

Exam Questions AWS-Certified-Security-Specialty

Amazon AWS Certified Security - Specialty

<https://www.2passeasy.com/dumps/AWS-Certified-Security-Specialty/>



NEW QUESTION 1

A company hosts a popular web application that connects to an Amazon RDS MySQL DB instance running in a private VPC subnet that was created with default ACL settings. The IT Security department has a suspicion that a DDos attack is coming from a suspecting IP. How can you protect the subnets from this attack? Please select:

- A. Change the Inbound Security Groups to deny access from the suspecting IP
- B. Change the Outbound Security Groups to deny access from the suspecting IP
- C. Change the Inbound NACL to deny access from the suspecting IP
- D. Change the Outbound NACL to deny access from the suspecting IP

Answer: C

Explanation:

Option A and B are invalid because by default the Security Groups already block traffic. You can use NACL's as an additional security layer for the subnet to deny traffic.

Option D is invalid since just changing the Inbound Rules is sufficient The AWS Documentation mentions the following

A network access control list (ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC.

The correct answer is: Change the Inbound NACL to deny access from the suspecting IP

NEW QUESTION 2

You are hosting a web site via website hosting on an S3 bucket - <http://demo.s3-website-us-east-1.amazonaws.com>. You have some web pages that use Javascript that access resources in another bucket which has web site hosting also enabled. But when users access the web pages , they are getting a blocked Javascript error. How can you rectify this? Please select:

- A. Enable CORS for the bucket
- B. Enable versioning for the bucket
- C. Enable MFA for the bucket
- D. Enable CRR for the bucket

Answer: A

Explanation:

Your answer is incorrect Answer-A

Such a scenario is also given in the AWS Documentation Cross-Origin Resource Sharing:

Use-case Scenarios

The following are example scenarios for using CORS:

- Scenario 1: Suppose that you are hosting a website in an Amazon S3 bucket named website as described in Hosting a Static Website on Amazon S3. Your users load the website endpoint <http://website.s3-website-us-east-1.amazonaws.com>. Now you want to use JavaScript on the webpages that are stored in this bucket to be able to make authenticated GET and PUT requests against the same bucket by using the Amazon S3 API endpoint for the bucket website.s3.amazonaws.com. A browser would normally block JavaScript from allowing those requests, but with CORS you can configure your bucket to explicitly enable cross-origin requests from website.s3-website-us-east-1.amazonaws.com.
- Scenario 2: Suppose that you want to host a web font from your S3 bucket. Again, browsers require a CORS check (also called a preflight check) for loading web fonts. You would configure the bucket that is hosting the web font to allow any origin to make these requests.

Option B is invalid because versioning is only to create multiple versions of an object and can help in accidental deletion of objects

Option C is invalid because this is used as an extra measure of caution for deletion of objects Option D is invalid because this is used for Cross region replication of objects

For more information on Cross Origin Resource sharing, please visit the following URL

- <https://docs.aws.amazon.com/AmazonS3/latest/dev/cors.html>

The correct answer is: Enable CORS for the bucket

Submit your Feedback/Queries to our Experts

NEW QUESTION 3

Your company has a requirement to monitor all root user activity by notification. How can this best be achieved? Choose 2 answers from the options given below. Each answer forms part of the solution Please select:

- A. Create a Cloudwatch Events Rule s
- B. Create a Cloudwatch Logs Rule
- C. Use a Lambda function
- D. Use Cloudtrail API call

Answer: AC

Explanation:

Below is a snippet from the AWS blogs on a solution

Option B is invalid because you need to create a Cloudwatch Events Rule and there is such thing as a Cloudwatch Logs Rule Option D is invalid because Cloud Trail API calls can be recorded but cannot be used to send across notifications For more information on this blog article, please visit the following URL:

<https://aws.amazon.com/blogs/mt/monitor-and-notify-on-aws-account-root-user-activity>

The correct answers are: Create a Cloudwatch Events Rule, Use a Lambda function Submit your Feedback/Queries to our Experts

NEW QUESTION 4

A company is hosting a website that must be accessible to users for HTTPS traffic. Also port 22 should be open for administrative purposes. The administrator's workstation has a static IP address of 203.0.113.1/32. Which of the following security group configurations are the MOST secure but still functional to support these requirements? Choose 2 answers from the options given below

Please select:

- A. Port 443 coming from 0.0.0.0/0
- B. Port 443 coming from 10.0.0.0/16
- C. Port 22 coming from 0.0.0.0/0
- D. Port 22 coming from 203.0.113.1/32

Answer: AD

Explanation:

Since HTTPS traffic is required for all users on the Internet, Port 443 should be open on all IP addresses. For port 22, the traffic should be restricted to an internal subnet.

Option B is invalid, because this only allow traffic from a particular CIDR block and not from the internet

Option C is invalid because allowing port 22 from the internet is a security risk For more information on AWS Security Groups, please visit the following UR

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/usins-network-security.html>

The correct answers are: Port 443 coming from 0.0.0.0/0, Port 22 coming from 203.0.113.1 /32 Submit your Feedback/Queries to our Experts

NEW QUESTION 5

Your company has an EC2 Instance that is hosted in an AWS VPC. There is a requirement to ensure that logs files from the EC2 Instance are stored accordingly. The access should also be limited for the destination of the log files. How can this be accomplished? Choose 2 answers from the options given below. Each answer forms part of the solution

Please select:

- A. Stream the log files to a separate Cloudtrail trail
- B. Stream the log files to a separate Cloudwatch Log group
- C. Create an IAM policy that gives the desired level of access to the Cloudtrail trail
- D. Create an IAM policy that gives the desired level of access to the Cloudwatch Log group

Answer: BD

Explanation:

You can create a Log group and send all logs from the EC2 Instance to that group. You can then limit the access to the Log groups via an IAM policy.

Option A is invalid because Cloudtrail is used to record API activity and not for storing log files Option C is invalid because Cloudtrail is the wrong service to be used for this requirement

For more information on Log Groups and Log Streams, please visit the following URL:

* <https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/Working>

For more information on Access to Cloudwatch logs, please visit the following URL:

* <https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/auth-and-access-control-cwl.html> The correct answers are: Stream the log files to a separate

Cloudwatch Log group. Create an IAM policy that gives the desired level of access to the Cloudwatch Log group

Submit your Feedback/Queries to our Experts

NEW QUESTION 6

You have a web site that is sitting behind AWS Cloudfront. You need to protect the web site against threats such as SQL injection and Cross site scripting attacks.

Which of the following service can help in such a scenario

Please select:

- A. AWS Trusted Advisor
- B. AWS WAF
- C. AWS Inspector
- D. AWS Config

Answer: B

Explanation:

The AWS Documentation mentions the following

AWS WAF is a web application firewall that helps detect and block malicious web requests targeted at your web applications. AWS WAF allows you to create rules that can help protect against common

web exploits like SQL injection and cross-site scripting. With AWS WAF you first identify the resource (either an Amazon CloudFront distribution or an Application Load Balancer) that you need to protect. Option A is invalid because this will only give advise on how you can better the security in your AWS account but not protect against threats mentioned in the question.

Option C is invalid because this can be used to scan EC2 Instances for vulnerabilities but not protect against threats mentioned in the question.

Option D is invalid because this can be used to check config changes but not protect against threats mentioned in the quest

For more information on AWS WAF, please visit the following URL: <https://aws.amazon.com/waf/details>;

The correct answer is: AWS WAF

Submit your Feedback/Queries to our Experts

NEW QUESTION 7

When you enable automatic key rotation for an existing CMK key where the backing key is managed by AWS, after how long is the key rotated?

Please select:

- A. After 30 days
- B. After 128 days
- C. After 365 days
- D. After 3 years

Answer: D

Explanation:

The AWS Documentation states the following

- AWS managed CM Ks: You cannot manage key rotation for AWS managed CMKs. AWS KMS automatically rotates AWS managed keys every three years (1095 days).

Note: AWS-managed CMKs are rotated every 3yrs, Customer-Managed CMKs are rotated every 365- days from when rotation is enabled.

Option A, B, C are invalid because the settings for automatic key rotation is not changeable. For more information on key rotation please visit the below URL <https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html>

AWS managed CMKs are CMKs in your account that are created, managed, and used on your behalf by an AWS service that is integrated with AWS KMS. This CMK is unique to your AWS account and region. Only the service that created the AWS managed CMK can use it

You can login to your IAM dashboard. Click on "Encryption Keys" You will find the list based on the services you are using as follows:

- aws/elasticfilesystem 1 aws/lightsail
- aws/s3
- aws/rds and many more Detailed Guide: KMS

You can recognize AWS managed CMKs because their aliases have the format aws/service-name, such as aws/redshift. Typically, a service creates its AWS managed CMK in your account when you set up the service or the first time you use the CMfC

The AWS services that integrate with AWS KMS can use it in many different ways. Some services create AWS managed CMKs in your account. Other services require that you specify a customer managed CMK that you have created. And, others support both types of CMKs to allow you the ease of an AWS managed CMK or the control of a customer-managed CMK

Rotation period for CMKs is as follows:

- AWS managed CMKs: 1095 days
- Customer managed CMKs: 365 days

Since question mentions about "CMK where backing keys is managed by AWS", its Amazon(AWS) managed and its rotation period turns out to be 1095 days(every 3 years)

For more details, please check below AWS Docs: <https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html> The correct answer is: After 3 years

Submit your Feedback/Queries to our Experts

NEW QUESTION 8

A company wants to have an Intrusion detection system available for their VPC in AWS. They want to have complete control over the system. Which of the following would be ideal to implement?

Please select:

- A. Use AWS WAF to catch all intrusions occurring on the systems in the VPC
- B. Use a custom solution available in the AWS Marketplace
- C. Use VPC Flow logs to detect the issues and flag them accordingly.
- D. Use AWS Cloudwatch to monitor all traffic

Answer: B

Explanation:

Sometimes companies want to have custom solutions in place for monitoring intrusions to their systems. In such a case, you can use the AWS Marketplace for looking at custom solutions.

Option A,C and D are all invalid because they cannot be used to conduct intrusion detection or prevention.

For more information on using custom security solutions please visit the below URL https://d1.awsstatic.com/Marketplace/security/AWSMP_Security_Solution%20Overview.pdf For more information on using custom security solutions please visit the below URL: https://d1.awsstatic.com/Marketplace/security/AWSMP_Security_Solution%20Overview.pdf The correct answer is: Use a custom solution available in the AWS Marketplace

Submit your Feedback/Queries to our Experts

NEW QUESTION 9

You want to get a list of vulnerabilities for an EC2 Instance as per the guidelines set by the Center of Internet Security. How can you go about doing this?

Please select:

- A. Enable AWS Guard Duty for the Instance
- B. Use AWS Trusted Advisor
- C. Use AWS Inspector
- D. Use AWS Macie

Answer: C

Explanation:

The AWS Inspector service can inspect EC2 Instances based on specific Rules. One of the rules packages is based on the guidelines set by the Center of Internet Security

Center for Internet security (CIS) Benchmarks

The CIS Security Benchmarks program provides well-defined, un-biased and consensus-based industry best practices to help organizations assess and improve their security. Amazon Web Services is a CIS Security Benchmarks Member company and the list of Amazon Inspector certifications can be viewed here.

Option A is invalid because this can be used to protect an instance but not give the list of vulnerabilities

Options B and D are invalid because these services cannot give a list of vulnerabilities For more information on the guidelines, please visit the below URL:

* https://docs.aws.amazon.com/inspector/latest/userguide/inspector_cis.html The correct answer is: Use AWS Inspector

Submit your Feedback/Queries to our Experts

NEW QUESTION 10

Your company has defined a number of EC2 Instances over a period of 6 months. They want to know if any of the security groups allow unrestricted access to a resource. What is the best option to accomplish this requirement?

Please select:

- A. Use AWS Inspector to inspect all the security Groups
- B. Use the AWS Trusted Advisor to see which security groups have compromised access.
- C. Use AWS Config to see which security groups have compromised access.
- D. Use the AWS CLI to query the security groups and then filter for the rules which have unrestricted access

Answer: B

Explanation:

The AWS Trusted Advisor can check security groups for rules that allow unrestricted access to a resource. Unrestricted access increases opportunities for malicious activity (hacking, denial-of-service attacks, loss of data).

If you go to AWS Trusted Advisor, you can see the details

Option A is invalid because AWS Inspector is used to detect security vulnerabilities in instances and not for security groups.

Option C is invalid because this can be used to detect changes in security groups but not show you security groups that have compromised access.

Option D is partially valid but would just be a maintenance overhead

For more information on the AWS Trusted Advisor, please visit the below URL: <https://aws.amazon.com/premiumsupport/trustedadvisor/best-practices>;

The correct answer is: Use the AWS Trusted Advisor to see which security groups have compromised access. Submit your Feedback/Queries to our Experts

NEW QUESTION 10

You have enabled Cloudtrail logs for your company's AWS account. In addition, the IT Security department has mentioned that the logs need to be encrypted. How can this be achieved?

Please select:

- A. Enable SSL certificates for the Cloudtrail logs
- B. There is no need to do anything since the logs will already be encrypted
- C. Enable Server side encryption for the trail
- D. Enable Server side encryption for the destination S3 bucket

Answer: B

Explanation:

The AWS Documentation mentions the following.

By default CloudTrail event log files are encrypted using Amazon S3 server-side encryption (SSE). You can also choose to encrypt your log files with an AWS Key Management Service (AWS KMS) key. You can store your log files in your bucket for as long as you want. You can also define Amazon S3 lifecycle rules to archive or delete log files automatically. If you want notifications about log file delivery and validation, you can set up Amazon SNS notifications.

Option A, C and D are not valid since logs will already be encrypted

For more information on how CloudTrail works, please visit the following URL: <https://docs.aws.amazon.com/awscloudtrail/latest/userguide/how-cloudtrail-works.html>

The correct answer is: There is no need to do anything since the logs will already be encrypted Submit your Feedback/Queries to our Experts

NEW QUESTION 15

You have just recently set up a web and database tier in a VPC and hosted the application. When testing the app, you are not able to reach the home page for the app. You have verified the security groups. What can help you diagnose the issue.

Please select:

- A. Use the AWS Trusted Advisor to see what can be done.
- B. Use VPC Flow logs to diagnose the traffic
- C. Use AWS WAF to analyze the traffic
- D. Use AWS Guard Duty to analyze the traffic

Answer: B

Explanation:

Option A is invalid because this can be used to check for security issues in your account, but not verify as to why you cannot reach the home page for your application

Option C is invalid because this used to protect your app against application layer attacks, but not verify as to why you cannot reach the home page for your application

Option D is invalid because this used to protect your instance against attacks, but not verify as to why you cannot reach the home page for your application

The AWS Documentation mentions the following

VPC Flow Logs capture network flow information for a VPC, subnet or network interface and stores it in Amazon CloudWatch Logs. Flow log data can help customers troubleshoot network issues; for example, to diagnose why specific traffic is not reaching an instance, which might be a result of overly restrictive security group rules. Customers can also use flow logs as a security tool to monitor the traffic that reaches their instances, to profile network traffic, and to look for abnormal traffic behaviors.

For more information on AWS Security, please visit the following URL: <https://aws.amazon.com/answers/networking/vpc-security-capabilities>

The correct answer is: Use VPC Flow logs to diagnose the traffic Submit your Feedback/Queries to our Experts

NEW QUESTION 17

A security team is creating a response plan in the event an employee executes unauthorized actions on AWS infrastructure. They want to include steps to determine if the employee's IAM permissions changed as part of the incident.

What steps should the team document in the plan? Please select:

- A. Use AWS Config to examine the employee's IAM permissions prior to the incident and compare them to the employee's current IAM permissions.
- B. Use IAM to examine the employee's IAM permissions prior to the incident and compare them to the employee's current IAM permissions.
- C. Use CloudTrail to examine the employee's IAM permissions prior to the incident and compare them to the employee's current IAM permissions.
- D. Use Trusted Advisor to examine the employee's IAM permissions prior to the incident and compare them to the employee's current IAM permissions.

Answer: A

Explanation:

You can use the AWSConfig history to see the history of a particular item. The below snapshot shows an example configuration for a user in AWS Config

Option B,C and D are all invalid because these services cannot be used to see the history of a particular configuration item. This can only be accomplished by AWS Config.

For more information on tracking changes in AWS Config, please visit the below URL:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/TrackChanges.html> The correct answer is: Use AWS Config to examine the employee's IAM permissions prior to the incident and compare them to the employee's current IAM permissions.

Submit your Feedback/Queries to our Experts

NEW QUESTION 20

A security team must present a daily briefing to the CISO that includes a report of which of the company's thousands of EC2 instances and on-premises servers are missing the latest security patches. All instances/servers must be brought into compliance within 24 hours so they do not show up on the next day's report.

How can the security team fulfill these requirements?

Please select:

- A. Use Amazon QuickSight and Cloud Trail to generate the report of out of compliance instances/server
- B. Redeploy all out of compliance instances/servers using an AMI with the latest patches.
- C. Use Systems Manager Patch Manager to generate the report of out of compliance instances/ server
- D. Use Systems Manager Patch Manager to install the missing patches.
- E. Use Systems Manager Patch Manager to generate the report of out of compliance instances/ server
- F. Redeploy all out of1 compliance instances/servers using an AMI with the latest patches.
- G. Use Trusted Advisor to generate the report of out of compliance instances/server
- H. Use Systems Manager Patch Manager to install the missing patches.

Answer: B

Explanation:

Use the Systems Manager Patch Manager to generate the report and also install the missing patches The AWS Documentation mentions the following AWS Systems Manager Patch Manager automates the process of patching managed instances with security-related updates. For Linux-based instances, you can also install patches for non-security updates. You can patch fleets of Amazon EC2 instances or your on-premises servers and virtual machines (VMs) by operating system type. This includes supported versions of Windows, Ubuntu

Server, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), and Amazon Linux. You can scan instances to see only a report of missing patches, or you can scan and automatically install all missing patches.

Option A is invalid because Amazon QuickSight and Cloud Trail cannot be used to generate the list of servers that don't meet compliance needs.

Option C is wrong because deploying instances via new AMI'S would impact the applications hosted on these servers

Option D is invalid because Amazon Trusted Advisor cannot be used to generate the list of servers that don't meet compliance needs.

For more information on the AWS Patch Manager, please visit the below URL: <https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-patch.html> (

The correct answer is: Use Systems Manager Patch Manager to generate the report of out of compliance instances/ servers. Use Systems Manager Patch Manager to install the missing patches. Submit your Feedback/Queries to our Experts

NEW QUESTION 23

Your development team has started using AWS resources for development purposes. The AWS account has just been created. Your IT Security team is worried about possible leakage of AWS keys. What is the first level of measure that should be taken to protect the AWS account. Please select:

- A. Delete the AWS keys for the root account
- B. Create IAM Groups
- C. Create IAM Roles
- D. Restrict access using IAM policies

Answer: A

Explanation:

The first level of measure that should be taken is to delete the keys for the IAM root user

When you log into your account and go to your Security Access dashboard, this is the first step that can be seen

Option B and C are wrong because creation of IAM groups and roles will not change the impact of leakage of AWS root access keys

Option D is wrong because the first key aspect is to protect the access keys for the root account For more information on best practises for Security Access keys, please visit the below URL: <https://docs.aws.amazon.com/eeneral/latest/gr/aws-access-keys-best-practices.html>

The correct answer is: Delete the AWS keys for the root account Submit your Feedback/Queries to our Experts

NEW QUESTION 28

Which of the following is used as a secure way to log into an EC2 Linux Instance? Please select:

- A. IAM User name and password
- B. Key pairs
- C. AWS Access keys
- D. AWS SDK keys

Answer: B

Explanation:

The AWS Documentation mentions the following

Key pairs consist of a public key and a private key. You use the private key to create a digital signature, and then AWS uses the corresponding public key to validate the signature. Key pairs are used only for Amazon EC2 and Amazon CloudFront.

Option A,C and D are all wrong because these are not used to log into EC2 Linux Instances For more information on AWS Security credentials, please visit the below URL: <https://docs.aws.amazon.com/eeneral/latest/er/aws-sec-cred-types.html>

The correct answer is: Key pairs

Submit your Feedback/Queries to our Experts

NEW QUESTION 31

You have setup a set of applications across 2 VPC's. You have also setup VPC Peering. The applications are still not able to communicate across the Peering connection. Which network troubleshooting steps should be taken to resolve the issue?

Please select:

- A. Ensure the applications are hosted in a public subnet
- B. Check to see if the VPC has an Internet gateway attached.
- C. Check to see if the VPC has a NAT gateway attached.
- D. Check the Route tables for the VPC's

Answer: D

Explanation:

After the VPC peering connection is established, you need to ensure that the route tables are modified to ensure traffic can between the VPCs

Option A ,B and C are invalid because allowing access the Internet gateway and usage of public subnets can help for Inter, access, but not for VPC Peering.

For more information on VPC peering routing, please visit the below URL:

[.com/AmazonVPC/latest/Peeri](#)

The correct answer is: Check the Route tables for the VPCs Submit your Feedback/Queries to our Experts

NEW QUESTION 35

A company requires that data stored in AWS be encrypted at rest. Which of the following approaches achieve this requirement? Select 2 answers from the options given below.

Please select:

- A. When storing data in Amazon EBS, use only EBS-optimized Amazon EC2 instances.
- B. When storing data in EBS, encrypt the volume by using AWS KMS.
- C. When storing data in Amazon S3, use object versioning and MFA Delete.
- D. When storing data in Amazon EC2 Instance Store, encrypt the volume by using KMS.
- E. When storing data in S3, enable server-side encryptio

Answer: BE

Explanation:

The AWS Documentation mentions the following

To create an encrypted Amazon EBS volume, select the appropriate box in the Amazon EBS section of the Amazon EC2 console. You can use a custom customer master key (CMK) by choosing one from the list that appears below the encryption box. If you do not specify a custom CMK, Amazon EBS uses the AWS-managed CMK for Amazon EBS in your account. If there is no AWS-managed CMK for Amazon EBS in your account, Amazon EBS creates one.

Data protection refers to protecting data while in-transit (as it travels to and from Amazon S3) and at rest (while it is stored on disks in Amazon S3 data centers).

You can protect data in transit by using

SSL or by using client-side encryption. You have the following options of protecting data at rest in Amazon S3.

- Use Server-Side Encryption - You request Amazon S3 to encrypt your object before saving it on disks in its data centers and decrypt it when you download the objects.

- Use Client-Side Encryption - You can encrypt data client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, the encryption keys, and related tools. Option A is invalid because using EBS-optimized Amazon EC2 instances alone will not guarantee protection of instances at rest. Option C is invalid because this will not encrypt data at rest for S3 objects. Option D is invalid because you don't store data in Instance store. For more information on EBS encryption, please visit the below URL: <https://docs.aws.amazon.com/kms/latest/developerguide/services-ebs.html>

For more information on S3 encryption, please visit the below URL: <https://docs.aws.amazon.com/AmazonS3/latest/dev/UsinEEncryption.html>

The correct answers are: When storing data in EBS, encrypt the volume by using AWS KMS. When storing data in S3, enable server-side encryption.

Submit your Feedback/Queries to our Experts

NEW QUESTION 38

You need to ensure that objects in an S3 bucket are available in another region. This is because of the criticality of the data that is hosted in the S3 bucket. How can you achieve this in the easiest way possible?

Please select:

- A. Enable cross region replication for the bucket
- B. Write a script to copy the objects to another bucket in the destination region
- C. Create an S3 snapshot in the destination region
- D. Enable versioning which will copy the objects to the destination region

Answer: A

Explanation:

Option B is partially correct but a big maintenance over head to create and maintain a script when the functionality is already available in S3

Option C is invalid because snapshots are not available in S3 Option D is invalid because versioning will not replicate objects The AWS Documentation mentions the following

Cross-region replication is a bucket-level configuration that enables automatic, asynchronous copying of objects across buck in different AWS Regions.

For more information on Cross region replication in the Simple Storage Service, please visit the below URL:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/crr.html>

The correct answer is: Enable cross region replication for the bucket Submit your Feedback/Queries to our Experts

NEW QUESTION 39

A company has a legacy application that outputs all logs to a local text file. Logs from all applications running on AWS must be continually monitored for security related messages.

What can be done to allow the company to deploy the legacy application on Amazon EC2 and still meet the monitoring requirement? Please select:

- A. Create a Lambda function that mounts the EBS volume with the logs and scans the logs for security incident
- B. Trigger the function every 5 minutes with a scheduled Cloudwatch event.
- C. Send the local text log files to CloudWatch Logs and configure a CloudWatch metric filte
- D. Trigger cloudwatch alarms based on the metrics.
- E. Install the Amazon inspector agent on any EC2 instance running the legacy applicatio
- F. Generate CloudWatch alerts a based on any Amazon inspector findings.
- G. Export the local text log files to CloudTrai
- H. Create a Lambda function that queries the CloudTrail logs for security ' incidents using Athena.

Answer: B

Explanation:

One can send the log files to Cloudwatch Logs. Log files can also be sent from On-premise servers. You can then specify metrii to search the logs for any specific values. And then create alarms based on these metrics.

Option A is invalid because this will be just a long over drawn process to achieve this requirement Option C is invalid because AWS Inspector cannot be used to monitor for security related messages. Option D is invalid because files cannot be exported to AWS Cloudtrail

For more information on Cloudwatch logs agent please visit the below URL:

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/QuickStartEC2Instance.hti>

The correct answer is: Send the local text log files to Cloudwatch Logs and configure a Cloudwatch metric filter. Trigger cloudwatch alarms based on the metrics.
Submit your Feedback/Queries to our Experts

NEW QUESTION 42

Every application in a company's portfolio has a separate AWS account for development and production. The security team wants to prevent the root user and all 1AM users in the production accounts from accessing a specific set of unneeded services. How can they control this functionality? Please select:

- A. Create a Service Control Policy that denies access to the service
- B. Assemble all production accounts in an organizational unit
- C. Apply the policy to that organizational unit.
- D. Create a Service Control Policy that denies access to the service
- E. Apply the policy to the root account.
- F. Create an 1AM policy that denies access to the service
- G. Associate the policy with an 1AM group and enlist all users and the root users in this group.
- H. Create an 1AM policy that denies access to the service
- I. Create a Config Rule that checks that all users have the policy assigned
- J. Trigger a Lambda function that adds the policy when found missing.

Answer: A

Explanation:

As an administrator of the master account of an organization, you can restrict which AWS services and individual API actions the users and roles in each member account can access. This restriction even overrides the administrators of member accounts in the organization. When AWS Organizations blocks access to a service or API action for a member account a user or role in that account can't access any prohibited service or API action, even if an administrator of a member account explicitly grants such permissions in an 1AM policy. Organization permissions overrule account permissions. Option B is invalid because service policies cannot be assigned to the root account at the account level.

Option C and D are invalid because 1AM policies alone at the account level would not be able to suffice the requirement

For more information, please visit the below URL [id=docs_orgs_console https://docs.aws.amazon.com/IAM/latest/UserGuide/manage-attach-policy.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/manage-attach-policy.html)

The correct answer is: Create a Service Control Policy that denies access to the services. Assemble all production accounts in an organizational unit. Apply the policy to that organizational unit

Submit your Feedback/Queries to our Experts

NEW QUESTION 47

An application running on EC2 instances in a VPC must call an external web service via TLS (port 443). The instances run in public subnets.

Which configurations below allow the application to function and minimize the exposure of the instances? Select 2 answers from the options given below
Please select:

- A. A network ACL with a rule that allows outgoing traffic on port 443.
- B. A network ACL with rules that allow outgoing traffic on port 443 and incoming traffic on ephemeral ports
- C. A network ACL with rules that allow outgoing traffic on port 443 and incoming traffic on port 443.
- D. A security group with a rule that allows outgoing traffic on port 443
- E. A security group with rules that allow outgoing traffic on port 443 and incoming traffic on ephemeral ports.
- F. A security group with rules that allow outgoing traffic on port 443 and incoming traffic on port 443.

Answer: BD

Explanation:

Since here the traffic needs to flow outbound from the Instance to a web service on Port 443, the outbound rules on both the Network and Security Groups need to allow outbound traffic. The Incoming traffic should be allowed on ephemeral ports for the Operating System on the Instance to allow a connection to be established on any desired or available port.

Option A is invalid because this rule alone is not enough. You also need to ensure incoming traffic on ephemeral ports

Option C is invalid because need to ensure incoming traffic on ephemeral ports and not only port 443 Option E and F are invalid since here you are allowing additional ports on Security groups which are not required

For more information on VPC Security Groups, please visit the below URL:

https://docs.aws.amazon.com/AmazonVPC/latest/UserGuideA/PC_SecurityGroups.html

The correct answers are: A network ACL with rules that allow outgoing traffic on port 443 and incoming traffic on ephemeral ports, A security group with a rule that allows outgoing traffic on port 443

Submit your Feedback/Queries to our Experts

NEW QUESTION 48

You are working in the media industry and you have created a web application where users will be able to upload photos they create to your website. This web application must be able to call the S3 API in order to be able to function. Where should you store your API credentials whilst maintaining the maximum level of security?

Please select:

- A. Save the API credentials to your PHP files.
- B. Don't save your API credentials, instead create a role in 1AM and assign this role to an EC2 instance when you first create it.
- C. Save your API credentials in a public Github repository.
- D. Pass API credentials to the instance using instance userdata

Answer: B

Explanation:

Applications must sign their API requests with AWS credentials. Therefore, if you are an application developer, you need a strategy for managing credentials for your applications that run on EC2 instances. For example, you can securely distribute your AWS credentials to the instances, enabling the applications on those instances to use your credentials to sign requests, while protecting your credentials from other users. However, it's challenging to securely distribute credentials to each instance. especially those that AWS creates on your behalf, such as Spot Instances or instances in Auto Scaling groups. You must also be able to update the credentials on each instance when you rotate your AWS credentials.

1AM roles are designed so that your applications can securely make API requests from your instances, without requiring you to manage the security credentials that

the applications use.

Option A.C and D are invalid because using AWS Credentials in an application in production is a direct no recommendation 1 secure access

For more information on 1AM Roles, please visit the below URL: <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html>

The correct answer is: Don't save your API credentials. Instead create a role in 1AM and assign this role to an EC2 instance when you first create it

Submit your Feedback/Queries to our Experts

NEW QUESTION 50

A company has a set of resources defined in AWS. It is mandated that all API calls to the resources be monitored. Also all API calls must be stored for lookup purposes. Any log data greater than 6 months must be archived. Which of the following meets these requirements? Choose 2 answers from the options given below. Each answer forms part of the solution.

Please select:

- A. Enable CloudTrail logging in all accounts into S3 buckets
- B. Enable CloudTrail logging in all accounts into Amazon Glacier
- C. Ensure a lifecycle policy is defined on the S3 bucket to move the data to EBS volumes after 6 months.
- D. Ensure a lifecycle policy is defined on the S3 bucket to move the data to Amazon Glacier after 6 months.

Answer: AD

Explanation:

Cloudtrail publishes the trail of API logs to an S3 bucket

Option B is invalid because you cannot put the logs into Glacier from CloudTrail

Option C is invalid because lifecycle policies cannot be used to move data to EBS volumes For more information on Cloudtrail logging, please visit the below URL:

<https://docs.aws.amazon.com/awscloudtrail/latest/useruide/cloudtrail-find-log-files.html>

You can then use Lifecycle policies to transfer data to Amazon Glacier after 6 months For more information on S3 lifecycle policies, please visit the below URL:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html>

The correct answers are: Enable CloudTrail logging in all accounts into S3 buckets. Ensure a lifecycle policy is defined on the bucket to move the data to Amazon Glacier after 6 months.

Submit your Feedback/Queries to our Experts

NEW QUESTION 53

A security engineer must ensure that all infrastructure launched in the company AWS account be monitored for deviation from compliance rules, specifically that all EC2 instances are launched from one of a specified list of AM Is and that all attached EBS volumes are encrypted. Infrastructure not in compliance should be terminated. What combination of steps should the Engineer implement? Select 2 answers from the options given below.

Please select:

- A. Set up a CloudWatch event based on Trusted Advisor metrics
- B. Trigger a Lambda function from a scheduled CloudWatch event that terminates non-compliant infrastructure.
- C. Set up a CloudWatch event based on Amazon inspector findings
- D. Monitor compliance with AWS Config Rules triggered by configuration changes
- E. Trigger a CLI command from a CloudWatch event that terminates the infrastructure

Answer: BD

Explanation:

You can use AWS Config to monitor for such Event

Option A is invalid because you cannot set Cloudwatch events based on Trusted Advisor checks.

Option C is invalid Amazon inspector cannot be used to check whether instances are launched from a specific A

Option E is invalid because triggering a CLI command is not the preferred option, instead you should use Lambda functions for all automation purposes.

For more information on Config Rules please see the below Link: <https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config-rules.html>

These events can then trigger a lambda function to terminate instances For more information on Cloudwatch events please see the below Link:

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/events/WhatIsCloudWatchEvents>.

(

The correct answers are: Trigger a Lambda function from a scheduled Cloudwatch event that terminates non-compliant infrastructure., Monitor compliance with AWS Config Rules triggered by configuration changes

Submit your Feedback/Queries to our Experts

NEW QUESTION 57

A company has external vendors that must deliver files to the company. These vendors have crossaccount that gives them permission to upload objects to one of the company's S3 buckets.

What combination of steps must the vendor follow to successfully deliver a file to the company? Select 2 answers from the options given below

Please select:

- A. Attach an 1AM role to the bucket that grants the bucket owner full permissions to the object
- B. Add a grant to the objects ACL giving full permissions to bucket owner.
- C. Encrypt the object with a KMS key controlled by the company.
- D. Add a bucket policy to the bucket that grants the bucket owner full permissions to the object
- E. Upload the file to the company's S3 bucket

Answer: BE

Explanation:

This scenario is given in the AWS Documentation

A bucket owner can enable other AWS accounts to upload objects. These objects are owned by the accounts that created them. The bucket owner does not own objects that were not created by the bucket owner. Therefore, for the bucket owner to grant access to these objects, the object owner must first grant permission to the bucket owner using an object ACL. The bucket owner can then delegate those permissions via a bucket policy. In this example, the bucket owner delegates permission to users in its own account.

Option A and D are invalid because bucket ACL's are used to give grants to bucket Option C is not required since encryption is not part of the requirement For more information on this scenario please see the below Link:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/example-walkthroughs-managing-accessesexample3.html>

The correct answers are: Add a grant to the objects ACL giving full permissions to bucket owner., Upload the file to the company's S3 bucket

Submit your Feedback/Queries to our Experts

NEW QUESTION 60

An application running on EC2 instances in a VPC must access sensitive data in the data center. The access must be encrypted in transit and have consistent low latency. Which hybrid architecture will meet these requirements?

Please select:

- A. Expose the data with a public HTTPS endpoint.
- B. A VPN between the VPC and the data center over a Direct Connect connection
- C. A VPN between the VPC and the data center.
- D. A Direct Connect connection between the VPC and data center

Answer: B

Explanation:

Since this is required over a consistency low latency connection, you should use Direct Connect. For encryption, you can make use of a VPN

Option A is invalid because exposing an HTTPS endpoint will not help all traffic to flow between a VPC and the data center.

Option C is invalid because low latency is a key requirement Option D is invalid because only Direct Connect will not suffice

For more information on the connection options please see the below Link: <https://aws.amazon.com/answers/networking/aws-multiple-vpc-vpn-connection-sharing>

The correct answer is: A VPN between the VPC and the data center over a Direct Connect connection Submit your Feedback/Queries to our Experts

NEW QUESTION 62

A company wishes to enable Single Sign On (SSO) so its employees can login to the management console using their corporate directory identity. Which steps below are required as part of the process? Select 2 answers from the options given below.

Please select:

- A. Create a Direct Connect connection between on-premise network and AWS
- B. Use an AD connector for connecting AWS with on-premise active directory.
- C. Create IAM policies that can be mapped to group memberships in the corporate directory.
- D. Create a Lambda function to assign IAM roles to the temporary security tokens provided to the users.
- E. Create IAM users that can be mapped to the employees' corporate identities
- F. Create an IAM role that establishes a trust relationship between IAM and the corporate directory identity provider (IdP)

Answer: AE

Explanation:

Create a Direct Connect connection so that corporate users can access the AWS account

Option B is incorrect because IAM policies are not directly mapped to group memberships in the corporate directory. It is IAM roles which are mapped.

Option C is incorrect because Lambda functions is an incorrect option to assign roles.

Option D is incorrect because IAM users are not directly mapped to employees' corporate identities. For more information on Direct Connect, please refer to below URL:

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

From the AWS Documentation, for federated access, you also need to ensure the right policy permissions are in place

Configure permissions in AWS for your federated users

The next step is to create an IAM role that establishes a trust relationship between IAM and your organization's IdP that identifies your IdP as a principal (trusted entity) for purposes of federation. The role also defines what users authenticated your organization's IdP are allowed to do in AWS. You can use the IAM console to create this role. When you create the trust policy that indicates who can assume the role, you specify the SAML provider that you created earlier in IAM along with one or more SAML attributes that a user must match to be allowed to assume the role. For example, you can

specify that only users whose SAML eduPersonOrgDN value is ExampleOrg are allowed to sign in. The role wizard automatically adds a condition to test the saml:aud attribute to make sure that the role is assumed only for sign-in to the AWS Management Console. The trust policy for the role might look like this:

For more information on SAML federation, please refer to below URL: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_enable

Note: What directories can I use with AWS SSO?

You can connect AWS SSO to Microsoft Active Directory, running either on-premises or in the AWS Cloud. AWS SSO supports AWS Directory Service for Microsoft Active Directory, also known as AWS Managed Microsoft AD, and AD Connector. AWS SSO does not support Simple AD. See AWS Directory Service Getting Started to learn more.

To connect to your on-premises directory with AD Connector, you need the following: VPC

Set up a VPC with the following:

- At least two subnets. Each of the subnets must be in a different Availability Zone.
- The VPC must be connected to your on-premises network through a virtual private network (VPN) connection or AWS Direct Connect.

- The VPC must have default hardware tenancy.

- <https://aws.amazon.com/single-sign-on/>

- <https://aws.amazon.com/single-sign-on/faqs/>

- <https://aws.amazon.com/blog/using-corporate-credentials/>

- <https://docs.aws.amazon.com/directoryservice/latest/admin-guide/>

The correct answers are: Create a Direct Connect connection between on-premise network and AWS. Use an AD connector connecting AWS with on-premise active directory.. Create an IAM role that establishes a trust relationship between IAM and corporate directory identity provider (IdP)

Submit your Feedback/Queries to our Experts

NEW QUESTION 63

A web application runs in a VPC on EC2 instances behind an ELB Application Load Balancer. The application stores data in an RDS MySQL DB instance. A Linux bastion host is used to apply schema updates to the database - administrators connect to the host via SSH from a corporate workstation. The following security groups are applied to the infrastructure-

* sgLB - associated with the ELB

* sgWeb - associated with the EC2 instances.

* sgDB - associated with the database

* sgBastion - associated with the bastion host Which security group configuration will allow the application to be secure and functional?

Please select: A.

sgLB :allow port 80 and 443 traffic from 0.0.0.0/0 sgWeb :allow port 80 and 443 traffic from 0.0.0.0/0 sgDB :allow port 3306 traffic from sgWeb and sgBastion
sgBastion: allow port 22 traffic from the corporate IP address range

B.

sgLB :allow port 80 and 443 traffic from 0.0.0.0/0 sgWeb :allow port 80 and 443 traffic from sgLB sgDB :allow port 3306 traffic from sgWeb and sgLB

sgBastion: allow port 22 traffic from the VPC IP address range C.

sgLB :allow port 80 and 443 traffic from 0.0.0.0/0 sgWeb :allow port 80 and 443 traffic from sgLB

sgDB :allow port 3306 traffic from sgWeb and sgBastion sgBastion: allow port 22 traffic from the VPC IP address range D.

sgLB :allow port 80 and 443 traffic from 0.0.0.0/0 sgWeb :allow port 80 and 443 traffic from sgLB

sgDB :allow port 3306 traffic from sgWeb and sgBastion sgBastion: allow port 22 traffic from the corporate IP address range

A.

Answer: D

Explanation:

The Load Balancer should accept traffic on ow port 80 and 443 traffic from 0.0.0.0/0 The backend EC2 Instances should accept traffic from the Load Balancer

The database should allow traffic from the Web server

And the Bastion host should only allow traffic from a specific corporate IP address range Option A is incorrect because the Web group should only allow traffic from the Load balancer For more information on AWS Security Groups, please refer to below URL: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/usins-network-security.html>

The correct answer is: sgLB :allow port 80 and 443 traffic from 0.0.0.0/0 sgWeb :allow port 80 and 443 traffic from sgLB

sgDB :allow port 3306 traffic from sgWeb and sgBastion sgBastion: allow port 22 traffic from the corporate IP address range Submit your Feedback/Queries to our Experts

NEW QUESTION 64

You need to have a requirement to store objects in an S3 bucket with a key that is automatically managed and rotated. Which of the following can be used for this purpose?

Please select:

A. AWS KMS

B. AWS S3 Server side encryption

C. AWS Customer Keys

D. AWS Cloud HSM

Answer: B

Explanation:

The AWS Documentation mentions the following

Server-side encryption protects data at rest. Server-side encryption with Amazon S3-managed encryption keys (SSE-S3) uses strong multi-factor encryption.

Amazon S3 encrypts each object with a unique key. As an additional safeguard, it encrypts the key itself with a master key that it rotates regularly. Amazon S3 server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt your data.

All other options are invalid since here you need to ensure the keys are manually rotated since you manage the entire key set Using AWS S3 Server side encryption, AWS will manage the rotation of keys automatically.

For more information on Server side encryption, please visit the following URL:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/UsineServerSideEncryption.html>

The correct answer is: AWS S3 Server side encryption Submit your Feedback/Queries to our Experts

NEW QUESTION 65

You need to inspect the running processes on an EC2 Instance that may have a security issue. How can you achieve this in the easiest way possible. Also you need to ensure that the process does not interfere with the continuous running of the instance.

Please select:

A. Use AWS Cloudtrail to record the processes running on the server to an S3 bucket.

B. Use AWS Cloudwatch to record the processes running on the server

C. Use the SSM Run command to send the list of running processes information to an S3 bucket.

D. Use AWS Config to see the changed process information on the server

Answer: C

Explanation:

The SSM Run command can be used to send OS specific commands to an Instance. Here you can check and see the running processes on an instance and then send the output to an S3 bucket. Option A is invalid because this is used to record API activity and cannot be used to record running processes.

Option B is invalid because Cloudwatch is a logging and metric service and cannot be used to record running processes.

Option D is invalid because AWS Config is a configuration service and cannot be used to record running processes.

For more information on the Systems Manager Run command, please visit the following URL: <https://docs.aws.amazon.com/systems-manageer/latest/useruide/execute-remote-commands.html>

The correct answer is: Use the SSM Run command to send the list of running processes information to an S3 bucket. Submit your Feedback/Queries to our Experts

NEW QUESTION 67

You are trying to use the AWS Systems Manager run command on a set of Instances. The run command on a set of Instances. What can you do to diagnose the issue? Choose 2 answers from the options given

Please select:

A. Ensure that the SSM agent is running on the target machine

B. Check the /var/log/amazon/ssm/errors.log file

C. Ensure the right AMI is used for the Instance

D. Ensure the security groups allow outbound communication for the instance

Answer: AB

Explanation:

The AWS Documentation mentions the following

If you experience problems executing commands using Run Command, there might be a problem with the SSM Agent. Use the following information to help you troubleshoot the agent

View Agent Logs

The SSM Agent logs information in the following files. The information in these files can help you troubleshoot problems.

On Windows

%PROGRAMDATA%\Amazon\SSM\Logs\amazon-ssm-agent.log

%PROGRAMDATA%\Amazon\SSM\Logs\error.log

The default filename of the seelog is seelog-xml.template. If you modify a seelog, you must rename the file to seelog.xml.

On Linux

/var/log/amazon/ssm/amazon-ssm-agentlog /var/log/amazon/ssm/errors.log

Option C is invalid because the right AMI has nothing to do with the issues. The agent which is used to execute run commands can run on a variety of AMI'S

Option D is invalid because security groups does not come into the picture with the communication between the agent and the SSM service

For more information on troubleshooting AWS SSM, please visit the following URL: <https://docs.aws.amazon.com/systems-manageer/latest/userguide/troubleshootine-remotecommands.html>

The correct answers are: Ensure that the SSM agent is running on the target machine. Check the

/var/log/amazon/ssm/errors.log file

Submit your Feedback/Queries to our Experts

NEW QUESTION 68

You are working for a company and been allocated the task for ensuring that there is a federated authentication mechanism setup between AWS and their On-premise Active Directory. Which of the following are important steps that need to be covered in this process? Choose 2 answers from the options given below. Please select:

- A. Ensure the right match is in place for On-premise AD Groups and 1AM Roles.
- B. Ensure the right match is in place for On-premise AD Groups and 1AM Groups.
- C. Configure AWS as the relying party in Active Directory
- D. Configure AWS as the relying party in Active Directory Federation services

Answer: AD

Explanation:

The AWS Documentation mentions some key aspects with regards to the configuration of Onpremise AD with AWS

One is the Groups configuration in AD Active Directory Configuration

Determining how you will create and delineate your AD groups and 1AM roles in AWS is crucial to how you secure access to your account and manage resources. SAML assertions to the AWS environment and the respective 1AM role access will be managed through regular expression (regex) matching between your on-premises AD group name to an AWS 1AM role.

One approach for creating the AD groups that uniquely identify the AWS 1AM role mapping is by selecting a common group naming convention. For example, your AD groups would start with an identifier, for example, AWS-, as this will distinguish your AWS groups from others within the organization. Next include the 12-digitAWS account number. Finally, add the matching role name within the AWS account. Here is an example:

And next is the configuration of the relying party which is AWS

ADFS federation occurs with the participation of two parties; the identity or claims provider (in this case the owner of the identity repository - Active Directory) and the relying party, which is another application that wishes to outsource authentication to the identity provider; in this case Amazon Secure Token Service (STS).

The relying party is a federation partner that is represented by a claims provider trust in the federation service.

Option B is invalid because AD groups should not be matched to 1AM Groups

Option C is invalid because the relying party should be configured in Active Directory Federation services

For more information on the federated access, please visit the following URL:

1 <https://aws.amazon.com/blogs/security/aws-federated-authentication-with-active-directoryfederation-services-ad-fs/>

The correct answers are: Ensure the right match is in place for On-premise AD Groups and 1AM Roles., Configure AWS as the relying party in Active Directory Federation services

Submit your Feedback/Queries to our Experts

NEW QUESTION 73

A company has an existing AWS account and a set of critical resources hosted in that account. The employee who was in-charge of the root account has left the company. What must be now done to secure the account. Choose 3 answers from the options given below.

Please select:

- A. Change the access keys for all 1AM users.
- B. Delete all custom created 1AM policies
- C. Delete the access keys for the root account
- D. Confirm MFAtoa secure device
- E. Change the password for the root account
- F. Change the password for all 1AM users

Answer: CDE

Explanation:

Now if the root account has a chance to be compromised, then you have to carry out the below steps

1. Delete the access keys for the root account
2. Confirm MFA to a secure device
3. Change the password for the root account

This will ensure the employee who has left has no change to compromise the resources in AWS. Option A is invalid because this would hamper the working of the current IAM users

Option B is invalid because this could hamper the current working of services in your AWS account Option F is invalid because this would hamper the working of the current IAM users

For more information on IAM root user, please visit the following URL: <https://docs.aws.amazon.com/IAM/latest/UserGuide/id-root-user.html>

The correct answers are: Delete the access keys for the root account Confirm MFA to a secure device. Change the password for the root account

Submit Your Feedback/Queries to our Experts

NEW QUESTION 75

A company had developed an incident response plan 18 months ago. Regular implementations of the response plan are carried out. No changes have been made to the response plan have been made since its creation. Which of the following is a right statement with regards to the plan?

Please select:

- A. It places too much emphasis on already implemented security controls.
- B. The response plan is not implemented on a regular basis
- C. The response plan does not cater to new services
- D. The response plan is complete in its entirety

Answer: C

Explanation:

So definitely the case here is that the incident response plan is not catering to newly created services. AWS keeps on changing and adding new services and hence the response plan must cater to these new services.

Option A and B are invalid because we don't know this for a fact.

Option D is invalid because we know that the response plan is not complete, because it does not cater to new features of AWS

For more information on incident response plan please visit the following URL: <https://aws.amazon.com/blogs/publicsector/buildins-a-cloud-specific-incident-response-plan>; The correct answer is: The response plan does not cater to new services Submit your Feedback/Queries to our Experts

NEW QUESTION 80

Your application currently uses customer keys which are generated via AWS KMS in the US east region. You now want to use the same set of keys from the EU-Central region. How can this be accomplished?

Please select:

- A. Export the key from the US east region and import them into the EU-Central region
- B. Use key rotation and rotate the existing keys to the EU-Central region
- C. Use the backing key from the US east region and use it in the EU-Central region
- D. This is not possible since keys from KMS are region specific

Answer: D

Explanation:

Option A is invalid because keys cannot be exported and imported across regions. Option B is invalid because key rotation cannot be used to export keys

Option C is invalid because the backing key cannot be used to export keys This is mentioned in the AWS documentation

What geographic region are my keys stored in?

Keys are only stored and used in the region in which they are created. They cannot be transferred to another region. For example; keys created in the EU-Central (Frankfurt) region are only stored and used within the EU-Central (Frankfurt) region

For more information on KMS please visit the following URL: <https://aws.amazon.com/kms/faqs/>

The correct answer is: This is not possible since keys from KMS are region specific Submit your Feedback/Queries to our Experts

NEW QUESTION 82

You currently have an S3 bucket hosted in an AWS Account. It holds information that needs be accessed by a partner account. Which is the MOST secure way to allow the partner account to access the S3 bucket in your account? Select 3 options.

Please select:

- A. Ensure an IAM role is created which can be assumed by the partner account.
- B. Ensure an IAM user is created which can be assumed by the partner account.
- C. Ensure the partner uses an external id when making the request
- D. Provide the ARN for the role to the partner account
- E. Provide the Account Id to the partner account
- F. Provide access keys for your account to the partner account

Answer: ACD

Explanation:

Option B is invalid because Roles are assumed and not IAM users

Option E is invalid because you should not give the account ID to the partner Option F is invalid because you should not give the access keys to the partner

The below diagram from the AWS documentation showcases an example on this wherein an IAM role and external ID is used to access an AWS account resources

For more information on creating roles for external ID'S please visit the following URL:

The correct answers are: Ensure an IAM role is created which can be assumed by the partner account. Ensure the partner uses an external id when making the request Provide the ARN for the role to the partner account

NEW QUESTION 84

Your company has created a set of keys using the AWS KMS service. They need to ensure that each key is only used for certain services. For example , they want one key to be used only for the S3 service. How can this be achieved?

Please select:

- A. Create an IAM policy that allows the key to be accessed by only the S3 service.
- B. Create a bucket policy that allows the key to be accessed by only the S3 service.
- C. Use the kms:ViaService condition in the Key policy
- D. Define an IAM user, allocate the key and then assign the permissions to the required service

Answer: C

Explanation:

Option A and B are invalid because mapping keys to services cannot be done via either the 1AM or bucket policy
Option D is invalid because keys for 1AM users cannot be assigned to services This is mentioned in the AWS Documentation
The kms:ViaService condition key limits use of a customer-managed CMK to requests from particular AWS services. (AWS managed CMKs in your account, such as aws/s3, are always restricted to the AWS service that created them.)
For example, you can use kms:V1aService to allow a user to use a customer managed CMK only for requests that Amazon S3 makes on their behalf. Or you can use it to deny the user permission to a CMK when a request on their behalf comes from AWS Lambda.
For more information on key policy's for KMS please visit the following URL: <https://docs.aws.amazon.com/kms/latest/developereuide/policy-conditions.html>
The correct answer is: Use the kms:ViaServtce condition in the Key policy Submit your Feedback/Queries to our Experts

NEW QUESTION 89

You are planning on hosting a web application on AWS. You create an EC2 Instance in a public subnet. This instance needs to connect to an EC2 Instance that will host an Oracle database. Which of the following steps should be followed to ensure a secure setup is in place? Select 2 answers.
Please select:

- A. Place the EC2 Instance with the Oracle database in the same public subnet as the Web server for faster communication
- B. Place the EC2 Instance with the Oracle database in a separate private subnet
- C. Create a database security group and ensure the web security group to allowed incoming access
- D. Ensure the database security group allows incoming traffic from 0.0.0.0/0

Answer: BC

Explanation:

The best secure option is to place the database in a private subnet. The below diagram from the AWS Documentation shows this setup. Also ensure that access is not allowed from all sources but just from the web servers.

Option A is invalid because databases should not be placed in the public subnet
Option D is invalid because the database security group should not allow traffic from the internet For more information on this type of setup, please refer to the below URL: https://docs.aws.amazon.com/AmazonVPC/latest/UserGuideA/PC_Scenario2.
The correct answers are: Place the EC2 Instance with the Oracle database in a separate private subnet Create a database security group and ensure the web security group to allowed incoming access
Submit your Feedback/Queries to our Experts

NEW QUESTION 93

An EC2 Instance hosts a Java based application that access a DynamoDB table. This EC2 Instance is currently serving production based users. Which of the following is a secure way of ensuring that the EC2 Instance access the Dynamo table
Please select:

- A. Use 1AM Roles with permissions to interact with DynamoDB and assign it to the EC2 Instance
- B. Use KMS keys with the right permissions to interact with DynamoDB and assign it to the EC2 Instance
- C. Use 1AM Access Keys with the right permissions to interact with DynamoDB and assign it to the EC2 Instance
- D. Use 1AM Access Groups with the right permissions to interact with DynamoDB and assign it to the EC2 Instance

Answer: A

Explanation:

To always ensure secure access to AWS resources from EC2 Instances, always ensure to assign a Role to the EC2 Instance Option B is invalid because KMS keys are not used as a mechanism for providing EC2 Instances access to AWS services. Option C is invalid Access keys is not a safe mechanism for providing EC2 Instances access to AWS services. Option D is invalid because there is no way access groups can be assigned to EC2 Instances. For more information on 1AM Roles, please refer to the below URL:
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html
The correct answer is: Use 1AM Roles with permissions to interact with DynamoDB and assign it to the EC2 Instance Submit your Feedback/Queries to our Experts

NEW QUESTION 98

An application running on EC2 instances processes sensitive information stored on Amazon S3. The information is accessed over the Internet. The security team is concerned that the Internet connectivity to Amazon S3 is a security risk. Which solution will resolve the security concern? Please select:

- A. Access the data through an Internet Gateway.
- B. Access the data through a VPN connection.
- C. Access the data through a NAT Gateway.
- D. Access the data through a VPC endpoint for Amazon S3

Answer: D

Explanation:

The AWS Documentation mentions the followii

A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network.

Option A,B and C are all invalid because the question specifically mentions that access should not be provided via the Internet

For more information on VPC endpoints, please refer to the below URL:

The correct answer is: Access the data through a VPC endpoint for Amazon S3

NEW QUESTION 100

Development teams in your organization use S3 buckets to store the log files for various applications hosted in development environments in AWS. The developers want to keep the logs for one month for troubleshooting purposes, and then purge the logs. What feature will enable this requirement? Please select:

- A. Adding a bucket policy on the S3 bucket.
- B. Configuring lifecycle configuration rules on the S3 bucket.
- C. Creating an IAM policy for the S3 bucket.
- D. Enabling CORS on the S3 bucket

Answer: B

Explanation:

The AWS Documentation mentions the following on lifecycle policies

Lifecycle configuration enables you to specify the lifecycle management of objects in a bucket. The configuration is a set of one or more rules, where each rule defines an action for Amazon S3 to apply to a group of objects. These actions can be classified as follows:

Transition actions - In which you define when objects transition to another . For example, you may choose to

transition objects to the STANDARD_IA (IA, for infrequent access) storage class 30 days after creation, or archive objects to the GLACIER storage class one year after creation.

Expiration actions - In which you specify when the objects expire. Then Amazon S3 deletes the expired objects on your behalf.

Option A and C are invalid because neither bucket policies nor IAM policy's can control the purging of logs Option D is invalid CORS is used for accessing objects across domains and not for purging of logs For more information on AWS S3 Lifecycle policies, please visit the following URL:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/>

The correct answer is: Configuring lifecycle configuration rules on the S3 bucket. Submit your Feedback/Queries to our Experts

NEW QUESTION 104

A customer has an instance hosted in the AWS Public Cloud. The VPC and subnet used to host the Instance have been created with the default settings for the Network Access Control Lists. They need to provide an IT Administrator secure access to the underlying instance. How can this be accomplished. Please select:

- A. Ensure the Network Access Control Lists allow Inbound SSH traffic from the IT Administrator's Workstation
- B. Ensure the Network Access Control Lists allow Outbound SSH traffic from the IT Administrator's Workstation
- C. Ensure that the security group allows Inbound SSH traffic from the IT Administrator's Workstation
- D. Ensure that the security group allows Outbound SSH traffic from the IT Administrator's Workstation

Answer: C

Explanation:

Options A & B are invalid as default NACL rule will allow all inbound and outbound traffic.

The requirement is that the IT administrator should be able to access this EC2 instance from his workstation. For that we need to enable the Security Group of EC2 instance to allow traffic from the IT administrator's workstation. Hence option C is correct.

Option D is incorrect as we need to enable the Inbound SSH traffic on the EC2 instance Security Group since the traffic originates from the IT admin's workstation.

The correct answer is: Ensure that the security group allows Inbound SSH traffic from the IT Administrator's Workstation Submit your Feedback/Queries to our Experts

NEW QUESTION 107

Your company hosts critical data in an S3 bucket. There is a requirement to ensure that all data is encrypted. There is also metadata about the information stored in the bucket that needs to be encrypted as well. Which of the below measures would you take to ensure that the metadata is encrypted? Please select:

- A. Put the metadata as metadata for each object in the S3 bucket and then enable S3 Server side encryption.
- B. Put the metadata as metadata for each object in the S3 bucket and then enable S3 Server KMS encryption.
- C. Put the metadata in a DynamoDB table and ensure the table is encrypted during creation time.
- D. Put the metadata in the S3 bucket itself

Answer: C

Explanation:

Option A ,B and D are all invalid because the metadata will not be encrypted in any case and this is a key requirement from the question.

One key thing to note is that when the S3 bucket objects are encrypted, the meta data is not encrypted. So the best option is to use an encrypted DynamoDB table Important

All GET and PUT requests for an object protected by AWS KMS will fail if they are not made via SSL or by using SigV4. SSE-KMS encrypts only the object data

A. Any object metadata is not encrypted. For

more information on using KMS encryption for S3, please refer to below URL: 1 <https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingKMSEncryption.html>

The correct answer is: Put the metadata in a DynamoDB table and ensure the table is encrypted during creation time. Submit your Feedback/Queries to our Experts

NEW QUESTION 108

One of the EC2 Instances in your company has been compromised. What steps would you take to ensure that you could apply digital forensics on the Instance.

Select 2 answers from the options given below

Please select:

- A. Remove the role applied to the Ec2 Instance
- B. Create a separate forensic instance
- C. Ensure that the security groups only allow communication to this forensic instance
- D. Terminate the instance

Answer: BC

Explanation:

Option A is invalid because removing the role will not help completely in such a situation

Option D is invalid because terminating the instance means that you cannot conduct forensic analysis on the instance

One way to isolate an affected EC2 instance for investigation is to place it in a Security Group that only the forensic investigators can access. Close all ports except to receive inbound SSH or RDP traffic from one single IP address from which the investigators can safely examine the instance.

For more information on security scenarios for your EC2 Instance, please refer to below URL: <https://d1.awsstatic.com/Marketplace/scenarios/security/SEC 11 TSB Final.pdf>

The correct answers are: Create a separate forensic instance. Ensure that the security groups only allow communication to this forensic instance

Submit your Feedback/Queries to our Experts

NEW QUESTION 109

One of your company's EC2 Instances have been compromised. The company has strict po thorough investigation on finding the culprit for the security breach. What would you do in from the options given below.

Please select:

- A. Take a snapshot of the EBS volume
- B. Isolate the machine from the network
- C. Make sure that logs are stored securely for auditing and troubleshooting purpose
- D. Ensure all passwords for all 1AM users are changed
- E. Ensure that all access keys are rotate

Answer: ABC

Explanation:

Some of the important aspects in such a situation are

1) First isolate the instance so that no further security harm can occur on other AWS resources

2) Take a snapshot of the EBS volume for further investigation. This is incase if you need to shutdown the initial instance and do a separate investigation on the data

3) Next is Option C. This indicates that we have already got logs and we need to make sure that it is stored securely so that n unauthorised person can access it and manipulate it.

Option D and E are invalid because they could have adverse effects for the other 1AM users. For more information on adopting a security framework, please refer to below URL [https://d1.awsstatic.com/whitepapers/compliance/NIST Cybersecurity Framework](https://d1.awsstatic.com/whitepapers/compliance/NIST_Cybersecurity_Framework.pdf)

Note:

In the question we have been asked to take actions to find the culprit and to help the investigation or to further reduce the damage that has happened due to the security breach. So by keeping logs secure is one way of helping the investigation.

The correct answers are: Take a snapshot of the EBS volume. Isolate the machine from the network. Make sure that logs are stored securely for auditing and troubleshooting purpose

Submit your Feedback/Queries to our Experts

NEW QUESTION 113

Your company has a set of EC2 Instances that are placed behind an ELB. Some of the applications hosted on these instances communicate via a legacy protocol. There is a security mandate that all traffic between the client and the EC2 Instances need to be secure. How would you accomplish this? Please select:

- A. Use an Application Load balancer and terminate the SSL connection at the ELB
- B. Use a Classic Load balancer and terminate the SSL connection at the ELB
- C. Use an Application Load balancer and terminate the SSL connection at the EC2 Instances
- D. Use a Classic Load balancer and terminate the SSL connection at the EC2 Instances

Answer: D

Explanation:

Since there are applications which work on legacy protocols, you need to ensure that the ELB can be used at the network layer as well and hence you should choose the Classic ELB. Since the traffic

needs to be secure till the EC2 Instances, the SSL termination should occur on the Ec2 Instances. Option A and C are invalid because you need to use a Classic Load balancer since this is a legacy application.

Option B is incorrect since encryption is required until the EC2 Instance

For more information on HTTPS listeners for classic load balancers, please refer to below URL

<https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-https-load-balancers.html> The correct answer is: Use a Classic Load balancer and terminate the SSL connection at the EC2 Instances

Submit your Feedback/Queries to our Experts

NEW QUESTION 118

A company has a large set of keys defined in AWS KMS. Their developers frequently use the keys for the applications being developed. What is one of the ways that can be used to reduce the cost of accessing the keys in the AWS KMS service.

Please select:

- A. Enable rotation of the keys
- B. Use Data key caching
- C. Create an alias of the key
- D. Use the right key policy

Answer: B

Explanation:

The AWS Documentation mentions the following

Data key caching stores data keys and related cryptographic material in a cache. When you encrypt or decrypt data, the AWS Encryption SDK looks for a matching data key in the cache. If it finds a match, it uses the cached data key rather than generating a new one. Data key caching can improve performance, reduce cost, and help you stay within service limits as your application scales. Option A, C and D are all incorrect since these options will not impact how the key is used.

For more information on data key caching, please refer to below URL: <https://docs.aws.amazon.com/encryption-sdk/latest/developer-guide/data-key-cache.html>

The correct answer is: Use Data key caching Submit your Feedback/Queries to our Experts

NEW QUESTION 121

A company has set up the following structure to ensure that their S3 buckets always have logging enabled

If there are any changes to the configuration to an S3 bucket, a config rule gets checked. If logging is disabled, then Lambda function is invoked. This Lambda function will again enable logging on the S3 bucket. Now there is an issue being encountered with the entire flow. You have verified that the Lambda function is being invoked. But when logging is disabled for the bucket, the lambda function does not enable it again. Which of the following could be an issue Please select:

- A. The AWS Config rule is not configured properly
- B. The AWS Lambda function does not have appropriate permissions for the bucket
- C. The AWS Lambda function should use Node.js instead of python.
- D. You need to also use the API gateway to invoke the lambda function

Answer: B

Explanation:

The most probable cause is that you have not allowed the Lambda functions to have the appropriate permissions on the S3 bucket to make the relevant changes. Option A is invalid because this is more of a permission instead of a configuration rule issue. Option C is invalid because changing the language will not be the core solution.

Option D is invalid because you don't necessarily need to use the API gateway service

For more information on accessing resources from a Lambda function, please refer to below URL <https://docs.aws.amazon.com/lambda/latest/ds/accessing-resources.html>

The correct answer is: The AWS Lambda function does not have appropriate permissions for the bucket Submit your Feedback/Queries to our Experts

NEW QUESTION 125

Your company hosts a large section of EC2 instances in AWS. There are strict security rules governing the EC2 Instances. During a potential security breach, you need to ensure quick investigation of the underlying EC2 Instance. Which of the following service can help you quickly provision a test environment to look into the breached instance.

Please select:

- A. AWS Cloudwatch
- B. AWS CloudFormation
- C. AWS Cloudtrail
- D. AWS Config

Answer: B

Explanation:

The AWS Security best practices mentions the following

Unique to AWS, security practitioners can use CloudFormation to quickly create a new, trusted environment in which to conduct deeper investigation. The CloudFormation template can preconfigure instances in an isolated environment that contains all the necessary tools forensic teams

need to determine the cause of the incident This cuts down on the time it takes to gather necessary tools, isolates systems under examination, and ensures that the team is operating in a clean room. Option A is incorrect since this is a logging service and cannot be used to provision a test environment

Option C is incorrect since this is an API logging service and cannot be used to provision a test environment

Option D is incorrect since this is a configuration service and cannot be used to provision a test environment

For more information on AWS Security best practises, please refer to below URL: <https://d1.awsstatic.com/whitepapers/architecture/AWS-Security-Pillar.pdf>

The correct answer is: AWS Cloudformation Submit your Feedback/Queries to our Experts

NEW QUESTION 130

Your company has a set of EBS volumes defined in AWS. The security mandate is that all EBS volumes are encrypted. What can be done to notify the IT admin staff if there are any unencrypted volumes in the account.

Please select:

- A. Use AWS Inspector to inspect all the EBS volumes
- B. Use AWS Config to check for unencrypted EBS volumes
- C. Use AWS Guard duty to check for the unencrypted EBS volumes
- D. Use AWS Lambda to check for the unencrypted EBS volumes

Answer: B

Explanation:

The enc config rule for AWS Config can be used to check for unencrypted volumes. encrypted-volumn

5 volumes that are in an attached state are encrypted. If you specify the ID of a KMS key for encryptio using the kmsId parameter, the rule checks if the EBS volumes in an attached state are encrypted

with that KMS key*1.

Options A and C are incorrect since these services cannot be used to check for unencrypted EBS volumes

Option D is incorrect because even though this is possible, trying to implement the solution alone with just the Lambda servk would be too difficult

For more information on AWS Config and encrypted volumes, please refer to below URL:

<https://docs.aws.amazon.com/config/latest/developerguide/encrypted-volumes.html> Submit your Feedback/Queries to our Experts

NEW QUESTION 132

You have a bucket and a VPC defined in AWS. You need to ensure that the bucket can only be accessed by the VPC endpoint. How can you accomplish this?

Please select:

- A. Modify the security groups for the VPC to allow access to the S3 bucket
- B. Modify the route tables to allow access for the VPC endpoint
- C. Modify the IAM Policy for the bucket to allow access for the VPC endpoint
- D. Modify the bucket Policy for the bucket to allow access for the VPC endpoint

Answer: D

Explanation:

This is mentioned in the AWS Documentation Restricting Access to a Specific VPC Endpoint

The following is an example of an S3 bucket policy that restricts access to a specific bucket,

examplebucket only from the VPC endpoint with the ID vpce-la2b3c4d. The policy denies all access to the bucket if the specified endpoint is not being used. The aws:sourceVpce condition is used to the specify the endpoint. The aws:sourceVpce condition does not require an ARN for the VPC endpoint resource, only the VPC endpoint ID. For more information about using conditions in a policy, see Specifying Conditions in a Policy.

Options A and B are incorrect because using Security Groups nor route tables will help to allow access specifically for that bucke via the VPC endpoint Here you specifically need to ensure the bucket policy is changed.

Option C is incorrect because it is the bucket policy that needs to be changed and not the IAM policy. For more information on example bucket policies for VPC endpoints, please refer to below URL: <https://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies-vpc-endpoint.html>

The correct answer is: Modify the bucket Policy for the bucket to allow access for the VPC endpoint Submit your Feedback/Queries to our Experts

NEW QUESTION 137

Which of the following is the responsibility of the customer? Choose 2 answers from the options given below.

Please select:

- A. Management of the Edge locations
- B. Encryption of data at rest
- C. Protection of data in transit
- D. Decommissioning of old storage devices

Answer: BC

Explanation:

Below is the snapshot of the Shared Responsibility Model

For more information on AWS Security best practises, please refer to below URL

[.awsstatic.com/whitepapers/Security/AWS_Practices.pdf](https://d1.awsstatic.com/whitepapers/Security/AWS_Practices.pdf)

The correct answers are: Encryption of data at rest Protection of data in transit Submit your Feedback/Queries to our Experts

NEW QUESTION 139

You want to track access requests for a particular S3 bucket. How can you achieve this in the easiest possible way?

Please select:

- A. Enable server access logging for the bucket
- B. Enable Cloudwatch metrics for the bucket
- C. Enable Cloudwatch logs for the bucket
- D. Enable AWS Config for the S3 bucket

Answer: A

Explanation:

The AWS Documentation mentions the foil

To track requests for access to your bucket you can enable access logging. Each access log record provides details about a single access request, such as the requester, bucket name, request time, request action, response status, and error code, if any.

Options B and C are incorrect Cloudwatch is used for metrics and logging and cannot be used to track access requests.

Option D is incorrect since this can be used for Configuration management but for not for tracking S3 bucket requests.

For more information on S3 server logs, please refer to below UF <https://docs.aws.amazon.com/AmazonS3/latest/dev/ServerLoes.html>

The correct answer is: Enable server access logging for the bucket Submit your Feedback/Queries to our Experts

NEW QUESTION 140

Your team is designing a web application. The users for this web application would need to sign in via an external ID provider such asfacebook or Google. Which of the following AWS service would you use for authentication?

Please select:

- A. AWS Cognito
- B. AWS SAML
- C. AWS IAM
- D. AWS Config

Answer: A

Explanation:

The AWS Documentation mentions the following

Amazon Cognito provides authentication, authorization, and user management for your web and mobile apps. Your users can sign in directly with a user name and password, or through a third party such as Facebook, Amazon, or Google.

Option B is incorrect since this is used for identity federation

Option C is incorrect since this is pure Identity and Access management Option D is incorrect since AWS is a configuration service

For more information on AWS Cognito please refer to the below Link: <https://docs.aws.amazon.com/cognito/latest/developerguide/what-is-amazon-cognito.html>

The correct answer is: AWS Cognito

Submit your Feedback/Queries to our Experts

NEW QUESTION 145

Your application currently use AWS Cognito for authenticating users. Your application consists of different types of users. Some users are only allowed read access to the application and others are given contributor access. How would you manage the access effectively?

Please select:

- A. Create different cognito endpoints, one for the readers and the other for the contributors.
- B. Create different cognito groups, one for the readers and the other for the contributors.
- C. You need to manage this within the application itself
- D. This needs to be managed via Web security tokens

Answer: B

Explanation:

The AWS Documentation mentions the following

You can use groups to create a collection of users in a user pool, which is often done to set the permissions for those users. For example, you can create separate groups for users who are readers, contributors, and editors of your website and app.

Option A is incorrect since you need to create cognito groups and not endpoints

Options C and D are incorrect since these would be overheads when you can use AWS Cognito For more information on AWS Cognito user groups please refer to the below Link: <https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-user-pools-user-groups.html> The correct answer is: Create different cognito groups, one for the readers and the other for the contributors. Submit your Feedback/Queries to our Experts

NEW QUESTION 146

Your company has a hybrid environment, with on-premise servers and servers hosted in the AWS cloud. They are planning to use the Systems Manager for patching servers. Which of the following is a pre-requisite for this to work;

Please select:

- A. Ensure that the on-premise servers are running on Hyper-V.
- B. Ensure that an IAM service role is created
- C. Ensure that an IAM User is created
- D. Ensure that an IAM Group is created for the on-premise servers

Answer: B

Explanation:

You need to ensure that an IAM service role is created for allowing the on-premise servers to communicate with the AWS Systems Manager.

Option A is incorrect since it is not necessary that servers should only be running Hyper-V Options C and D are incorrect since it is not necessary that IAM users and groups are created For more information on the Systems Manager role please refer to the below URL:

[.com/systems-manager/latest/userguide/sysman-!](https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-!)

The correct answer is: Ensure that an IAM service role is created Submit your Feedback/Queries to our Experts

NEW QUESTION 149

You have several S3 buckets defined in your AWS account. You need to give access to external AWS accounts to these S3 buckets. Which of the following can allow you to define the permissions for the external accounts? Choose 2 answers from the options given below

Please select:

- A. IAM policies

- B. Buckets ACL's
- C. IAM users
- D. Bucket policies

Answer: BD

Explanation:

The AWS Security whitepaper gives the type of access control and to what level the control can be given

Options A and C are incorrect since for external access to buckets, you need to use either Bucket policies or Bucket ACL's or more information on Security for storage services role please refer to the below URL:

[https://d1.awsstatic.com/whitepapers/Security/Security Storage Services Whitepaper.pdf](https://d1.awsstatic.com/whitepapers/Security/Security%20Storage%20Services%20Whitepaper.pdf) The correct answers are: Buckets ACL's, Bucket policies

Submit your Feedback/Queries to our Experts

NEW QUESTION 154

A large organization is planning on AWS to host their resources. They have a number of autonomous departments that wish to use AWS. What could be the strategy to adopt for managing the accounts. Please select:

- A. Use multiple VPCs in the account each VPC for each department
- B. Use multiple IAM groups, each group for each department
- C. Use multiple IAM roles, each group for each department
- D. Use multiple AWS accounts, each account for each department

Answer: D

Explanation:

A recommendation for this is given in the AWS Security best practices

Option A is incorrect since this would be applicable for resources in a VPC Options B and C are incorrect since operationally it would be difficult to manage For more information on AWS Security best practices please refer to the below URL

[https://d1.awsstatic.com/whitepapers/Security/AWS Security Best Practices.pdf](https://d1.awsstatic.com/whitepapers/Security/AWS%20Security%20Best%20Practices.pdf)

The correct answer is: Use multiple AWS accounts, each account for each department Submit your Feedback/Queries to our Experts

NEW QUESTION 156

You have been given a new brief from your supervisor for a client who needs a web application set up on AWS. The a most important requirement is that MySQL must be used as the database, and this database must not be hosted in the public cloud, but rather at the client's data center due to security risks. Which of the following solutions would be the ^ best to assure that the client's requirements are met? Choose the correct answer from the options below Please select:

- A. Build the application server on a public subnet and the database at the client's data center
- B. Connect them with a VPN connection which uses IPsec.
- C. Use the public subnet for the application server and use RDS with a storage gateway to access and synchronize the data securely from the local data center.
- D. Build the application server on a public subnet and the database on a private subnet with a NAT instance between them.
- E. Build the application server on a public subnet and build the database in a private subnet with a secure ssh connection to the private subnet from the client's data center.

Answer: A

Explanation:

Since the database should not be hosted on the cloud all other options are invalid. The best option is to create a VPN connection for securing traffic as shown below.

Option B is invalid because this is the incorrect use of the Storage gateway Option C is invalid since this is the incorrect use of the NAT instance Option D is invalid since this is an incorrect configuration For more information on VPN connections, please visit the below URL

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html

The correct answer is: Build the application server on a public subnet and the database at the client's data center. Connect them with a VPN connection which uses IPsec

Submit your Feedback/Queries to our Experts

NEW QUESTION 160

A company has been using the AWS KMS service for managing its keys. They are planning on carrying out housekeeping activities and deleting keys which are no longer in use. What are the ways that can be incorporated to see which keys are in use? Choose 2 answers from the options given below

Please select:

- A. Determine the age of the master key
- B. See who is assigned permissions to the master key
- C. See Cloudtrail for usage of the key
- D. Use AWS cloudwatch events for events generated for the key

Answer: BC

Explanation:

The direct ways that can be used to see how the key is being used is to see the current access permissions and cloudtrail logs

Option A is invalid because seeing how long ago the key was created would not determine the usage of the key

Option D is invalid because Cloudtrail Event is better for seeing for events generated by the key This is also mentioned in the AWS Documentation

Examining CMK Permissions to Determine the Scope of Potential Usage

Determining who or what currently has access to a customer master key (CMK) might help you determine how widely the CM was used and whether it is still needed. To learn how to determine who or what currently has access to a CMK, go to Determining Access to an AWS KMS Customer Master Key.

Examining AWS CloudTrail Logs to Determine Actual Usage

AWS KMS is integrated with AWS CloudTrail, so all AWS KMS API activity is recorded in CloudTrail log files. If you have CloudTrail turned on in the region where your customer master key (CMK) is

located, you can examine your CloudTrail log files to view a history of all AWS KMS API activity for a particular CMK, and thus its usage history. You might be able to use a CMK's usage history to help you determine whether or not you still need it

For more information on determining the usage of CMK keys, please visit the following URL: <https://docs.aws.amazon.com/kms/latest/developerguide/deleting-keys-determining-usage.html>

The correct answers are: See who is assigned permissions to the master key. See Cloudtrail for usage of the key Submit your Feedback/Queries to our Experts

NEW QUESTION 161

Which of the following is the correct sequence of how KMS manages the keys when used along with the Redshift cluster service

Please select:

- A. The master keys encrypts the cluster ke
- B. The cluster key encrypts the database ke
- C. The database key encrypts the data encryption keys.
- D. The master keys encrypts the database ke
- E. The database key encrypts the data encryption keys.
- F. The master keys encrypts the data encryption key
- G. The data encryption keys encrypts the database key
- H. The master keys encrypts the cluster key, database key and data encryption keys

Answer: A

Explanation:

This is mentioned in the AWS Documentation

Amazon Redshift uses a four-tier, key-based architecture for encryption. The architecture consists of data encryption keys, a database key, a cluster key, and a master key.

Data encryption keys encrypt data blocks in the cluster. Each data block is assigned a randomly generated AES-256 key. These keys are encrypted by using the database key for the cluster.

The database key encrypts data encryption keys in the cluster. The database key is a randomly generated AES-256 key. It is stored on disk in a separate network from the Amazon Redshift cluster and passed to the cluster across a secure channel.

The cluster key encrypts the database key for the Amazon Redshift cluster.

Option B is incorrect because the master key encrypts the cluster key and not the database key Option C is incorrect because the master key encrypts the cluster key and not the data encryption keys

Option D is incorrect because the master key encrypts the cluster key only

For more information on how keys are used in Redshift, please visit the following URL: <https://docs.aws.amazon.com/kms/latest/developerguide/services-redshift.html>

The correct answer is: The master keys encrypts the cluster key. The cluster key encrypts the database key. The database key encrypts the data encryption keys. Submit your Feedback/Queries to our Experts

NEW QUESTION 164

A company wants to use Cloudtrail for logging all API activity. They want to segregate the logging of data events and management events. How can this be achieved? Choose 2 answers from the options given below
Please select:

- A. Create one Cloudtrail log group for data events
- B. Create one trail that logs data events to an S3 bucket
- C. Create another trail that logs management events to another S3 bucket
- D. Create another Cloudtrail log group for management events

Answer: BC

Explanation:

The AWS Documentation mentions the following

You can configure multiple trails differently so that the trails process and log only the events that you specify. For example, one trail can log read-only data and management events, so that all read-only events are delivered to one S3 bucket. Another trail can log only write-only data and management events, so that all write-only events are delivered to a separate S3 bucket

Options A and D are invalid because you have to create a trail and not a log group

For more information on managing events with cloudtrail, please visit the following URL:

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/loHEing-manasement-and-dataevents-with-cloudtrai>

The correct answers are: Create one trail that logs data events to an S3 bucket. Create another trail that logs management events to another S3 bucket

Submit your Feedback/Queries to our Experts

NEW QUESTION 165

Your company has been using AWS for hosting EC2 Instances for their web and database applications. They want to have a compliance check to see the following

Whether any ports are left open other than admin ones like SSH and RDP

Whether any ports to the database server other than ones from the web server security group are

open Which of the following can help achieve this in the easiest way possible. You don't want to carry out an extra configuration changes?

Please select:

- A. AWS Config
- B. AWS Trusted Advisor
- C. AWS Inspector
- D. AWS GuardDuty

Answer: B

Explanation:

Trusted Advisor checks for compliance with the following security recommendations:

Limited access to common administrative ports to only a small subset of addresses. This includes ports 22 (SSH), 23 (Telnet) 3389 (RDP), and 5500 (VNC).

Limited access to common database ports. This includes ports 1433 (MSSQL Server), 1434 (MSSQL Monitor), 3306 (MySQL), Oracle (1521) and 5432 (PostgreSQL).

Option A is partially correct but then you would need to write custom rules for this. The AWS trusted advisor can give you all o these checks on its dashboard

Option C is incorrect. Amazon Inspector needs a software agent to be installed on all EC2 instances that are included in th.

assessment target, the security of which you want to evaluate with Amazon Inspector. It monitors the behavior of the EC2

instance on which it is installed, including network, file system, and process activity, and collects a wide set of behavior and

configuration data (telemetry), which it then passes to the Amazon Inspector service.

Our question's requirement is to choose a choice that is easy to implement. Hence Trusted Advisor is more appropriate for this) question.

Options D is invalid because this service dont provide these details.

For more information on the Trusted Advisor, please visit the following URL <https://aws.amazon.com/premiumsupport/trustedadvisor>

The correct answer is: AWS Trusted Advisor Submit your Feedback/Queries to our Experts

NEW QUESTION 167

An application is designed to run on an EC2 Instance. The application needs to work with an S3 bucket. From a security perspective, what is the ideal way for the EC2 instance/application to be configured?

Please select:

- A. Use the AWS access keys ensuring that they are frequently rotated.
- B. Assign an IAM user to the application that has specific access to only that S3 bucket
- C. Assign an IAM Role and assign it to the EC2 Instance
- D. Assign an IAM group and assign it to the EC2 Instance

Answer: C

Explanation:

The below diagram from the AWS whitepaper shows the best security practice of allocating a role that has access to the S3 bucket

Options A, B and D are invalid because using users, groups or access keys is an invalid security practice when giving access to resources from other AWS resources.

For more information on the Security Best practices, please visit the following URL: https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf

The correct answer is: Assign an IAM Role and assign it to the EC2 Instance Submit your Feedback/Queries to our Experts

NEW QUESTION 171

Which of the below services can be integrated with the AWS Web application firewall service. Choose 2 answers from the options given below

Please select:

- A. AWS CloudFront
- B. AWS Lambda
- C. AWS Application Load Balancer
- D. AWS Classic Load Balancer

Answer: AC

Explanation:

The AWS documentation mentions the following on the Application Load Balancer

AWS WAF can be deployed on Amazon CloudFront and the Application Load Balancer (ALB). As part of Amazon CloudFront it can be part of your Content Distribution Network (CDN) protecting your resources and content at the Edge locations and as part of the Application Load Balancer it can protect your origin web servers running behind the ALBs.

Options B and D are invalid because only CloudFront and the Application Load Balancer services are supported by AWS WAF.

For more information on the web application firewall please refer to the below URL: <https://aws.amazon.com/waf/faq>;

The correct answers are: AWS CloudFront AWS Application Load Balancer Submit your Feedback/Queries to our Experts

NEW QUESTION 173

An organization has launched 5 instances: 2 for production and 3 for testing. The organization wants that one particular group of IAM users should only access the test instances and not the production ones. How can the organization set that as a part of the policy?

Please select:

- A. Launch the test and production instances in separate regions and allow region wise access to the group
- B. Define the IAM policy which allows access based on the instance ID
- C. Create an IAM policy with a condition which allows access to only small instances
- D. Define the tags on the test and production servers and add a condition to the IAM policy which allows access to specification tags

Answer: D

Explanation:

Tags enable you to categorize your AWS resources in different ways, for example, by purpose, owner, or environment. This is useful when you have many

resources of the same type — you can quickly identify a specific resource based on the tags you've assigned to it

Option A is invalid because this is not a recommended practices

Option B is invalid because this is an overhead to maintain this in policies Option C is invalid because the instance type will not resolve the requirement For information on resource tagging, please visit the below URL: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Usine_Tags.html

The correct answer is: Define the tags on the test and production servers and add a condition to the 1AM policy which allows access to specific tags

Submit your Feedback/Queries to our Experts

NEW QUESTION 175

Your company is planning on AWS on hosting its AWS resources. There is a company policy which mandates that all security keys are completely managed within the company itself. Which of the following is the correct measure of following this policy?

Please select:

- A. Using the AWS KMS service for creation of the keys and the company managing the key lifecycle thereafter.
- B. Generating the key pairs for the EC2 Instances using puttygen
- C. Use the EC2 Key pairs that come with AWS
- D. Use S3 server-side encryption

Answer: B

Explanation:

y ensuring that you generate the key pairs for EC2 Instances, you will have complete control of the access keys.

Options A,C and D are invalid because all of these processes means that AWS has ownership of the keys. And the question specifically mentions that you need ownership of the keys

For information on security for Compute Resources, please visit the below URL: <https://d1.awsstatic.com/whitepapers/Security/Security Compute Services Whitepaper.pdf>

The correct answer is: Generating the key pairs for the EC2 Instances using puttygen Submit your Feedback/Queries to our Experts

NEW QUESTION 178

A company has a set of EC2 instances hosted in AWS. These instances have EBS volumes for storing critical information. There is a business continuity requirement and in order to boost the agility of the business and to ensure data durability which of the following options are not required.

Please select:

- A. Use lifecycle policies for the EBS volumes
- B. Use EBS Snapshots
- C. Use EBS volume replication
- D. Use EBS volume encryption

Answer: CD

Explanation:

Data stored in Amazon EBS volumes is redundantly stored in multiple physical locations as part of normal operation of those services and at no additional charge. However, Amazon EBS replication is stored within the same availability zone, not across multiple zones; therefore, it is highly recommended that you conduct regular snapshots to Amazon S3 for long-term data durability.

You can use Amazon Data Lifecycle Manager (Amazon DLM) to automate the creation, retention, and deletion of snapshots taken to back up your Amazon EBS volumes.

With lifecycle management, you can be sure that snapshots are cleaned up regularly and keep costs under control.

EBS Lifecycle Policies

A lifecycle policy consists of these core settings:

- Resource type—The AWS resource managed by the policy, in this case, EBS volumes.
- Target tag—The tag that must be associated with an EBS volume for it to be managed by the policy.
- Schedule—Defines how often to create snapshots and the maximum number of snapshots to keep. Snapshot creation starts within an hour of the specified start time. If creating a new snapshot exceeds the maximum number of snapshots to keep for the volume, the oldest snapshot is deleted.

Option C is correct. Each Amazon EBS volume is automatically replicated within its Availability Zone to protect you from component failure, offering high availability and durability. But it does not have an explicit feature like that.

Option D is correct Encryption does not ensure data durability

For information on security for Compute Resources, please visit the below URL <https://d1.awsstatic.com/whitepapers/Security/Security Compute Services Whitepaper.pdf>

The correct answers are: Use EBS volume replication. Use EBS volume encryption Submit your Feedback/Queries to our Experts

NEW QUESTION 182

The CFO of a company wants to allow one of his employees to view only the AWS usage report page. Which of the below mentioned 1AM policy statements allows the user to have access to the AWS usage report page?

Please select:

- A. "Effect": "Allow". "Action": ["Describe"], "Resource": "Billing"
- B. "Effect": "Allow", "Action": ["AccountUsage"], "Resource": "**"
- C. "Effect": "Allow", "Action": ["aws-portal:ViewUsage", "aws-portal:ViewBilling"], "Resource": "**"
- D. "Effect": "Allow", "Action": ["aws-portal: ViewBilling"], "Resource": "**"

Answer: C

Explanation:

the aws documentation, below is the access required for a user to access the Usage reports page and as per this, Option C is the right answer.

NEW QUESTION 185

Your company has the following setup in AWS

- A. A set of EC2 Instances hosting a web application
- B. An application load balancer placed in front of the EC2 Instances
- C. Which of the following can be used to protect against these requests? Please select:
- D. Use Security Groups to block the IP addresses
- E. Use VPC Flow Logs to block the IP addresses
- F. Use AWS inspector to block the IP addresses
- G. Use AWS WAF to block the IP addresses

Answer: D

Explanation:

Your answer is incorrect Answer -D

The AWS Documentation mentions the following on AWS WAF which can be used to protect Application Load Balancers and Cloud front

A web access control list (web ACL) gives you fine-grained control over the web requests that your Amazon CloudFront distributions or Application Load Balancers respond to. You can allow or block the following types of requests:

Originate from an IP address or a range of IP addresses Originate from a specific country or countries

Contain a specified string or match a regular expression (regex) pattern in a particular part of requests

Exceed a specified length

Appear to contain malicious SQL code (known as SQL injection)

Appear to contain malicious scripts (known as cross-site scripting)

Option A is invalid because by default Security Groups have the Deny policy

Options B and C are invalid because these services cannot be used to block IP addresses For information on AWS WAF, please visit the below URL:

<https://docs.aws.amazon.com/waf/latest/developerguide/web-acl.html>

The correct answer is: Use AWS WAF to block the IP addresses Submit your Feedback/Queries to our Experts

NEW QUESTION 190

You are creating a Lambda function which will be triggered by a Cloudwatch Event. The data from these events needs to be stored in a DynamoDB table. How should the Lambda function be given access to the DynamoDB table?

Please select:

- A. Put the AWS Access keys in the Lambda function since the Lambda function by default is secure
- B. Use an IAM role which has permissions to the DynamoDB table and attach it to the Lambda function.
- C. Use the AWS Access keys which has access to DynamoDB and then place it in an S3 bucket.
- D. Create a VPC endpoint for the DynamoDB table
- E. Access the VPC endpoint from the Lambda function.

Answer: B

Explanation:

AWS Lambda functions uses roles to interact with other AWS services. So use an IAM role which has permissions to the DynamoDB table and attach it to the Lambda function.

Options A and C are all invalid because you should never use AWS keys for access. Option D is invalid because the VPC endpoint is used for VPCs

For more information on Lambda function Permission model, please visit the URL <https://docs.aws.amazon.com/lambda/latest/dg/intro-permission-model.html>

The correct answer is: Use an IAM role which has permissions to the DynamoDB table and attach it to the Lambda function. Submit your Feedback/Queries to our Experts

NEW QUESTION 195

There is a set of EC2 Instances in a private subnet. The application hosted on these EC2 Instances need to access a DynamoDB table. It needs to be ensured that traffic does not flow out to the internet. How can this be achieved?

Please select:

- A. Use a VPC endpoint to the DynamoDB table
- B. Use a VPN connection from the VPC
- C. Use a VPC gateway from the VPC
- D. Use a VPC Peering connection to the DynamoDB table

Answer: A

Explanation:

The following diagram from the AWS Documentation shows how you can access the DynamoDB service from within a V without going to the Internet This can be done with the help of a VPC endpoint

Option B is invalid because this is used for connection between an on-premise solution and AWS Option C is invalid because there is no such option

Option D is invalid because this is used to connect 2 VPCs

For more information on VPC endpoints for DynamoDB, please visit the URL:

The correct answer is: Use a VPC endpoint to the DynamoDB table Submit your Feedback/Queries to our Experts

NEW QUESTION 200

You need to establish a secure backup and archiving solution for your company, using AWS. Documents should be immediately accessible for three months and available for five years for compliance reasons. Which AWS service fulfills these requirements in the most cost-effective way?

Choose the correct answer

Please select:

- A. Upload data to S3 and use lifecycle policies to move the data into Glacier for long-term archiving.
- B. Upload the data on EBS, use lifecycle policies to move EBS snapshots into S3 and later into Glacier for long-term archiving.
- C. Use Direct Connect to upload data to S3 and use IAM policies to move the data into Glacier for long-term archiving.

D. Use Storage Gateway to store data to S3 and use lifecycle policies to move the data into Redshift for long-term archiving.

Answer: A

Explanation:

amazon Glacier is a secure, durable, and extremely low-cost cloud storage service for data archiving and long-term backup. Customers can reliably store large or small amounts of data for as little as \$0,004 per gigabyte per month, a significant savings compared to on-premises solutions. With Amazon lifecycle policies you can create transition actions in which you define when objects transition to another Amazon S3 storage class. For example, you may choose to transition objects to the STANDARD_IA (IA, for infrequent access) storage class 30 days after creation, or archive objects to the GLACIER storage class one year after creation. Option B is invalid because lifecycle policies are not available for EBS volumes Option C is invalid because IAM policies cannot be used to move data to Glacier Option D is invalid because lifecycle policies is not used to move data to Redshift For more information on S3 lifecycle policies, please visit the URL: <http://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html> The correct answer is: Upload data to S3 and use lifecycle policies to move the data into Glacier for long-term archiving. Submit your Feedback/Queries to our Experts

NEW QUESTION 204

Your company is hosting a set of EC2 Instances in AWS. They want to have the ability to detect if any port scans occur on their AWS EC2 Instances. Which of the following can help in this regard?
Please select:

- A. Use AWS inspector to consciously inspect the instances for port scans
- B. Use AWS Trusted Advisor to notify of any malicious port scans
- C. Use AWS Config to notify of any malicious port scans
- D. Use AWS Guard Duty to monitor any malicious port scans

Answer: D

Explanation:

The AWS blogs mention the following to support the use of AWS GuardDuty
GuardDuty voraciously consumes multiple data streams, including several threat intelligence feeds, staying aware of malicious addresses, devious domains, and more importantly, learning to accurately identify malicious or unauthorized behavior in your AWS accounts. In combination with information gleaned from your VPC Flow Logs, AWS CloudTrail Event Logs, and DNS logs, th allows GuardDuty to detect many different types of dangerous and mischievous behavior including probes for known vulnerabilities, port scans and probes, and access from unusual locations. On the AWS side, it looks for suspicious AWS account activity such as unauthorized deployments, unusual CloudTrail activity, patterns of access to AWS API functions, and attempts to exceed multiple service limits. GuardDuty will also look for compromised EC2 instances talking to malicious entities or services, data exfiltration attempts, and instances that are mining cryptocurrency. Options A, B and C are invalid because these services cannot be used to detect port scans For more information on AWS Guard Duty, please refer to the below Link: <https://aws.amazon.com/blogs/aws/amazon-guardduty-continuous-security-monitoring-threatdetection/>; (The correct answer is: Use AWS Guard Duty to monitor any malicious port scans Submit your Feedback/Queries to our Experts

NEW QUESTION 207

You have an Amazon VPC that has a private subnet and a public subnet in which you have a NAT instance server. You have created a group of EC2 instances that configure themselves at startup by downloading a bootstrapping script from S3 that deploys an application via GIT.
Which one of the following setups would give us the highest level of security? Choose the correct answer from the options given below.
Please select:

- A. EC2 instances in our public subnet, no EIPs, route outgoing traffic via the IGW
- B. EC2 instances in our public subnet, assigned EIPs, and route outgoing traffic via the NAT
- C. EC2 instance in our private subnet, assigned EIPs, and route our outgoing traffic via our IGW
- D. EC2 instances in our private subnet, no EIPs, route outgoing traffic via the NAT

Answer: D

Explanation:

The below diagram shows how the NAT instance works. To make EC2 instances very secure, they need to be in a private sub such as the database server shown below with no EIP and all traffic routed via the NAT.

Options A and B are invalid because the instances need to be in the private subnet
Option C is invalid because since the instance needs to be in the private subnet, you should not attach an EIP to the instance
For more information on NAT instance, please refer to the below Link: <http://docs.aws.amazon.com/AmazonVPC/latest/UserGuideA/PC Instance.html>!
The correct answer is: EC2 instances in our private subnet no EIPs, route outgoing traffic via the NAT Submit your Feedback/Queries to our Experts

NEW QUESTION 208

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual AWS-Certified-Security-Specialty 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-Security-Specialty Product From:

<https://www.2passeasy.com/dumps/AWS-Certified-Security-Specialty/>

Money Back Guarantee

AWS-Certified-Security-Specialty Practice Exam Features:

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