Free Questions for CLF-C02 by certsinside

Shared by Rivers on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which AWS service or tool can be used to set up a firewall to control traffic going into and coming out of an Amazon VPC subnet?

Options:

A- Security group

B- AWS WAF

C- AWS Firewall Manager

D- Network ACL

Answer:

D

Explanation:

A network ACL (NACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You can create a network ACL and associate it with a subnet to apply rules that allow or deny traffic to or from the subnet.

Network ACLs are stateless, meaning that they evaluate the source and destination IP addresses for both inbound and outbound traffic.You can also use network ACLs to block IP address ranges that are known to be malicious12.

The other options are not AWS services or tools that can be used to set up a firewall to control traffic going into and coming out of an Amazon VPC subnet. Security groups are another layer of security for your VPC that act as a firewall for your EC2 instances. Security groups are stateful, meaning that they automatically allow return traffic for allowed inbound traffic.Security groups can only filter traffic based on protocols, ports, and source or destination IP addresses, not on IP ranges3. AWS WAF is a web application firewall that helps protect your web applications from common web exploits. AWS WAF can filter web requests based on rules that you define, such as IP addresses, HTTP headers, HTTP body, or URI strings.AWS WAF does not apply to non-web traffic or to traffic within a VPC4. AWS Firewall Manager is a service that helps you centrally configure and manage firewall rules across your accounts and resources in AWS Organizations. You can use Firewall Manager to apply AWS WAF rules, AWS Network Firewall policies, and Amazon VPC security groups across your AWS accounts. AWS Firewall Manager does not provide a firewall service itself, but rather helps you manage other firewall services

Question 2

Question Type: **MultipleChoice**

A company has deployed applications on Amazon EC2 instances. The company needs to assess application vulnerabilities and must identify infrastructure deployments that do not meet best practices. Which AWS service can the company use to meet these requirements?

Options:

A- AWS Trusted Advisor

B- Amazon Inspector

C- AWSConfig

D- Amazon GuardDuty

Answer:

B

Explanation:

Amazon Inspector is a service that provides automated security assessment and management for AWS resources, such as Amazon EC2 instances. Amazon Inspector can scan applications for common vulnerabilities, such as SQL injection, cross-site scripting, and remote code execution. Amazon Inspector can also check the configuration of AWS resources against security best practices, such as the CIS Benchmarks and the AWS Security Best Practices.Amazon Inspector can help customers identify and remediate security issues, comply with security standards, and improve the security posture of their AWS environment12.Reference:

Amazon Inspector

Improved, Automated Vulnerability Management for Cloud Workloads with a New Amazon Inspector | AWS News Blog

Question 3

Question Type: MultipleChoice

Which AWS service or tool gives users the ability to connect with AWS and deploy resources programmatically?

Options:

A- Amazon quickSight

B- AWS PrivateLink

C- AWS Direct Connect

D- AWS SDKs

Answer:

D

Explanation:

AWS SDKs are a set of tools that allow users to connect with AWS and deploy resources programmatically. AWS SDKs provide libraries, code samples, documentation, and other resources to help users write code that interacts with AWS APIs. AWS SDKs support

various programming languages, such as Java, Python, Ruby, .NET, Node.js, Go, and more. AWS SDKs make it easier for users to access AWS services, such as Amazon S3, Amazon EC2, Amazon DynamoDB, AWS Lambda, and more, from their applications. AWS SDKs also handle tasks such as authentication, error handling, retries, and data serialization, so users can focus on their application logic .

The other options are not AWS services or tools that give users the ability to connect with AWS and deploy resources programmatically.Amazon QuickSight is a business intelligence service that lets users create and share interactive dashboards and visualizations1.AWS PrivateLink is a service that enables users to securely access services hosted on AWS in a scalable and cost-effective manner2.AWS Direct Connect is a service that establishes a dedicated network connection between a user's premises and AWS3.

Question 4

Question Type: **MultipleChoice**

A company needs to track the activity in its AWS accounts, and needs to know when an API call is made against its AWS resources. Which AWS tool or service can be used to meet these requirements?

Options:

A- Amazon CloudWatch

B- Amazon Inspector

C- AWS CloudTrail

D- AWS IAM

Answer:

C

Explanation:

AWS CloudTrail is the service that can be used to meet these requirements. AWS CloudTrail is a service that records AWS API calls for your account and delivers log files to you.The recorded information includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the AWS service1. You can use CloudTrail to track the activity in your AWS accounts, such as who made an API call, when it was made, and what resources were affected.You can also use CloudTrail to monitor the compliance, security, and governance of your AWS environment2. The other services are not designed to track the activity and API calls in your AWS accounts. Amazon CloudWatch is a service that monitors and collects metrics, logs, and events from your AWS resources and applications.You can use CloudWatch to set alarms, visualize data, and automate actions based on predefined thresholds or rules3. Amazon Inspector is a service that helps you improve the security and compliance of your applications running on AWS.Inspector automatically assesses applications for exposure, vulnerabilities, and deviations from best practices4. AWS IAM is a service that enables you to manage access to AWS services and resources securely. IAM allows you to create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources.Reference:AWS CloudTrail,AWS CloudTrail -- Capture AWS API Activity,Amazon CloudWatch,Amazon Inspector, [AWS IAM]

Question 5

Question Type: MultipleChoice

A user wants to allow applications running on an Amazon EC2 instance to make calls to other AWS services. The access granted must be secure. Which AWS service or feature should be used?

Options:

A- Security groups

B- AWS Firewall Manager

C- IAM roles

D- IAM user SSH keys

Answer:

C

Explanation:

IAM roles are a secure way to grant permissions to applications running on an Amazon EC2 instance to make calls to other AWS services. IAM roles are entities that have specific permissions policies attached to them. You can create an IAM role and associate it with an EC2 instance when you launch it or later. The applications on the instance can then use the temporary credentials provided by the role to access AWS resources that the role allows.This way, you do not have to store any long-term credentials or access keys on the instance, which reduces the risk of compromise or misuse12.

The other options are not correct, because:

Security groups are virtual firewalls that control the inbound and outbound traffic for your EC2 instances.Security groups do not grant permissions to access other AWS services, but rather filter the network traffic based on rules that you define3.

AWS Firewall Manager is a service that helps you centrally configure and manage firewall rules across your accounts and resources. AWS Firewall Manager works with AWS WAF, AWS Shield Advanced, and Amazon VPC security groups.AWS Firewall Manager does not grant permissions to access other AWS services, but rather helps you enforce consistent security policies across your AWS infrastructure4.

IAM user SSH keys are credentials that allow you to connect to your EC2 instance using SSH.SSH keys do not grant permissions to access other AWS services, but rather authenticate your identity when you log in to your instance5.

Using an IAM role to grant permissions to applications running on Amazon EC2 instances - AWS Identity and Access Management

IAM roles for Amazon EC2 - Amazon Elastic Compute Cloud

Security groups for your VPC - Amazon Virtual Private Cloud

What is AWS Firewall Manager? - AWS Firewall Manager

Connecting to your Linux instance using SSH - Amazon Elastic Compute Cloud

Question 6

Question Type: MultipleChoice

A company is migrating to the AWS Cloud and plans to run experimental workloads for 3 to 6 months on AWS. Which pricing model will meet these requirements?

Options:

A- Use Savings Plans for a 3-year term.

B- Use Dedicated Hosts.

C- Buy Reserved Instances.

D- Use On-Demand Instances.

Answer:

D

Explanation:

On-Demand Instances are the most flexible and cost-effective pricing model for short-term, experimental, or unpredictable workloads on AWS. On-Demand Instances let you pay only for the resources you use, without any long-term commitments or upfront fees. You can easily start and stop instances as needed, and scale up or down depending on your demand.

Savings Plans, Reserved Instances, and Dedicated Hosts are all pricing models that require a commitment for a certain amount of usage or capacity for a one- or three-year term. These pricing models offer lower prices than On-Demand Instances, but they are not suitable for workloads that only run for 3 to 6 months or have variable usage patterns. Savings Plans and Reserved Instances also offer flexibility to change instance types, sizes, or regions within the same family or pool, while Dedicated Hosts are physical servers that can only run specific instance types.

Question 7

Question Type: MultipleChoice

A systems administrator created a new 1AM user for a developer and assigned the user an access key instead of a user name and password. What is the access key used for?

Options:

A- To access the AWS account as the AWS account root user

B- To access the AWS account through the AWS Management Console

C- To access the AWS account through a CLI

D- To access all of a company's AWS accounts

Answer:

C

Explanation:

An access key is a pair of long-term credentials that consists of an access key ID and a secret access key. An access key is used to sign programmatic requests to the AWS CLI or AWS API (directly or using the AWS SDK).An access key allows a user to access the AWS account through a CLI, which is a tool that enables users to interact with AWS services using commands in a terminal or a script12.

The other options are not correct, because:

To access the AWS account as the AWS account root user, a user needs the email address and password associated with the account. The root user has complete access to all AWS resources and services in the account.However, it is not recommended to use the root user for everyday tasks3.

To access the AWS account through the AWS Management Console, a user needs a user name and password.The console is a web-based interface that allows users to manage their AWS resources and services using a graphical user interface4.

To access all of a company's AWS accounts, a user needs to use AWS Organizations, which is a service that enables users to centrally manage and govern multiple AWS accounts.AWS Organizations allows users to create groups of accounts and apply policies to them5.

Managing access keys for IAM users - AWS Identity and Access Management

What Is the AWS Command Line Interface? - AWS Command Line Interface

AWS account root user - AWS Identity and Access Management

What Is the AWS Management Console? - AWS Management Console

What Is AWS Organizations? - AWS Organizations

Question 8

Question Type: **MultipleChoice**

A network engineer needs to build a hybrid cloud architecture connecting on-premises networks to the AWS Cloud using AWS Direct Connect. The company has a few VPCs in a single AWS Region and expects to increase the number of VPCs to hundreds over time.

Which AWS service or feature should the engineer use to simplify and scale this connectivity as the VPCs increase in number?

Options:

A- VPC endpoints

B- AWS Transit Gateway

C- Amazon Route 53

D- AWS Secrets Manager

Answer:

B

Explanation:

AWS Transit Gateway is a network transit hub that you can use to interconnect your VPCs and on-premises networks through a central gateway. AWS Transit Gateway simplifies and scales the connectivity between your on-premises networks and AWS, as you only need to create and manage a single connection from the central gateway to each on-premises network, rather than individual connections to each VPC.You can also use AWS Transit Gateway to connect to other AWS services, such as Amazon S3, Amazon DynamoDB, and AWS PrivateLink12.AWS Transit Gateway supports thousands of VPCs per gateway, and enables you to peer Transit Gateways across AWS Regions3.

The other options are not AWS services or features that can simplify and scale the connectivity between on-premises networks and hundreds of VPCs using AWS Direct Connect.VPC endpoints enable private connectivity between your VPCs and supported AWS services, but do not support on-premises networks4.Amazon Route 53 is a DNS service that helps you route internet traffic to your resources, but does not provide network connectivity5.AWS Secrets Manager is a service that helps you securely store and manage

secrets, such as database credentials and API keys, but does not relate to network connectivity

Question 9

Question Type: MultipleChoice

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

Options:

A- Maintain the security of the AWS Cloud.

B- Configure firewalls and networks.

C- Patch the operating system of Amazon RDS instances.

D- Implement physical and environmental controls.

Answer:

B

Explanation:

According to the AWS shared responsibility model, the customer is responsible for the security in the cloud, which includes configuring firewalls and networks. AWS provides security groups and network access control lists (NACLs) as firewall features that customers can use to control the traffic to and from their AWS resources. Customers are also responsible for managing their own virtual private clouds (VPCs), subnets, route tables, internet gateways, and other network components.AWS is responsible for the security of the cloud, which includes the physical security of the facilities, the host operating system and virtualization layer, and the AWS global network infrastructure12.Reference:

Shared Responsibility Model - Amazon Web Services (AWS)

Shared responsibility model - Amazon Web Services: Risk and Compliance

Question 10

Question Type: MultipleChoice

Which AWS services or features provide disaster recovery solutions for Amazon EC2 instances? (Select TWO.)

Options:

A- EC2 Reserved Instances

B- EC2 Amazon Machine Images (AMIs)

C- Amazon Elastic Block Store (Amazon EBS) snapshots

D- AWS Shield

E- Amazon GuardDuty

Answer:

B, C

Explanation:

The correct answer isBandC. EC2 Amazon Machine Images (AMIs) and Amazon Elastic Block Store (Amazon EBS) snapshots are two AWS services that provide disaster recovery solutions for Amazon EC2 instances.

EC2 AMIsare preconfigured templates that contain the software configuration and data required to launch an EC2 instance. You can create AMIs from your running EC2 instances and use them to launch new instances in the same or different AWS Regions.This way, you can quickly recover your EC2 instances in case of a disaster that affects your primary Region or Availability Zone1.

Amazon EBS snapshotsare incremental backups of your Amazon EBS volumes. You can create snapshots of your volumes and store them in Amazon S3, which is a highly durable and scalable storage service. You can use snapshots to restore your volumes to a previous point in time or to create new volumes from snapshots.Snapshots can also be copied across AWS Regions, enabling you to recover your data in another Region in case of a disaster2.

The other options are not directly related to disaster recovery for EC2 instances:

EC2 Reserved Instancesare a pricing model that allows you to reserve EC2 capacity for a specific period of time and receive a discount on the hourly charge.Reserved Instances do not provide any disaster recovery benefits, as they are only a billing option3.

AWS Shieldis a managed service that protects your AWS resources from distributed denial-of-service (DDoS) attacks. AWS Shield provides basic protection for all AWS customers at no additional charge, and advanced protection for customers who need higher levels of detection and mitigation.AWS Shield does not provide any disaster recovery benefits, as it is only a security service4.

Amazon GuardDutyis a threat detection service that monitors your AWS account and workloads for malicious or unauthorized activity. Amazon GuardDuty analyzes various data sources, such as AWS CloudTrail, Amazon VPC Flow Logs, and DNS logs, to identify potential threats and alert you via Amazon CloudWatch Events or AWS Lambda.Amazon GuardDuty does not provide any disaster recovery benefits, as it is only a monitoring service5.

Question 11

Question Type: MultipleChoice

A social media company wants to protect its web application from common web exploits such as SQL injections and cross-site scripting. Which AWS service will meet these requirements?

Options:

A- Amazon Inspector

B- AWS WAF

C- Amazon GuardDuty

D- Amazon CloudWatch

Answer:

B

Explanation:

AWS WAF is a web application firewall service that helps protect web applications from common web exploits that could affect availability, compromise security, or consume excessive resources. AWS WAF gives you control over which traffic to allow or block to your web applications by defining customizable web security rules.You can use AWS WAF to create rules that block common attack patterns, such as SQL injection or cross-site scripting, and rules that filter out specific traffic patterns you define1.AWS WAF also integrates with other AWS services, such as Amazon CloudFront, Amazon API Gateway, AWS AppSync, and AWS Load Balancer, to provide a comprehensive defense against web attacks2. Therefore, AWS WAF meets the requirements of the social media company, compared to the other options.

The other options are not suitable for the social media company's requirements, because:

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.However, Amazon Inspector does not provide a web application firewall service that can block malicious web requests3.

Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts, workloads, and data stored in Amazon S3. Amazon GuardDuty analyzes and processes the following data sources: VPC Flow Logs, AWS CloudTrail event logs, and DNS logs.However, Amazon GuardDuty does not provide a web application firewall service that can block malicious web requests4.

Amazon CloudWatch is a monitoring and observability service that provides data and actionable insights to monitor your applications, respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health. Amazon CloudWatch collects monitoring and operational data in the form of logs, metrics, and events, and visualizes it using automated dashboards, alarms, and notifications. However, Amazon CloudWatch does not provide a web application firewall service that can block malicious web requests.

What Is AWS WAF? - AWS WAF, AWS Firewall Manager, and AWS Shield Advanced

AWS WAF Features - AWS WAF, AWS Firewall Manager, and AWS Shield Advanced

What Is Amazon Inspector? - Amazon Inspector

What Is Amazon GuardDuty? - Amazon GuardDuty

[What Is Amazon CloudWatch? - Amazon CloudWatch]

Question 12

Question Type: MultipleChoice

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?

Options:

A- AWS Ground Station

B- AWS Shield

C- AWS loT Device Defender

D- AWS CloudFormation

Answer:

D

Explanation:

AWS CloudFormation is a service that allows developers to model and provision their AWS infrastructure in a repeatable and declarative way, using code and templates. AWS CloudFormation enables developers to define the resources they need for their development and

production environments, such as compute, storage, network, and application services, and automate their creation and configuration.AWS CloudFormation also provides features such as change sets, nested stacks, and rollback triggers to help developers manage and update their infrastructure safely and efficiently12.Reference:

AWS CloudFormation

What is AWS CloudFormation?