1. Right Answer:

Amazon 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.

Amazon S3 Versioning Overview: via
- https://docs.aws.amazon.com/AmazonS3/latest/dev/ObjectVersioning.html

Wrong Answer:

Amazon S3 lifecycle configuration - To manage your Amazon S3 objects so that they are stored cost-effectively throughout their lifecycle, configure their Amazon S3 Lifecycle. With Amazon S3 Lifecycle configuration rules, you can tell Amazon S3 to transition objects to less expensive storage classes, or archive or delete them. Amazon S3 lifecycle configuration will do the hard lifting of moving your data into cost-effective storage classes without user intervention. Amazon S3 Lifecycle configuration is not meant to protect from accidental deletion of data.

Amazon 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.

Amazon S3 Transfer Acceleration (Amazon S3TA) - Amazon S3 Transfer Acceleration (Amazon S3TA) enables fast, easy, and secure transfers of files over long distances between your client and an S3 bucket. Amazon S3 Transfer Acceleration (Amazon S3TA) 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. Amazon S3 Transfer Acceleration (Amazon S3TA) cannot be used to protect from accidental deletion of data.

Additional Resources:

https://docs.aws.amazon.com/AmazonS3/latest/dev/ObjectVersioning.html

2. **Right Answer:**

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. Amazon 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.

Amazon 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.

Wrong Answer:

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. Amazon 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.

Additional Resources:

https://aws.amazon.com/kendra/

3. Right Answer:

Virtual Multi-Factor Authentication (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 Multi-Factor Authentication (MFA) device assigned to a user must be unique. A user cannot type a code from another user's virtual Multi-Factor Authentication (MFA) device to authenticate.

Google Authenticator is an example of a Virtual Multi-Factor Authentication (MFA) device:

Wrong Answer:

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 Multi-Factor Authentication (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 Multi-Factor Authentication (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 Multi-Factor Authentication (MFA) device - This is a made-up option and has been added as a distractor.

Additional Resources:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa.html

4. Right Answer:

Amazon Simple Storage Service (Amazon S3)

All Amazon S3 buckets have encryption configured by default, and objects are automatically encrypted by using server-side encryption with Amazon S3 managed keys (SSE-S3). This encryption setting applies to all objects in your Amazon S3 buckets.

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).

Wrong Answer:

Amazon Elastic Block Store (Amazon EBS) - Amazon Elastic Block Store (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 Elastic File System (Amazon EFS) - Encryption is not a default setting, but an optional configuration for Amazon EFS drives. Amazon EFS supports two forms of encryption for file systems, encryption of data in transit and encryption at rest.

Additional Resources:

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

https://docs.aws.amazon.com/AmazonS3/latest/userguide/bucket-encryption.html

5. **Right Answer:**

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.

Wrong Answer:

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

building your applications. AWS Fargate removes the need to provision and manage servers, lets you specify and pay for resources per application, and improves security through application isolation by design. With AWS Fargate, you do not have access to the underlying servers, so this option is incorrect.

How AWS 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. AWS Lambda does not support running container applications.

Amazon Elastic Container Registry (Amazon ECR) - Amazon Elastic Container Registry (Amazon ECR) can be used to store, manage, and deploy Docker container images. Amazon Elastic Container Registry (Amazon ECR) eliminates the need to operate your container repositories. Amazon Elastic Container Registry (Amazon ECR) does not support running container applications.

Additional Resources:

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

6.   Right Answer:

You must use an Amazon Machine Image (AMI) from the same region as that of the Amazon EC2 instance. The region of the Amazon Machine Image (AMI) has no bearing on the performance of the Amazon EC2 instance

An Amazon Machine Image (AMI) provides the information required to launch an instance. You must specify an Amazon Machine Image (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 Amazon Machine Image (AMI) must be in the same region as that of the Amazon EC2 instance to be launched. If the Amazon Machine Image (AMI) exists in a different region, you can copy that Amazon Machine Image (AMI) to the region where you want to launch the EC2 instance. The region of Amazon Machine Image (AMI) has no bearing on the performance of the Amazon EC2 instance.

Amazon Machine Images (AMI) Overview: via - https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html

Wrong Answer:

You can use an Amazon Machine Image (AMI) from a different region, but it degrades the performance of the Amazon EC2 instance

You should use an Amazon Machine Image (AMI) from the same region, as it improves the performance of the Amazon EC2 instance

An Amazon Machine Image (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.

Additional Resources:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html

7.   Right Answer:

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/

Wrong Answer:

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 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 AWS CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. AWS 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.

AWS Config is focused on the configuration of your AWS resources and reports with detailed snapshots on how your resources have changed. Whereas AWS 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. Amazon 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.

Additional Resources:

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

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

8. **Right Answer:**

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.

Wrong Answer:

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 AWS CodePipeline Works: via - https://aws.amazon.com/codepipeline/

Additional Resources:

https://aws.amazon.com/codedeploy/

9. Right Answer:

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.

AWS Shared Responsibility Model Overview: via
- https://aws.amazon.com/compliance/shared-responsibility-model/

Wrong Answer:

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.

Additional Resources:

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

10. Right Answer:

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. AWS 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.

Wrong Answer:

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 om-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 AWS Transit Gateway without ending up with a complex VPC peering network. AWS Transit Gateway is not a data migration solution.

Additional Resources:

https://aws.amazon.com/snowball/

11. Right Answer:

Failover routing

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

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

Wrong Answer:

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

Latency-based routing - 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.

Additional Resources:

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

12. Right Answer:

Auto Scaling group scales out and adds more number of Amazon EC2 instances to match an increase in demand

Auto Scaling group scales in and reduces the number of Amazon 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.

Wrong Answer:

Auto Scaling group scales down and reduces the number of Amazon EC2 instances to match a decrease in demand - A scale down refers to a downgrade to a less powerful Amazon EC2 instance. Therefore this option is incorrect.

Auto Scaling group scales down and downgrades to a less powerful Amazon EC2 instance to match a decrease in demand

Auto Scaling group scales up and upgrades to a more powerful Amazon 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.

Additional Resources:

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

13. **Right Answer:**

Cloud Foundations

Cloud Foundations provides a guided path to help customers deploy, configure, and secure their new workloads while ensuring they are ready for on-going operations in the cloud. Cloud Foundations helps customers navigate through the decisions they need to make through curated AWS Services, AWS Solutions, Partner Solutions, and Guidance.

Cloud Foundations: via - https://aws.amazon.com/architecture/cloud-foundations/

Wrong Answer:

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

AWS Shared Responsibility Model - Under the AWS 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.

Additional Resources:

https://aws.amazon.com/architecture/cloud-foundations/

14. Right Answer:

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.

Wrong Answer:

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.

Additional Resources:

https://wa.aws.amazon.com/wat.pillar.operationalExcellence.en.html

15. Right Answer:

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: via
- https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/cost-alloc-tags.html

Wrong Answer:

Tags help in organizing 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.

Additional Resources:

https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/cost-alloc-tags.html

16. Right Answer:

AWS 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.

AWS Database Migration Service (AWS DMS)

AWS Database Migration Service (AWS DMS) 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 (AWS DMS) 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 AWS Database Migration Service (AWS DMS): via - https://aws.amazon.com/dms/

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

Wrong Answer:

AWS 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.

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 is a connectivity service and it does not specialize in data migration.

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. Transit Gateway is a connectivity service and it does not specialize in data migration.

Additional Resources:

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/

17. Right Answer:

AWS Migration Evaluator

AWS Migration Evaluator (Formerly TSO Logic) is a complimentary service to create data-driven business cases for AWS Cloud planning and migration.

AWS Migration Evaluator quickly provides a business case to make sound AWS planning and migration decisions. With AWS 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.

Wrong Answer:

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. AWS 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 AWS 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.

Additional Resources:

https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/ce-exploring-data.html

18. Right Answer:

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.

Wrong Answer:

The company should use AWS 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. AWS CloudFormation cannot help with moving data and applications into another Region.

The company should use AWS Database Migration Service (AWS DMS) to move the resources (including any data and applications) from source AWS Region to destination AWS Region - AWS Database Migration Service (AWS DMS) 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 (AWS DMS) can migrate your data to and from the most widely used commercial and open-source databases. AWS Database Migration Service (AWS DMS) 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.

19. Right Answer:

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/.

Wrong Answer:

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 Health Dashboard - service health - Amazon Web Services publishes up-to-the-minute information on service availability in a tabular form through its AWS Health Dashboard - service health 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://health.aws.amazon.com/health/status.

Additional Resources:

https://aws.amazon.com/premiumsupport/knowledge-center/

https://health.aws.amazon.com/health/status

20. Right Answer:

Number of requests for the AWS Lambda function

The time it takes for the lambda function to execute

AWS Lambda lets you run code without provisioning or managing servers. With AWS 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. AWS 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.

Wrong Answer:

The language runtime of the AWS Lambda function - AWS Lambda supports many programming language runtimes such as NodeJS, Python, Go, C# etc. The pricing for an AWS Lambda function is not dependent on the language runtime of the function.

The number of lines of code for the AWS Lambda function - The pricing for an AWS Lambda function is not dependent on the number of lines of code for the function.

The size of the deployment package for the AWS Lambda function - The pricing for an AWS Lambda function is not dependent on the size of the deployment package for the function.

Additional Resources:

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

21. Right Answer:

A security group is stateful, that is, it automatically allows the return traffic

A network access control list (network ACL) 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: via
- https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html

A network access control list (network ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets (i.e. it works at subnet level). A network access control list (network ACL) contains a numbered list of rules. A network access control list (network ACL) 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 (network ACL) overview: via
- https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html

Wrong Answer:

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 network access control list (network ACL) 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.

Additional Resources:

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

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

22. Right Answer:

Use Amazon CloudWatch Logs for both the Amazon Elastic Compute Cloud (Amazon 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.

Amazon 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.

Wrong Answer:

Use AWS Lambda to send log data from Amazon Elastic Compute Cloud (Amazon EC2) instance as well as on-premises servers to Amazon 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 Amazon Elastic Compute Cloud (Amazon EC2) instances and on-premises servers.

Use Amazon CloudWatch Logs for the Amazon Elastic Compute Cloud (Amazon EC2) instance and AWS CloudTrail for the on-premises servers

Use AWS CloudTrail for the Amazon Elastic Compute Cloud (Amazon EC2) instance and Amazon 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 AWS CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. AWS 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. AWS CloudTrail cannot be used to centralize the server logs for Amazon Elastic Compute Cloud (Amazon EC2) instances or on-premises servers, so both these options are incorrect.

Additional Resources:

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

https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/AgentReference.html

23. Right Answer:

Under the AWS 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 Amazon Elastic Compute Cloud (Amazon 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 Amazon Simple Storage Service (Amazon S3) buckets

In the AWS 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.

AWS Shared Responsibility Model Overview: via
- https://aws.amazon.com/compliance/shared-responsibility-model/

Wrong Answer:

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.

Additional Resources:

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

24. Right Answer:

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

Wrong Answer:

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.

Subnet - 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.

Additional Resources:

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

25. Right Answer:

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 Software as a Service (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 Software as a Service (SaaS).

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

Wrong Answer:

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. Amazon EC2 is an example of Infrastructure as a Service (IaaS).

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. AWS Elastic Beanstalk is an example of Platform as a Service (PaaS).

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. AWS Lambda is an example of Function as a service (FaaS).

Additional Resources:

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

26. **Right Answer:**

You will pay a fee each time you read from or write data stored on the Amazon Elastic File System (Amazon EFS) - Infrequent Access storage class

Amazon Elastic File System (Amazon EFS) - Infrequent Access storage class is cost-optimized for files accessed less frequently. Data stored on the Amazon Elastic File System (Amazon EFS) - 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 Elastic Block Store (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. Amazon EBS Snapshots are stored incrementally, which means you are billed only for the changed blocks stored.

Wrong Answer:

Amazon Elastic Compute Cloud (Amazon EC2) data transfer charges will apply for all Amazon Elastic Block Store (Amazon EBS) direct APIs for Snapshots - When using Amazon EBS direct APIs for Snapshots, additional Amazon EC2 data transfer charges will apply only when you use external or cross-region data transfers.

Amazon Elastic Block Store (Amazon EBS) Snapshot storage pricing is based on the amount of space your data consumes in Amazon Elastic Block Store (Amazon 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 Amazon EBS snapshots is charged for the data transferred across regions. After the snapshot is copied, standard Amazon EBS snapshot charges apply for storage in the destination region.

With AWS Backup, you pay only for the amount of Amazon Elastic File System (Amazon 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.

Additional Resources:

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

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

27. Right Answer:

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.

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 Simple Storage Service (Amazon S3)

Amazon DynamoDB

Exam Tip:

You may see a question around this concept in the exam. Just remember that only Amazon S3 and Amazon DynamoDB support VPC gateway endpoint. All other services that support VPC Endpoints use a VPC interface endpoint (note that Amazon S3 supports the VPC interface endpoint as well).

Wrong Answer:

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.

Additional Resources:

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

28. Right Answer:

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

Wrong Answer:

Elasticity

Documentation

Change Management

These three options are made-up and have no importance in the context of AWS Trusted Advisor.

Additional Resources:

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

29. Right Answer:

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 Amazon ElastiCache Works: via - https://aws.amazon.com/elasticache/

Wrong Answer:

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. It provides cost-efficient and resizable capacity while automating time-consuming administration tasks such as hardware provisioning, database setup, patching, and backups. Amazon Relational Database Service (Amazon 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. Amazon DynamoDB supports both key-value and document data models. This enables Amazon DynamoDB to have a flexible schema, so each row can have any number of columns at any point in time. This allows you to easily adapt the tables as your business requirements change, without having to redefine the table schema as you would in relational databases. Amazon 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. Amazon Athena is serverless, so there is no infrastructure to manage, and you pay only for the queries that you run. Amazon Athena cannot be used as an in-memory database.

Additional Resources:

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

30. Right Answer:

72

Reserved instances (RI) provide you with significant savings (up to 72%) on your Amazon Elastic Compute Cloud (Amazon EC2) costs compared to on-demand instance pricing. Reserved Instances (RI) are not physical instances, but rather a billing discount applied to the use of on-demand instances in your account. You can purchase a reserved instance (RI) for a one-year or three-year commitment, with the three-year commitment offering a bigger discount.

Amazon Elastic Compute Cloud (Amazon EC2) Pricing Options Overview: via - https://aws.amazon.com/ec2/pricing/

Wrong Answer:

90

50

40

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

Additional Resources:

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

31. Right Answer:

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.

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

Wrong Answer:

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

Additional Resources:

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

32. Right Answer:

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

Exam Tip:

Please review the differences between Amazon RDS Multi-AZ, Multi-Region and Read Replica deployments for RDS: via - https://aws.amazon.com/rds/features/multi-az/

Wrong Answer:

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 - Amazon Relational Database Service (Amazon RDS) with Read Replicas increases the database costs compared to the standard deployment. So this option is incorrect.

Additional Resources:

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

33. **Right Answer:**

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 - Reserved Instance (RI) utilization budgets (This lets you see if your Reserved Instances (RI) are unused or under-utilized), Reserved Instance (RI) coverage budgets (This lets you see how much of your instance usage is covered by a reservation).

Wrong Answer:

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.

Additional Resources:

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

34. **Right Answer:**

EC2 instances can access files on an Amazon Elastic File System (Amazon EFS) file system across many Availability Zones (AZ), 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: via - https://aws.amazon.com/efs/

Wrong Answer:

EC2 instances can access files on an Amazon Elastic File System (Amazon EFS) file system only in one Availability Zone (AZ)

EC2 instances can access files on an Amazon Elastic File System (Amazon EFS) file system across many Availability Zones (AZ) but not across VPCs and Regions

EC2 instances can access files on an Amazon Elastic File System (Amazon EFS) file system across many Availability Zones (AZ) and VPCs but not across Regions

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

Additional Resources:

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

35. **Right Answer:**

AWS Cost & Usage Report (AWS CUR)

AWS Cost & Usage Report (AWS CUR) contains the most comprehensive set of cost and usage data available. You can use AWS Cost & Usage Report (AWS CUR) 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 & Usage Report (AWS CUR) Overview: via
- https://docs.aws.amazon.com/cur/latest/userguide/what-is-cur.html

Wrong Answer:

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 Amazon 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. AWS 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 Tip:

Please review the differences between "AWS Cost & Usage Report (AWS CUR)" and "AWS Cost Explorer". Think of "AWS Cost & Usage Report (AWS CUR)" 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 Amazon 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 & Usage Report (AWS CUR)": via
- https://aws.amazon.com/aws-cost-management/aws-cost-explorer/

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

Additional Resources:

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/

36. **Right Answer:**

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. All of your data is stored on solid-state disks (SSDs) and is automatically replicated across multiple Availability Zones (AZ) in an AWS Region, providing built-in high availability and data durability.

Amazon DynamoDB High Availability: via
- https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Introduction.html

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 a regional service storing data within and across multiple Availability Zones (AZ) for high availability and durability.

Amazon EFS High Availability: via - https://aws.amazon.com/efs/faq/

Wrong Answer:

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.

Amazon Redshift only supports single Availability Zone (AZ) deployments: via
- https://aws.amazon.com/redshift/faqs/

Amazon Elastic Block Store (Amazon EBS) - Amazon Elastic Block Store (Amazon 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 Availability Zone (AZ) entities.

Additional Resources:

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/

37. **Right Answer:**

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:

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

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

Wrong Answer:

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.

Additional Resources:

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

38. **Right Answer:**

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.

Wrong Answer:

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. 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 Amazon 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. Amazon DynamoDB supports both key-value and document data models. This enables Amazon DynamoDB to have a flexible schema, so each row can have any number of columns at any point in time. This allows you to easily adapt the tables as your business requirements change, without having to redefine the table schema as you would in relational databases. Amazon 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. Amazon ElastiCache cannot be used for online analytical processing.

Additional Resources:

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

39. **Right Answer:**

Amazon S3 Glacier Deep Archive

Amazon 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. Amazon 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.

Amazon S3 Glacier Deep Archive Overview: via
- https://aws.amazon.com/s3/storage-classes/

Wrong Answer:

Amazon S3 Glacier Flexible Retrieval - Amazon S3 Glacier Flexible Retrieval (formerly S3 Glacier) is the ideal storage class for archiving data that does not require immediate access but needs the flexibility to retrieve large sets of data at no cost, such as backup or disaster recovery use cases. Amazon S3 Glacier Deep Archive is a better fit as it is more cost-optimal than Amazon S3 Glacier Flexible Retrieval 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). AWS Storage Gateway cannot be used for data archival.

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.

Additional Resources:

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

40. **Right Answer:**

Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)

Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) is for data that is accessed less frequently but requires rapid access when needed. Unlike other Amazon S3 Storage Classes which store data in a minimum of three Availability Zones (AZ), Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) stores data in a single Availability Zone (AZ).

Please review this illustration for Amazon S3 Storage Classes availability. You don't need to memorize the actual numbers, just remember that Amazon S3 One Zone-

Infrequent Access (S3 One Zone-IA) offers the lowest availability: via
- https://aws.amazon.com/s3/storage-classes/

Wrong Answer:

Amazon S3 Standard - Amazon S3 Standard offers high durability, availability, and performance object storage for frequently accessed data.

Amazon S3 Intelligent-Tiering - The Amazon 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.

Amazon S3 Glacier Flexible Retrieval - Amazon S3 Glacier Flexible Retrieval 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.

Additional Resources:

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

41. **Right Answer:**

AWS Transit Gateway

AWS Transit Gateway connects Amazon Virtual Private Clouds (Amazon VPC) 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 AWS Transit Gateway can simplify your network: via
- https://aws.amazon.com/transit-gateway/

Wrong Answer:

VPC peering connection - A VPC peering connection is a networking connection between two Amazon Virtual Private Clouds (Amazon VPC) that enables you to route traffic between them privately. VPC peering connection 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 connection is not allowed: via
- https://docs.aws.amazon.com/vpc/latest/peering/invalid-peering-configurations.html

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. AWS Direct Connect cannot be used to interconnect VPCs.

AWS 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. AWS Site-to-Site VPN cannot be used to interconnect VPCs.

Additional Resources:

https://aws.amazon.com/transit-gateway/

42. **Right Answer:**

Amazon Machine Image (AMI)

An Amazon Machine Image (AMI) provides the information required to launch an instance. You must specify an Amazon Machine Image (AMI) when you launch an instance.

An Amazon Machine Image (AMI) includes the following:

One or more Amazon Elastic Block Store (Amazon 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 Amazon Machine Image (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 Amazon Machine Image (AMI) lifecycle: via
- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html

Wrong Answer:

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

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

Additional Resources:

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

43. **Right Answer:**

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

Wrong Answer:

Amazon Elastic Block Store (Amazon EBS) - Amazon Elastic Block Store (Amazon EBS) is an easy to use, high-performance block storage service designed for use with Amazon Elastic Compute Cloud (Amazon EC2) for both throughput and transaction-intensive workloads at any scale. 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. Amazon EBS is not a good fit for caching information on Amazon EC2 instances.

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

consistent low latencies. Amazon EFS is not a good fit for caching information on Amazon EC2 instances.

Amazon Simple Storage Service (Amazon S3) - Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. Amazon S3 is not a good fit for caching information on Amazon EC2 instances.

Additional Resources:

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

44. **Right Answer:**

Amazon GuardDuty

Amazon GuardDuty is a threat detection service that monitors malicious activity and unauthorized behavior to protect your AWS account. Amazon GuardDuty analyzes billions of events across your AWS accounts from AWS CloudTrail (AWS user and API activity in your accounts), Amazon VPC Flow Logs (network traffic data), and DNS Logs (name query patterns). 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 Amazon GuardDuty Works: via - https://aws.amazon.com/guardduty/

Wrong Answer:

AWS CloudTrail - AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With AWS CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. Think account-specific activity and audit; think AWS CloudTrail. AWS CloudTrail cannot detect threats to your AWS account.

Amazon CloudWatch - Amazon CloudWatch is a monitoring and observability service built for DevOps engineers, developers, site reliability engineers (SREs), and IT managers. Amazon CloudWatch provides data and actionable insights to monitor 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 Amazon CloudWatch. Amazon CloudWatch cannot detect threats to your AWS account.

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 AWS Trusted Advisor regularly help

keep your solutions provisioned optimally. AWS Trusted Advisor cannot detect threats to your AWS account.

Additional Resources:

https://aws.amazon.com/guardduty

45. **Right Answer:**

Amazon S3 Glacier Flexible Retrieval

Amazon S3 Glacier Flexible Retrieval (formerly S3 Glacier) is the ideal storage class for archiving data that does not require immediate access but needs the flexibility to retrieve large sets of data at no cost, such as backup or disaster recovery use cases. It 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.

You can further review the use-cases for S3 Glacier Flexible Retrieval: via - https://aws.amazon.com/glacier/

S3 Storage Classes Overview: via - https://aws.amazon.com/s3/storage-classes/

Wrong Answer:

Amazon S3 Standard - Amazon S3 Standard offers high durability, availability, and performance object storage for frequently accessed data. It is not suitable for data archival.

Amazon S3 Intelligent-Tiering - The Amazon 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.

Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) - Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) is for data that is accessed less frequently, but requires rapid access when needed. Unlike other S3 Storage Classes which store data in a minimum of three Availability Zones (AZ), Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) stores data in a single Availability Zone (AZ). It is not suitable for data archival.

Additional Resources:

https://aws.amazon.com/glacier/

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

46. **Right Answer:**

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 AWS Trusted Advisor Works: via
- https://aws.amazon.com/premiumsupport/technology/trusted-advisor/

How AWS Trusted Advisor identifies low utilization Amazon EC2 instances: 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 AWS Cost Explorer helps you identify cost-saving opportunities by downsizing or terminating Amazon EC2 instances. You can see all of your underutilized Amazon EC2 instances across member accounts in a single view to immediately identify how much you can save.

Wrong Answer:

AWS Cost & Usage Report (AWS CUR) - The AWS Cost & Usage Report (AWS CUR) contains the most comprehensive set of cost and usage data available. You can use AWS Cost & Usage Report (AWS CUR) 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 & Usage Report (AWS CUR) cannot be used to identify under-utilized Amazon 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. Amazon CloudWatch cannot be used to identify under-utilized Amazon EC2 instances without manually configuring an alarm with the appropriate threshold to track the Amazon 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. AWS 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.

Additional Resources:

https://aws.amazon.com/premiumsupport/technology/trusted-advisor/best-practice-checklist/#Cost_Optimization

https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/ce-rightsizing.html

47. **Right Answer:**

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.

Wrong Answer:

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.

Additional Resources:

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

48. **Right Answer:**

Virtual private gateway (VGW)

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 (VGW) / Transit Gateway and Customer Gateway are the components of a VPC.

A virtual private gateway (VGW) is the VPN concentrator on the Amazon side of the AWS 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: via
- https://docs.aws.amazon.com/vpn/latest/s2svpn/how_it_works.html

Wrong Answer:

AWS 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.

Network Address Translation gateway (NAT gateway) - A Network Address Translation gateway (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. Network Address Translation gateway (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.

Additional Resources:

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

49. **Right Answer:**

Amazon Elastic Block Store (Amazon EBS) - Amazon Elastic Block Store (Amazon EBS) is an easy to use, high-performance block storage service designed for use with Amazon Elastic Compute Cloud (Amazon EC2) for both throughput and transaction-intensive workloads at any scale. 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. Amazon EC2 instance store cannot be used for file sharing between instances.

Wrong Answer:

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

Amazon Simple Storage Service (Amazon S3) - Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. This means customers of all sizes and industries can use it to store and protect any amount of data for a range of use cases, such as websites, mobile applications, backup and restore, archive, enterprise applications, IoT devices, and big data analytics.

Amazon Elastic Container Service (Amazon ECS) - Amazon Elastic Container Service (Amazon ECS) is a highly scalable, high-performance container management service that supports Docker containers and allows you to easily run applications on a managed cluster of Amazon EC2 instances. This is not a storage service and has been added as a distractor.

Additional Resources:

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

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

50. **Right Answer:**

Enable multi-factor authentication (MFA) for all users

AWS recommends that you require multi-factor authentication (MFA) for all users in your account. With multi-factor authentication (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: via
- https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html

Wrong Answer:

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.

Additional Resources:

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

51. **Right Answer:**

AWS Health Dashboard – Your account health

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

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

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

Wrong Answer:

Amazon GuardDuty - Amazon GuardDuty is a threat detection service that monitors malicious activity and unauthorized behavior to protect your AWS account. Amazon GuardDuty analyzes billions of events across your AWS accounts from AWS CloudTrail (AWS user and API activity in your accounts), Amazon VPC Flow Logs (network traffic data), and DNS Logs (name query patterns).

AWS Config - AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. AWS 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 AWS Trusted Advisor on a regular basis help keep your solutions provisioned optimally.

Additional Resources:

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

52. **Right Answer:**

Storing files in an accessible location to satisfy audit requirements

The Amazon EFS Standard-Infrequent Access (EFS 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 Elastic File System (Amazon EFS) provides.

AWS recommends Amazon EFS Standard-Infrequent Access (EFS Standard-IA) storage class 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. Amazon EFS Standard-Infrequent Access (EFS Standard-IA) storage is compatible with all Amazon EFS features, and is available in all AWS Regions where Amazon EFS is available.

Wrong Answer:

Storing data in a single AWS Availability Zone (AZ) - Amazon EFS One Zone-Infrequent Access (EFS One Zone-IA) 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 (AZ), or in the event of Availability Zone (AZ) destruction.

Object storage for workloads that need sub-second latency speeds for accessing the data - Amazon EFS is a file system service and not an object storage service. You should use Amazon S3 for object storage. So, this option is incorrect.

Use as boot volume for highly available Amazon Elastic Compute Cloud (Amazon EC2) instances - Amazon EFS cannot be used as a boot volume for Amazon Elastic Compute Cloud (Amazon EC2) instances. For boot volumes, Amazon Elastic Block Storage (Amazon EBS) volumes are used.

Additional Resources:

https://docs.aws.amazon.com/efs/latest/ug/storage-classes.html

https://aws.amazon.com/efs/features/infrequent-access/

53. **Right Answer:**

Use S3 cross-region replication (S3 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. S3 cross-region replication (S3 CRR) allows you to replicate data between distant AWS Regions to satisfy these requirements.

Wrong Answer:

Use S3 same-region replication (S3 SRR) to replicate data between distant AWS Regions - S3 same-region replication (S3 SRR) is used to copy objects across Amazon S3 buckets in the same AWS Region, so this option is incorrect.

Exam Tip:

Please review the differences between S3 same-region replication (S3 SRR) and S3 cross-region replication (S3 CRR): via
- https://docs.aws.amazon.com/AmazonS3/latest/dev/replication.html

For every new object, trigger an AWS Lambda function to write data into a bucket in another AWS Region - Although this solution is feasible, it's not resource efficient as the AWS Lambda is used to do something which S3 cross-region replication (S3 CRR) can achieve off-the-shelf.

Run a daily job on an Amazon Elastic Compute Cloud (Amazon EC2) instance to copy objects into another Region - Creating a daily job on Amazon Elastic Compute Cloud (Amazon EC2) instance to copy objects into another Region involves a lot of development effort. It is much better to use S3 cross-region replication (S3 CRR) for this task.

Additional Resources:

https://docs.aws.amazon.com/AmazonS3/latest/dev/replication.html

54. **Right Answer:**

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.

Wrong Answer:

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.

Additional Resources:

https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/billing-what-is.html

55. **Right Answer:**

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.

Wrong Answer:

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 Tip:

Please review the benefits of Cloud Computing:

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

Additional Resources:

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

56. **Right Answer:**

Maintain versions of an AWS Lambda function

Under the AWS 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 AWS 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 an AWS Lambda function.

AWS Shared Responsibility Model Overview: via
- https://aws.amazon.com/compliance/shared-responsibility-model/

Wrong Answer:

Patch underlying OS for the AWS Lambda function infrastructure

Maintain all runtime environments for AWS Lambda functions

Configure networking infrastructure for the AWS Lambda functions

As mentioned earlier, all these options fall under the ambit of AWS as far as the AWS Shared Responsibility Model is concerned.

Additional Resources:

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

57. **Right Answer:**

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.

Wrong Answer:

Sid, Principal

Action, Condition

Effect, Sid

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

Additional Resources:

https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html#access_policies-json

58. Right Answer:

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.

Wrong Answer:

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 Amazon 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 AWS Secrets Manager APIs, eliminating the need to hardcode sensitive information in plain text.

Additional Resources:

https://aws.amazon.com/security/penetration-testing/

59. Right Answer:

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

AWS Lambda

AWS Lambda is a compute service that lets you run code without provisioning or managing servers. AWS Lambda executes your code only when needed and scales

automatically, from a few requests per day to thousands per second. AWS Lambda 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. Amazon Rekognition is a regional service.

Wrong Answer:

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

Amazon CloudFront - 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 Web Application Firewall (AWS WAF) - By using AWS Web Application Firewall (AWS WAF), you can configure web access control lists (Web ACLs) on your CloudFront distributions or Application Load Balancers to filter and block requests based on request signatures.

As mentioned earlier, these three services are global in scope.

Exam Tip:

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.

60. Right Answer:

Fix the Amazon 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: 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: via
- https://docs.aws.amazon.com/AmazonS3/latest/dev/WebsiteAccessPermissions Reqd.html

Wrong Answer:

Disable Amazon S3 encryption

Enable Amazon S3 versioning

Enable Amazon S3 replication

Disabling Amazon S3 encryption, enabling Amazon S3 versioning or enabling Amazon S3 replication have no bearing on deploying a static website on Amazon S3, so these options are not correct.

Additional Resources:

https://docs.aws.amazon.com/AmazonS3/latest/dev/WebsiteHosting.html

https://docs.aws.amazon.com/AmazonS3/latest/dev/WebsiteAccessPermissionsR eqd.html

61. **Right Answer:**

Use Amazon CloudFront to improve the performance of your website

You can use Amazon CloudFront to improve the performance of your website. Amazon 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, Amazon 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.

Wrong Answer:

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

Use Amazon S3 Transfer Acceleration (Amazon S3TA) to improve the performance of your website - Amazon S3 Transfer Acceleration (Amazon S3TA) enables fast, easy, and secure transfers of files over long distances between your client and an S3 bucket. Amazon S3 Transfer Acceleration (Amazon S3TA) 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. Amazon S3 Transfer Acceleration (Amazon S3TA) cannot be used to improve the performance of a static website.

Additional Resources:

https://docs.aws.amazon.com/AmazonS3/latest/dev/website-hosting-cloudfront-walkthrough.html

https://docs.aws.amazon.com/AmazonS3/latest/dev/transfer-acceleration.html

62. **Right Answer:**

AWS Lambda

AWS Lambda lets you run code without provisioning or managing servers. You pay only for the compute time you consume. With AWS 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 AWS Lambda to thumbnail images, transcode videos, index files, process logs, validate content, and aggregate and filter data in real-time.

How AWS Lambda executes code in response to a trigger from S3: via - https://aws.amazon.com/lambda/

Wrong Answer:

Amazon Elastic Compute Cloud (Amazon EC2) - Amazon EC2 is a web service that provides secure, resizable compute capacity in the AWS cloud. You can use Amazon EC2 to provision virtual servers on AWS Cloud. Amazon EC2 cannot execute code via a trigger from S3.

Amazon Elastic Container Service (Amazon ECS) - Amazon Elastic Container Service (Amazon ECS) is a highly scalable, fast, container management service that makes it easy to run, stop, and manage Docker containers on a cluster. Amazon ECS cannot execute code via a trigger from S3.

Amazon Simple Queue Service (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. Using Amazon 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 Amazon SQS can be triggered from an Amazon S3 event, but Amazon SQS cannot execute code as its a message queuing service.

Additional Resources:

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

63.Right Answer:

Business

The AWS Cloud Adoption Framework (AWS CAF) leverages AWS experience and best practices to help you digitally transform and accelerate your business outcomes through innovative use of AWS. AWS CAF identifies specific organizational capabilities that underpin successful cloud transformations.

AWS CAF groups its capabilities in six perspectives: Business, People, Governance, Platform, Security, and Operations.

Wrong Answer:

Process

Product

Architecture

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

Additional Resources:

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

64. Right Answer:

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.

Wrong Answer:

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.

Additional Resources:

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