

Exam Questions AWS-Certified-Cloud-Practitioner

Amazon AWS Certified Cloud Practitioner

<https://www.2passeasy.com/dumps/AWS-Certified-Cloud-Practitioner/>



NEW QUESTION 1

- (Topic 2)

Which task is the responsibility of AWS when using AWS services?

- A. Management of IAM user permissions
- B. Creation of security group rules for outbound access
- C. Maintenance of physical and environmental controls
- D. Application of Amazon EC2 operating system patches

Answer: C

Explanation:

AWS is responsible for maintaining the physical and environmental controls of the AWS Cloud, such as power, cooling, fire suppression, and physical security¹. The customer is responsible for managing the IAM user permissions, creating security group rules for outbound access, applying Amazon EC2 operating system patches, and other aspects of security in the cloud¹.

NEW QUESTION 2

- (Topic 2)

A company migrated its core application onto multiple workloads in the AWS Cloud. The company wants to improve the application's reliability.

Which cloud design principle should the company implement to achieve this goal?

- A. Maximize utilization.
- B. Decouple the components.
- C. Rightsize the resources.
- D. Adopt a consumption model.

Answer: B

Explanation:

Decoupling the components of an application means reducing the dependencies and interactions between them, which can improve the application's reliability, scalability, and performance. Decoupling can be achieved by using services such as Amazon Simple Queue Service (Amazon SQS), Amazon Simple Notification Service (Amazon SNS), and AWS Lambda¹

NEW QUESTION 3

- (Topic 2)

Which tasks are the responsibility of AWS according to the AWS shared responsibility model? (Select TWO.)

- A. Configure AWS Identity and Access Management (IAM).
- B. Configure security groups on Amazon EC2 instances.
- C. Secure the access of physical AWS facilities.
- D. Patch applications that run on Amazon EC2 instances.
- E. Perform infrastructure patching and maintenance.

Answer: CE

Explanation:

The tasks that are the responsibility of AWS according to the AWS shared responsibility model are securing the access of physical AWS facilities and performing infrastructure patching and maintenance. The AWS shared responsibility model defines the division of responsibilities between AWS and the customer for security and compliance. AWS is responsible for the security of the cloud, which includes the physical security of the hardware, software, networking, and facilities that run the AWS services. AWS is also responsible for the maintenance and patching of the infrastructure that supports the AWS services. The customer is responsible for the security in the cloud, which includes the configuration and management of the AWS resources and applications that they use. Configuring AWS Identity and Access Management (IAM), configuring security groups on Amazon EC2 instances, and patching applications that run on Amazon EC2 instances are tasks that are the responsibility of the customer, not AWS.

NEW QUESTION 4

- (Topic 2)

A company is preparing to launch a redesigned website on AWS. Users from around the world will download digital handbooks from the website.

Which AWS solution should the company use to provide these static files securely?

- A. Amazon Kinesis Data Streams
- B. Amazon CloudFront with Amazon S3
- C. Amazon EC2 instances with an Application Load Balancer
- D. Amazon Elastic File System (Amazon EFS)

Answer: B

Explanation:

Amazon CloudFront with Amazon S3 is a solution that allows you to provide static files securely to users from around the world. 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. Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance. You can use Amazon S3 to store and retrieve any amount of data from anywhere. You can also configure Amazon S3 to work with Amazon CloudFront to distribute your content to edge locations near your users for faster delivery and lower latency. Amazon Kinesis Data Streams is a service that enables you to build custom applications that process or analyze streaming data for specialized needs. This option is not relevant for providing static files securely. Amazon EC2 instances with an Application Load Balancer is a solution that allows you to distribute incoming traffic across multiple targets, such as EC2 instances, in multiple Availability Zones. This option is suitable for dynamic web applications, but not necessary for static files. Amazon Elastic File System (Amazon EFS) is a service that provides a simple, scalable, fully managed elastic NFS file system for use with AWS Cloud services and on-premises resources. This option is not relevant for providing static files securely.

NEW QUESTION 5

- (Topic 2)

A company wants to run its production workloads on AWS. The company needs concierge service, a designated AWS technical account manager (TAM), and technical support that is available 24 hours a day, 7 days a week.

Which AWS Support plan will meet these requirements?

- A. AWS Basic Support
- B. AWS Enterprise Support
- C. AWS Business Support
- D. AWS Developer Support

Answer: B

Explanation:

B is correct because AWS Enterprise Support is the AWS Support plan that provides concierge service, a designated AWS technical account manager (TAM), and technical support that is available 24 hours a day, 7 days a week. This plan is designed for customers who run mission-critical workloads on AWS and need the highest level of support. A is incorrect because AWS Basic Support is the AWS Support plan that provides customer service and support for billing and account issues, service limit increases, and technical support for a limited set of AWS services. It does not provide concierge service, a designated TAM, or 24/7 technical support. C is incorrect because AWS Business Support is the AWS Support plan that provides customer service and support for billing and account issues, service limit increases, and technical support for all AWS services, as well as access to AWS Trusted Advisor and AWS Support API. It does not provide concierge service or a designated TAM. D is incorrect because AWS Developer Support is the AWS Support plan that provides customer service and support for billing and account issues, service limit increases, and technical support for all AWS services, as well as access to AWS Trusted Advisor. It does not provide concierge service, a designated TAM, or 24/7 technical support.

NEW QUESTION 6

- (Topic 2)

A company wants an in-memory data store that is compatible with open source in the cloud.

Which AWS service should the company use?

- A. Amazon DynamoDB
- B. Amazon ElastiCache
- C. Amazon Elastic Block Store (Amazon EBS)
- D. Amazon Redshift

Answer: B

Explanation:

Amazon ElastiCache is a fully managed in-memory data store service that is compatible with open source engines such as Redis and Memcached¹. It provides fast and scalable performance for applications that require high throughput and low latency¹. Amazon DynamoDB is a fully managed NoSQL database service that provides consistent and single-digit millisecond latency at any scale². Amazon EBS is a block storage service that provides persistent and durable storage volumes for Amazon EC2 instances³. Amazon Redshift is a fully managed data warehouse service that allows users to run complex analytic queries using SQL⁴.

NEW QUESTION 7

- (Topic 2)

A company wants to use Amazon EC2 instances for a stable production workload that will run for 1 year.

Which instance purchasing option meets these requirements MOST cost-effectively?

- A. Dedicated Hosts
- B. Reserved Instances
- C. On-Demand Instances
- D. Spot Instances

Answer: B

Explanation:

B is correct because Reserved Instances are the instance purchasing option that offers the most cost-effective way to use Amazon EC2 instances for a stable production workload that will run for 1 year, as they provide significant discounts compared to On-Demand Instances in exchange for a commitment to use a specific amount of computing power for a period of time. A is incorrect because Dedicated Hosts are the instance purchasing option that allows customers to use physical servers that are fully dedicated to their use, which is more expensive and less flexible than Reserved Instances. C is incorrect because On-Demand Instances are the instance purchasing option that allows customers to pay for compute capacity by the hour or second with no long-term commitments, which is more suitable for short-term, variable, and unpredictable workloads. D is incorrect because Spot Instances are the instance purchasing option that allows customers to bid on spare Amazon EC2 computing capacity, which is more suitable for flexible, scalable, and fault-tolerant workloads that can tolerate interruptions.

NEW QUESTION 8

- (Topic 1)

Which AWS service will help protect applications running on AWS from DDoS attacks?

- A. Amazon GuardDuty
- B. AWS WAF
- C. AWS Shield
- D. Amazon Inspector

Answer: C

Explanation:

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 protection³.

NEW QUESTION 9

- (Topic 1)

Which AWS features will meet these requirements? (Select TWO.)

- A. Security groups
- B. Network ACLs
- C. S3 bucket policies
- D. IAM user policies
- E. S3 bucket versioning

Answer: CD

Explanation:

The correct answers are C and D because S3 bucket policies and IAM user policies are AWS features that will meet the requirements. S3 bucket policies are access policies that can be attached to Amazon S3 buckets to grant or deny permissions to the bucket and the objects it contains. S3 bucket policies can be used to control who has permission to read, write, or delete objects that the company stores in the S3 bucket. IAM user policies are access policies that can be attached to IAM users to grant or deny permissions to AWS resources and actions. IAM user policies can be used to control who has permission to read, write, or delete objects that the company stores in the S3 bucket. The other options are incorrect because they are not AWS features that will meet the requirements. Security groups and network ACLs are AWS features that act as firewalls to control inbound and outbound traffic to and from Amazon EC2 instances and subnets. Security groups and network ACLs do not control who has permission to read, write, or delete objects that the company stores in the S3 bucket. S3 bucket versioning is an AWS feature that enables users to keep multiple versions of the same object in the same bucket. S3 bucket versioning can be used to recover from accidental overwrites or deletions of objects, but it does not control who has permission to read, write, or delete objects that the company stores in the S3 bucket. Reference: Using Bucket Policies and User Policies, Security Groups for Your VPC, Network ACLs, [Using Versioning]

NEW QUESTION 10

- (Topic 1)

Which of the following are pillars of the AWS Well-Architected Framework? (Select TWO.)

- A. Availability
- B. Reliability
- C. Scalability
- D. Responsive design
- E. Operational excellence

Answer: BE

Explanation:

The correct answers to the questions are B and E because reliability and operational excellence are pillars of the AWS Well-Architected Framework. The AWS Well-Architected Framework is a set of best practices and guidelines for designing and operating reliable, secure, efficient, and cost-effective systems in the cloud. The AWS Well-Architected Framework consists of five pillars: operational excellence, security, reliability, performance efficiency, and cost optimization. Each pillar has a set of design principles that describe the characteristics of a well-architected system. Reliability is the pillar that focuses on the ability of a system to recover from failures and meet business and customer demand. Operational excellence is the pillar that focuses on the ability of a system to run and monitor processes that support business outcomes and continually improve. The other options are incorrect because they are not pillars of the AWS Well-Architected Framework. Availability, scalability, and responsive design are important aspects of cloud architecture, but they are not separate pillars in the framework. Availability and scalability are related to the reliability and performance efficiency pillars, while responsive design is related to the customer experience and user interface. Reference: AWS Well-Architected Framework

NEW QUESTION 10

- (Topic 1)

A company has an application with robust hardware requirements. The application must be accessed by students who are using lightweight, low-cost laptops. Which AWS service will help the company deploy the application without investing in backend infrastructure or high end client hardware?

- A. Amazon AppStream 2.0
- B. AWS AppSync
- C. Amazon WorkLink
- D. AWS Elastic Beanstalk

Answer: A

Explanation:

The correct answer is A because Amazon AppStream 2.0 is a service that will help the company deploy the application without investing in backend infrastructure or high end client hardware. Amazon AppStream 2.0 is a fully managed, secure application streaming service that allows customers to stream desktop applications from AWS to any device running a web browser. Amazon AppStream 2.0 handles the provisioning, scaling, patching, and maintenance of the backend infrastructure, and delivers high performance and responsive user experience. The other options are incorrect because they are not services that will help the company deploy the application without investing in backend infrastructure or high end client hardware. AWS AppSync is a service that enables customers to create flexible APIs for synchronizing data across multiple data sources. Amazon WorkLink is a service that enables customers to provide secure, one-click access to internal websites and web apps from mobile devices. AWS Elastic Beanstalk is a service that enables customers to deploy and manage web applications using popular platforms such as Java, .NET, PHP, and Node.js. Reference: [Amazon AppStream 2.0 FAQs]

NEW QUESTION 12

- (Topic 1)

A cloud practitioner is analyzing Amazon EC2 instance performance and usage to provide recommendations for potential cost savings. Which cloud concept does this analysis demonstrate?

- A. Auto scaling
- B. Rightsizing
- C. Load balancing
- D. High availability

Answer: B

Explanation:

Rightsizing is the cloud concept that this analysis demonstrates. Rightsizing is the process of optimizing the performance and cost of your AWS resources by selecting the most appropriate type, size, and configuration based on your workload requirements and usage patterns. Rightsizing can help you achieve potential cost savings by reducing the over-provisioning or under-utilization of your resources. You can use various AWS tools and services, such as AWS Cost Explorer, AWS Compute Optimizer, and AWS Trusted Advisor, to analyze your resource utilization and performance metrics, and receive recommendations for rightsizing.

NEW QUESTION 13

- (Topic 1)

A company wants to establish a security layer in its VPC that will act as a firewall to control subnet traffic.

Which AWS service or feature will meet this requirement?

- A. Routing tables
- B. Network access control lists (network ACLs)
- C. Security groups
- D. Amazon GuardDuty

Answer: C

Explanation:

Security groups are the service or feature that meets the requirement of establishing a security layer in a VPC that will act as a firewall to control subnet traffic. Security groups are stateful firewalls that control the inbound and outbound traffic at the instance level. You can assign one or more security groups to each instance in a VPC, and specify the rules that allow or deny traffic based on the protocol, port, and source or destination. Security groups are associated with network interfaces, and therefore apply to all the instances in the subnets that use those network interfaces. Routing tables are used to direct traffic between subnets and gateways, not to filter traffic. Network ACLs are stateless firewalls that control the inbound and outbound traffic at the subnet level, but they are less granular and more cumbersome to manage than security groups. Amazon GuardDuty is a threat detection service that monitors your AWS account and workloads for malicious or unauthorized activity, not a firewall service.

NEW QUESTION 17

- (Topic 1)

Which AWS service or feature offers HTTP attack protection to users running public-facing web applications?

- A. Security groups
- B. Network ACLs
- C. AWS Shield Standard
- D. AWS WAF

Answer: D

Explanation:

AWS WAF is the AWS service or feature that offers HTTP attack protection to users running public-facing web applications. AWS WAF is a web application firewall that helps users protect their web applications from common web exploits, such as SQL injection, cross-site scripting, and bot attacks. Users can create custom rules to define the web traffic that they want to allow, block, or count. Users can also use AWS Managed Rules, which are pre-configured rules that are curated and maintained by AWS or AWS Marketplace Sellers. AWS WAF can be integrated with other AWS services, such as Amazon CloudFront, Amazon API Gateway, and Application Load Balancer, to provide comprehensive security for web applications. [AWS WAF Overview] AWS Certified Cloud Practitioner - aws.amazon.com

NEW QUESTION 18

- (Topic 1)

A company is hosting a web application in a Docker container on Amazon EC2. AWS is responsible for which of the following tasks?

- A. Scaling the web application and services developed with Docker
- B. Provisioning or scheduling containers to run on clusters and maintain their availability
- C. Performing hardware maintenance in the AWS facilities that run the AWS Cloud
- D. Managing the guest operating system, including updates and security patches

Answer: C

Explanation:

AWS is responsible for performing hardware maintenance in the AWS facilities that run the AWS Cloud. This is part of the shared responsibility model, where AWS is responsible for the security of the cloud, and the customer is responsible for security in the cloud. AWS is also responsible for the global infrastructure that runs all of the services offered in the AWS Cloud, including the hardware, software, networking, and facilities that run AWS Cloud services³. The customer is responsible for the guest operating system, including updates and security patches, as well as the web application and services developed with Docker⁴.

NEW QUESTION 23

- (Topic 1)

A company wants to centrally manage security policies and billing services within a multi- account AWS environment. Which AWS service should the company use to meet these requirements?

- A. AWS Identity and Access Management (IAM)
- B. AWS Organizations
- C. AWS Resource Access Manager (AWS RAM)
- D. AWS Config

Answer: B

Explanation:

AWS Organizations is a service that helps you centrally manage and govern your environment as you grow and scale your AWS resources. You can use AWS Organizations to create groups of accounts and apply policies to them. You can also use AWS Organizations to consolidate billing for multiple accounts. Therefore, the correct answer is B. You can learn more about AWS Organizations and its features from this page.

NEW QUESTION 25

- (Topic 1)

Which AWS service or tool provides users with the ability to monitor AWS service quotas?

- A. AWS CloudTrail
- B. AWS Cost and Usage Reports
- C. AWS Trusted Advisor
- D. AWS Budgets

Answer: C

Explanation:

The correct answer is C because AWS Trusted Advisor is an AWS service or tool that provides users with the ability to monitor AWS service quotas. AWS Trusted Advisor is an online tool that provides users with real-time guidance to help them provision their resources following AWS best practices. One of the categories of checks that AWS Trusted Advisor performs is service limits, which monitors the usage of each AWS service and alerts users when they are close to reaching the default limit. The other options are incorrect because they are not AWS services or tools that provide users with the ability to monitor AWS service quotas. AWS CloudTrail is a service that enables users to track user activity and API usage across their AWS account. AWS Cost and Usage Reports is a tool that enables users to access comprehensive information about their AWS costs and usage. AWS Budgets is a tool that enables users to plan their service usage, costs, and reservations. Reference: [AWS Trusted Advisor FAQs]

NEW QUESTION 27

- (Topic 1)

A company has a social media platform in which users upload and share photos with other users. The company wants to identify and remove inappropriate photos. The company has no machine learning (ML) scientists and must build this detection capability with no ML expertise.

Which AWS service should the company use to build this capability?

- A. Amazon SageMaker
- B. Amazon Textract
- C. Amazon Rekognition
- D. Amazon Comprehend

Answer: C

Explanation:

Amazon Rekognition is the AWS service that the company should use to build the capability of identifying and removing inappropriate photos. Amazon Rekognition is a service that uses deep learning technology to analyze images and videos for various purposes, such as face detection, object recognition, text extraction, and content moderation. Amazon Rekognition can help users detect unsafe or inappropriate content in images and videos, such as nudity, violence, or drugs, and provide confidence scores for each label. Amazon Rekognition does not require any machine learning expertise, and users can easily integrate it with other AWS services

NEW QUESTION 30

- (Topic 1)

Which AWS service or feature is used to send both text and email messages from distributed applications?

- A. Amazon Simple Notification Service (Amazon SNS)
- B. Amazon Simple Email Service (Amazon SES)
- C. Amazon CloudWatch alerts
- D. Amazon Simple Queue Service (Amazon SQS)

Answer: A

Explanation:

Amazon Simple Notification Service (Amazon SNS) is the AWS service or feature that is used to send both text and email messages from distributed applications. Amazon SNS is a fully managed pub/sub messaging service that enables the user to send messages to multiple subscribers or endpoints, such as email addresses, phone numbers, HTTP endpoints, AWS Lambda functions, and more. Amazon SNS can be used to send notifications, alerts, confirmations, and reminders from applications to users or other applications⁴.

NEW QUESTION 31

- (Topic 1)

Which design principle should be considered when architecting in the AWS Cloud?

- A. Think of servers as non-disposable resources.
- B. Use synchronous integration of services.
- C. Design loosely coupled components.
- D. Implement the least permissive rules for security groups.

Answer: C

Explanation:

Designing loosely coupled components is a design principle that should be considered when architecting in the AWS Cloud. Loose coupling is a way of designing systems to reduce interdependencies and minimize the impact of changes. Loose coupling allows components to interact with each other through well-defined interfaces, rather than direct references. This reduces the risk of failures and errors propagating across the system, and enables greater scalability, availability, and maintainability⁵.

NEW QUESTION 36

- (Topic 1)

A company needs to identify the last time that a specific user accessed the AWS Management Console.

Which AWS service will provide this information?

- A. Amazon Cognito
- B. AWS CloudTrail
- C. Amazon Inspector
- D. Amazon GuardDuty

Answer: B

Explanation:

AWS CloudTrail is the service that will provide the information about the last time that a specific user accessed the AWS Management Console. AWS CloudTrail is a service that records the API calls and events made by or on behalf of your AWS account. You can use AWS CloudTrail to view, search, and download the history of AWS console sign-in events, which include the user name, date, time, source IP address, and other details of the sign-in activity. Amazon Cognito, Amazon Inspector, and Amazon GuardDuty are not services that will provide this information. Amazon Cognito is a service that provides user authentication and authorization for web and mobile applications. Amazon Inspector is a service that assesses the security and compliance of your applications running on AWS. Amazon GuardDuty is a service that monitors your AWS account and workloads for malicious or unauthorized activity.

NEW QUESTION 40

- (Topic 1)

Which of the following is a cloud benefit that AWS offers to its users?

- A. The ability to configure AWS data center hypervisors
- B. The ability to purchase hardware in advance of increased traffic
- C. The ability to deploy to AWS on a global scale
- D. Compliance audits for user IT environments

Answer: C

Explanation:

The ability to deploy to AWS on a global scale is a cloud benefit that AWS offers to its users. AWS has a global infrastructure that consists of AWS Regions, Availability Zones, and edge locations. Users can choose from multiple AWS Regions around the world to deploy their applications and data closer to their end users, while also meeting their compliance and regulatory requirements. Users can also leverage AWS services, such as Amazon CloudFront, Amazon Route 53, and AWS Global Accelerator, to improve the performance and availability of their global applications. AWS also provides tools and guidance to help users optimize their global deployments, such as AWS Well-Architected Framework, AWS CloudFormation, and AWS Migration Hub. AWS Global Infrastructure [AWS Cloud Value Framework] AWS Certified Cloud Practitioner - aws.amazon.com

NEW QUESTION 43

- (Topic 1)

Which task requires the use of AWS account root user credentials?

- A. The deletion of IAM users
- B. The change to a different AWS Support plan
- C. The creation of an organization in AWS Organizations
- D. The deletion of Amazon EC2 instances

Answer: C

Explanation:

The creation of an organization in AWS Organizations requires the use of AWS account root user credentials. The AWS account root user is the email address that was used to create the AWS account. The root user has complete access to all AWS services and resources in the account, and can perform sensitive tasks such as changing the account settings, closing the account, or creating an organization. The root user credentials should be used sparingly and securely, and only for tasks that cannot be performed by IAM users or roles.

NEW QUESTION 48

- (Topic 1)

A company needs to use standard SQL to query and combine exabytes of structured and semi-structured data across a data warehouse, operational database, and data lake.

Which AWS service meets these requirements?

- A. Amazon DynamoDB
- B. Amazon Aurora
- C. Amazon Athena
- D. Amazon Redshift

Answer: D

Explanation:

Amazon Redshift is the service that meets the requirements of using standard SQL to query and combine exabytes of structured and semi-structured data across a data warehouse, operational database, and data lake. Amazon Redshift is a fully managed, petabyte-scale data warehouse service that allows you to run complex analytic queries using standard SQL and your existing business intelligence tools. Amazon Redshift also supports Redshift Spectrum, a feature that allows you to directly query and join data stored in Amazon S3 using the same SQL syntax. Amazon Redshift can scale up or down to handle any volume of data and deliver fast query performance.

NEW QUESTION 50

- (Topic 1)

A company's user base needs to remotely access virtual desktop computers from the internet. Which AWS service provides this functionality?

- A. Amazon Connect
- B. Amazon Cognito
- C. Amazon Workspaces
- D. Amazon Upstream 2.0

Answer: C

Explanation:

Amazon Workspaces is the AWS service that provides the functionality of remotely accessing virtual desktop computers from the internet. Amazon Workspaces is a fully managed, secure desktop-as-a-service (DaaS) solution that allows users to provision cloud-based virtual desktops and access them from anywhere, using any supported device. Amazon Workspaces helps users reduce the complexity and cost of managing and maintaining physical desktops, and provides a consistent and secure user experience

NEW QUESTION 51

- (Topic 1)

Which AWS service aggregates, organizes, and prioritizes security alerts and findings from multiple AWS services?

- A. Amazon Detective
- B. Amazon Inspector
- C. Amazon Macie
- D. AWS Security Hub

Answer: D

Explanation:

The correct answer is D because AWS Security Hub is a service that aggregates, organizes, and prioritizes security alerts and findings from multiple AWS services, such as Amazon GuardDuty, Amazon Inspector, Amazon Macie, AWS Firewall Manager, and AWS IAM Access Analyzer. The other options are incorrect because they are not services that aggregate security alerts and findings from multiple AWS services. Amazon Detective is a service that helps users analyze and visualize security data to investigate and remediate potential issues. Amazon Inspector is a service that helps users find security vulnerabilities and deviations from best practices in their Amazon EC2 instances. Amazon Macie is a service that helps users discover, classify, and protect sensitive data stored in Amazon S3. Reference: AWS Security Hub FAQs

NEW QUESTION 52

- (Topic 1)

A company needs to migrate all of its development teams to a cloud-based integrated development environment (IDE). Which AWS service should the company use?

- A. AWS CodeBuild
- B. AWS Cloud9
- C. AWS OpsWorks
- D. AWS Cloud Development Kit (AWS CDK)

Answer: B

Explanation:

The correct answer is B because AWS Cloud9 is an AWS service that enables users to run their existing custom, nonproduction workloads in the AWS Cloud quickly and cost-effectively. AWS Cloud9 is a cloud-based integrated development environment (IDE) that allows users to write, run, and debug code from a web browser. AWS Cloud9 supports multiple programming languages, such as Python, Java, Node.js, and more. AWS Cloud9 also provides users with a terminal that can access AWS services and resources, such as Amazon EC2 instances, AWS Lambda functions, and AWS CloudFormation stacks. The other options are incorrect because they are not AWS services that enable users to run their existing custom, nonproduction workloads in the AWS Cloud quickly and cost-effectively. AWS CodeBuild is an AWS service that enables users to compile, test, and package their code for deployment. AWS OpsWorks is an AWS service that enables users to configure and manage their applications using Chef or Puppet. AWS Cloud Development Kit (AWS CDK) is an AWS service that enables users to define and provision their cloud infrastructure using familiar programming languages, such as TypeScript, Python, Java, and C#. Reference: AWS Cloud9 FAQs

NEW QUESTION 55

- (Topic 1)

Which task is a customer's responsibility, according to the AWS shared responsibility model?

- A. Management of the guest operating systems
 - B. Maintenance of the configuration of infrastructure devices
 - C. Management of the host operating systems and virtualization
 - D. Maintenance of the software that powers Availability Zones
- A company has refined its workload to use specific AWS services to improve efficiency and reduce cost.

Answer: A

Explanation:

Management of the guest operating systems is a customer's responsibility, according to the AWS shared responsibility model. The AWS shared responsibility model defines the different security and compliance responsibilities of AWS and the customer. AWS is responsible for the security of the cloud, which includes the physical infrastructure, hardware, software, and facilities that run the AWS Cloud. The customer is responsible for security in the cloud, which includes the configuration and management of the guest operating systems, applications, data, and network traffic protection

NEW QUESTION 56

- (Topic 1)

Which AWS service or tool can be used to consolidate payments for a company with multiple AWS accounts?

- A. AWS Cost and Usage Report
- B. AWS Organizations
- C. Cost Explorer
- D. AWS Budgets

Answer: B

Explanation:

AWS Organizations is an account management service that enables you to consolidate multiple AWS accounts into an organization that you create and centrally manage. AWS Organizations includes consolidated billing and account management capabilities that enable you to better meet the budgetary, security, and compliance needs of your business¹.

NEW QUESTION 59

- (Topic 1)

A company is running applications on Amazon EC2 instances in the same AWS account for several different projects. The company wants to track the infrastructure costs for each of the projects separately. The company must conduct this tracking with the least possible impact to the existing infrastructure and with no additional cost.

What should the company do to meet these requirements?

- A. Use a different EC2 instance type for each project.
- B. Publish project-specific custom Amazon CloudWatch metrics for each application.
- C. Deploy EC2 instances for each project in a separate AWS account.
- D. Use cost allocation tags with values that are specific to each project.

Answer: D

Explanation:

The correct answer is D because cost allocation tags are a way to track the infrastructure costs for each of the projects separately. Cost allocation tags are key-value pairs that can be attached to AWS resources, such as EC2 instances, and used to categorize and group them for billing purposes. The other options are incorrect because they do not meet the requirements of the question. Use a different EC2 instance type for each project does not help to track the costs for each project, and may impact the performance and compatibility of the applications. Publish project-specific custom Amazon CloudWatch metrics for each application does not help to track the costs for each project, and may incur additional charges for using CloudWatch. Deploy EC2 instances for each project in a separate AWS account does help to track the costs for each project, but it impacts the existing infrastructure and incurs additional charges for using multiple accounts.

Reference: Using Cost Allocation Tags

NEW QUESTION 61

- (Topic 1)

Which AWS service should a cloud practitioner use to receive real-time guidance for provisioning resources, based on AWS best practices related to security, cost optimization, and service limits?

- A. AWS Trusted Advisor
- B. AWS Config
- C. AWS Security Hub
- D. AWS Systems Manager

Answer: A

Explanation:

AWS Trusted Advisor is the AWS service that provides real-time guidance for provisioning resources, based on AWS best practices related to security, cost optimization, and service limits. AWS Trusted Advisor inspects the user's AWS environment and provides recommendations for improving performance, security, and reliability, reducing costs, and following best practices. AWS Trusted Advisor also alerts the user when they are approaching or exceeding their service limits, and helps them request limit increases³.

NEW QUESTION 62

- (Topic 1)

What is the total amount of storage offered by Amazon S3?

- A. WOMB
- B. 5 GB
- C. 5 TB
- D. Unlimited

Answer: D

Explanation:

Amazon S3 offers unlimited storage for any amount of data. You can store as many objects as you want, and each object can be as large as 5 terabytes. You pay only for the storage space that you actually use, and there are no minimum commitments or upfront fees. Amazon S3 also provides high durability, availability, scalability, and security for your data.

NEW QUESTION 66

- (Topic 1)

A large company has a workload that requires hardware to remain on premises. The company wants to use the same management and control plane services that it currently uses on AWS.

Which AWS service should the company use to meet these requirements?

- A. AWS Device Farm
- B. AWS Fargate
- C. AWS Outposts
- D. AWS Ground Station

Answer: C

Explanation:

The correct answer is C because AWS Outposts is an AWS service that enables the company to meet the requirements. AWS Outposts is a fully managed service that extends AWS infrastructure, services, APIs, and tools to virtually any datacenter, co- location space, or on-premises facility. AWS Outposts allows customers to run their workloads on the same hardware and software that AWS uses in its cloud, while maintaining local access and control. The other options are

incorrect because they are not AWS services that enable the company to meet the requirements. AWS Device Farm is an AWS service that enables customers to test their mobile and web applications on real devices in the AWS Cloud. AWS Fargate is an AWS service that enables customers to run containers without having to manage servers or clusters. AWS Ground Station is an AWS service that enables customers to communicate with satellites and downlink data from orbit.
Reference: AWS Outposts FAQs

NEW QUESTION 71

- (Topic 1)

Which AWS network services or features allow CIDR block notation when providing an IP address range?
(Select TWO.)

- A. Security groups
- B. Amazon Machine Image (AMI)
- C. Network access control list (network ACL)
- D. AWS Budgets
- E. Amazon Elastic Block Store (Amazon EBS)

Answer: AC

Explanation:

Security groups and network access control lists (network ACLs) are two AWS network services or features that allow CIDR block notation when providing an IP address range. Security groups act as a firewall for associated Amazon EC2 instances, controlling both inbound and outbound traffic at the instance level. Network ACLs act as a firewall for associated subnets, controlling both inbound and outbound traffic at the subnet level. Both security groups and network ACLs use CIDR block notation to specify the IP address ranges that are allowed or denied

NEW QUESTION 73

- (Topic 1)

Which of the following is a benefit of decoupling an AWS Cloud architecture?

- A. Reduced latency
- B. Ability to upgrade components independently
- C. Decreased costs
- D. Fewer components to manage

Answer: B

Explanation:

A benefit of decoupling an AWS Cloud architecture is the ability to upgrade components independently. Decoupling is a way of designing systems to reduce interdependencies and minimize the impact of changes. Decoupling allows components to interact with each other through well-defined interfaces, rather than direct references. This reduces the risk of failures and errors propagating across the system, and enables greater scalability, availability, and maintainability. By decoupling an AWS Cloud architecture, the user can upgrade or modify one component without affecting the other components.

NEW QUESTION 78

- (Topic 1)

A company deploys its application to multiple AWS Regions and configures automatic failover between those Regions.
Which cloud concept does this architecture represent?

- A. Security
- B. Reliability
- C. Scalability
- D. Cost optimization

Answer: B

Explanation:

Reliability is the cloud concept that this architecture represents. Reliability is 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. Deploying an application to multiple AWS Regions and configuring automatic failover between those Regions enhances the reliability of the application by reducing the impact of regional failures and increasing the availability of the application.

NEW QUESTION 82

- (Topic 3)

A company wants to set up a high-speed connection between its data center and its applications that run on AWS. The company must not transfer data over the internet.

Which action should the company take to meet these requirements?

- A. Transfer data to AWS by using AWS Snowball.
- B. Transfer data to AWS by using AWS Storage Gateway.
- C. Set up a VPN connection between the data center and an AWS Region.
- D. Set up an AWS Direct Connect connection between the company network and AWS.

Answer: D

Explanation:

AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from a customer's premises to AWS. AWS Direct Connect does not involve the public internet, and therefore can reduce network costs, increase bandwidth throughput, and provide a more consistent network experience than internet-based connections. AWS Snowball is a petabyte-scale data transport service that uses secure devices to transfer large amounts of data into and out of the AWS Cloud. AWS Storage Gateway is a hybrid cloud storage service that gives customers on-premises access to virtually unlimited cloud storage. A VPN connection enables customers to establish a secure and private connection between their network and AWS.

NEW QUESTION 85

- (Topic 3)

A company wants to migrate a database from an on-premises environment to Amazon RDS.

After the migration is complete, which management task will the company still be responsible for?

- A. Hardware lifecycle management
- B. Application optimization
- C. Server maintenance
- D. Power, network, and cooling provisioning

Answer: B

Explanation:

Amazon RDS is a managed database service that handles most of the common database administration tasks, such as hardware provisioning, server maintenance, backup and recovery, patching, scaling, and replication. However, Amazon RDS does not optimize the application that interacts with the database. The company is still responsible for tuning the performance, security, and availability of the application according to its business requirements and best practices¹². References:

? What is Amazon Relational Database Service (Amazon RDS)?

? Perform common DBA tasks for Amazon RDS DB instances

NEW QUESTION 86

- (Topic 3)

A company deployed an Amazon EC2 instance last week. A developer realizes that the EC2 instance is no longer running. The developer reviews a list of provisioned EC2 instances, and the EC2 instance is no longer on the list.

What can the developer do to generate a recent history of the EC2 instance?

- A. Run Cost Explorer to identify the start time and end time of the EC2 instance.
- B. Use Amazon Inspector to find out when the EC2 instance was stopped.
- C. Perform a search in AWS CloudTrail to find all EC2 instance-related events.
- D. Use AWS Secrets Manager to display hidden termination logs of the EC2 instance.

Answer: C

Explanation:

AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of a customer's AWS account. AWS CloudTrail allows customers to track user activity and API usage across their AWS infrastructure. AWS CloudTrail can also provide a history of EC2 instance events, such as launch, stop, terminate, and reboot. Cost Explorer is a tool that enables customers to visualize, understand, and manage their AWS costs and usage over time. Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. AWS Secrets Manager helps customers protect secrets needed to access their applications, services, and IT resources.

NEW QUESTION 91

- (Topic 2)

A company wants to migrate to the AWS Cloud. The company needs the ability to acquire resources when the resources are necessary.

The company also needs the ability to release those resources when the resources are no longer necessary.

Which architecture concept of the AWS Cloud meets these requirements?

- A. Elasticity
- B. Availability
- C. Reliability
- D. Durability

Answer: A

Explanation:

The architecture concept of the AWS Cloud that meets the requirements of the company that wants to migrate to the AWS Cloud and needs the ability to acquire and release resources as needed is elasticity. Elasticity means that AWS customers can quickly and easily provision and scale up or down AWS resources as their demand changes, without any upfront costs or long-term commitments. AWS provides various tools and services that enable customers to achieve elasticity, such as Amazon EC2 Auto Scaling, Amazon CloudWatch, and AWS CloudFormation. Elasticity helps customers optimize their performance, availability, and cost efficiency. Availability, reliability, and durability are other architecture concepts of the AWS Cloud, but they are not directly related to the ability to acquire and release resources as needed. Availability means that AWS customers can access their AWS resources and applications whenever and wherever they need them. Reliability means that AWS customers can depend on their AWS resources and applications to function correctly and consistently. Durability means that AWS customers can preserve their data and objects for long periods of time without loss or corruption¹²

NEW QUESTION 95

- (Topic 2)

A company wants to securely store Amazon RDS database credentials and automatically rotate user passwords periodically.

Which AWS service or capability will meet these requirements?

- A. Amazon S3
- B. AWS Systems Manager Parameter Store
- C. AWS Secrets Manager
- D. AWS CloudTrail

Answer: C

Explanation:

AWS Secrets Manager is a service that helps you protect access to your applications, services, and IT resources. This service enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle¹. Amazon S3 is a storage service that does not offer automatic rotation of credentials. AWS Systems Manager Parameter Store is a service that provides secure, hierarchical storage for configuration data management and secrets management², but it does not offer automatic rotation of credentials. AWS CloudTrail is a service that enables governance, compliance, operational

auditing, and risk auditing of your AWS account³, but it does not store or rotate credentials.

NEW QUESTION 100

- (Topic 2)

Which AWS service can a company use to securely store and encrypt passwords for a database?

- A. AWS Shield
- B. AWS Secrets Manager
- C. AWS Identity and Access Management (IAM)
- D. Amazon Cognito

Answer: B

Explanation:

AWS Secrets Manager is an AWS service that can be used to securely store and encrypt passwords for a database. It allows users to manage secrets, such as database credentials, API keys, and tokens, in a centralized and secure way. It also provides features such as automatic rotation, fine-grained access control, and auditing. AWS Shield is an AWS service that provides protection against Distributed Denial of Service (DDoS) attacks for AWS resources and services. It does not store or encrypt passwords for a database. AWS Identity and Access Management (IAM) is an AWS service that allows users to manage access to AWS resources and services. It can be used to create users, groups, roles, and policies that control who can do what in AWS. It does not store or encrypt passwords for a database. Amazon Cognito is an AWS service that provides user identity and data synchronization for web and mobile applications. It can be used to authenticate and authorize users, manage user profiles, and sync user data across devices. It does not store or encrypt passwords for a database.

NEW QUESTION 101

- (Topic 2)

Which design principles should a company apply to AWS Cloud workloads to maximize sustainability and minimize environmental impact? (Select TWO.)

- A. Maximize utilization of Amazon EC2 instances.
- B. Minimize utilization of Amazon EC2 instances.
- C. Minimize usage of managed services.
- D. Force frequent application reinstallations by users.
- E. Reduce the need for users to reinstall applications.

Answer: AE

Explanation:

To maximize sustainability and minimize environmental impact, a company should apply the following design principles to AWS Cloud workloads: maximize utilization of Amazon EC2 instances and reduce the need for users to reinstall applications. Maximizing utilization of Amazon EC2 instances means that the company can optimize the performance and efficiency of their compute resources, and avoid wasting energy and money on idle or underutilized instances. The company can use features such as Amazon EC2 Auto Scaling, Amazon EC2 Spot Instances, and AWS Compute Optimizer to automatically adjust the number and type of instances based on demand, cost, and performance. Reducing the need for users to reinstall applications means that the company can minimize the amount of data and bandwidth required to deliver their applications to users, and avoid unnecessary downloads and updates that consume energy and resources. The company can use services such as Amazon CloudFront, AWS AppStream 2.0, and AWS Amplify to deliver their applications faster, more securely, and more efficiently to users across the globe. Minimizing utilization of Amazon EC2 instances, minimizing usage of managed services, and forcing frequent application reinstallations by users are not design principles that would maximize sustainability and minimize environmental impact. Minimizing utilization of Amazon EC2 instances would reduce the performance and efficiency of the compute resources, and potentially increase the costs and complexity of the cloud workloads. Minimizing usage of managed services would increase the operational overhead and responsibility of the company, and potentially expose them to more security and reliability risks. Forcing frequent application reinstallations by users would increase the amount of data and bandwidth required to deliver the applications to users, and potentially degrade the user experience and satisfaction.

NEW QUESTION 102

- (Topic 2)

A company wants to use Amazon EC2 instances to run a stateless and restartable process after business hours.

Which AWS service provides DNS resolution?

- A. Amazon CloudFront
- B. Amazon VPC
- C. Amazon Route 53
- D. AWS Direct Connect

Answer: C

Explanation:

Amazon Route 53 is the AWS service that provides DNS resolution. DNS (Domain Name System) is a service that translates domain names into IP addresses. Amazon Route 53 is a highly available and scalable cloud DNS service that offers domain name registration, DNS routing, and health checking. Amazon Route 53 can route the traffic to various AWS services, such as Amazon EC2, Amazon S3, and Amazon CloudFront. Amazon Route 53 can also integrate with other AWS services, such as AWS Certificate Manager, AWS Shield, and AWS WAF. For more information, see [What is Amazon Route 53?] and [Amazon Route 53 Features].

NEW QUESTION 107

- (Topic 2)

Which of the following is entirely the responsibility of AWS, according to the AWS shared responsibility model?

- A. Security awareness and training
- B. Development of an IAM password policy
- C. Patching of the guest operating system
- D. Physical and environmental controls

Answer: D

Explanation:

Physical and environmental controls are entirely the responsibility of AWS, according to the AWS shared responsibility model. The AWS shared responsibility model defines the division of responsibilities between AWS and the customer for security and compliance. AWS is responsible for the security of the cloud, which includes the physical and environmental controls of the AWS global infrastructure, such as power, cooling, fire suppression, and physical access. The customer is responsible for the security in the cloud, which includes the configuration and management of the AWS resources and applications. For more information, see [AWS Shared Responsibility Model] and [AWS Cloud Security].

NEW QUESTION 108

- (Topic 2)

A user is moving a workload from a local data center to an architecture that is distributed between the local data center and the AWS Cloud. Which type of migration is this?

- A. On-premises to cloud native
- B. Hybrid to cloud native
- C. On-premises to hybrid
- D. Cloud native to hybrid

Answer: C

Explanation:

C is correct because moving a workload from a local data center to an architecture that is distributed between the local data center and the AWS Cloud is an example of an on-premises to hybrid migration. A hybrid cloud is a cloud computing environment that uses a mix of on-premises, private cloud, and public cloud services with orchestration between the platforms. A is incorrect because on-premises to cloud native migration is the process of moving a workload from a local data center to an architecture that is fully hosted and managed on the AWS Cloud. B is incorrect because hybrid to cloud native migration is the process of moving a workload from an architecture that is distributed between the local data center and the AWS Cloud to an architecture that is fully hosted and managed on the AWS Cloud. D is incorrect because cloud native to hybrid migration is the process of moving a workload from an architecture that is fully hosted and managed on the AWS Cloud to an architecture that is distributed between the local data center and the AWS Cloud.

NEW QUESTION 110

- (Topic 2)

A company wants to move its data warehouse application to the AWS Cloud. The company wants to run and scale its analytics services without needing to provision and manage data warehouse clusters. Which AWS service will meet these requirements?

- A. Amazon Redshift provisioned data warehouse
- B. Amazon Redshift Serverless
- C. Amazon Athena
- D. Amazon S3

Answer: B

Explanation:

Amazon Redshift Serverless is the AWS service that will meet the requirements of the company that wants to move its data warehouse application to the AWS Cloud and run and scale its analytics services without needing to provision and manage data warehouse clusters. Amazon Redshift Serverless is a new feature of Amazon Redshift, which is a fully managed data warehouse service that allows customers to run complex queries and analytics on large volumes of structured and semi-structured data. Amazon Redshift Serverless automatically scales the compute and storage resources based on the workload demand, and customers only pay for the resources they consume. Amazon Redshift Serverless also simplifies the management and maintenance of the data warehouse, as customers do not need to worry about choosing the right cluster size, resizing the cluster, or distributing the data across the nodes. Amazon Redshift provisioned data warehouse, Amazon Athena, and Amazon S3 are not the best services to meet the requirements of the company. Amazon Redshift provisioned data warehouse requires customers to choose the number and type of nodes for their cluster, and manually resize the cluster if their workload changes. Amazon Athena is a serverless query service that allows customers to analyze data stored in Amazon S3 using standard SQL, but it is not a data warehouse service that can store and organize the data. Amazon S3 is a scalable object storage service that can store any amount and type of data, but it is not a data warehouse service that can run complex queries and analytics on the data.

NEW QUESTION 115

- (Topic 2)

A company is running an order processing system on Amazon EC2 instances. The company wants to migrate microservices-based application. Which combination of AWS services can the application use to meet these requirements? (Select TWO.)

- A. Amazon Simple Queue Service (Amazon SQS)
- B. AWS Lambda
- C. AWS Migration Hub
- D. AWS AppSync
- E. AWS Application Migration Service

Answer: AB

Explanation:

The combination of AWS services that the application can use to migrate to a microservices-based application are Amazon Simple Queue Service (Amazon SQS) and AWS Lambda. Amazon SQS is a fully managed message queuing service that enables customers to decouple and scale microservices, distributed systems, and serverless applications. The application can use Amazon SQS to send, store, and receive messages between the microservices, ensuring that each message is processed only once and in the right order. AWS Lambda is a serverless compute service that allows customers to run code without provisioning or managing servers. The application can use AWS Lambda to create and deploy microservices as functions that are triggered by events, such as messages from Amazon SQS. AWS Migration Hub, AWS AppSync, and AWS Application Migration Service are not the best services to use for migrating to a microservices-based application. AWS Migration Hub is a service that provides a single location to track the progress of application migrations across multiple AWS and partner solutions. AWS AppSync is a service that simplifies the development of GraphQL APIs for real-time and offline data synchronization. AWS Application Migration Service is a service that enables customers to migrate their on-premises applications to AWS without making any changes to the applications, servers, or databases.

NEW QUESTION 118

- (Topic 2)

A company wants to improve its security and audit posture by limiting Amazon EC2 inbound access. According to the AWS shared responsibility model, which task is the responsibility of the customer?

- A. Protect the global infrastructure that runs all of the services offered in the AWS Cloud.
- B. Configure logical access controls for resources, and protect account credentials.
- C. Configure the security used by managed services.
- D. Patch and back up Amazon Aurora.

Answer: B

Explanation:

According to the AWS shared responsibility model, the customer is responsible for configuring logical access controls for resources, and protecting account credentials. This includes managing IAM user permissions, security group rules, network ACLs, encryption keys, and other aspects of access management¹. AWS is responsible for protecting the global infrastructure that runs all of the services offered in the AWS Cloud, such as the hardware, software, networking, and facilities. AWS is also responsible for configuring the security used by managed services, such as Amazon RDS, Amazon DynamoDB, and Amazon Aurora².

NEW QUESTION 121

- (Topic 2)

Which of the following is the customer's responsibility, according to the AWS shared responsibility model?

- A. Identity and access management
- B. Hard drive initialization
- C. Protection of data center hardware
- D. Security of Availability Zones

Answer: A

Explanation:

Identity and access management is the customer's responsibility, according to the AWS shared responsibility model. This means that the customer is responsible for managing user access to the AWS resources, using tools such as AWS Identity and Access Management (IAM), AWS Single Sign-On (SSO), and AWS Organizations. The customer is also responsible for securing their data in transit and at rest, using encryption, key management, and other methods. Hard drive initialization, protection of data center hardware, and security of Availability Zones are AWS's responsibility, as they are part of the infrastructure, physical security, and network security that AWS provides to the customer¹².

NEW QUESTION 126

- (Topic 2)

Which group shares responsibility with AWS for security and compliance of AWS accounts and resources?

- A. Third-party vendors
- B. Customers
- C. Reseller partners
- D. Internet providers

Answer: B

Explanation:

Customers share responsibility with AWS for security and compliance of AWS accounts and resources. This is part of the AWS shared responsibility model, which defines the division of responsibilities between AWS and the customer for security and compliance. AWS is responsible for the security of the cloud, which includes the physical and environmental controls of the AWS global infrastructure, such as power, cooling, fire suppression, and physical access. The customer is responsible for the security in the cloud, which includes the configuration and management of the AWS resources and applications, such as identity and access management, encryption, firewall, and backup.

For more information, see AWS Shared Responsibility Model and AWS Cloud Security.

NEW QUESTION 129

- (Topic 2)

A company is running workloads for multiple departments within a single VPC. The company needs to be able to bill each department for its resource usage. Which action should the company take to accomplish this goal with the LEAST operational overhead?

- A. Add a department tag to each resource and configure cost allocation tags.
- B. Move each department resource to its own VPC.
- C. Move each department resource to its own AWS account.
- D. Use AWS Organizations to get a billing report for each department.

Answer: A

Explanation:

Adding a department tag to each resource and configuring cost allocation tags is an action that can help you accomplish the goal of billing each department for its resource usage with the least operational overhead. Tags are simple labels consisting of a key and an optional value that you can assign to AWS resources. You can use tags to organize your resources and track your AWS costs on a detailed level. Cost allocation tags enable you to track your AWS costs on a detailed level. After you activate cost allocation tags, AWS uses the cost allocation tags to organize your resource costs on your cost allocation report, to make it easier for you to categorize and track your AWS costs². Moving each department resource to its own VPC or its own AWS account is an action that can help you isolate and control the resources for each department, but it would incur more operational overhead than using tags. Using AWS Organizations to get a billing report for each department is an action that can help you consolidate billing and payment across multiple AWS accounts, but it would not help you bill each department for its resource usage within a single VPC.

NEW QUESTION 133

- (Topic 2)

Which perspective of the AWS Cloud Adoption Framework (AWS CAF) connects technology and business?

- A. Operations
- B. People
- C. Security
- D. Governance

Answer: D

Explanation:

The perspective of the AWS Cloud Adoption Framework (AWS CAF) that connects technology and business is governance. The governance perspective focuses on the alignment of the IT strategy and processes with the business strategy and goals, as well as the management of the IT budget, risk, and compliance. The governance perspective capabilities are portfolio management, business performance management, and IT governance. The governance perspective helps organizations ensure that their cloud adoption delivers the expected business value and outcomes, and that their cloud solutions are secure, reliable, and compliant. Operations, people, and security are other perspectives of the AWS CAF, but they do not directly connect technology and business. The operations perspective focuses on the management and monitoring of the cloud resources and applications, as well as the automation and optimization of the operational processes. The people perspective focuses on the development and empowerment of the human resources, as well as the transformation of the organizational culture and structure. The security perspective focuses on the protection of the information assets and systems in the cloud, as well as the implementation of the security policies and controls.

NEW QUESTION 134

- (Topic 2)

A company plans to migrate its on-premises workload to AWS. Before the migration, the company needs to estimate its future AWS service costs. Which AWS service or tool should the company use to meet this requirement?

- A. AWS Trusted Advisor
- B. AWS Budgets
- C. AWS Pricing Calculator
- D. AWS Cost Explorer

Answer: C

Explanation:

AWS Pricing Calculator is the AWS service or tool that the company should use to estimate its future AWS service costs before the migration. AWS Pricing Calculator is a web-based tool that allows the company to create cost estimates for various AWS services and scenarios. AWS Pricing Calculator helps the company to compare the costs of running the workload on premises versus on AWS, and to optimize the costs by choosing the best options for the workload. AWS Pricing Calculator also provides a detailed breakdown of the cost components and a downloadable report. For more information, see [AWS Pricing Calculator] and [Getting Started with AWS Pricing Calculator].

NEW QUESTION 137

- (Topic 2)

A company wants to create multiple isolated networks in the same AWS account. Which AWS service or component will provide this functionality?

- A. AWS Transit Gateway
- B. Internet gateway
- C. Amazon VPC
- D. Amazon EC2

Answer: C

Explanation:

Amazon Virtual Private Cloud (Amazon VPC) is the AWS service that allows customers to create multiple isolated networks in the same AWS account. A VPC is a logically isolated section of the AWS Cloud where customers can launch AWS resources in a virtual network that they define. Customers can create multiple VPCs within an AWS account, each with its own IP address range, subnets, route tables, security groups, network access control lists, gateways, and other components. AWS Transit Gateway, Internet gateway, and Amazon EC2 are not services or components that provide the functionality of creating multiple isolated networks in the same AWS account. AWS Transit Gateway is a service that enables customers to connect their Amazon VPCs and their on- premises networks to a single gateway. An Internet gateway is a component that enables communication between instances in a VPC and the Internet. Amazon EC2 is a service that provides scalable compute capacity in the cloud³⁴

NEW QUESTION 141

- (Topic 2)

Which statements explain the business value of migration to the AWS Cloud? (Select TWO.)

- A. The migration of enterprise applications to the AWS Cloud makes these applications automatically available on mobile devices.^S
- B. AWS availability and security provide the ability to improve service level agreements (SLAs) while reducing risk and unplanned downtime.
- C. Companies that migrate to the AWS Cloud eliminate the need to plan for high availability and disaster recovery.
- D. Companies that migrate to the AWS Cloud reduce IT costs related to infrastructure, freeing budget for reinvestment in other areas.
- E. Applications are modernized because migration to the AWS Cloud requires companies to rearchitect and rewrite all enterprise applications.

Answer: BD

Explanation:

B and D are correct because AWS availability and security enable customers to improve their SLAs while reducing risk and unplanned downtime¹, and AWS reduces IT costs related to infrastructure, allowing customers to reinvest in other areas². A is incorrect because migrating to the AWS Cloud does not automatically make applications available on mobile devices, as it depends on the application design and compatibility. C is incorrect because companies that migrate to the AWS Cloud still need to plan for high availability and disaster recovery, as AWS is a shared responsibility model³. E is incorrect because migrating to the AWS Cloud does not require companies to rearchitect and rewrite all enterprise applications, as AWS offers different migration strategies depending on the application complexity and business objectives⁴.

NEW QUESTION 144

- (Topic 2)

Which AWS service is designed to help users build conversational interfaces into applications using voice and text?

- A. Amazon Lex
- B. Amazon Transcribe
- C. Amazon Comprehend
- D. Amazon Timestream

Answer: A

Explanation:

A is correct because Amazon Lex is the AWS service that helps users build conversational interfaces into applications using voice and text. B is incorrect because Amazon Transcribe is the AWS service that helps users convert speech to text. C is incorrect because Amazon Comprehend is the AWS service that helps users analyze text using natural language processing. D is incorrect because Amazon Timestream is the AWS service that helps users collect, store, and process time series data.

NEW QUESTION 149

- (Topic 2)

A company is hosting a web application on Amazon EC2 instances. The company wants to implement custom conditions to filter and control inbound web traffic. Which AWS service will meet these requirements?

- A. Amazon GuardDuty
- B. AWS WAF
- C. Amazon Macie
- D. AWS Shield

Answer: B

Explanation:

The AWS service that will meet the requirements of the company that is hosting a web application on Amazon EC2 instances and wants to implement custom conditions to filter and control inbound web traffic is AWS WAF. AWS WAF is a web application firewall that helps protect web applications from common web exploits that could affect availability, compromise security, or consume excessive resources. The company can use AWS WAF to create custom rules that block malicious requests that match certain patterns, such as SQL injection or cross-site scripting. AWS WAF can be applied to web applications that are behind an Application Load Balancer, Amazon CloudFront, or Amazon API Gateway. Amazon GuardDuty, Amazon Macie, and AWS Shield are not the best services to use for this purpose. Amazon GuardDuty is a threat detection service that monitors for malicious activity and unauthorized behavior across the AWS accounts and resources. Amazon Macie is a data security and data privacy service that uses machine learning and pattern matching to discover, classify, and protect sensitive data stored in Amazon S3. AWS Shield is a managed distributed denial of service (DDoS) protection service that safeguards web applications running on AWS. These services are more useful for detecting and preventing different types of threats and attacks, rather than filtering and controlling inbound web traffic based on custom conditions.

NEW QUESTION 153

- (Topic 2)

A company wants to implement controls (guardrails) in a newly created AWS Control Tower landing zone.

Which AWS services or features can the company use to create and define these controls (guardrails)? (Select TWO.)

- A. AWS Config
- B. Service control policies (SCPs)
- C. Amazon GuardDuty
- D. AWS Identity and Access Management (IAM)
- E. Security groups

Answer: AB

Explanation:

AWS Config and service control policies (SCPs) are AWS services or features that the company can use to create and define controls (guardrails) in a newly created AWS Control Tower landing zone. AWS Config is a service that enables users to assess, audit, and evaluate the configurations of their AWS resources. It can be used to create rules that check for compliance with the desired configurations and report any deviations. AWS Control Tower provides a set of predefined AWS Config rules that can be enabled as guardrails to enforce compliance across the landing zone¹. Service control policies (SCPs) are a type of policy that can be used to manage permissions in AWS Organizations. They can be used to restrict the actions that the users and roles in the member accounts can perform on the AWS resources. AWS Control Tower provides a set of predefined SCPs that can be enabled as guardrails to prevent access to certain services or regions across the landing zone². Amazon GuardDuty is a service that provides intelligent threat detection and continuous monitoring for AWS accounts and resources. It is not a feature that can be used to create and define controls (guardrails) in a landing zone. AWS Identity and Access Management (IAM) is a service that allows users to manage access to AWS resources and services. It can be used to create users, groups, roles, and policies that control who can do what in AWS. It is not a feature that can be used to create and define controls (guardrails) in a landing zone. Security groups are virtual firewalls that control the inbound and outbound traffic for Amazon EC2 instances. They can be used to allow or deny access to an EC2 instance based on the port, protocol, and source or destination. They are not a feature that can be used to create and define controls (guardrails) in a landing zone.

NEW QUESTION 156

- (Topic 2)

A company that is planning to migrate to the AWS Cloud is based in an isolated area that has limited internet connectivity. The company needs to perform local data processing on premises. The company needs a solution that can operate without a stable internet connection.

Which AWS service will meet these requirements?

- A. Amazon S3
- B. AWS Snowball Edge
- C. AWS StorageGateway
- D. AWS Backup

Answer: B

Explanation:

AWS Snowball Edge is a service that provides a physical device that can store up to 100 TB of data and perform local data processing on premises. It enables users to transfer data to and from the AWS Cloud in areas with limited or no internet connectivity. It also supports AWS Greengrass, which allows users to run AWS Lambda functions and other AWS services locally without a stable internet connection. Amazon S3 is a storage service that provides scalable, durable, and secure object storage. It requires a stable internet connection to transfer data to and from the AWS Cloud. AWS Storage Gateway is a service that provides a hybrid storage solution that connects on-premises applications to AWS Cloud storage services, such as Amazon S3, Amazon S3 Glacier, and Amazon EBS. It requires a stable internet connection to synchronize data between the on-premises and cloud storage. AWS Backup is a service that provides a centralized and automated solution to back up data across AWS services and on-premises resources. It requires a stable internet connection to transfer data to and from the AWS Cloud.

NEW QUESTION 157

- (Topic 2)

Which AWS service or tool offers consolidated billing?

- A. AWS Artifact
 - B. AWS Budgets
 - C. AWS Organizations
 - D. AWS Trusted Advisor
- A company wants to limit its employees' AWS access to a portfolio of predefined AWS resources.

Answer: C

Explanation:

AWS Organizations is a service that enables you to consolidate multiple AWS accounts into an organization that you create and centrally manage. With AWS Organizations, you can create a single payment method for all the AWS accounts in your organization through consolidated billing. Consolidated billing enables you to see a combined view of AWS charges incurred by all accounts in your organization, as well as get a detailed cost report for each individual AWS account associated with your organization. AWS Artifact is a service that provides on-demand access to AWS' security and compliance reports and select online agreements. AWS Budgets is a service that enables you to plan your service usage, service costs, and instance reservations. AWS Trusted Advisor is a service that provides real-time guidance to help you provision your resources following AWS best practices. None of these services or tools offer consolidated billing.

NEW QUESTION 160

- (Topic 2)

Which AWS solution should the company use to meet this requirement?

- A. AWS Config
- B. AWS software development kits (SDKs)
- C. AWS Service Catalog
- D. AWS AppSync

Answer: C

Explanation:

AWS Service Catalog is a service that allows you to create and manage catalogs of IT services that are approved for use on AWS. You can use AWS Service Catalog to centrally manage commonly deployed IT services and help your organization achieve consistent governance and meet your compliance requirements, while enabling users to quickly deploy only the approved IT services they need¹. AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. AWS software development kits (SDKs) are tools that enable you to easily integrate your applications with AWS services using your preferred programming language. AWS AppSync is a service that simplifies application development by letting you create a flexible API to securely access, manipulate, and combine data from one or more data sources. None of these services can help you limit your employees' AWS access to a portfolio of predefined AWS resources.

NEW QUESTION 165

- (Topic 2)

A company is running an application that is hosted on Amazon EC2 instances. The usage of the EC2 instances is higher during daytime hours than nighttime hours. The company wants to optimize the number of EC2 instances based on this usage pattern.

Which AWS service or instance purchasing option should the company use to meet these requirements?

- A. Spot Instances
- B. Reserved Instances
- C. AWS CloudFormation
- D. AWS Auto Scaling

Answer: D

Explanation:

AWS Auto Scaling is the AWS service that allows users to optimize the number of EC2 instances based on the usage pattern, as it automatically adjusts the capacity to maintain steady and predictable performance at the lowest possible cost. Spot Instances are a way to reduce the cost of EC2 instances by bidding on unused EC2 capacity, but they are not suitable for applications that require steady and reliable performance. Reserved Instances are a way to reduce the cost of EC2 instances by committing to a certain amount of usage for a period of time, but they are not flexible to adjust to the usage pattern. AWS CloudFormation is a way to automate the creation and management of AWS resources, but it does not optimize the number of EC2 instances based on the usage pattern. These concepts are explained in the AWS Cloud Practitioner Essentials course³.

NEW QUESTION 166

- (Topic 2)

A developer needs to maintain a development environment infrastructure and a production environment infrastructure in a repeatable fashion.

Which AWS service should the developer use to meet these requirements?

- A. AWS Ground Station
- B. AWS Shield
- C. AWS IoT Device Defender
- D. AWS CloudFormation

Answer: D

Explanation:

AWS CloudFormation is a service that allows you to model and provision your AWS and third-party application resources in a repeatable and predictable way. You can use AWS CloudFormation to create, update, and delete a collection of resources as a single unit, called a stack. You can also use AWS CloudFormation to manage your development and production environments in a consistent and efficient manner⁴.

NEW QUESTION 167

- (Topic 2)

A company suspects that its AWS resources are being used for illegal activities. Which AWS group or team should the company notify?

- A. AWS Abuse team
- B. AWS Support team
- C. AWS technical account managers
- D. AWS Professional Services team

Answer: A

Explanation:

AWS Abuse team is the AWS group or team that the company should notify if it suspects that its AWS resources are being used for illegal activities. AWS Abuse team is a dedicated team that handles reports of abuse, such as spam, phishing, malware, denial-of-service attacks, and unauthorized access, involving AWS resources. The company can contact the AWS Abuse team by filling out the [Report Abuse of AWS Resources form] or sending an email to abuse@amazonaws.com. The company should provide as much information as possible, such as the source and destination IP addresses, timestamps, log files, and screenshots, to help the AWS Abuse team investigate and take appropriate actions. For more information, see [Reporting Abuse] and [AWS Acceptable Use Policy].

NEW QUESTION 169

- (Topic 2)

Which AWS services or tools are designed to protect a workload from SQL injections, cross-site scripting, and DDoS attacks? (Select TWO.)

- A. VPC endpoint
- B. Virtual private gateway
- C. AWS Shield Standard
- D. AWS Config
- E. AWS WAF

Answer: C

Explanation:

AWS Shield Standard and AWS WAF are the AWS services or tools that are designed to protect a workload from SQL injections, cross-site scripting, and DDoS attacks.

According to the AWS Shield Developer Guide, "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."⁵ According to the AWS WAF Developer Guide, "AWS WAF is a web application firewall that helps protect your web applications or APIs against common web exploits that may affect availability, compromise security, or consume excessive resources. AWS WAF gives you control over how traffic reaches your applications by enabling you to create security rules that block common attack patterns, such as SQL injection or cross-site scripting, and rules that filter out specific traffic patterns you define." VPC endpoint, virtual private gateway, and AWS Config are not designed to protect a workload from these types of attacks.

NEW QUESTION 174

- (Topic 1)

A company wants to track its AWS account's service costs. The company also wants to receive notifications when costs are forecasted to reach a specific level. Which AWS service or tool provides this functionality?

- A. AWS Budgets
- B. AWS Cost Explorer
- C. Savings Plans
- D. AWS Billing Conductor

Answer: A

Explanation:

AWS Budgets gives you the ability to set custom budgets that alert you when your costs or usage exceed (or are forecasted to exceed) your budgeted amount. You can also use AWS Budgets to set reservation utilization or coverage targets and receive alerts when your utilization drops below the threshold you define².

NEW QUESTION 179

- (Topic 1)

Which benefit is included with an AWS Enterprise Support plan?

- A. AWS Partner Network (APN) support at no cost
- B. Designated support from an AWS technical account manager (TAM)
- C. On-site support from AWS engineers
- D. AWS managed compliance as code with AWS Config

Answer: B

Explanation:

AWS offers different support plans to meet the needs of different customers. The AWS Enterprise Support plan is the highest level of support that provides

customers with concierge-like service, where the main focus is helping them achieve their outcomes and find success in the cloud. One of the benefits of the AWS Enterprise Support plan is that customers get designated support from an AWS technical account manager (TAM), who provides consultative architectural and operational guidance based on their applications and use cases. Therefore, the correct answer is B. You can learn more about AWS support plans and their benefits from this page.

NEW QUESTION 182

- (Topic 1)

What is a benefit of moving to the AWS Cloud in terms of improving time to market?

- A. Decreased deployment speed
- B. Increased application security
- C. Increased business agility
- D. Increased backup capabilities

Answer: C

Explanation:

Increased business agility is a benefit of moving to the AWS Cloud in terms of improving time to market. Business agility refers to the ability of a company to adapt to changing customer needs, market conditions, and competitive pressures. Moving to the AWS Cloud enables business agility by providing faster access to resources, lower upfront costs, and greater scalability and flexibility. By using the AWS Cloud, companies can launch new products and services, experiment with new ideas, and respond to customer feedback more quickly and efficiently. For more information, see [Benefits of Cloud Computing] and [Business Agility].

NEW QUESTION 185

- (Topic 1)

How can an AWS user conduct security assessments of Amazon EC2 instances, NAT gateways, and Elastic Load Balancers in a way that is approved by AWS?

- A. Flood a target with requests.
- B. Use Amazon Inspector.
- C. Perform penetration testing.
- D. Use the AWS Service Health Dashboard.

Answer: B

Explanation:

Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for exposure, vulnerabilities, and deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity2.

NEW QUESTION 188

- (Topic 1)

A company needs to configure rules to identify threats and protect applications from malicious network access. Which AWS service should the company use to meet these requirements?

- A. AWS Identity and Access Management (IAM)
- B. Amazon QuickSight
- C. AWS WAF
- D. Amazon Detective

Answer: C

Explanation:

AWS WAF is the AWS service that the company should use to configure rules to identify threats and protect applications from malicious network access. AWS WAF is a web application firewall that helps to filter, monitor, and block malicious web requests based on customizable rules. AWS WAF can be integrated with other AWS services, such as Amazon CloudFront, Amazon API Gateway, and Application Load Balancer. For more information, see What is AWS WAF? and How AWS WAF Works.

NEW QUESTION 191

- (Topic 1)

Which AWS service should a cloud engineer use to view API calls to AWS services?

- A. Amazon CloudWatch
- B. AWS CloudTrail
- C. AWS Config
- D. AWS Artifact

Answer: B

Explanation:

The correct answer is B because AWS CloudTrail is an AWS service that a cloud engineer can use to view API calls to AWS services. AWS CloudTrail is a service that enables customers to track user activity and API usage across their AWS account. AWS CloudTrail records the details of every API call made to AWS services, such as the identity of the caller, the time of the call, the source IP address of the caller, the parameters and responses of the call, and more. Customers can use AWS CloudTrail to audit, monitor, and troubleshoot their AWS resources and actions. The other options are incorrect because they are not AWS services that a cloud engineer can use to view API calls to AWS services. Amazon CloudWatch is an AWS service that enables customers to collect, analyze, and visualize metrics, logs, and events from their AWS resources and applications. AWS Config is an AWS service that enables customers to assess, audit, and evaluate the configurations of their AWS resources. AWS Artifact is an AWS service that provides customers with on-demand access to AWS compliance reports and select online agreements. Reference: AWS CloudTrail FAQs

NEW QUESTION 192

- (Topic 1)

Which AWS service or feature is used to Troubleshoot network connectivity issues between Amazon EC2 instances?

- A. AWS Certificate Manager (ACM)
- B. Internet gateway
- C. VPC Flow Logs
- D. AWS CloudHSM

Answer: C

Explanation:

VPC Flow Logs is the AWS service or feature that is used to troubleshoot network connectivity issues between Amazon EC2 instances. VPC Flow Logs is a feature that enables users to capture information about the IP traffic going to and from network interfaces in their VPC. VPC Flow Logs can help users monitor and diagnose network-related issues, such as traffic not reaching an instance, or an instance not responding to requests. VPC Flow Logs can be published to Amazon CloudWatch Logs, Amazon S3, or Amazon Kinesis Data Firehose for analysis and storage.

NEW QUESTION 194

- (Topic 1)

Which AWS service can a company use to perform complex analytical queries?

- A. Amazon RDS
- B. Amazon DynamoDB
- C. Amazon Redshift
- D. Amazon ElastiCache

Answer: C

Explanation:

Amazon Redshift is a fully managed, petabyte-scale data warehouse service in the cloud. You can start with just a few hundred gigabytes of data and scale to a petabyte or more. This enables you to use your data to acquire new insights for your business and customers. Amazon Redshift is designed for complex analytical queries that often involve aggregations and joins across very large tables. Amazon Redshift supports standard SQL and integrates with many existing business intelligence tools¹.

NEW QUESTION 199

- (Topic 1)

A company is developing an application that uses multiple AWS services. The application needs to use temporary, limited-privilege credentials for authentication with other AWS APIs. Which AWS service or feature should the company use to meet these authentication requirements?

- A. Amazon API Gateway
- B. IAM users
- C. AWS Security Token Service (AWS STS)
- D. IAM instance profiles

Answer: C

Explanation:

AWS Security Token Service (AWS STS) is a service that enables applications to request temporary, limited-privilege credentials for authentication with other AWS APIs. AWS STS can be used to grant access to AWS resources to users who are federated (using IAM roles), switched (using IAM users), or cross-account (using IAM roles). AWS STS can also be used to assume a role within the same account or a different account. The credentials issued by AWS STS are short-term and have a limited scope, which can enhance the security and compliance of the application. AWS STS OverviewAWS Certified Cloud Practitioner - aws.amazon.com

NEW QUESTION 200

- (Topic 1)

Which task is the responsibility of AWS, according to the AWS shared responsibility model?

- A. Set up multi-factor authentication (MFA) for each Workspaces user account.
- B. Ensure the environmental safety and security of the AWS infrastructure that hosts Workspaces.
- C. Provide security for Workspaces user accounts through AWS Identity and Access Management (IAM).
- D. Configure AWS CloudTrail to log API calls and user activity.A company stores data in an Amazon S3 bucket
- E. The company must control who has permission to read, write, or delete objects that the company stores in the S3 bucket.

Answer: B

Explanation:

The correct answer is B because ensuring the environmental safety and security of the AWS infrastructure that hosts Workspaces is the responsibility of AWS, according to the AWS shared responsibility model. The AWS shared responsibility model is a framework that defines the division of responsibilities between AWS and the customer for security and compliance. AWS is responsible for the security of the cloud, which includes the global infrastructure, such as the regions, availability zones, and edge locations; the hardware, software, networking, and facilities that run the AWS services; and the virtualization layer that separates the customer instances and storage. The customer is responsible for the security in the cloud, which includes the customer data, the guest operating systems, the applications, the identity and access management, the firewall configuration, and the encryption. The other options are incorrect because they are the responsibility of the customer, according to the AWS shared responsibility model. Setting up multi-factor authentication (MFA) for each Workspaces user account, providing security for Workspaces user accounts through AWS Identity and Access Management (IAM), configuring AWS CloudTrail to log API calls and user activity, and encrypting data at rest and in transit are all tasks that the customer has to perform to secure their Workspaces environment. Reference: AWS Shared Responsibility Model, Amazon WorkSpaces Security

NEW QUESTION 204

- (Topic 1)

Which of the following are user authentication services managed by AWS? (Select TWO.)

- A. Amazon Cognito
- B. AWS Lambda
- C. AWS License Manager
- D. AWS Identity and Access Management (IAM)
- E. AWS CodeStar

Answer: AD

Explanation:

The user authentication services managed by AWS are: Amazon Cognito and AWS Identity and Access Management (IAM). These services help users securely manage and control access to their AWS resources and applications. Amazon Cognito is a service that provides user sign-up, sign-in, and access control for web and mobile applications. Amazon Cognito supports various identity providers, such as Facebook, Google, and Amazon, as well as custom user pools. AWS IAM is a service that enables users to create and manage users, groups, roles, and permissions for AWS services and resources. AWS IAM supports various authentication methods, such as passwords, access keys, and multi-factor authentication (MFA)

NEW QUESTION 208

- (Topic 1)

A company is designing a web application that will run on Amazon EC2 instances.

Which AWS services and features will improve availability and reduce the impact of failures for this application?

(Select TWO.)

- A. Amazon EC2 Auto Scaling for the EC2 instances
- B. VPC subnet ACLs to check the health of a service
- C. Resources that are distributed across multiple Availability Zones
- D. Configuration of AWS Server Migration Service (AWS SMS) to move the EC2 instances to a different AWS Region
- E. Resources that are distributed across multiple AWS points of presence

Answer: AC

Explanation:

The correct answers are A and C because Amazon EC2 Auto Scaling and resources that are distributed across multiple Availability Zones are AWS services and features that will improve availability and reduce the impact of failures for the web application. Amazon EC2 Auto Scaling is a service that enables users to automatically adjust the number of Amazon EC2 instances in response to changes in demand or performance. Amazon EC2 Auto Scaling helps users to maintain optimal availability and performance of their applications by adding or removing instances as needed. Resources that are distributed across multiple Availability Zones are AWS features that enable users to increase the fault tolerance and resilience of their applications. Availability Zones are isolated locations within an AWS Region that have independent power, cooling, and networking. Users can launch their resources, such as Amazon EC2 instances, in multiple Availability Zones to protect their applications from the failure of a single location. The other options are incorrect because they are not AWS services and features that will improve availability and reduce the impact of failures for the web application. VPC subnet ACLs are AWS features that enable users to control the inbound and outbound traffic to and from their subnets within a VPC. VPC subnet ACLs do not check the health of a service, but rather filter the network traffic based on rules. Configuration of AWS Server Migration Service (AWS SMS) is an AWS service that enables users to migrate their on-premises servers to AWS. Configuration of AWS SMS does not help to move the Amazon EC2 instances to a different AWS Region, but rather to migrate the servers from the source environment to AWS. Resources that are distributed across multiple AWS points of presence are AWS features that enable users to deliver content to their end users with low latency and high performance. AWS points of presence are edge locations that are part of the AWS Global Infrastructure. Users can use services such as Amazon CloudFront and AWS Global Accelerator to distribute their content across multiple AWS points of presence. Reference: Amazon EC2 Auto Scaling, [Regions, Availability Zones, and Local Zones]

NEW QUESTION 212

- (Topic 1)

A company moves its infrastructure from on premises to the AWS Cloud. The company can now provision additional Amazon EC2 instances whenever the instances are required. With this ability, the company can launch new marketing campaigns in 3 days instead of 3 weeks.

Which benefit of the AWS Cloud does this scenario demonstrate?

- A. Cost savings
- B. Improved operational resilience
- C. Increased business agility
- D. Enhanced security

Answer: C

Explanation:

Increased business agility is the benefit of the AWS Cloud that this scenario demonstrates. Business agility refers to the ability of a company to adapt to changing customer needs, market conditions, and competitive pressures. Moving to the AWS Cloud enables business agility by providing faster access to resources, lower upfront costs, and greater scalability and flexibility. By using the AWS Cloud, the company can launch new marketing campaigns in 3 days instead of 3 weeks, which shows that it can respond to customer feedback more quickly and efficiently. For more information, see Benefits of Cloud Computing and [Business Agility].

NEW QUESTION 213

- (Topic 1)

Which of the following promotes AWS Cloud architectural best practices for designing and operating reliable, secure, efficient, and cost-effective systems?

- A. AWS Serverless Application Model framework
- B. AWS Business Support
- C. Principle of least privilege
- D. AWS Well-Architected Framework

Answer: D

Explanation:

AWS Well-Architected Framework promotes AWS Cloud architectural best practices for designing and operating reliable, secure, efficient, and cost-effective

systems. AWS Well-Architected Framework is a set of guidelines and best practices that help the user to evaluate and improve the architecture of their applications and workloads on AWS. AWS Well-Architected Framework consists of five pillars: operational excellence, security, reliability, performance efficiency, and cost optimization. Each pillar provides a set of design principles, questions, and best practices that help the user to achieve the desired outcomes for their systems.

NEW QUESTION 218

- (Topic 1)

Which tasks are the responsibility of AWS, according to the AWS shared responsibility model? (Select TWO.)

- A. Patch AWS network devices.
- B. Set user password rules.
- C. Provide physical security for compute resources.
- D. Configure security groups.
- E. Patch the operating system of an Amazon EC2 instance.

Answer: AC

Explanation:

The correct answers are A and C because patching AWS network devices and providing physical security for compute resources are tasks that are the responsibility of AWS, according to the AWS shared responsibility model. The AWS shared responsibility model is a framework that defines the division of responsibilities between AWS and the customer for security and compliance. AWS is responsible for the security of the cloud, which includes the global infrastructure, such as the regions, availability zones, and edge locations; the hardware, software, networking, and facilities that run the AWS services; and the virtualization layer that separates the customer instances and storage. The customer is responsible for the security in the cloud, which includes the customer data, the guest operating systems, the applications, the identity and access management, the firewall configuration, and the encryption. The other options are incorrect because they are tasks that are the responsibility of the customer, according to the AWS shared responsibility model. Setting user password rules, configuring security groups, and patching the operating system of an Amazon EC2 instance are all tasks that the customer has to perform to secure their AWS environment. Reference: AWS Shared Responsibility Model

NEW QUESTION 220

- (Topic 1)

Amazon Elastic File System (Amazon EFS) and Amazon FSx offer which type of storage?

- A. File storage
- B. Object storage
- C. Block storage
- D. Instance store

Answer: A

Explanation:

Amazon Elastic File System (Amazon EFS) and Amazon FSx offer file storage. File storage is a type of storage that organizes data into files and folders, and allows multiple users or applications to access and share the same files over a network. Amazon EFS is a fully managed, scalable, and elastic file system that supports the Network File System (NFS) protocol and can be used with Amazon EC2 instances and AWS Lambda functions. Amazon FSx is a fully managed service that provides two file system options: Amazon FSx for Windows File Server, which supports the Server Message Block (SMB) protocol and is compatible with Microsoft Windows applications; and Amazon FSx for Lustre, which is a high-performance file system that is optimized for compute-intensive workloads

NEW QUESTION 223

- (Topic 1)

A company needs a content delivery network that provides secure delivery of data, videos, applications, and APIs to users globally with low latency and high transfer speeds.

Which AWS service meets these requirements?

- A. Amazon CloudFront
- B. Elastic Load Balancing
- C. Amazon S3
- D. Amazon Elastic Transcoder

Answer: A

Explanation:

The correct answer is A because Amazon CloudFront is an AWS service that provides secure delivery of data, videos, applications, and APIs to users globally with low latency and high transfer speeds. Amazon CloudFront is a fast content delivery network (CDN) that integrates with other AWS services, such as Amazon S3, Amazon EC2, AWS Lambda, and AWS Shield. Amazon CloudFront delivers content through a worldwide network of edge locations that are located close to the end users. The other options are incorrect because they are not AWS services that provide secure delivery of data, videos, applications, and APIs to users globally with low latency and high transfer speeds. Elastic Load Balancing is an AWS service that distributes incoming traffic across multiple targets, such as Amazon EC2 instances, containers, and IP addresses. Amazon S3 is an AWS service that provides object storage for data of any size and type. Amazon Elastic Transcoder is an AWS service that converts media files from their original source format into different formats that will play on various devices. Reference: Amazon CloudFront FAQs

NEW QUESTION 228

- (Topic 3)

A company is migrating its workloads to the AWS Cloud. The company must retain full control of patch management for the guest operating systems that host its applications.

Which AWS service should the company use to meet these requirements?

- A. Amazon DynamoDB
- B. Amazon EC2
- C. AWS Lambda
- D. Amazon RDS

Answer: B

Explanation:

Amazon EC2 is the AWS service that the company should use to meet its requirements of retaining full control of patch management for the guest operating systems that host its applications. Amazon EC2 is a service that provides secure, resizable compute capacity in the cloud. Users can launch virtual servers, called instances, that run various operating systems, such as Linux, Windows, macOS, and more. Users have full administrative access to their instances and can install and configure any software, including patches and updates, on their instances. Users are responsible for managing the security and maintenance of their instances, including patching the guest operating system and applications. Users can also use AWS Systems Manager to automate and simplify the patching process for their EC2 instances. AWS Systems Manager is a service that helps users manage their AWS and on-premises resources at scale. Users can use AWS Systems Manager Patch Manager to scan their instances for missing patches, define patch baselines and maintenance windows, and apply patches automatically or manually across their instances. Users can also use AWS Systems Manager to monitor the patch compliance status and patching history of their instances. References: What is Amazon EC2?, AWS Systems Manager Patch Manager

NEW QUESTION 230

- (Topic 3)

Which AWS services or features can a company use to connect the network of its on- premises data center to AWS? (Select TWO.)

- A. AWS VPN
- B. AWS Directory Service
- C. AWS Data Pipeline
- D. AWS Direct Connect
- E. AWS CloudHSM

Answer: AD

Explanation:

AWS VPN and AWS Direct Connect are two services that enable customers to connect their on-premises data center network to the AWS Cloud. AWS VPN establishes a secure and encrypted connection over the public internet, while AWS Direct Connect establishes a dedicated and private connection through a partner network. You can learn more about AWS VPN from [this webpage] or [this digital course]. You can learn more about AWS Direct Connect from [this webpage] or [this digital course].

NEW QUESTION 232

- (Topic 3)

A company needs to set a maximum spending limit on AWS services each month. The company also needs to set up alerts for when the company reaches its spending limit.

Which AWS service or tool should the company use to meet these requirements?

- A. Cost Explorer
- B. AWS Trusted Advisor
- C. Service Quotas
- D. AWS Budgets

Answer: D

Explanation:

AWS Budgets is a service that helps you plan your service usage, service costs, and instance reservations, and track how close your plan is to your budgeted amount. You can set custom budgets that alert you when you exceed (or are forecasted to exceed) your budgeted thresholds. You can also use AWS Budgets to set a maximum spending limit on AWS services each month and set up alerts for when you reach your spending limit. Cost Explorer is a service that enables you to visualize, understand, and manage your AWS costs and usage over time. You can use Cost Explorer to view charts and graphs that show how your costs are trending, identify areas that need further inquiry, and see the impact of your cost management actions. However, Cost Explorer does not allow you to set a maximum spending limit or alerts for your AWS services. AWS Trusted Advisor is a service that provides you real time guidance to help you provision your resources following AWS best practices, including security and performance. It can help you monitor for cost optimization opportunities, such as unused or underutilized resources, but it does not allow you to set a maximum spending limit or alerts for your AWS services. Service Quotas is a service that enables you to view and manage your quotas, also referred to as limits, from a central location. Quotas, also referred to as limits, are the maximum number of resources that you can create in your AWS account. However, Service Quotas does not allow you to set a maximum spending limit or alerts for your AWS services.

NEW QUESTION 234

- (Topic 3)

A company is planning to host its workloads on AWS.

Which AWS service requires the company to update and patch the guest operating system?

- A. Amazon DynamoDB
- B. Amazon S3
- C. Amazon EC2
- D. Amazon Aurora

Answer: C

Explanation:

Amazon EC2 is an AWS service that provides scalable, secure, and resizable compute capacity in the cloud. Amazon EC2 allows customers to launch and manage virtual servers, called instances, that run a variety of operating systems and applications. Customers have full control over the configuration and management of their instances, including the guest operating system. Therefore, customers are responsible for updating and patching the guest operating system on their EC2 instances, as well as any other software or utilities installed on the instances. AWS provides tools and services, such as AWS Systems Manager and AWS OpsWorks, to help customers automate and simplify the patching process. References: Shared Responsibility Model, Shared responsibility model, [Amazon EC2]

NEW QUESTION 237

- (Topic 3)

A company needs to apply security rules to specific Amazon EC2 instances. Which AWS service or feature provides this functionality?

- A. AWS Shield
- B. Network ACLs
- C. Security groups
- D. AWS Firewall Manager

Answer: C

Explanation:

Security groups act as a firewall for associated Amazon EC2 instances, controlling both inbound and outbound traffic at the instance level. You can use security groups to set rules that allow or deny traffic to or from your instances. You can modify the rules for a security group at any time; the new rules are automatically applied to all instances that are associated with the security group.

NEW QUESTION 241

- (Topic 3)

A company's headquarters is located on a different continent from where the majority of the company's customers live. The company wants an AWS Cloud environment setup that will provide the lowest latency to the customers.

A company wants to automate the creation of new AWS accounts and automatically prevent all users from creating Amazon EC2 instances.

Which AWS service provides this functionality?

- A. AWS Service Catalog
- B. AWS Organizations
- C. EC2 Image Builder
- D. AWS Systems Manager

Answer: B

Explanation:

AWS Organizations is a service that enables you to create and manage multiple AWS accounts centrally. You can use AWS Organizations to automate account creation, apply policies to control access and permissions, and consolidate billing across your accounts. You can also use AWS Organizations to prevent users from creating Amazon EC2 instances in certain regions or with certain configurations²

NEW QUESTION 244

- (Topic 3)

An ecommerce company wants to provide relevant product recommendations to its customers. The recommendations will include products that are frequently purchased with other products that the customer already purchased. The recommendations also will include products of a specific color and products from the customer's favorite brand.

Which AWS service or feature should the company use to meet these requirements with the LEAST development effort?

- A. Amazon Comprehend
- B. Amazon Forecast
- C. Amazon Personalize
- D. Amazon SageMaker Studio

Answer: C

Explanation:

Amazon Personalize is a service that provides real-time personalized recommendations based on the user's behavior, preferences, and context. It can also incorporate metadata such as product color and brand to generate more relevant recommendations. Amazon Comprehend is a natural language processing (NLP) service that can analyze text for entities, sentiments, topics, and more. Amazon Forecast is a service that provides accurate time-series forecasting based on machine learning. Amazon SageMaker Studio is a web-based integrated development environment (IDE) for machine learning.

NEW QUESTION 249

- (Topic 3)

A company is expecting a short-term spike in internet traffic for its application. During the traffic increase, the application cannot be interrupted. The company also needs to minimize cost and maximize flexibility.

A company needs to use a serverless interactive query service to analyze data in Amazon S3. The query service must support standard SQL.

Which AWS service will meet these requirements?

- A. Amazon Redshift
- B. AWS Glue
- C. Amazon Athena
- D. Amazon Kinesis Data Streams

Answer: C

Explanation:

Amazon Athena is a serverless interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL. Athena is ideal for quick, ad-hoc querying but it can also handle complex analysis, including large joins, window functions, and arrays. Athena scales automatically—executing queries in parallel—so results are fast, even with large datasets and complex queries. Amazon Redshift is a fully managed, petabyte-scale data warehouse service that can run complex analytic queries against structured and semi-structured data using standard SQL. However, it is not a serverless service and requires provisioning and managing clusters of nodes. AWS Glue is a fully managed extract, transform, and load (ETL) service that makes it easy to prepare and load your data for analytics. However, it is not a query service and does not support standard SQL. Amazon Kinesis Data Streams is a service that enables you to build custom applications that process or analyze streaming data for specialized needs. However, it is not a query service and does not support standard SQL.

NEW QUESTION 250

- (Topic 3)

Which AWS service offers object storage?

- A. Amazon RDS

- B. Amazon Elastic File System (Amazon EFS)
- C. Amazon S3
- D. Amazon DynamoDB

Answer: C

Explanation:

Amazon S3 is the AWS service that offers object storage. Object storage is a technology that stores and manages data in an unstructured format called objects. Each object consists of the data, metadata, and a unique identifier. Object storage is ideal for storing large amounts of unstructured data, such as photos, videos, email, web pages, sensor data, and audio files¹. Amazon S3 provides industry-leading scalability, data availability, security, and performance for object storage². Amazon RDS is the AWS service that offers relational database storage. Relational database storage is a technology that stores and manages data in a structured format called tables. Each table consists of rows and columns that define the attributes and values of the data. Relational database storage is ideal for storing structured or semi-structured data, such as customer records, inventory, transactions, and analytics³. Amazon Elastic File System (Amazon EFS) is the AWS service that offers file storage. File storage is a technology that stores and manages data in a hierarchical format called files and folders. Each file consists of the data and metadata, and each folder consists of files or subfolders. File storage is ideal for storing shared data that can be accessed by multiple users or applications, such as home directories, content repositories, media libraries, and configuration files⁴. Amazon DynamoDB is the AWS service that offers NoSQL database storage. NoSQL database storage is a technology that stores and manages data in a flexible format called documents or key-value pairs. Each document or key-value pair consists of the data and metadata, and can have different attributes and values depending on the schema. NoSQL database storage is ideal for storing dynamic or unstructured data that requires high performance, scalability, and availability, such as web applications, social media, gaming, and IoT.

NEW QUESTION 251

- (Topic 3)

A company wants to establish a private network connection between AWS and its corporate network. Which AWS service or feature will meet this requirement?

- A. Amazon Connect
- B. Amazon Route 53
- C. AWS Direct Connect
- D. VPC peering

Answer: C

Explanation:

AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect, you can establish private connectivity between AWS and your datacenter, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than internet-based connections¹². References: 1: Dedicated Network Connection - AWS Direct Connect - AWS, 2: What is AWS Direct Connect? - AWS Direct Connect

NEW QUESTION 255

- (Topic 3)

How does the AWS Enterprise Support Concierge team help users?

- A. Supporting application development
- B. Providing architecture guidance
- C. Answering billing and account inquiries
- D. Answering questions regarding technical support cases

Answer: C

Explanation:

The AWS Enterprise Support Concierge team is a group of billing and account experts who specialize in working with enterprise customers. They can help customers with questions about billing, account management, cost optimization, and other non-technical issues. They can also assist customers with navigating and optimizing their AWS environment, such as setting up consolidated billing, applying for service limit increases, or requesting refunds. References:

? AWS Support Plan Comparison

? AWS Enterprise Support Plan

? Answer Explained: Which AWS Support plan provides access to AWS Concierge Support team for account assistance?

NEW QUESTION 257

- (Topic 3)

A company wants to migrate its PostgreSQL database to AWS. The company does not use the database frequently. Which AWS service or resource will meet these requirements with the LEAST management overhead?

- A. PostgreSQL on Amazon EC2
- B. Amazon RDS for PostgreSQL
- C. Amazon Aurora PostgreSQL-Compatible Edition
- D. Amazon Aurora Serverless

Answer: D

Explanation:

Amazon Aurora Serverless is an on-demand, auto-scaling configuration for Amazon Aurora PostgreSQL-Compatible Edition. It is a fully managed service that automatically scales up and down based on the application's actual needs. Amazon Aurora Serverless is suitable for applications that have infrequent, intermittent, or unpredictable database workloads, and that do not require the full power and range of options provided by provisioned Aurora clusters. Amazon Aurora Serverless eliminates the need to provision and manage database instances, and reduces the management overhead associated with database administration tasks such as scaling, patching, backup, and recovery. References: Amazon Aurora Serverless, Choosing between Aurora Serverless and provisioned Aurora DB clusters, [AWS Cloud Practitioner Essentials: Module 4 - Databases in the Cloud]

NEW QUESTION 260

- (Topic 3)

Which mechanism allows developers to access AWS services from application code?

- A. AWS Software Development Kit
- B. AWS Management Console
- C. AWS CodePipeline
- D. AWS Config

Answer: A

Explanation:

AWS Software Development Kit (SDK) is a set of platform-specific building tools for developers. It allows developers to access AWS services from application code using familiar programming languages. It provides pre-built components and libraries that can be incorporated into applications, as well as tools to debug, monitor, and optimize performance². References: What is SDK? - SDK Explained - AWS

NEW QUESTION 263

- (Topic 3)

A company wants to migrate its server-based applications to the AWS Cloud. The company wants to determine the total cost of ownership for its compute resources that will be hosted on the AWS Cloud.

Which combination of AWS services or tools will meet these requirements?

- A. AWS Pricing Calculator
- B. Migration Evaluator
- C. AWS Support Center
- D. AWS Application Discovery Service
- E. AWS Database Migration Service (AWS DMS)

Answer: AD

Explanation:

AWS Pricing Calculator and AWS Application Discovery Service are the best combination of AWS services or tools to meet the requirements of determining the total cost of ownership for compute resources that will be hosted on the AWS Cloud. AWS Pricing Calculator is a tool that enables you to estimate the cost of using AWS services based on your usage scenarios and requirements. You can use AWS Pricing Calculator to compare the costs of running your applications on-premises or on AWS, and to optimize your AWS spending. AWS Application Discovery Service is a service that helps you plan your migration to the AWS Cloud by collecting and analyzing information about your on-premises servers, applications, and dependencies. You can use AWS Application Discovery Service to identify the inventory of your on-premises infrastructure, group servers by applications, and estimate the performance and resource utilization of your applications⁴⁵

NEW QUESTION 264

- (Topic 3)

A company wants to use the latest technologies and wants to minimize its capital investment. Instead of upgrading on-premises infrastructure, the company wants to move to the AWS Cloud.

Which AWS Cloud benefit does this scenario describe?

- A. Increased speed to market
- B. The trade of infrastructure expenses for operating expenses
- C. Massive economies of scale
- D. The ability to go global in minutes

Answer: B

Explanation:

The trade of infrastructure expenses for operating expenses is one of the benefits of the AWS Cloud. By moving to the AWS Cloud, the company can avoid the upfront costs of purchasing and maintaining on-premises infrastructure, such as servers, storage, network, and software. Instead, the company can pay only for the AWS resources and services that they use, as they use them. This reduces the risk and complexity of planning and managing IT infrastructure, and allows the company to focus on innovation and growth. Increased speed to market, massive economies of scale, and the ability to go global in minutes are also benefits of the AWS Cloud, but they are not the best ones to describe this scenario. Increased speed to market means that the company can launch new products and services faster by using AWS services and tools. Massive economies of scale means that the company can benefit from the lower costs and higher performance that AWS achieves by operating at a large scale. The ability to go global in minutes means that the company can deploy their applications and data in multiple regions and availability zones around the world to reach their customers faster and improve performance and reliability⁵

NEW QUESTION 268

- (Topic 3)

A company has deployed an Amazon EC2 instance.

Which option is an AWS responsibility under the AWS shared responsibility model?

- A. Managing and encrypting application data
- B. Installing updates and security patches of guest operating system
- C. Configuration of infrastructure devices
- D. Configuration of security groups on each instance

Answer: C

Explanation:

According to the AWS shared responsibility model, AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud, such as data centers, hardware, software, networking, and facilities¹. This includes the configuration of infrastructure devices, such as routers, switches, firewalls, and load balancers². Customers are responsible for managing their data, applications, operating systems, security groups, and other aspects of their AWS environment¹. Therefore, options A, B, and D are customer responsibilities, not AWS responsibilities. References: 1: AWS Well-Architected Framework - Elasticity; 2: Reactive Systems on AWS - Elastic

NEW QUESTION 269

- (Topic 3)

Which type of AWS storage is ephemeral and is deleted when an Amazon EC2 instance is stopped or terminated?

- A. Amazon Elastic Block Store (Amazon EBS)
- B. Amazon EC2 instance store
- C. Amazon Elastic File System (Amazon EFS)
- D. Amazon S3

Answer: B

Explanation:

Amazon EC2 instance store provides temporary block-level storage for your EC2 instance. This storage is located on disks that are physically attached to the host computer. Instance store is ideal for temporary storage of information that changes frequently, such as buffers, caches, scratch data, and other temporary content. It can also be used to store temporary data that you replicate 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 and instance size. 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 or more instance store volumes have ephemeral0, ephemeral1, and so on. Instance store pricing Instance store volumes are included as part of the instance's usage cost. The data on an instance store volume persists even if the instance is rebooted. However, the data does not persist if the instance is stopped, hibernated, or terminated. When the instance is stopped, hibernated, or terminated, every block of the instance store volume is cryptographically erased. Therefore, do not rely on instance store volumes for valuable, long-term data. If you need to retain the data stored on an instance store volume beyond the lifetime of the instance, you need to manually copy that data to more persistent storage, such as an Amazon EBS volume, an Amazon S3 bucket, or an Amazon EFS file system. There are some events that can result in your data not persisting throughout the lifetime of the instance. The following table indicates whether data on instance store volumes is persisted during specific events, for both virtualized and bare metal instances¹. References: Amazon EC2 instance store - Amazon Elastic Compute Cloud

NEW QUESTION 274

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual AWS-Certified-Cloud-Practitioner Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the AWS-Certified-Cloud-Practitioner Product From:

<https://www.2passeasy.com/dumps/AWS-Certified-Cloud-Practitioner/>

Money Back Guarantee

AWS-Certified-Cloud-Practitioner Practice Exam Features:

- * AWS-Certified-Cloud-Practitioner Questions and Answers Updated Frequently
- * AWS-Certified-Cloud-Practitioner Practice Questions Verified by Expert Senior Certified Staff
- * AWS-Certified-Cloud-Practitioner Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * AWS-Certified-Cloud-Practitioner Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year