your organization. No permissions are granted by an SCP. An SCP defines a guardrail, or sets limits, on the actions that the account's administrator can delegate to the IAM users and roles in the affected accounts. The administrator must still attach identity-based or resource-based policies to IAM users or roles, or to the resources in your accounts to actually grant permissions. The effective permissions are the logical intersection between what is allowed by the SCP and what is allowed by the IAM and resource-based policies.

Service Control Policies (SCPs), by default, affect all the users in the AWS Organization. They have to be configured to affect only the member accounts if needed - SCPs don't affect users or roles in the management account. They affect only the member accounts in your organization.

References:

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps.html

<https://aws.amazon.com/controlltower/faqs/>

Question 34:

Skipped

A company is planning to move their traditional CRM application running on MySQL to an AWS database service. Which database service is the right fit for this requirement?



Amazon Aurora

(Correct)



Amazon Neptune



Amazon DynamoDB



Amazon ElastiCache

Explanation

Correct option:

Amazon Aurora - Amazon Aurora is a relational database engine that combines the speed and reliability of high-end commercial databases with the simplicity and cost-effectiveness of open source databases. Amazon Aurora MySQL delivers up to five times the performance of MySQL without requiring any changes to most MySQL applications; similarly, Amazon Aurora PostgreSQL delivers up to three times the performance of PostgreSQL. Amazon RDS manages your Amazon Aurora databases, handling time-consuming tasks such as provisioning, patching, backup, recovery, failure detection and repair. You pay a simple monthly charge for each Amazon Aurora database instance you use. There are no upfront costs or long-term commitments required.

Amazon Aurora features a distributed, fault-tolerant, self-healing storage system that auto-scales up to 128TB per database instance. It delivers high performance and availability with up to 15 low-latency read replicas, point-in-time recovery, continuous backup to Amazon S3, and replication across three Availability Zones (AZs).

You can use the standard mysqldump utility to export data from MySQL and mysqlimport utility to import data to Amazon Aurora, and vice-versa. You can also use Amazon RDS's DB Snapshot migration feature to migrate an RDS MySQL DB Snapshot to Amazon Aurora using the AWS Management Console. Migration completes for most customers in under an hour, though the duration depends on format and data set size.

Incorrect options:

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-active, durable database with built-in security, backup and restore, and in-memory caching for internet-scale applications. DynamoDB can handle more than 10 trillion requests per day and can support peaks of more than 20 million requests per second. DynamoDB is not for relational databases.

Amazon Neptune - Amazon Neptune is a fast, reliable, fully-managed graph database service that makes it easy to build and run applications that work with highly connected datasets. The core of Amazon Neptune is a purpose-built, high-performance graph database engine optimized for storing billions of relationships and querying the graph with milliseconds latency. Amazon Neptune is tailor-built for use cases like Knowledge Graphs, Identity Graphs, Fraud Detection, Recommendation Engines, Social Networking, Life Sciences, and so on. Amazon Neptune is not for relational databases.

Amazon ElastiCache - Amazon ElastiCache allows you to seamlessly set up, run, and scale popular open-source compatible in-memory data stores in the cloud. Build data-intensive apps or boost the performance of your existing databases by retrieving data from high throughput and low latency in-memory data stores. ElastiCache however, is not a relational database solution.

Reference:

<https://aws.amazon.com/rds/aurora/>

Question 35:

Skipped

Which of the following statements are correct regarding the AWS Support Plans? (Select two)

- **A designated Technical Account Manager is available only for Enterprise support plans**
(Correct)
- **Infrastructure Event Management is included for free for Business and Enterprise support plans and can be extended to a Developer support plan for an additional fee**
- **Both Basic and Developer Support plans have access to 7 core Trusted Advisor checks**
(Correct)
- **Contextual guidance based on customer use-case, is available only for Enterprise support plans**
- **AWS Concierge service is available for Business and Enterprise support plans**

Explanation

Correct options:

A designated Technical Account Manager is available only for Enterprise support plans - A designated Technical Account Manager (TAM) is the primary point of contact who provides guidance, architectural review, and ongoing communication to keep the customer informed and well prepared as they plan, deploy, and proactively optimize their AWS solutions. As the cornerstone of the Enterprise Support plan, your TAM serves as your guide and advocate, focused on delivering the right resources to support the success and ongoing operational health of your AWS infrastructure.

Both Basic and Developer Support plans have access to 7 core Trusted Advisor checks - AWS Trusted Advisor draws upon best practices learned from the aggregated operational history of serving hundreds of thousands of AWS customers. Trusted Advisor inspects your AWS environment and alerts you to opportunities to save money, improve system availability and performance, or help close

security gaps. Access to the 7 core Trusted Advisor checks, and guidance to resources provision following best practices to increase performance and improve security are part of Basic and Developer support plans.

Incorrect options:

AWS Concierge service is available for Business and Enterprise support plans - AWS Concierge is a senior customer service agent who is assigned to your account when you subscribe to an Enterprise or qualified Reseller Support plan. This Concierge agent is your primary point of contact for billing or account inquiries; when you don't know whom to call, they will find the right people to help. In most cases, the AWS Concierge is available during regular business hours in your headquarters' geography.

Contextual guidance based on customer use-case, is available only for Enterprise support plans - Contextual guidance on how services fit together to meet your specific use-case, workload, or application is part of Business support plans.

Infrastructure Event Management is included for free for Business and Enterprise support plans and can be extended to a Developer support plan for an additional fee - AWS Infrastructure Event Management is a short-term engagement with AWS Support, available as part of the Enterprise-level Support product offering, and available for additional purchase for Business-level Support subscribers. AWS Infrastructure Event Management partners with your technical and project resources to gain a deep understanding of your use case and provide architectural and scaling guidance for an event. Common use-case examples for AWS Event Management include advertising launches, new product launches, and infrastructure migrations to AWS.

Reference:

<https://aws.amazon.com/premiumsupport/plans/>

Question 36:

Skipped

Which tool/service will help you get a forecast of your spending for the next 12 months?

-
-

AWS Marketplace

-
-

AWS Cost Explorer

(Correct)

-
-

Consolidated Billing of AWS Organizations

-
-

AWS Pricing Calculator

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 a number of filtering dimensions (e.g., AWS Service, Region, Member 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.

You can explore your usage and costs using the main graph, the Cost Explorer cost, and usage reports, or the Cost Explorer RI report. You can view data for up to the last 12 months, forecast how much you're likely to spend for the next 12 months, and get recommendations for what Reserved Instances to purchase. You can use Cost Explorer to identify areas that need further inquiry and see trends that you can use to understand your costs.

You can view your costs and usage using the Cost Explorer user interface free of charge. You can also access your data programmatically using the Cost Explorer API.

When you first sign up for Cost Explorer, AWS prepares the data about your costs for the current month and the last 12 months and then calculates the forecast for the next 12 months. The current month's data is available for viewing in about 24 hours. The rest of your data takes a few days longer. Cost Explorer updates your cost data at least once every 24 hours. After you sign up, Cost Explorer can display up to 12 months of historical data (if you have that much), the current month, and the forecasted costs for the next 12 months.

Incorrect options:

Consolidated Billing of AWS Organizations - AWS products and services are designed to accommodate every size of the company, from small start-ups to enterprises. If your company is large or likely to grow, you might want to set up multiple AWS accounts that reflect your company's structure. If you create multiple accounts, you can use the Consolidated Billing feature of AWS Organizations to combine all member accounts under a management account and receive a single bill.

AWS Pricing Calculator - AWS Pricing Calculator lets you explore AWS services and create an estimate for the cost of your use cases on AWS. You can model your solutions before building them, explore the price points and calculations behind your estimate, and find the available instance types and contract terms that meet your needs. This enables you to make informed decisions about using AWS. You cannot use this service to get a forecast of your spending for the next 12 months.

AWS Marketplace - AWS Marketplace is a digital catalog with thousands of software listings from independent software vendors that make it easy to find, test, buy, and deploy software that runs on AWS.

References:

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/ce-what-is.html>

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/billing-what-is.html>

<https://aws.amazon.com/aws-cost-management/>

Question 37:

Skipped

AWS Support plans are designed to give the right mix of tools and access to expertise for successfully running a business using AWS.

Which support plan(s) offer the full set of checks for AWS Trusted Advisor best practices and also provide support for programmatic case management?

-
- Business support plans after paying an additional fee and Enterprise support plans**
-
- Only Enterprise support plans**
-
- Developer, Business and Enterprise support plans**
-
- Business and Enterprise support plans**

(Correct)

Explanation

Correct option:

Business and Enterprise support plans

AWS Trusted Advisor provides you with real-time guidance to help you provision your resources following AWS best practices.

The full set of Trusted Advisor checks are included with Business and Enterprise Support plans. These checks can help optimize your AWS infrastructure, increase security and performance, reduce your overall costs, and monitor service limits.

AWS Support API provides 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. AWS Support API is only available for Business and Enterprise Support plans.

Comparing AWS Support
Plans:

	Developer	Business	Enterprise
	<i>Recommended if you are experimenting or testing in AWS.</i>	<i>Minimum recommended tier 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	Service Quota and basic Security 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 hours** System impaired: < 12 hours**	General guidance: < 24 hours System impaired: < 12 hours	General guidance: < 24 hours System impaired: < 12 hours Production system impaired: < 4 hours Production system down: < 1 hour Business/Mission-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

via - <https://aws.amazon.com/premiumsupport/plans/>

Incorrect options:

Only Enterprise support plans

Developer, Business and Enterprise support plans

Business support plans after paying an additional fee and Enterprise support plans

These three options contradict the explanation provided above, so these options are incorrect.

Reference:

<https://aws.amazon.com/premiumsupport/plans/>

Question 38:

Skipped

Which of the following AWS services is delivered globally rather than regionally?



AWS Snowmobile



Amazon Elastic File System



Amazon S3 buckets

-

Amazon WorkSpaces

(Correct)

Explanation

Correct option:

Amazon WorkSpaces - AWS offers a broad set of global cloud-based products including compute, storage, database, analytics, networking, machine learning and AI, mobile, developer tools, IoT, security, enterprise applications, and much more.

Due to the nature of the service, some AWS services are delivered globally rather than regionally, such as Amazon Route 53, Amazon Chime, Amazon WorkDocs, Amazon WorkMail, Amazon WorkSpaces, Amazon WorkLink.

Amazon WorkSpaces is a managed, secure Desktop-as-a-Service (DaaS) solution. You can use Amazon WorkSpaces to provision either Windows or Linux desktops in just a few minutes and quickly scale to provide thousands of desktops to workers across the globe.

Incorrect options:

Amazon S3 buckets - You specify an AWS Region when you create your Amazon S3 bucket and hence the S3 buckets are region-specific. For S3 on Outposts, your data is stored in your Outpost on-premises environment, unless you manually choose to transfer it to an AWS Region.

Amazon Elastic File System - Amazon Elastic File System is AWS region-based service. You can use AWS DataSync to copy files between different AWS regions.

AWS Snowmobile - Snowmobile can be made available for use with AWS services in specific AWS regions and hence is a region-specific service. Once all the data is copied into Snowmobile, Snowmobile will be returned to your designated AWS region where your data will be uploaded into the AWS storage services you have selected, such as S3 or Glacier.

Reference:

https://aws.amazon.com/about-aws/global-infrastructure/regions_az/

Question 39:

Skipped

Which of the following statements are correct regarding Amazon API Gateway? (Select two)

-

If an API response is served by the cached data, it is not considered an API call for billing purposes

-

API Gateway can call an AWS Lambda function to create the front door of a serverless application

(Correct)

-

API Gateway creates RESTful APIs, Storage Gateway creates WebSocket APIs

-

API Gateway can be configured to send data directly to Amazon Kinesis Data Stream

(Correct)

-

API Gateway does not yet support API result caching

Explanation

Correct options:

API Gateway can call an AWS Lambda function to create the front door of a serverless application -

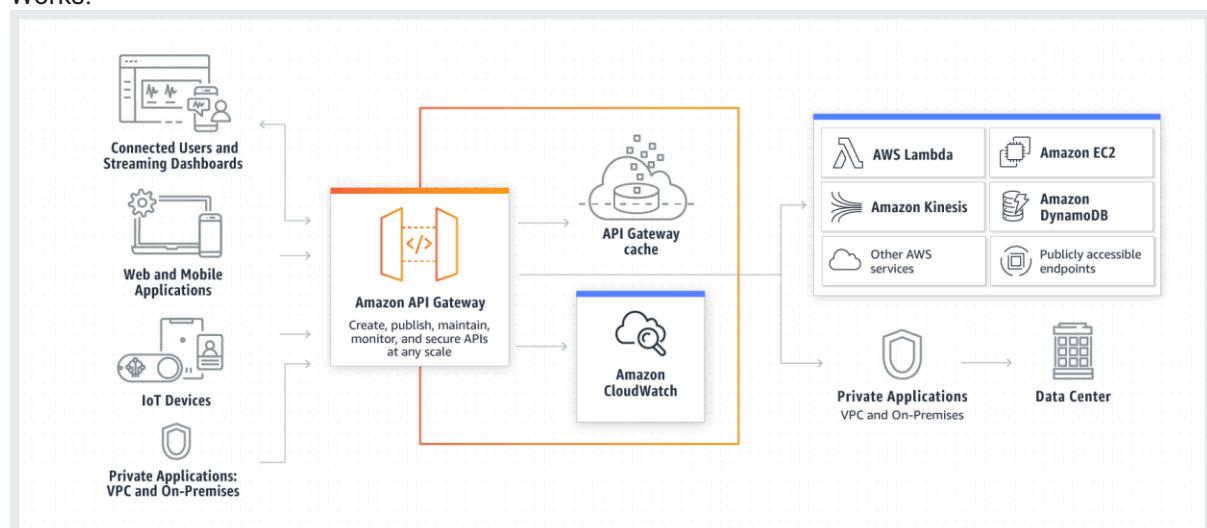
Amazon API Gateway is an AWS service for creating, publishing, maintaining, monitoring, and securing REST, HTTP, and WebSocket APIs at any scale. API developers can create APIs that access AWS or other web services, as well as data stored in the AWS Cloud.

API Gateway acts as a "front door" for applications to access data, business logic, or functionality from your backend services, such as workloads running on Amazon Elastic Compute Cloud (Amazon EC2), code running on AWS Lambda, any web application, or real-time communication applications.

API Gateway can be configured to send data directly to Amazon Kinesis Data Stream - Amazon API Gateway can execute AWS Lambda functions in your account, start AWS Step Functions state machines, or call HTTP endpoints hosted on AWS Elastic Beanstalk, Amazon EC2, and also non-AWS hosted HTTP based operations that are accessible via the public Internet. API Gateway also allows you to specify a mapping template to generate static content to be returned, helping you mock your APIs before the backend is ready. You can also integrate API Gateway with other AWS services directly – for example, you could expose an API method in API Gateway that sends data directly to Amazon Kinesis.

How API Gateway

Works:



via - <https://aws.amazon.com/api-gateway/>

Incorrect options:

API Gateway creates RESTful APIs, Storage Gateway creates WebSocket APIs - Amazon API Gateway is an AWS service for creating, publishing, maintaining, monitoring, and securing REST, HTTP, and WebSocket APIs. AWS Storage Gateway is a hybrid storage solution offered by AWS.

API Gateway does not yet support API result caching - API Gateway supports result caching. You can add caching to API calls by provisioning an API Gateway cache and specifying its size in gigabytes.

If an API response is served by cached data, it is not considered an API call for billing purposes - API calls are counted equally for billing purposes whether the response is handled by your backend operations or by the Amazon API Gateway caching operation.

References:

<https://aws.amazon.com/api-gateway/>

<https://aws.amazon.com/api-gateway/faqs/>

Question 40:

Skipped

Which pillar of AWS Well-Architected Framework focuses on using IT and computing resources efficiently, while considering the right resource types and sizes based on workload requirements?

-
-

Operational Excellence Pillar

-
-

Cost Optimization Pillar

-
-

Reliability Pillar

-
-

Performance Efficiency Pillar

(Correct)

Explanation

Correct option:

Performance Efficiency Pillar - 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.

Performance Efficiency uses the following design principles to help achieve and maintain efficient workloads in the cloud: Democratize advanced technologies, Go global in minutes, Use serverless architectures, Experiment more often and Consider mechanical sympathy.

More information on the Design principles of the Performance Efficiency pillar: via
- <https://d1.awsstatic.com/whitepapers/architecture/AWS-Performance-Efficiency-Pillar.pdf>

Incorrect options:

Operational Excellence Pillar - The operational excellence pillar focuses on running and monitoring systems to deliver business value, and continually improving processes and procedures. Key topics include automating changes, responding to events, and defining standards to manage daily operations.

Cost Optimization Pillar - The cost optimization pillar focuses on avoiding unnecessary costs. Key topics include understanding and controlling where the 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.

Reliability Pillar - The reliability pillar focuses on ensuring a workload performs its intended function correctly and consistently when it's expected to. A resilient workload quickly recovers from failures to meet business and customer demand. Key topics include distributed system design, recovery planning, and how to handle change.

Reference:

<https://aws.amazon.com/architecture/well-architected/>

Question 41:

Skipped

Which of the following represents the correct scenario where an Auto Scaling group's (ASG) predictive scaling can be effectively used to maintain the required number of AWS resources?

- **To manage a fixed number of resources in the Auto Scaling group**
 -
 - **To help configure a scaling policy to keep the average aggregate CPU utilization of your Auto Scaling group at 40 percent**
 -
- To manage a workload that exhibits recurring load patterns that are specific to the day of the week or the time of day**

(Correct)

-

To help configure a CloudWatch Amazon SQS metric like `ApproximateNumberOfMessagesVisible` for scaling the group based on the value of the metric

Explanation

Correct option:

To manage a workload that exhibits recurring load patterns that are specific to the day of the week or the time of day - Predictive scaling uses machine learning to predict capacity requirements based on historical data from CloudWatch. The machine learning algorithm consumes the available historical data and calculates capacity that best fits the historical load pattern, and then continuously learns based on new data to make future forecasts more accurate.

Predictive scaling is well suited for situations where you have:

1. Cyclical traffic, such as high use of resources during regular business hours and low use of resources during evenings and weekends
2. Recurring on-and-off workload patterns, such as batch processing, testing, or periodic data analysis
3. Applications that take a long time to initialize, causing a noticeable latency impact on application performance during scale-out events

Incorrect options:

To help configure a scaling policy to keep the average aggregate CPU utilization of your Auto Scaling group at 40 percent - Target tracking scaling policy is the best fit for this use case. With target tracking scaling policies, you select a scaling metric and set a target value. Amazon EC2 Auto Scaling creates and manages the CloudWatch alarms that trigger the scaling policy and calculates the scaling adjustment based on the metric and the target value. The scaling policy adds or removes capacity as required to keep the metric at, or close to, the specified target value.

To help configure a CloudWatch Amazon SQS metric like `ApproximateNumberOfMessagesVisible` for scaling the group based on the value of the metric - Target tracking scaling policy with `backlog per instance metric` is the best fit for this use case. That's because the number of messages in your SQS queue does not solely define the number of instances needed. The number of instances in your Auto Scaling group can be driven by multiple factors, including how long it takes to process a message and the acceptable amount of latency (queue delay).

To manage a fixed number of resources in the Auto Scaling group - Maintaining current instance levels at all times to a fixed number is a basic way to configure an ASG. Predictive Scaling is not needed to maintain a fixed number of resources.

References:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-predictive-scaling.html>

https://docs.aws.amazon.com/autoscaling/ec2/userguide/scaling_plan.html

Question 42:

Skipped

Historically, IT departments had to over-provision for peak demand. IT professionals may bring this legacy mindset to the table when they build their cloud infrastructure leading to over-provisioned resources and unnecessary costs. Right-sizing of resources is necessary to reduce infrastructure costs while still using cloud functionality optimally.

Which feature of the AWS Cloud refers to right sizing the resources?



Reliability



Resiliency



Elasticity

(Correct)



Horizontal scaling

Explanation

Correct option:

Elasticity - Most people, when thinking of cloud computing, think of the ease with which they can procure resources when needed. This is only one aspect to elasticity. The other aspect is to contract when they no longer need resources. Scale out and scale in. Scale up and scale down.

The ability to acquire resources as you need them and release resources when you no longer need them. In the cloud, you want to do this automatically.

Some AWS services do this as part of their service: Amazon S3, Amazon SQS, Amazon SNS, Amazon SES, Amazon Aurora, etc. Some require vertical scaling, like Amazon RDS. Others integrate with AWS Auto Scaling, like Amazon EC2, Amazon ECS, AWS Fargate, Amazon EKS, and Amazon DynamoDB. Amazon Aurora Serverless and Amazon Athena also qualify as elastic.

Incorrect options:

Reliability - The ability of a workload to perform its intended function correctly and consistently when it's expected to. This includes the ability to operate and test the workload through its total lifecycle.

Resiliency - The ability of a workload to recover from infrastructure or service disruptions, dynamically acquire computing resources to meet demand, and mitigate disruptions, such as misconfigurations or transient network issues.

Horizontal scaling - A "horizontally scalable" system can increase capacity by adding more computers to the system. This is in contrast to a "vertically scalable" system, which is constrained to running its processes on only one computer; in such systems, the only way to increase performance is to add more resources into one computer in the form of faster (or more) CPUs, memory or storage.

References:

<https://wa.aws.amazon.com/wellarchitected/2020-07-02T19-33-23/wat.concept.elasticity.en.html>

<https://wa.aws.amazon.com/wellarchitected/2020-07-02T19-33-23/wat.concepts.wa-concepts.en.html>

Question 43:

Skipped

Which AWS service allows you to connect any number of IoT devices to the cloud without requiring you to provision or manage servers?

-

AWS IoT Gateway

-

AWS IoT Core

(Correct)

-

AWS Control Tower

-

Amazon Connect

Explanation

Correct option:

AWS IoT Core - AWS IoT Core lets you connect IoT devices to the AWS cloud without the need to provision or manage servers. AWS IoT Core can support billions of devices and trillions of messages and can process and route those messages to AWS endpoints and to other devices reliably and securely. With AWS IoT Core, your applications can keep track of and communicate with all your devices, all the time, even when they aren't connected.

AWS IoT Core also makes it easy to use AWS and Amazon services like AWS Lambda, Amazon Kinesis, Amazon S3, Amazon SageMaker, Amazon DynamoDB, Amazon CloudWatch, AWS CloudTrail, Amazon QuickSight, and Alexa Voice Service to build IoT applications that gather, process, analyze and act on data generated by connected devices, without having to manage any infrastructure.

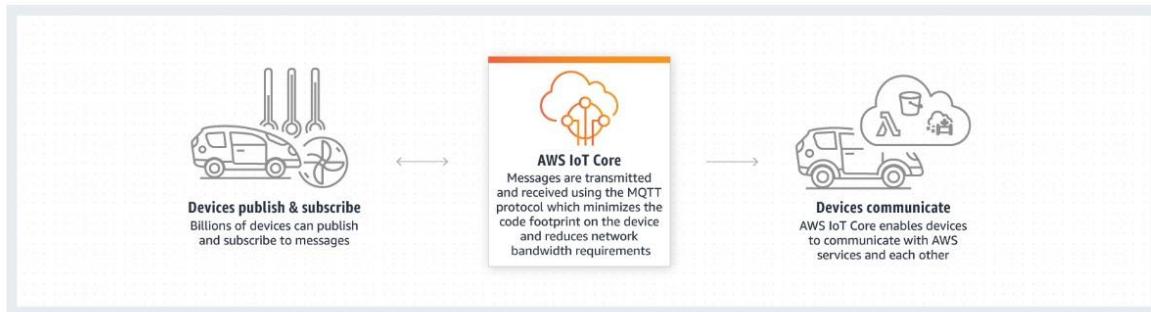
AWS IoT Core lets you select the communication protocol most appropriate for your use case to connect and manage IoT devices. AWS IoT Core supports MQTT (Message Queuing and Telemetry Transport), HTTPS (Hypertext Transfer Protocol - Secure), MQTT over WSS (WebSockets Secure), and LoRaWAN (low-power long-range wide-area network).

AWS IoT Core provides automated configuration and authentication upon a device's first connection to AWS IoT Core, as well as end-to-end encryption throughout all points of connection, so that data is never exchanged between devices and AWS IoT Core without proven identity. In addition, you can secure access to your devices and applications by applying policies with granular permissions.

AWS IoT Core
capabilities:

Publish and subscribe to messages with message broker

The Message Broker is a high throughput publish/subscribe (pub/sub) message broker that securely transmits messages to and from all of your IoT devices and applications with low latency. AWS IoT Core supports devices and clients that use the MQTT and the MQTT over WSS protocols to pub/sub to messages, and devices and clients that use the HTTPS protocol to publish messages.



via - <https://aws.amazon.com/iot-core/>

Incorrect options:

Amazon Connect - Amazon Connect is an easy to use omnichannel cloud contact center that helps you provide superior customer service at a lower cost. Designed from the ground up to be omnichannel, Amazon Connect provides a seamless experience across voice and chat for your customers and agents. This includes one set of tools for skills-based routing, task management, powerful real-time and historical analytics, and intuitive management tools – all with pay-as-you-go pricing, which means Amazon Connect simplifies contact center operations, improves agent efficiency, and lowers costs.

AWS IoT Gateway - This is a made-up option and has been added as a distractor.

AWS Control Tower - AWS Control Tower provides the easiest way to set up and govern a new, secure, multi-account AWS environment based on best practices established through AWS' experience working with thousands of enterprises as they move to the cloud. Control Tower provides mandatory and strongly recommended high-level rules, called guardrails, that help enforce your policies using service control policies (SCPs), or detect policy violations using AWS Config rules.

References:

<https://docs.aws.amazon.com/iot/latest/developerguide/what-is-aws-iot.html>

<https://aws.amazon.com/connect/>

<https://aws.amazon.com/transit-gateway/>

<https://aws.amazon.com/controlltower/>

Question 44:

Skipped

By default, which of the following events are logged by AWS CloudTrail?

-
-

Management events

(Correct)



Data events and Insights events



Insights events



Data events

Explanation

Correct option:

Management events - An event in CloudTrail is the record of an activity in an AWS account. This activity can be an action taken by a user, role, or service that is monitorable by CloudTrail. CloudTrail events provide a history of both API and non-API account activity made through the AWS Management Console, AWS SDKs, command line tools, and other AWS services.

There are three types of events that can be logged in CloudTrail: management events, data events, and CloudTrail Insights events.

By default, CloudTrail logs all management events and does not include data events or Insights events. Additional charges apply for data and Insights events. All event types use the same CloudTrail JSON log format.

Management events provide information about management operations that are performed on resources in your AWS account. These are also known as control plane operations. Examples include registering devices, configuring rules for routing data, setting up logging etc.

Incorrect options:

Data events - Data events provide information about the resource operations performed on or in a resource. These are also known as data plane operations. Data events are often high-volume activities. The following data types are recorded: Amazon S3 object-level API activity, AWS Lambda function execution activity, Amazon S3 object-level API activity on AWS Outposts.

Data events are not logged by default when you create a trail. To record CloudTrail data events, you must explicitly add to a trail the supported resources or resource types for which you want to collect activity. Additional charges apply for logging data events.

Insights events - CloudTrail Insights events capture unusual activity in your AWS account. If you have Insights events enabled, and CloudTrail detects unusual activity, Insights events are logged to a different folder or prefix in the destination S3 bucket for your trail. You can also see the type of insight and the incident time period when you view Insights events on the CloudTrail console.

Insights events are disabled by default when you create a trail. To record CloudTrail Insights events, you must explicitly enable Insights event collection on a new or existing trail. Additional charges apply for logging CloudTrail Insights events.

Data events and Insights events - As mentioned above, this option is incorrect.

Reference:

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-concepts.html#cloudtrail-concepts-events>

Question 45:

Skipped

A company is moving its on-premises application to AWS Cloud. The application uses in-memory caches for running custom workloads. Which Amazon EC2 instance type is the right choice for the given requirement?

-
- **Accelerated computing instance types**
-
- **Compute Optimized instance types**
-
- **Memory Optimized instance types**
- **(Correct)**
-
- **Storage Optimized instance types**

Explanation

Correct option:

Memory Optimized instance types - Memory optimized instances are designed to deliver fast performance for workloads that process large data sets in memory. Memory-optimized instances offer large memory size for memory intensive applications including in-memory applications, in-memory databases, in-memory analytics solutions, High Performance Computing (HPC), scientific computing, and other memory-intensive applications.

Amazon EC2 R6g instances are the next-generation of memory-optimized instances powered by Arm-based AWS Graviton2 Processors.

Incorrect options:

Compute Optimized instance types - Compute Optimized instances are designed for applications that benefit from high compute power. These applications include compute-intensive applications like high-performance web servers, high-performance computing (HPC), scientific modelling, distributed analytics, and machine learning inference.

Amazon EC2 C6g instances are the next-generation of compute-optimized instances powered by Arm-based AWS Graviton2 Processors.

Storage Optimized instance types - Dense-storage instances are designed for workloads that require high sequential read and write access to very large data sets, such as Hadoop distributed computing, massively parallel processing data warehousing, and log processing applications. The Dense-storage instances offer the best price/GB-storage and price/disk-throughput across other EC2 instances.

Accelerated computing instance types - Accelerated Computing instance family is a family of instances that use hardware accelerators, or co-processors, to perform some functions, such as floating-point number calculation and graphics processing, more efficiently than is possible in software running on CPUs. Amazon EC2 provides three types of Accelerated Computing instances – GPU compute instances for general-purpose computing, GPU graphics instances for graphics-intensive applications, and FPGA programmable hardware compute instances for advanced scientific workloads.

Reference:

<https://aws.amazon.com/ec2/faqs/>

Question 46:

Skipped

Which of the following AWS services will help provision a logically isolated network for your AWS resources?



Amazon Route 53



AWS PrivateLink



AWS Firewall Manager



Amazon Virtual Private Cloud (Amazon VPC)

(Correct)

Explanation

Correct option:

Amazon VPC - Amazon Virtual Private Cloud (Amazon VPC) is a service that lets you launch AWS resources in a logically isolated virtual network that you define. You have complete control over your virtual networking environment, including the selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways. You can use both IPv4 and IPv6 for most resources in your virtual private cloud, helping to ensure secure and easy access to resources and applications.

As one of AWS's foundational services, Amazon VPC makes it easy to customize your VPC's network configuration. You can create a public-facing subnet for your web servers that have access to the internet. It also lets you place your backend systems, such as databases or application servers, in a private-facing subnet with no internet access. Amazon VPC lets you use multiple layers of security, including security groups and network access control lists, to help control access to Amazon EC2 instances in each subnet.

Incorrect options:

AWS PrivateLink - AWS PrivateLink provides private connectivity between VPCs and services hosted on AWS or on-premises, securely on the Amazon network. By providing a private endpoint to access your services, AWS PrivateLink ensures your traffic is not exposed to the public internet.

Amazon Route 53 - Amazon Route 53 is a highly available and scalable cloud Domain Name System (DNS) web service. It is designed to give developers and businesses an extremely reliable and cost-effective way to route end users to Internet applications by translating names like www.example.com into the numeric IP addresses like 192.0.2.1 that computers use to connect to each other. Amazon Route 53 is fully compliant with IPv6 as well.

AWS Firewall Manager - AWS Firewall Manager is a security management service that allows you to centrally configure and manage firewall rules across your accounts and applications in AWS Organizations. As new applications are created, Firewall Manager makes it easy to bring new applications and resources into compliance by enforcing a common set of security rules.

Reference:

<https://aws.amazon.com/vpc/>

Question 47:

Skipped

A company is looking for ways to make its desktop applications available to the employees from browsers on their devices/laptops. Which AWS service will help achieve this requirement without having to procure servers or maintain infrastructure?

-

Amazon WorkSpaces

-

Amazon Outposts

-

Amazon AppStream 2.0

(Correct)

-

Amazon Snowball

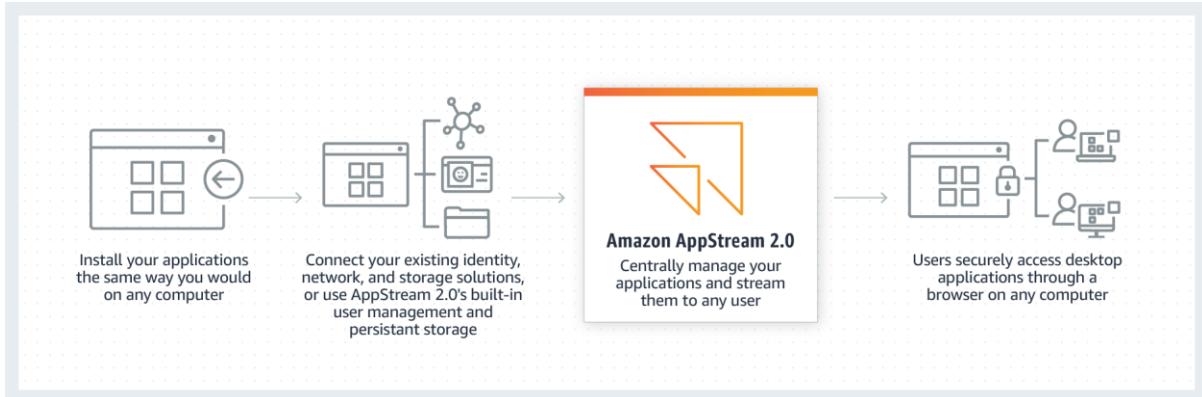
Explanation

Correct option:

Amazon AppStream 2.0 - Amazon AppStream 2.0 is a fully managed non-persistent application and desktop streaming service. You centrally manage your desktop applications on AppStream 2.0 and securely deliver them to any computer. You can easily scale to any number of users across the globe without acquiring, provisioning, and operating hardware or infrastructure. AppStream 2.0 is built on AWS, so you benefit from a data center and network architecture designed for the most security-sensitive organizations. Each end-user has a fluid and responsive experience because your applications run on virtual machines optimized for specific use cases and each streaming session automatically adjusts to network conditions.

Users can access the desktop applications they need at any time. AppStream 2.0 streams your applications from AWS to any computer, including Chromebooks, Macs, and PCs. AppStream 2.0 connects to your Active Directory, network, cloud storage, and file shares. Users access applications using their existing credentials and your existing security policies manage access. Extensive APIs integrate AppStream 2.0 with your IT solutions.

How Amazon AppStream 2.0 Works:



via - <https://aws.amazon.com/appstream2/>

Incorrect options:

Amazon WorkSpaces - Amazon WorkSpaces is a managed, secure Desktop-as-a-Service (DaaS) solution. You can use Amazon WorkSpaces to provision either Windows or Linux desktops in just a few minutes and quickly scale to provide thousands of desktops to workers across the globe. Amazon WorkSpaces helps you eliminate the complexity in managing hardware inventory, OS versions and patches, and Virtual Desktop Infrastructure (VDI), which helps simplify your desktop delivery strategy. With Amazon WorkSpaces, your users get a fast, responsive desktop of their choice that they can access anywhere, anytime, from any supported device.

While Amazon AppStream 2.0 helps move desktop applications to AWS Cloud, so they can be accessed from anywhere; Workspaces provides the entire Desktop environment needed for the workforce.

AWS Outposts - AWS Outposts is a fully managed service that offers the same AWS infrastructure, AWS services, APIs, and tools to virtually any data center, co-location space, or on-premises facility for a truly consistent hybrid experience. AWS Outposts is ideal for workloads that require low latency access to on-premises systems, local data processing, data residency, and migration of applications with local system interdependencies.

AWS Snowball - AWS Snowball, a part of the AWS Snow Family, is an edge computing, data migration, and edge storage device that comes in two options. Snowball Edge Storage Optimized devices provide both block storage and Amazon S3-compatible object storage, and 40 vCPUs. They are well suited for local storage and large scale data transfer.

References:

<https://aws.amazon.com/appstream2/>

<https://aws.amazon.com/workspaces/>

Question 48:

Skipped

A manufacturing company is looking at a service that can offer AWS infrastructure, AWS services, APIs, and tools to its on-premises data center for running low latency applications.

Which of the following service/tool is the best fit for the given requirement?



AWS Outposts

(Correct)



AWS Snow Family



AWS Local Zones



AWS Wavelength

Explanation

Correct option:

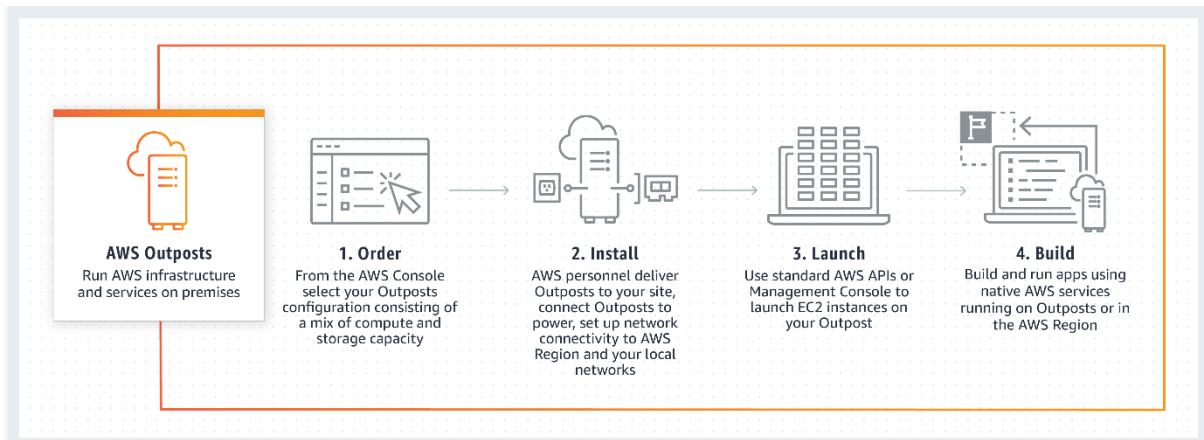
AWS Outposts - AWS Outposts is a fully managed service that offers the same AWS infrastructure, AWS services, APIs, and tools to virtually any data center, co-location space, or on-premises facility for a truly consistent hybrid experience. AWS Outposts is ideal for workloads that require low latency access to on-premises systems, local data processing, data residency, and migration of applications with local system interdependencies.

AWS compute, storage, database, and other services run locally on Outposts, and you can access the full range of AWS services available in the Region to build, manage, and scale your on-premises applications using familiar AWS services and tools.

You can use Outposts to support your applications that have low latency or local data processing requirements. These applications may need to generate near real-time responses to end-user applications or need to communicate with other on-premises systems or control on-site equipment. These can include workloads running on factory floors for automated operations in manufacturing, real-time patient diagnosis or medical imaging, and content and media streaming. You can use Outposts to securely store and process customer data that needs to remain on-premises or in countries where there is no AWS region. You can run data-intensive workloads on Outposts and process data locally when transmitting data to the cloud is expensive and wasteful and for better control on data analysis, back-up and restore.

How Outposts

Works:



via - <https://aws.amazon.com/outposts/>

Incorrect options:

AWS Snow Family - The AWS Snow Family is a collection of physical devices that help migrate large amounts of data into and out of the cloud without depending on networks. This helps you apply the wide variety of AWS services for analytics, file systems, and archives to your data. You can use AWS Snow Family services for data transfer and occasional pre-processing on location. Some large data transfer examples include cloud migration, disaster recovery, data center relocation, and/or remote data collection projects. These projects typically require you to migrate large amounts of data in the shortest, and most cost-effective, amount of time.

AWS Wavelength - AWS Wavelength is an AWS Infrastructure offering optimized for mobile edge computing applications. Wavelength Zones are AWS infrastructure deployments that embed AWS compute and storage services within communications service providers' (CSP) data centers at the edge of the 5G network, so application traffic from 5G devices can reach application servers running in Wavelength Zones without leaving the telecommunications network.

AWS Local Zones - AWS Local Zones are a type of AWS infrastructure deployment that places AWS compute, storage, database, and other select services close to a large population, industry, and IT centers. With AWS Local Zones, you can easily run applications that need single-digit millisecond latency closer to end-users in a specific geography. AWS Local Zones are ideal for use cases such as media & entertainment content creation, real-time gaming, live video streaming, and machine learning inference.

Reference:

<https://aws.amazon.com/outposts/>

Question 49:

Skipped

Which of the following statements are true about AWS Shared Responsibility Model? (Select two)

-

AWS maintains the configuration of its infrastructure devices and is responsible for configuring the guest operating systems, databases, and applications

-

AWS is responsible for patching and fixing flaws within the infrastructure, but customers are responsible for patching their guest OS and applications

(Correct)

-

AWS trains AWS employees, but a customer must train their own employees

(Correct)

-

For abstracted services, such as Amazon S3, AWS operates the infrastructure layer, the operating system, platforms, encryption options, and appropriate permissions for accessing the S3 resources

-

Amazon Elastic Compute Cloud (Amazon EC2) is categorized as Infrastructure as a Service (IaaS) and hence AWS will perform all of the necessary security configuration and management tasks

Explanation

Correct options:

AWS is responsible for patching and fixing flaws within the infrastructure, but customers are responsible for patching their guest OS and applications

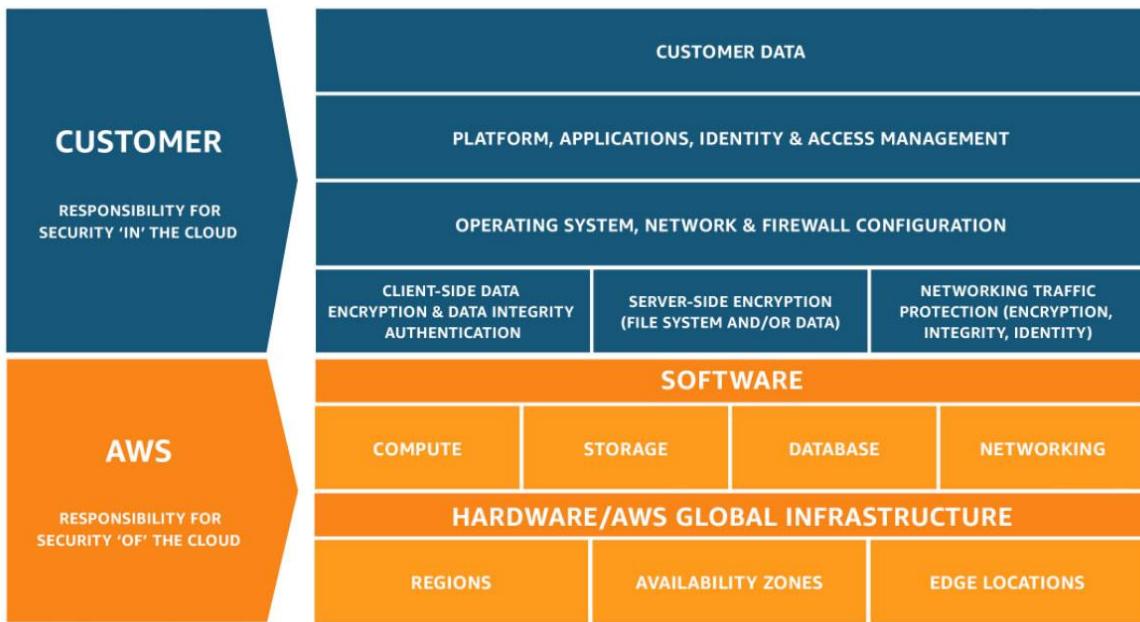
AWS trains AWS employees, but a customer must train their own employees

"Security of the Cloud" is the responsibility of AWS - 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. As part of Patch Management, a Shared Control responsibility of AWS Shared Responsibility Model, AWS is responsible for patching and fixing flaws within the infrastructure, but customers are responsible for patching their guest OS and applications.

"Security in the Cloud" is the responsibility of the customer. Customer responsibility will be determined by the AWS Cloud services that a customer selects. This determines the amount of configuration work the customer must perform as part of their security responsibilities.

As part of Awareness & Training, a Shared Control responsibility of the AWS Shared Responsibility Model, AWS trains AWS employees, but a customer must train their own employees.

AWS Shared Responsibility Model:



via - <https://aws.amazon.com/compliance/shared-responsibility-model/>

Incorrect options:

AWS maintains the configuration of its infrastructure devices and is responsible for configuring the guest operating systems, databases, and applications - As part of Configuration Management, a Shared Control responsibility of the AWS Shared Responsibility Model, AWS maintains the configuration of its infrastructure devices, but a customer is responsible for configuring their own guest operating systems, databases, and applications.

Amazon Elastic Compute Cloud (Amazon EC2) is categorized as Infrastructure as a Service (IaaS) and hence AWS will perform all of the necessary security configuration and management tasks - A service such as Amazon Elastic Compute Cloud (Amazon EC2) is categorized as Infrastructure as a Service (IaaS) and, as such, requires the customer to perform all of the necessary security configuration and management tasks. Customers that deploy an Amazon EC2 instance are responsible for the management of the guest operating system (including updates and security patches), any application software or utilities installed by the customer on the instances, and the configuration of the AWS-provided firewall (called a security group) on each instance.

For abstracted services, such as Amazon S3, AWS operates the infrastructure layer, the operating system, platforms, encryption options, and appropriate permissions for accessing the S3 resources - For abstracted services, such as Amazon S3 and Amazon DynamoDB, AWS operates the infrastructure layer, the operating system, and platforms, and customers access the endpoints to store and retrieve data. Customers are responsible for managing their data (including encryption options), classifying their assets, and using IAM tools to apply the appropriate permissions.

Reference:

<https://aws.amazon.com/compliance/shared-responsibility-model/>

Question 50:

Skipped

An e-learning company wants to build a knowledge graph by leveraging a fully managed database. Which of the following is the best fit for this requirement?



Amazon Neptune

(Correct)



Amazon RDS



Amazon DocumentDB



Amazon DynamoDB

Explanation

Correct option:

Amazon Neptune - Amazon Neptune is a fast, reliable, fully-managed graph database service that makes it easy to build and run applications that work with highly connected datasets. The core of Amazon Neptune is a purpose-built, high-performance graph database engine optimized for storing billions of relationships and querying the graph with milliseconds latency. Amazon Neptune is tailor-built for use cases like Knowledge Graphs, Identity Graphs, Fraud Detection, Recommendation Engines, Social Networking, Life Sciences, and so on.

Amazon Neptune supports popular graph models Property Graph and W3C's RDF, and their respective query languages Apache TinkerPop Gremlin and SPARQL, allowing you to easily build queries that efficiently navigate highly connected datasets. Neptune powers graph use cases such as recommendation engines, fraud detection, knowledge graphs, drug discovery, and network security.

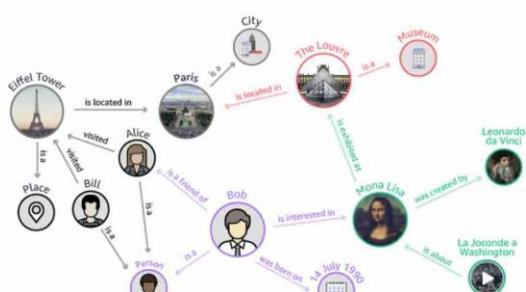
Amazon Neptune is highly available, with read-replicas, point-in-time recovery, continuous backup to Amazon S3, and replication across Availability Zones. Neptune is secure with support for HTTPS encrypted client connections and encryption at rest. Neptune is fully managed, so you no longer need to worry about database management tasks such as hardware provisioning, software patching, setup, configuration, or backups.

Fraud Detection with Amazon Neptune:

Knowledge Graphs

Amazon Neptune helps you build knowledge graph applications. A knowledge graph allows you to store information in a graph model and use graph queries to enable your users to easily navigate highly connected datasets. Neptune supports open source and open standard APIs to allow you to quickly leverage existing information resources to build your knowledge graphs and host them on a fully managed service. For example, if a user is interested in The Mona Lisa, you can also help them discover other works of art by Leonardo da Vinci, or other works of art located in The Louvre. Using a knowledge graph, you can add topical information to product catalogs, build and query complex models of regulatory rules, or model general information, like Wikidata.

Learn more about [Knowledge Graphs on AWS](#).



via - <https://aws.amazon.com/neptune/>

Incorrect options:

Amazon DocumentDB - Amazon DocumentDB (with MongoDB compatibility) is a fast, scalable, highly available, and fully managed document database service that supports MongoDB workloads. As a document database, Amazon DocumentDB makes it easy to store, query, and index JSON data.

Amazon DocumentDB is a non-relational database service designed from the ground-up to give you the performance, scalability, and availability you need when operating mission-critical MongoDB workloads at scale. In Amazon DocumentDB, the storage and compute are decoupled, allowing each to scale independently, and you can increase the read capacity to millions of requests per second by adding up to 15 low latency read replicas in minutes, regardless of the size of your data.

Amazon DynamoDB - Amazon DynamoDB is a key-value and document database that delivers single-digit millisecond performance at any scale. It's a fully managed, multi-region, multi-active, durable database with built-in security, backup and restore, and in-memory caching for internet-scale applications. DynamoDB can handle more than 10 trillion requests per day and can support peaks of more than 20 million requests per second. For highly connected datasets Amazon Neptune is a better choice.

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. Amazon RDS is available on several database instance types - optimized for memory, performance, or I/O - and provides you with six familiar database engines to choose from, including Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle Database, and SQL Server.

Reference:

<https://aws.amazon.com/neptune/>

Question 51:

Skipped

Which of the following is a repository service that helps in maintaining application dependencies via integration with commonly used package managers and build tools like Maven, Gradle, npm, etc?

-
- AWS CodeBuild**
-
- AWS CodeArtifact**
- (Correct)**
-
- AWS CodeStar**
-
- AWS CodeCommit**

Explanation

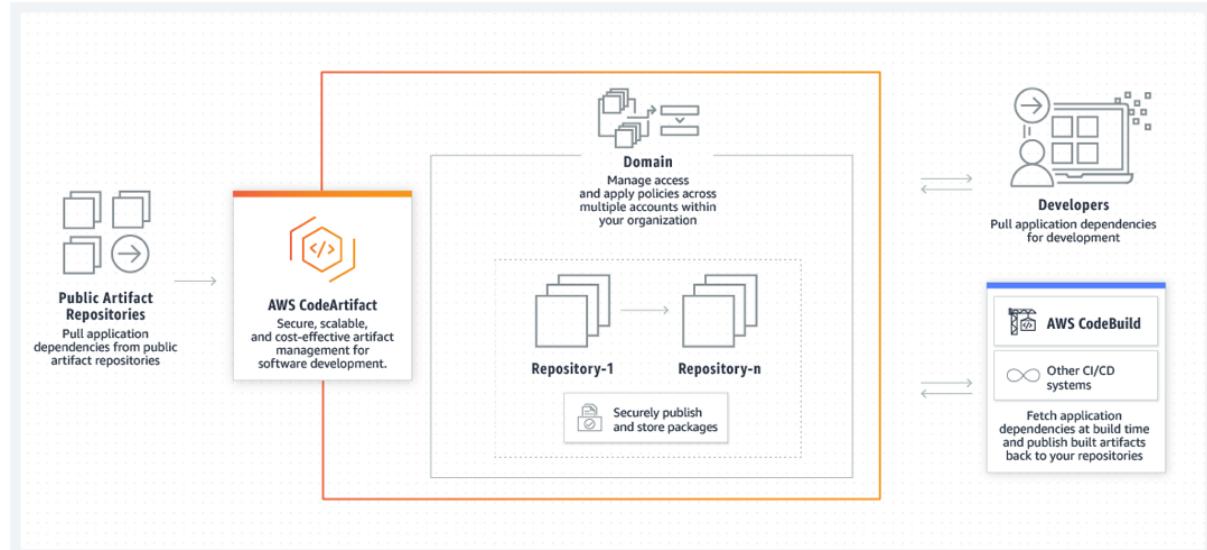
Correct option:

AWS CodeArtifact - AWS CodeArtifact is a fully managed artifact repository service that makes it easy for organizations of any size to securely store, publish, and share software packages used in their software development process. CodeArtifact can be configured to automatically fetch software packages and dependencies from public artifact repositories so developers have access to the latest versions. CodeArtifact works with commonly used package managers and build tools like Maven, Gradle, npm, yarn, twine, pip, and NuGet making it easy to integrate into existing development workflows.

Development teams often rely on both open-source software packages and those packages built within their organization. IT leaders need to be able to control access to and validate the safety of these software packages. Teams need a way to find up-to-date packages that have been approved for use by their IT leaders. To address these challenges, IT leaders turn to central artifact repository services to store and share packages. However, existing solutions often require teams to purchase licenses for software solutions that are complex to set up, scale, and operate.

AWS CodeArtifact is a pay-as-you-go artifact repository service that scales based on the needs of the organization. With CodeArtifact there is no software to update or servers to manage. In just a few clicks, IT leaders can set-up central repositories that make it easy for development teams to find and use the software packages they need. IT leaders can also approve packages and control distribution across the organization, ensuring development teams consume software packages that are safe for use.

How CodeArtifact works:



via - <https://aws.amazon.com/codeartifact/>

Incorrect options:

AWS CodeCommit - AWS CodeCommit is a fully-managed source control service that hosts secure Git-based repositories. It makes it easy for teams to collaborate on code in a secure and highly scalable ecosystem. CodeCommit eliminates the need to operate your own source control system or worry about scaling its infrastructure. You can use CodeCommit to securely store anything from source code to binaries, and it works seamlessly with your existing Git tools.

AWS CodeBuild - AWS CodeBuild is a fully managed continuous integration service that compiles source code, runs tests, and produces software packages that are ready to deploy. With CodeBuild, you don't need to provision, manage, and scale your own build servers. CodeBuild scales continuously.

and processes multiple builds concurrently, so your builds are not left waiting in a queue. You can get started quickly by using prepackaged build environments, or you can create custom build environments that use your own build tools.

AWS CodeStar - AWS CodeStar is a cloud-based development service that provides the tools you need to quickly develop, build, and deploy applications on AWS. With AWS CodeStar, you can set up your entire continuous delivery toolchain in minutes, allowing you to start releasing code faster. AWS CodeStar makes it easy for your whole team to work together securely, with built-in role-based policies that allow you to easily manage access and add owners, contributors, and viewers to your projects.

Each CodeStar project includes development tools, including AWS CodePipeline, AWS CodeCommit, AWS CodeBuild, and AWS CodeDeploy, that can be used on their own and with existing AWS applications.

Reference:

<https://aws.amazon.com/codeartifact/>

Question 52:

Skipped

An e-commerce company has its on-premises data storage on an NFS file system that is accessed in parallel by multiple applications. The company is looking at moving the applications and data stores to AWS Cloud.

Which storage service should the company use to move their files to AWS Cloud seamlessly if the application is hosted on Amazon EC2 instances?



AWS Storage Gateway



Amazon Simple Storage Service (Amazon S3)



Amazon Elastic Block Store (EBS)



Amazon Elastic File System (Amazon EFS)

(Correct)

Explanation

Correct option:

Amazon Elastic File System (Amazon EFS) - Amazon Elastic File System (Amazon EFS) provides a simple, scalable, fully managed elastic NFS file system for use with AWS Cloud services and on-premises resources. It is built to scale on-demand to petabytes without disrupting applications,

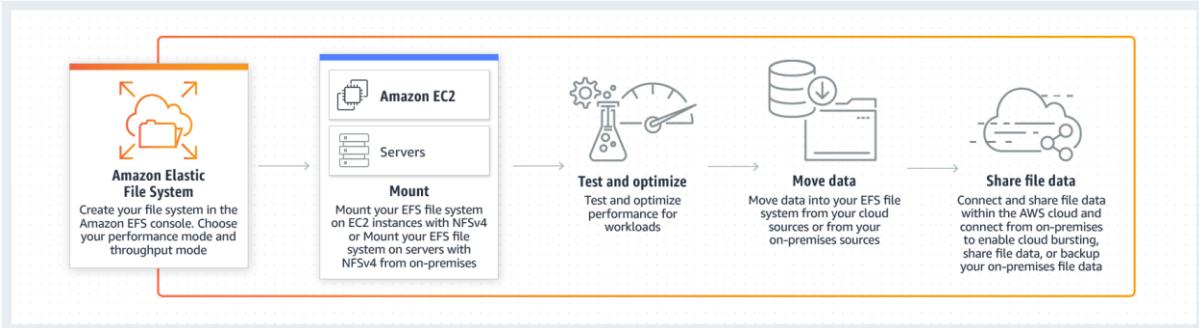
growing and shrinking automatically as you add and remove files, eliminating the need to provision and manage capacity to accommodate growth.

Amazon EFS is designed to provide massively parallel shared access to thousands of Amazon EC2 instances, enabling your applications to achieve high levels of aggregate throughput and IOPS with consistent low latencies.

Amazon EFS is well suited to support a broad spectrum of use cases from home directories to business-critical applications. Customers can use EFS to lift-and-shift existing enterprise applications to the AWS Cloud. Other use cases include big data analytics, web serving and content management, application development and testing, media and entertainment workflows, database backups, and container storage.

Amazon EFS offers two storage classes: the Standard storage class, and the Infrequent Access storage class (EFS IA). EFS IA provides price/performance that's cost-optimized for files not accessed every day. By simply enabling EFS Lifecycle Management on your file system, files not accessed according to the lifecycle policy you choose will be automatically and transparently moved into EFS IA.

How Amazon EFS Works:



via - <https://aws.amazon.com/efs/>

Incorrect options:

Amazon Elastic Block Store (EBS) - Amazon Elastic Block Store (EBS) is an easy to use, high-performance, block-storage service designed for use with Amazon Elastic Compute Cloud (EC2) for both throughput and transaction-intensive workloads at any scale. A broad range of workloads, such as relational and non-relational databases, enterprise applications, containerized applications, big data analytics engines, file systems, and media workflows are widely deployed on Amazon EBS. EBS is a block storage service and not a file storage service like EFS.

Amazon Simple Storage Service (Amazon S3) - Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. This means customers of all sizes and industries can use it to store and protect any amount of data for a range of use cases, such as data lakes, websites, mobile applications, backup and restore, archive, enterprise applications, IoT devices, and big data analytics. Parallel access of NFS file systems is not a feature Amazon S3 is capable of and hence EFS is the right choice here.

AWS Storage Gateway - AWS Storage Gateway is a hybrid cloud storage service that gives you on-premises access to virtually unlimited cloud storage. Customers use Storage Gateway to simplify storage management and reduce costs for key hybrid cloud storage use cases. These include moving backups to the cloud, using on-premises file shares backed by cloud storage, and providing low latency access to data in AWS for on-premises applications.

Reference:

<https://aws.amazon.com/efs/>

Question 53:

Skipped

A company provides you with a completed product that is run and managed by the company itself. As a customer, you only use the product without worrying about maintaining or managing the product.

Which cloud computing model does this kind of product belong to?

- **Infrastructure as a Service (IaaS)**
-
- **Software as a Service (SaaS)**
(Correct)
-
- **Platform as a Service (PaaS)**
-
- **Product as a Service (Paas)**

Explanation

Correct option:

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 the web-based email where you can send and receive email without having to manage feature additions to the email product or maintaining the servers and operating systems that the email program is running on.

Incorrect options:

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.

*Product as a Service (Paas)** - This is a made-up option, given only as a distractor.

Reference:

<https://aws.amazon.com/types-of-cloud-computing/>

Question 54:

Skipped

AWS Support offers four support plans for its customers. Identify the features that are covered as part of the AWS Basic Support Plan? (Select two)

-

Best practice guidance

-

One-on-one responses to account and billing questions

(Correct)

-

Infrastructure event management

-

Service health checks

(Correct)

-

Use-case guidance – What AWS products, features, and services to use to best support your specific needs

Explanation

Correct options:

One-on-one responses to account and billing questions

Service health checks

AWS Support offers four support plans: Basic, Developer, Business, and Enterprise.

The Basic plan offers support for account and billing questions and service quota increases. The other plans offer a number of technical support cases with pay-by-the-month pricing and no long-term contracts. All AWS customers automatically have 24/7 access to these features of the Basic support plan: 1. One-on-one responses to account and billing questions 2. Support forums 3. Service health checks 4. Documentation, technical papers, and best practice guides

Incorrect options:

Best practice guidance - Customers with a Developer, Business or Enterprise support plan have access to best practice guidance.

Use-case guidance – What AWS products, features, and services to use to best support your specific needs - Customers with a Business or Enterprise support plan have access to use-case guidance.

Infrastructure event management - Customers with an Enterprise support plan have access to infrastructure event management which is a short-term engagement with AWS Support to get a deep understanding of customer use-cases. After analysis, AWS provides architectural and scaling guidance for an event.

Reference:

<https://docs.aws.amazon.com/awssupport/latest/user/getting-started.html>

Question 55:

Skipped

Which of the following is the least effort way to encrypt data for AWS services only in your AWS account using AWS Key Management Service (KMS)?

-
- Use AWS managed master keys that are automatically created in your account for each service**
(Correct)
-
- Use AWS owned CMK in the service you wish to use**
-
- Create your own customer master keys (CMKs) in AWS KMS**
-
- Use AWS KMS APIs to encrypt data within your own application by using the AWS Encryption SDK**

Explanation

Correct option:

Customer master keys are the primary resources in AWS KMS. A customer master key (CMK) is a logical representation of a master key. The CMK includes metadata, such as the key ID, creation date, description, and key state. The CMK also contains the key material used to encrypt and decrypt data.

Use AWS managed master keys that are automatically created in your account for each service - AWS managed CMKs are CMKs in your account that are created, managed, and used on your behalf by an AWS service that is integrated with AWS KMS. Some AWS services support only an AWS managed CMK. Others use an AWS owned CMK or offer you a choice of CMKs. AWS managed CMK can be used only for your AWS account.

You can view the AWS managed CMKs in your account, view their key policies, and audit their use in AWS CloudTrail logs. However, you cannot manage these CMKs, rotate them, or change their key policies. And, you cannot use AWS managed CMKs in cryptographic operations directly; the service that creates them uses them on your behalf.

AWS managed CMKs appear on the AWS managed keys page of the AWS Management Console for AWS KMS. You can also identify most AWS managed CMKs by their aliases, which have the format aws/service-name, such as aws/redshift.

You do not pay a monthly fee for AWS managed CMKs. They can be subject to fees for use in excess of the free tier, but some AWS services cover these costs for you.

Incorrect options:

Create your own customer master keys (CMKs) in AWS KMS - Customer managed CMKs are CMKs in your AWS account that you create, own, and manage. You have full control over these CMKs, including establishing and maintaining their key policies, IAM policies, and grants, enabling and disabling them, rotating their cryptographic material, adding tags, creating aliases that refer to the CMK, and scheduling the CMKs for deletion.

Customer managed CMKs incur a monthly fee and a fee for use in excess of the free tier. They are counted against the AWS KMS quotas for your account. This option requires extra effort for key management, so this is incorrect for the given use-case.

Use AWS KMS APIs to encrypt data within your own application by using the AWS Encryption SDK - AWS KMS APIs can also be accessed directly through the AWS KMS Command Line Interface or AWS SDK for programmatic access. AWS KMS APIs can also be used indirectly to encrypt data within your own applications by using the AWS Encryption SDK. This requires code changes and is not the easiest way to achieve encryption.

Use AWS owned CMK in the service you wish to use encryption - AWS owned CMKs are a collection of CMKs that an AWS service owns and manages for use in multiple AWS accounts. Although AWS owned CMKs are not in your AWS account, an AWS service can use its AWS owned CMKs to protect the resources in your account. AWS owned CMK can be used for multiple AWS accounts.

You do not need to create or manage the AWS owned CMKs. However, you cannot view, use, track, or audit them. You are not charged a monthly fee or usage fee for AWS owned CMKs and they do not count against the AWS KMS quotas for your account.

Reference:

https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#master_keys

Question 56:

Skipped

An e-commerce company needs to generate custom reports and graphs every week for analyzing the product sales data. The company is looking at a tool/service that will help them analyze this data using interactive dashboards with minimal effort. The dashboards also need to be accessible from any device.

Which AWS tool/service will you recommend for this use-case?



Amazon Athena



Amazon SageMaker



Amazon Quicksight

(Correct)



AWS Glue

Explanation

Correct option:

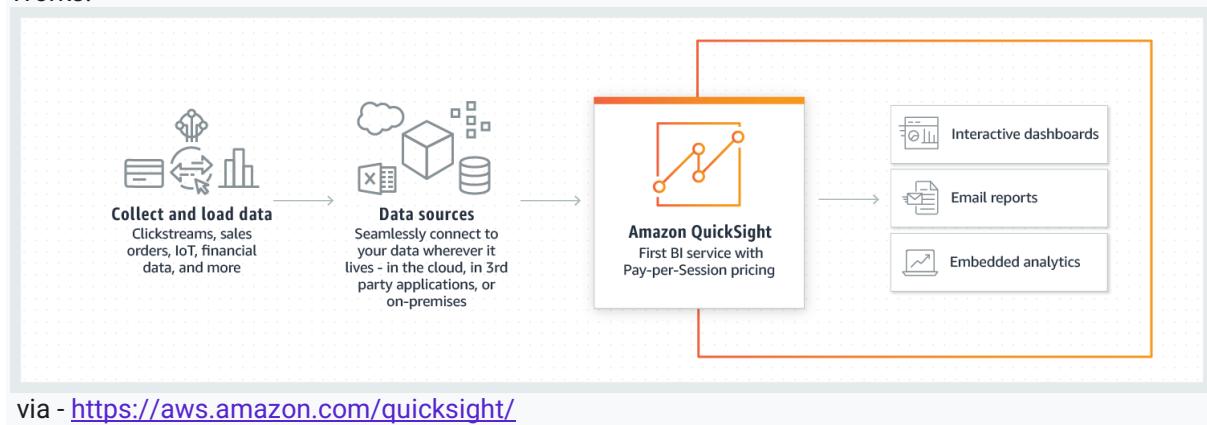
Amazon Quicksight - Amazon QuickSight is a scalable, serverless, embeddable, machine learning-powered business intelligence (BI) service built for the cloud. QuickSight lets you easily create and publish interactive BI dashboards that include Machine Learning-powered insights. QuickSight dashboards can be accessed from any device, and seamlessly embedded into your applications, portals, and websites.

With QuickSight, you can quickly embed interactive dashboards into your applications, websites, and portals. QuickSight provides a rich set of APIs and SDKs that allow you to easily customize the look and feel of the dashboards to match applications. With QuickSight, you can manage your dashboard versions, grant dashboard authoring privileges, and share usage reports with your end-customers. If your application is used by customers that belong to different teams or organizations, QuickSight ensures that their data is always siloed and secure.

Amazon QuickSight has a serverless architecture that automatically scales to tens of thousands of users without the need to set up, configure, or manage your own servers. It also ensures that your users don't have to deal with slow dashboards during peak-hours when multiple BI users are accessing the same dashboards or datasets. And with pay-per-session pricing, you only pay when your users access the dashboards or reports, which makes it cost-effective for deployments with lots of users. There are no upfront costs or annual commitments for using QuickSight.

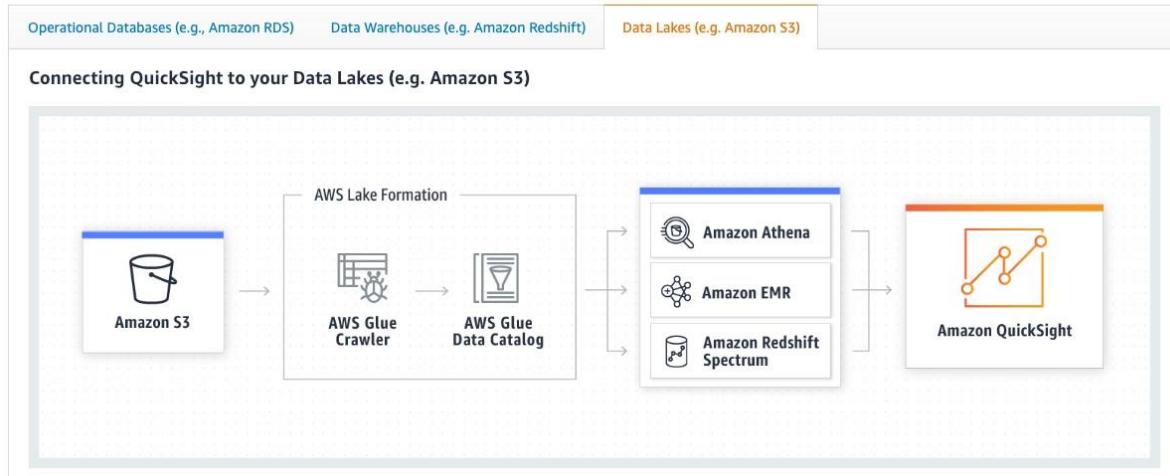
How QuickSight

Works:



Connecting QuickSight to your Data Lakes (e.g. Amazon S3):

Use cases



via - <https://aws.amazon.com/quicksight/>

Incorrect options:

AWS Glue - AWS Glue is a serverless data integration service that makes it easy to discover, prepare, and combine data for analytics, machine learning, and application development. AWS Glue provides all of the capabilities needed for data integration, so you can start analyzing your data and putting it to use in minutes instead of months. You should use AWS Glue to discover properties of the data you own, transform it, and prepare it for analytics. Glue can automatically discover both structured and semi-structured data stored in your data lake on Amazon S3, data warehouse in Amazon Redshift, and various databases running on AWS.

Amazon SageMaker - Amazon SageMaker is a fully managed service that provides every developer and data scientist with the ability to build, train, and deploy machine learning (ML) models quickly. SageMaker removes the heavy lifting from each step of the machine learning process to make it easier to develop high-quality models. Amazon SageMaker ensures that ML model artifacts and other system artifacts are encrypted in transit and at rest.

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 easy to use. Simply point to your data in Amazon S3, define the schema, and start querying using standard SQL. Most results are delivered within seconds. With Athena, there's no need for complex ETL jobs to prepare your data for analysis. This makes it easy for anyone with SQL skills to quickly analyze large-scale datasets.

Athena is integrated out-of-the-box with AWS Glue Data Catalog, allowing you to create a unified metadata repository across various services, crawl data sources to discover schemas, and populate your Catalog with new and modified table and partition definitions, and maintain schema versioning.

As discussed in the example above, Athena can be used to analyze data, while Quicksight can be used to visualize this data via advanced interactive dashboards.

References:

<https://aws.amazon.com/quicksight/>

<https://aws.amazon.com/athena/>

<https://aws.amazon.com/glue/>

Question 57:

Skipped

A company stores all their media files to Amazon S3 storage service which is accessed by an application hosted on Amazon EC2 instances. The company wants to convert these media files into formats that users can playback on mobile devices.

Which AWS service/tool helps you achieve this requirement?



Amazon Transcribe



AWS Glue



Amazon Comprehend



Amazon Elastic Transcoder

(Correct)

Explanation

Correct option:

Amazon Elastic Transcoder - Amazon Elastic Transcoder lets you convert media files that you have stored in Amazon S3 into media files in the formats required by consumer playback devices. For example, you can convert large, high-quality digital media files into formats that users can playback on mobile devices, tablets, web browsers, and connected televisions.

Amazon Elastic Transcoder manages all aspects of the media transcoding process for you transparently and automatically. There's no need to administer software, scale hardware, tune performance, or otherwise manage transcoding infrastructure. You simply create a transcoding "job" specifying the location of your source media file and how you want it transcoded. Amazon Elastic Transcoder also provides transcoding presets for popular output formats, which means that you don't need to guess about which settings work best on particular devices. All these features are available via service API, AWS SDKs and the AWS Management Console.

Incorrect options:

Amazon Transcribe - Amazon Transcribe makes it easy for developers to add speech to text capabilities to their applications. Audio data is virtually impossible for computers to search and analyze. Therefore, recorded speech needs to be converted to text before it can be used in applications.

Amazon Transcribe uses a deep learning process called automatic speech recognition (ASR) to convert speech to text quickly and accurately. Amazon Transcribe can be used to transcribe customer service calls, automate subtitling, and generate metadata for media assets to create a fully searchable archive.

Amazon Comprehend - Amazon Comprehend is a natural language processing (NLP) service that uses machine learning to find insights and relationships in a text. Amazon Comprehend uses machine learning to help you uncover the insights and relationships in your unstructured data. The service identifies the language of the text; extracts key phrases, places, people, brands, or events; understands how positive or negative the text is; analyzes text using tokenization and parts of speech, and automatically organizes a collection of text files by topic.

AWS Glue - AWS Glue is a serverless data integration service that makes it easy to discover, prepare, and combine data for analytics, machine learning, and application development. AWS Glue provides all of the capabilities needed for data integration, so you can start analyzing your data and putting it to use in minutes instead of months. You should use AWS Glue to discover properties of the data you own, transform it, and prepare it for analytics. Glue can automatically discover both structured and semi-structured data stored in your data lake on Amazon S3, data warehouse in Amazon Redshift, and various databases running on AWS.

References:

<https://aws.amazon.com/elastictranscoder/>

<https://aws.amazon.com/comprehend/>

<https://aws.amazon.com/transcribe/>

Question 58:

Skipped

Which of the following AWS services are offered free of cost? (Select two)

-

AWS Elastic Beanstalk

(Correct)

-

CloudWatch facilitated detailed monitoring of EC2 instances

-

An Elastic IP address, which is chargeable as long as it is associated with an EC2 instance

-

Amazon EC2 Spot Instances

-

AWS Auto Scaling

(Correct)

Explanation

Correct options:

AWS Elastic Beanstalk - There is no additional charge for AWS Elastic Beanstalk. You pay for AWS resources (e.g. EC2 instances or S3 buckets) you create to store and run your application. You only pay for what you use, as you use it; there are no minimum fees and no upfront commitments.

AWS Auto Scaling - There is no additional charge for AWS Auto Scaling. You pay only for the AWS resources needed to run your applications and Amazon CloudWatch monitoring fees.

Incorrect options:

Amazon EC2 Spot Instances - Amazon EC2 Spot Instances let you take advantage of unused EC2 capacity in the AWS cloud. Spot Instances are available at up to a 90% discount compared to On-Demand prices. Spot Instances are, however, not free.

CloudWatch facilitated detailed monitoring of EC2 instances - If you enable detailed monitoring, you are charged per metric that is sent to CloudWatch. You are not charged for data storage. Data is available in 1-minute periods, as opposed to 5-minute periods at no charge, for basic monitoring.

An Elastic IP address, which is chargeable as long as it is associated with an EC2 instance - An Elastic IP address doesn't incur charges as long as all the following conditions are true: The Elastic IP address is associated with an EC2 instance, The instance associated with the Elastic IP address is running, The instance has only one Elastic IP address attached to it and the Elastic IP address is associated with an attached network interface, such as a Network Load Balancer or NAT gateway.

References:

<https://aws.amazon.com/elasticbeanstalk/pricing/>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-cloudwatch-new.html>

<https://aws.amazon.com/premiumsupport/knowledge-center/elastic-ip-charges/>

Question 59:

Skipped

As part of a flexible pricing model, AWS offers two types of Savings Plans. Which of the following are the Savings Plans from AWS?

-

Compute Savings Plans, EC2 Instance Savings Plans

(Correct)

-

Reserved Instances Savings Plans, EC2 Instance Savings Plans

- ○

Compute Savings Plans, Storage Savings Plans

- ○

Instance Savings Plans, Storage Savings Plans

Explanation

Correct option:

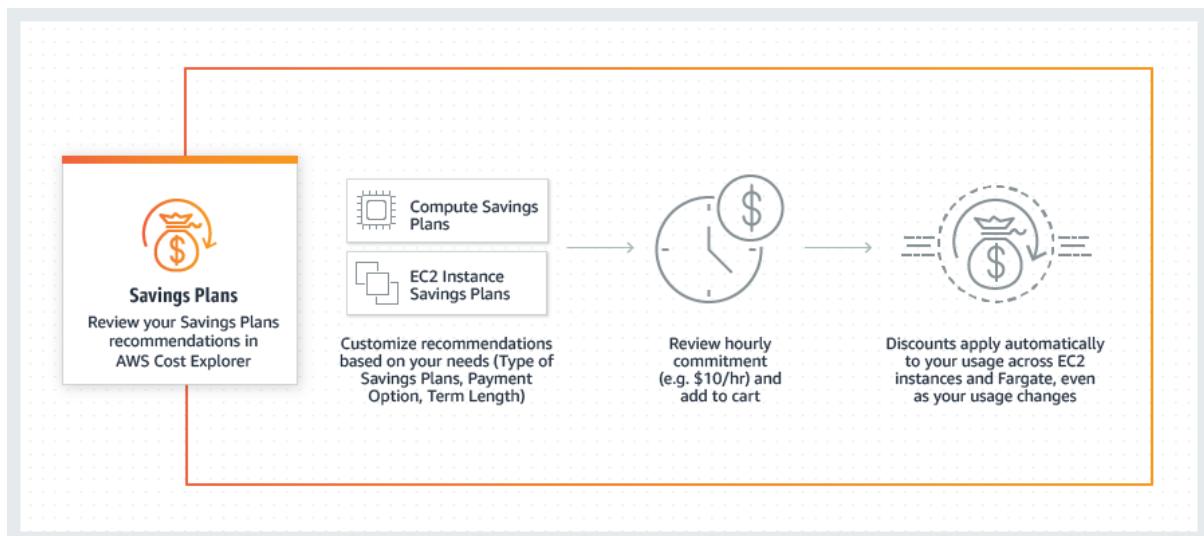
Compute Savings Plans, EC2 Instance Savings Plans - Savings Plans is a flexible pricing model that provides savings of up to 72% on your AWS compute usage. This pricing model offers lower prices on Amazon EC2 instances usage, regardless of instance family, size, OS, tenancy or AWS Region, and also applies to AWS Fargate and AWS Lambda usage.

Savings Plans offer significant savings over On-Demand, just like EC2 Reserved Instances, in exchange for a commitment to use a specific amount of compute power (measured in \$/hour) for a one or three-year period. You can sign up for Savings Plans for a 1- or 3-year term and easily manage your plans by taking advantage of recommendations, performance reporting and budget alerts in the AWS Cost Explorer.

AWS offers two types of Savings Plans:

1. Compute Savings Plans provide the most flexibility and help to reduce your costs by up to 66%. These plans automatically apply to EC2 instance usage regardless of instance family, size, AZ, region, OS or tenancy, and also apply to Fargate and Lambda usage. For example, with Compute Savings Plans, you can change from C4 to M5 instances, shift a workload from EU (Ireland) to EU (London), or move a workload from EC2 to Fargate or Lambda at any time and automatically continue to pay the Savings Plans price.
2. EC2 Instance Savings Plans provide the lowest prices, offering savings up to 72% in exchange for a commitment to the usage of individual instance families in a region (e.g. M5 usage in N. Virginia). This automatically reduces your cost on the selected instance family in that region regardless of AZ, size, OS or tenancy. EC2 Instance Savings Plans give you the flexibility to change your usage between instances within a family in that region. For example, you can move from c5.xlarge running Windows to c5.2xlarge running Linux and automatically benefit from the Savings Plans prices.

How Savings Plans Work:



via - <https://aws.amazon.com/savingsplans/>

Incorrect options:

Compute Savings Plans, Storage Savings Plans

Reserved Instances Savings Plans, EC2 Instance Savings Plans

Instance Savings Plans, Storage Savings Plans

These three options contradict the explanation above, so these options are incorrect.

References:

<https://aws.amazon.com/savingsplans/>

<https://aws.amazon.com/savingsplans/faq/>

Question 60:

Skipped

An e-commerce application sends out messages to a downstream application whenever an order is created. The downstream application processes the messages and updates its own systems. Currently, the two applications directly communicate with each other.

Which service will you use to decouple this architecture, without any communication loss between the two systems?

-

Amazon Simple Notification Service (Amazon SNS)

-

Amazon Simple Queue Service (SQS)

(Correct)

•

Amazon Kinesis Data Streams

•

AWS Lambda

Explanation

Correct option:

Amazon Simple Queue Service (SQS) - Amazon Simple Queue Service (SQS) is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SQS 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. Get started with SQS in minutes using the AWS console, Command Line Interface or SDK of your choice, and three simple commands.

Amazon SQS uses a pull mechanism, i.e. the messages in the queue are available till a registered process pulls the messages to process them. This decouples the architecture since the second application does not need to be available all the time to process messages coming from application one.

Incorrect options:

Amazon Simple Notification Service (Amazon SNS) - Amazon Simple Notification Service (Amazon SNS) is a fully managed messaging service for both application-to-application (A2A) and application-to-person (A2P) communication. The A2A pub/sub functionality provides topics for high-throughput, push-based, many-to-many messaging between distributed systems, microservices, and event-driven serverless applications. Amazon SNS allows applications to send time-critical messages to multiple subscribers through a “push” mechanism, which implies that the receiving applications have to be present and running to receive the messages. There is a scope for message loss in SNS and hence SQS is the right choice for this use case.

Amazon Kinesis data stream - Amazon Kinesis Data Streams enables you to build custom applications that process or analyze streaming data for specialized needs. You can continuously add various types of data such as clickstreams, application logs, and social media to an Amazon Kinesis data stream from hundreds of thousands of sources. Within seconds, the data will be available for your Amazon Kinesis Applications to read and process from the stream. Kinesis Data streams are overkill for this use-case since Kinesis Data Streams are meant for real-time processing of streaming big data.

AWS Lambda - AWS Lambda is a serverless compute service that lets you run code without provisioning or managing servers, creating workload-aware cluster scaling logic, maintaining event integrations, or managing runtimes. With Lambda, you can run code for virtually any type of application or backend service - all with zero administration. Just upload your code as a ZIP file or container image, and Lambda automatically and precisely allocates compute execution power and runs your code based on the incoming request or event, for any scale of traffic. Lambda functions cannot self invoke and need to be called. Also, Lambda functions cannot store data for later processing.

Reference:

<https://aws.amazon.com/sqs/>

Question 61:

Skipped

Which free tool helps to review the state of your workloads and compares them to the latest AWS architectural best practices after you have answered a series of questions about your workload?

-
- **AWS Well-Architected Framework**
-
- **AWS Trusted Advisor**
-
- **AWS Technical Account Manager (TAM)**
-
- **AWS Well-Architected Tool**

(Correct)

Explanation

Correct option:

AWS Well-Architected Tool - The AWS Well-Architected Tool helps you review the state of your workloads and compares them to the latest AWS architectural best practices. The tool is based on the AWS Well-Architected Framework, developed to help cloud architects build secure, high-performing, resilient, and efficient application infrastructure.

To use this free tool, available in the AWS Management Console, just define your workload and answer a set of questions regarding operational excellence, security, reliability, performance efficiency, and cost optimization. The AWS Well-Architected Tool then provides a plan on how to architect for the cloud using established best practices.

The AWS Well-Architected Tool gives you access to knowledge and best practices used by AWS architects, whenever you need it. You answer a series of questions about your workload, and the tool delivers an action plan with step-by-step guidance on how to build better workloads for the cloud.

How Well-Architected Tool works:



A. Identify the workload to document. Then answer a series of questions about your architecture.

B. Review your answers against the five pillars established by the Well-Architected Framework that are visually depicted via the icons in the column above; a) Operational excellence, b) Security, c) Reliability, d) Performance efficiency, & e) Cost optimization.

C. You can 1) get videos and documentation 2) generate a report that summarizes your workload review, & 3) see the results of reviews in a single dashboard.

via - <https://aws.amazon.com/well-architected-tool/>

Incorrect options:

AWS Well-Architected Framework - AWS Well-Architected helps cloud architects build secure, high-performing, resilient, and efficient infrastructure for their applications and workloads. Based on six pillars – operational excellence, security, reliability, performance efficiency, cost optimization and sustainability – AWS Well-Architected provides a consistent approach for customers and partners to evaluate architectures, and implement designs that can scale over time. This is a framework based on which Well-Architected Tool and AWS Trusted Advisor offer guidance, suggestions and improvements.

AWS Trusted Advisor - AWS Trusted Advisor is an online tool that provides you real-time guidance to help you provision your resources following AWS best practices. Trusted Advisor checks help optimize your AWS infrastructure, increase security and performance, reduce your overall costs, and monitor service limits. Whether establishing new workflows, developing applications, or as part of ongoing improvement, take advantage of the recommendations provided by Trusted Advisor on a regular basis to help keep your solutions provisioned optimally.

While Trusted advisor checks are based on the support plan the customer has. Both Basic and Developer support plans have access to the 7 core Trusted Advisor checks. Unlike documentation-based guidance (like AWS Well-Architected Tool), this tool provides recommendations against AWS Well Architected Framework best practices and is able to track against your current AWS architecture.

AWS Technical Account Manager (TAM) - 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).

A Technical Account Manager (TAM) is your designated technical point of contact who helps you onboard, provides advocacy and guidance to help plan and build solutions using best practices, coordinates access to subject matter experts, assists with case management, presents insights and recommendations on your AWS spend, workload optimization, and event management, and proactively keeps your AWS environment healthy.

Reference:

<https://aws.amazon.com/well-architected-tool/>

Question 62:

Skipped

A university provides access to AWS services for its students to submit their research data for analysis. The university is looking at a cost-effective approach for mitigating data loss or data corruption.

Which disaster recovery strategy is well-suited for this use case?

-

Pilot light strategy

-

Warm standby strategy

-

Backup and restore strategy

(Correct)

-

Multi-site active/active strategy

Explanation

Correct option:

Backup and restore strategy

When selecting your DR strategy, you must weigh the benefits of lower RTO (recovery time objective) and RPO (recovery point objective) vs the costs of implementing and operating a strategy. The Backup and restore strategy offers a good balance of benefits and cost for the current use case. This is the cheapest of all the disaster recovery options available with AWS.

Backup and restore is a suitable approach for mitigating data loss. This approach can also be used to mitigate against a regional disaster by replicating data to other AWS Regions or to mitigate the lack of redundancy for workloads deployed to a single Availability Zone. In addition to data, you must redeploy the infrastructure, configuration, and application code in the recovery Region.

Comparing different DR strategies:

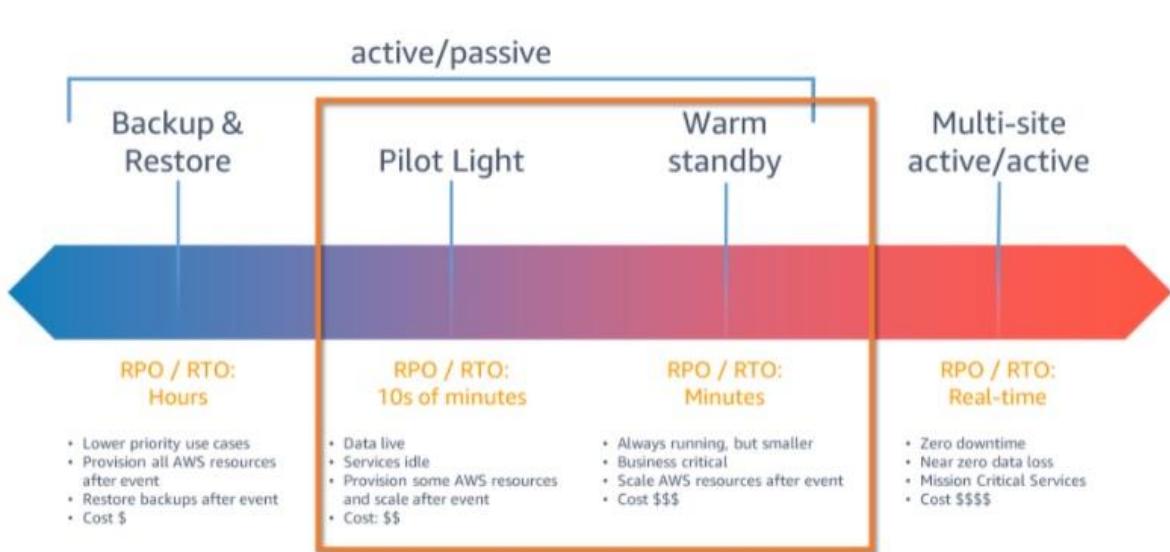


Figure 1. DR strategies

via - <https://aws.amazon.com/blogs/architecture/disaster-recovery-dr-architecture-on-aws-part-iii-pilot-light-and-warm-standby/>

Incorrect options:

Pilot light strategy - With the pilot light approach, you replicate your data from one Region to another and provision a copy of your core workload infrastructure. Resources required to support data replication and backup, such as databases and object storage, are always on. Other elements, such as application servers, are loaded with application code and configurations but are switched off and are only used during testing or when disaster recovery failover is invoked. Unlike the backup and restore approach, your core infrastructure is always available and you always have the option to quickly provision a full-scale production environment by switching on and scaling out your application servers. This also implies that the cost incurred is higher than what it is for the backup and restore approach.

Multi-site active/active strategy - You can run your workload simultaneously in multiple Regions as part of a multi-site active/active strategy. Multi-site active/active serves traffic from all regions to which it is deployed. With a multi-site active/active approach, users can access the workload in any of the Regions in which it is deployed. This approach is the most complex and costliest for disaster recovery.

Warm standby strategy - The warm standby approach involves ensuring that there is a scaled-down but fully functional copy of your production environment in another Region. This approach extends the pilot light concept and decreases the time to recovery because your workload is always-on in another Region. This approach also allows you to more easily perform testing or implement continuous testing to increase confidence in your ability to recover from a disaster. This strategy is costly and is used only for business-critical applications.

Reference:

<https://docs.aws.amazon.com/whitepapers/latest/disaster-recovery-workloads-on-aws/disaster-recovery-options-in-the-cloud.html>

Question 63:

Skipped

A weather tracking application is built using Amazon DynamoDB. The performance of the application has been consistently good. But lately, the team has realized that during holidays and travel seasons, the load on the application is high and the read requests consume most of the database resources, thereby drastically increasing the overall application latency.

Which feature/service will help resolve this issue?

-
- DynamoDB Regulator**
-
- DynamoDB Accelerator**
- (Correct)**
-
- Amazon CloudFront**
-
- Amazon ElastiCache**

Explanation

Correct option:

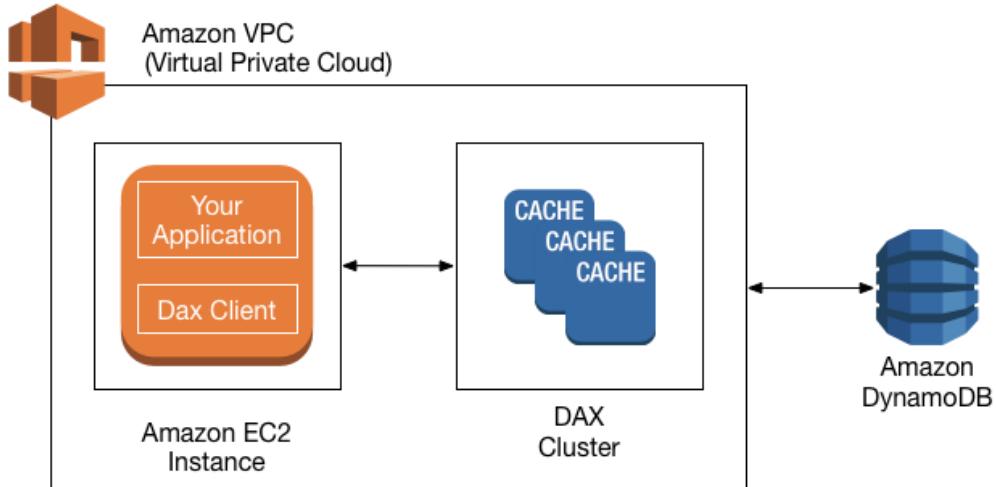
DynamoDB Accelerator - Amazon DynamoDB is designed for scale and performance. In most cases, the DynamoDB response times can be measured in single-digit milliseconds. However, there are certain use cases that require response times in microseconds. For these use cases, DynamoDB Accelerator (DAX) delivers fast response times for accessing eventually consistent data.

DAX is a DynamoDB-compatible caching service that enables you to benefit from fast in-memory performance for demanding applications. DAX addresses three core scenarios:

1. As an in-memory cache, DAX reduces the response times of eventually consistent read workloads by an order of magnitude from single-digit milliseconds to microseconds.
2. DAX reduces operational and application complexity by providing a managed service that is API-compatible with DynamoDB. Therefore, it requires only minimal functional changes to use with an existing application.
3. For read-heavy or bursty workloads, DAX provides increased throughput and potential operational cost savings by reducing the need to overprovision read capacity units. This is especially beneficial for applications that require repeated reads for individual keys.

How DAX

Works:



via - <https://aws.amazon.com/dynamodb/dax/>

Incorrect options:

DynamoDB Regulator - This is a made-up option, used only as a distractor.

Amazon ElastiCache - Amazon ElastiCache is a web service that makes it easy to deploy, operate, and scale an in-memory data store and cache in the cloud. The service improves the performance of web applications by allowing you to retrieve information from fast, managed, in-memory data stores, instead of relying entirely on slower disk-based databases. Amazon ElastiCache supports two open-source in-memory engines: Redis, Memcached. AWS recommends using DAX for DynamoDB, which is an out-of-box caching solution for DynamoDB.

Amazon CloudFront - Amazon CloudFront is a global content delivery network (CDN) service that accelerates delivery of your websites, APIs, video content or other web assets. It integrates with other Amazon Web Services products to give developers and businesses an easy way to accelerate content to end-users with no minimum usage commitments. It is not a caching solution.

Reference:

<https://aws.amazon.com/caching/aws-caching/>

Question 64:

Skipped

Which member of the AWS Snow Family is used by the Edge computing applications for IoT use cases for facilitating the collection and processing of data to gain immediate insights and then transfer the data to AWS?



AWS Snowposts



AWS Snowball Edge Storage Optimized

- AWS Snowmobile
- AWS Snowcone

AWS Snowcone

(Correct)

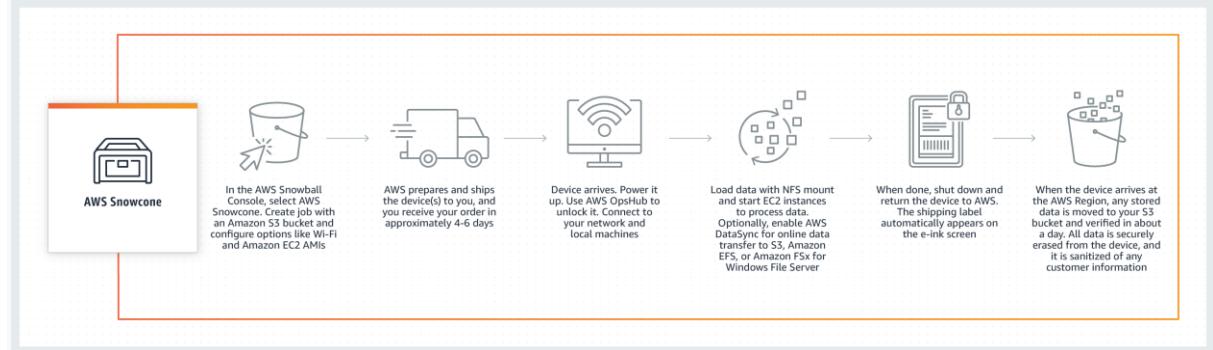
Explanation

Correct option:

AWS Snowcone - AWS Snowcone is the smallest member of the AWS Snow Family of edge computing, edge storage, and data transfer devices, weighing in at 4.5 pounds (2.1 kg) with 8 terabytes of usable storage. Snowcone is ruggedized, secure, and purpose-built for use outside of a traditional data center. Its small form factor makes it a perfect fit for tight spaces or where portability is a necessity and network connectivity is unreliable. You can use Snowcone in backpacks on first responders, or for IoT, vehicular, and drone use cases. You can execute compute applications on the edge, and you can ship the device with data to AWS for offline data transfer, or you can transfer data online with AWS DataSync from edge locations.

Like AWS Snowball, Snowcone has multiple layers of security and encryption. You can use either of these services to run edge computing workloads, or to collect, process, and transfer data to AWS. Snowcone is designed for data migration needs up to 8 terabytes per device and from space-constrained environments where AWS Snowball devices will not fit.

How AWS Snowcone works:



via - <https://aws.amazon.com/snowcone/>

Feature comparison in members of Snow Family:

Feature comparison

	AWS Snowcone	AWS Snowball Edge Storage Optimized	AWS Snowball Edge Compute Optimized	AWS Snowmobile
Usage Scenario	Edge computing, Data transfer, Edge storage	Data transfer, Edge storage	Edge computing, Data transfer	Data transfer
Usable HDD Storage	8 TB	80 TB	42 TB	100 PB
Usable SSD Storage	No	1 TB	7.68 TB	No
Usable vCPUs	2 vCPUs	40 vCPUs	52 vCPUs	N/A
Usable Memory	4 GB	80 GB	208 GB	N/A
GPU	No	No	nVidia V100 (optional)	No
Onboard Computing Options	AWS IoT Greengrass Amazon EC2 AMIs	AWS IoT Greengrass Amazon EC2 AMIs	AWS IoT Greengrass Amazon EC2 AMIs	N/A
DataSync	Yes	No	No	No
Transfers via NFS	Yes	Yes	Yes	Yes
Transfers via S3 API	No	Yes	Yes	No
Network Interfaces	2x 1/10 Gbit - RJ45	2x 10 Gbit - RJ45 1x 25 Gbit - SFP+ 1x 100 Gbit - QSFP28	2x 10 Gbit - RJ45 1x 25 Gbit - SFP+ 1x 100 Gbit - QSFP28	6x 40 Gbit
Device Size	9 inches long, 6 inches wide, and 3 inches tall (227 mm x 148.6 mm x 82.65 mm)	28.3 inches long, 10.6 inches wide, and 15.5 inches tall (548 mm x 320 mm x 501 mm)	28.3 inches long, 10.6 inches wide, and 15.5 inches tall (548 mm x 320 mm x 501 mm)	N/A
Device Weight	4.5 lbs. (2.1 kg)	49.7 lbs. (22.3 kg)	49.7 lbs. (22.3 kg)	N/A
Encryption	Yes, 256-bit	Yes, 256-bit	Yes, 256-bit	Yes, 256-bit
Portability	Battery-based Operation	No	No	No
Wireless	Wi-Fi	No	No	No
Storage Clustering	No	Yes, 5-10 nodes	Yes, 5-10 nodes	N/A
HIPAA Compliant	Yes, eligible	Yes, eligible	Yes, eligible	No
Typical Job Lifetime	Offline or Online Data Transfer: Days-Weeks Edge Compute: Weeks-Years	Offline Data Transfer: Days-Weeks	Edge Compute: Weeks-Years	Data Migration: Months

via - https://aws.amazon.com/snow/#Feature_comparison

Incorrect options:

AWS Snowball Edge Storage Optimized - AWS Snowball, a part of the AWS Snow Family, is an edge computing, data migration, and edge storage device that comes in two options. Snowball Edge Storage Optimized devices provide both block storage and Amazon S3-compatible object storage, and 40 vCPUs. They are well suited for local storage and large scale data transfer.

Snowball Edge Compute Optimized devices provide 52 vCPUs, block and object storage, and an optional GPU for use cases like advanced machine learning and full-motion video analysis in disconnected environments. You can use these devices for data collection, machine learning and processing, and storage in environments with intermittent connectivity or in extremely remote locations before shipping them back to AWS.

AWS Snowposts - This is a made-up option, used only as a distractor.

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.

Reference:

<https://aws.amazon.com/snowcone/>

Question 65:

Skipped

A supply chain company is looking for a database that provides a centrally verifiable history of all changes made to data residing in it. This functionality is critical for the product and needs to be available off-the-shelf without the need for any customizations.

Which of the following databases is the right choice for this use-case?

-
- **Amazon Managed Blockchain**
-
- **Amazon Neptune**
-
- **Amazon Timestream**
-
- **Amazon Quantum Ledger Database**

(Correct)

Explanation

Correct option:

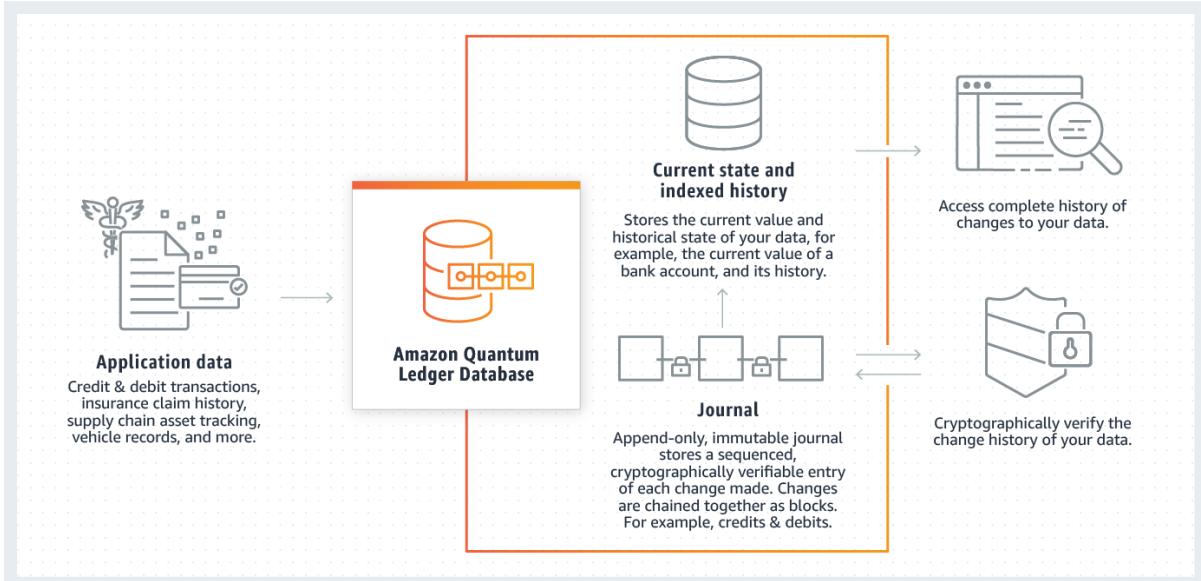
Amazon Quantum Ledger Database - Amazon QLDB is a fully managed ledger database that provides a transparent, immutable, and cryptographically verifiable transaction log owned by a central trusted authority. Amazon QLDB can be used to track each and every application data change and maintains a complete and verifiable history of changes over time.

Ledgers are typically used to record a history of economic and financial activity in an organization. Many organizations build applications with ledger-like functionality because they want to maintain an accurate history of their applications' data, for example, tracking the history of credits and debits in banking transactions, verifying the data lineage of an insurance claim, or tracing the movement of an item in a supply chain network. Ledger applications are often implemented using custom audit tables or audit trails created in relational databases.

Amazon QLDB is a new class of database that eliminates the need to engage in the complex development effort of building your own ledger-like applications. With QLDB, your data's change history is immutable – it cannot be altered or deleted – and using cryptography, you can easily verify that there have been no unintended modifications to your application's data. QLDB uses an immutable transactional log, known as a journal, that tracks each application data change and maintains a complete and verifiable history of changes over time. QLDB is easy to use because it provides developers with a familiar SQL-like API, a flexible document data model, and full support for transactions. QLDB's streaming capability provides a near real-time flow of your data stored within

QLDB, allowing you to develop event-driven workflows, real-time analytics, and to replicate data to other AWS services to support advanced analytical processing. QLDB is also serverless, so it automatically scales to support the demands of your application. There are no servers to manage and no read or write limits to configure. With QLDB, you only pay for what you use.

How Amazon Quantum Ledger Database Works:



via - <https://aws.amazon.com/qldb/>

Incorrect options:

Amazon Neptune - Amazon Neptune is a fast, reliable, fully-managed graph database service that makes it easy to build and run applications that work with highly connected datasets. The core of Amazon Neptune is a purpose-built, high-performance graph database engine optimized for storing billions of relationships and querying the graph with milliseconds latency. Amazon Neptune is tailor-built for use cases like Knowledge Graphs, Identity Graphs, Fraud Detection, Recommendation Engines, Social Networking, Life Sciences, and so on.

Amazon Timestream - Amazon Timestream is a fast, scalable, and serverless time series database service for IoT and operational applications that makes it easy to store and analyze trillions of events per day up to 1,000 times faster and at as little as 1/10th the cost of relational databases. Amazon Timestream saves you time and costs in managing the lifecycle of time series data by keeping recent data in memory and moving historical data to a cost-optimized storage tier based upon user-defined policies.

Amazon Managed Blockchain - Amazon Managed Blockchain is a fully managed service that allows you to join public networks or set up and manage scalable private networks using popular open-source frameworks. Amazon Managed Blockchain eliminates the overhead required to create the network or join a public network and automatically scales to meet the demands of thousands of applications running millions of transactions.

While QLDB is a ledger database purpose-built for customers who need to maintain a complete and verifiable history of data changes in an application that they own and manage in a centralized way, QLDB is not a blockchain technology. Instead, blockchain technologies focus on enabling multiple parties to transact and share data securely in a decentralized way; without a trusted, central authority. Every member in a network has an independently verifiable copy of an immutable ledger, and members can create and endorse transactions in the network.

References:

<https://aws.amazon.com/qldb/>

<https://aws.amazon.com/managed-blockchain/>