

Amazon

Exam Questions AWS-Certified-Security-Specialty

Amazon 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 designing a custom IAM policy that would allow users to list buckets in S3 only if they are MFA authenticated. Which of the following would best match this requirement?

A.

B.

C.

D.

A.

Answer: A

Explanation:

The Condition clause can be used to ensure users can only work with resources if they are MFA authenticated.

Option B and C are wrong since the `aws:MultiFactorAuthPresent` clause should be marked as true. Here you are saying that only if the user has been MFA activated, that means it is true, then allow access.

Option D is invalid because the `Bool` clause is missing in the evaluation for the condition clause. Boolean conditions let you construct Condition elements that restrict access based on comparing a key to "true" or "false."

Here in this scenario the `Bool` attribute in the condition element will return a value True for option A which will ensure that access is allowed on S3 resources.

For more information on an example on such a policy, please visit the following URL:

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

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 5

You have an EC2 Instance in a private subnet which needs to access the KMS service. Which of the following methods can help fulfil this requirement, keeping security in perspective
Please select:

- A. Use a VPC endpoint
- B. Attach an Internet gateway to the subnet
- C. Attach a VPN connection to the VPC
- D. Use VPC Peering

Answer: A

Explanation:

The AWS Documentation mentions the following

You can connect directly to AWS KMS through a private endpoint in your VPC instead of connecting over the internet. When you use a VPC endpoint communication between your VPC and AWS KMS is conducted entirely within the AWS network.

Option B is invalid because this could open threats from the internet

Option C is invalid because this is normally used for communication between on-premise environments and AWS.

Option D is invalid because this is normally used for communication between VPCs

For more information on accessing KMS via an endpoint, please visit the following URL <https://docs.aws.amazon.com/kms/latest/developerguide/kms-vpc-endpoint.html>

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

NEW QUESTION 6

Your company has a set of resources defined in the AWS Cloud. Their IT audit department has requested to get a list of resources that have been defined across the account. How can this be achieved in the easiest manner? Please select:

- A. Create a powershell script using the AWS CLI
- B. Query for all resources with the tag of production.
- C. Create a bash shell script with the AWS CLI
- D. Query for all resources in all region
- E. Store the results in an S3 bucket.
- F. Use Cloud Trail to get the list of all resources
- G. Use AWS Config to get the list of all resources

Answer: D

Explanation:

The most feasible option is to use AWS Config. When you turn on AWS Config, you will get a list of resources defined in your AWS Account.

A sample snapshot of the resources dashboard in AWS Config is shown below

Option A is incorrect because this would give the list of production based resources and not all resources

Option B is partially correct But this will just add more maintenance overhead.

Option C is incorrect because this can be used to log API activities but not give an account of all resources For more information on AWS Config, please visit the below URL: <https://docs.aws.amazon.com/config/latest/developerguide/how-does-config-work.html>

The correct answer is: Use AWS Config to get the list of all resources Submit your Feedback/Queries to our Experts

NEW QUESTION 7

A Lambda function reads metadata from an S3 object and stores the metadata in a DynamoDB table.

The function is triggered whenever an object is stored within the S3 bucket.

How should the Lambda function be given access to the DynamoDB table? Please select:

- A. Create a VPC endpoint for DynamoDB within a VPC
- B. Configure the Lambda function to access resources in the VPC.
- C. Create a resource policy that grants the Lambda function permissions to write to the DynamoDB table

- D. Attach the poll to the DynamoDB table.
- E. Create an IAM user with permissions to write to the DynamoDB table.
- F. Store an access key for that user in the Lambda environment variables.
- G. Create an IAM service role with permissions to write to the DynamoDB table.
- H. Associate that role with the Lambda function.

Answer: D

Explanation:

The ideal way is to create an IAM role which has the required permissions and then associate it with the Lambda function

The AWS Documentation additionally mentions the following

Each Lambda function has an IAM role (execution role) associated with it. You specify the IAM role when you create your Lambda function. Permissions you grant to this role determine what AWS Lambda can do when it assumes the role. There are two types of permissions that you grant to the IAM role:

If your Lambda function code accesses other AWS resources, such as to read an object from an S3 bucket or write logs to CloudWatch Logs, you need to grant permissions for relevant Amazon S3 and CloudWatch actions to the role.

If the event source is stream-based (Amazon Kinesis Data Streams and DynamoDB streams), AWS Lambda polls these streams on your behalf. AWS Lambda needs permissions to poll the stream and read new records on the stream so you need to grant the relevant permissions to this role.

Option A is invalid because the VPC endpoint allows access instances in a private subnet to access DynamoDB

Option B is invalid because resource policies are present for resources such as S3 and KMS, but not AWS Lambda

Option C is invalid because AWS Roles should be used and not IAM Users

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

The correct answer is: Create an IAM service role with permissions to write to the DynamoDB table. Associate that role with the Lambda function.

Submit your Feedback/Queries to our Experts

NEW QUESTION 8

Your company has defined privileged users for their AWS Account. These users are administrators for key resources defined in the company. There is now a mandate to enhance the security

authentication for these users. How can this be accomplished?

Please select:

- A. Enable MFA for these user accounts
- B. Enable versioning for these user accounts
- C. Enable accidental deletion for these user accounts
- D. Disable root access for the users

Answer: A

Explanation:

The AWS Documentation mentions the following as a best practices for IAM users. For extra security, enable multi-factor authentication (MFA) for privileged IAM users (users who are allowed access to sensitive resources or APIs). With MFA, users have a device that generates unique authentication code (a one-time password, or OTP). Users must provide both their normal credentials (like their user name and password) and the OTP. The MFA device can either be a special piece of hardware, or it can be a virtual device (for example, it can run in an app on a smartphone).

Option B,C and D are invalid because no such security options are available in AWS For more information on IAM best practices, please visit the below URL

<https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html> The correct answer is: Enable MFA for these user accounts

Submit your Feedback/Queries to our Experts

NEW QUESTION 9

An application running on EC2 instances must use a username and password to access a database. The developer has stored those secrets in the SSM Parameter Store with type SecureString using the default KMS CMK. Which combination of configuration steps will allow the application to access the secrets via the API? Select 2 answers from the options below

Please select:

- A. Add the EC2 instance role as a trusted service to the SSM service role.
- B. Add permission to use the KMS key to decrypt to the SSM service role.
- C. Add permission to read the SSM parameter to the EC2 instance role.
- D. Add permission to use the KMS key to decrypt to the EC2 instance role
- E. Add the SSM service role as a trusted service to the EC2 instance role

Answer: CD

Explanation:

The below example policy from the AWS Documentation is required to be given to the EC2 Instance in order to read a secure string from AWS KMS. Permissions need to be given to the Get Parameter API and the KMS API call to decrypt the secret.

Option A is invalid because roles can be attached to EC2 and not EC2 roles to SSM Option B is invalid because the KMS key does not need to decrypt the SSM service role.

Option E is invalid because this configuration is valid For more information on the parameter store, please visit the below URL:

<https://docs.aws.amazon.com/kms/latest/developerguide/services-parameter-store.html>

The correct answers are: Add permission to read the SSM parameter to the EC2 instance role., Add permission to use the KMS key to decrypt to the EC2 instance role

Submit your Feedback/Queries to our Experts

NEW QUESTION 10

You have a 2 tier application hosted in AWS. It consists of a web server and database server (SQL Server) hosted on separate EC2 Instances. You are devising the security groups for these EC2 Instances. The Web tier needs to be accessed by users across the Internet. You have created a web security group(wg-123) and database security group(db-345). Which combination of the following security group rules will allow the application to be secure and functional. Choose 2 answers from the options given below.

Please select:

- A. wg-123 -Allow ports 80 and 443 from 0.0.0.0/0
- B. db-345 - Allow port 1433 from wg-123
- C. wg-123 - Allow port 1433 from wg-123
- D. db-345 -Allow ports 1433 from 0.0.0.0/0

Answer: AB

Explanation:

The Web security groups should allow access for ports 80 and 443 for HTTP and HTTPS traffic to all users from the internet.

The database security group should just allow access from the web security group from port 1433. Option C is invalid because this is not a valid configuration

Option D is invalid because database security should not be allowed on the internet For more information on Security Groups please visit the below URL:

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

The correct answers are: wg-123 - Allow ports 80 and 443 from 0.0.0.0/0, db-345 - Allow port 1433 from wg-123

Submit your Feedback/Queries to our Experts

NEW QUESTION 10

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 14

Your company has mandated that all calls to the AWS KMS service be recorded. How can this be achieved?

Please select:

- A. Enable logging on the KMS service
- B. Enable a trail in Cloudtrail
- C. Enable Cloudwatch logs
- D. Use Cloudwatch metrics

Answer: B

Explanation:

The AWS Documentation states the following

AWS KMS is integrated with CloudTrail, a service that captures API calls made by or on behalf of AWS KMS in your AWS account and delivers the log files to an Amazon S3 bucket that you specify. CloudTrail captures API calls from the AWS KMS console or from the AWS KMS API. Using the information collected by CloudTrail, you can determine what request was made, the source IP

address from which the request was made, who made the request when it was made, and so on. Option A is invalid because logging is not possible in the KMS service

Option C and D are invalid because Cloudwatch cannot be used to monitor API calls For more information on logging using Cloudtrail please visit the below URL

<https://docs.aws.amazon.com/kms/latest/developerguide/looking-usine-cloudtrail.html> The correct answer is: Enable a trail in Cloudtrail

Submit your Feedback/Queries to our Experts

NEW QUESTION 17

A company is using CloudTrail to log all AWS API activity for all regions in all of its accounts. The CISO has asked that additional steps be taken to protect the integrity of the log files.

What combination of steps will protect the log files from intentional or unintentional alteration? Choose 2 answers from the options given below

Please select:

- A. Create an S3 bucket in a dedicated log account and grant the other accounts write only access
- B. Deliver all log files from every account to this S3 bucket.
- C. Write a Lambda function that queries the Trusted Advisor Cloud Trail check
- D. Run the function every 10 minutes.
- E. Enable CloudTrail log file integrity validation
- F. Use Systems Manager Configuration Compliance to continually monitor the access policies of S3 buckets containing Cloud Trail logs.
- G. Create a Security Group that blocks all traffic except calls from the CloudTrail service
- H. Associate the security group with) all the Cloud Trail destination S3 buckets.

Answer: AC

Explanation:

The AWS Documentation mentions the following

To determine whether a log file was modified, deleted, or unchanged after CloudTrail delivered it you can use CloudTrail log file integrity validation. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.

Option B is invalid because there is no such thing as Trusted Advisor Cloud Trail checks Option D is invalid because Systems Manager cannot be used for this purpose.

Option E is invalid because Security Groups cannot be used to block calls from other services For more information on Cloudtrail log file validation, please visit the below URL: <https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-log-file-validation-intro.html>

For more information on delivering Cloudtrail logs from multiple accounts, please visit the below URL:

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-receive-logs-from-multipleaccounts.html>

The correct answers are: Create an S3 bucket in a dedicated log account and grant the other accounts write only access. Deliver all log files from every account to this S3 bucket, Enable Cloud Trail log file integrity validation

Submit your Feedback/Queries to our Experts

NEW QUESTION 19

Your IT Security team has advised to carry out a penetration test on the resources in their company's AWS Account. This is as part of their capability to analyze the security of the Infrastructure. What should be done first in this regard?

Please select:

- A. Turn on Cloud trail and carry out the penetration test
- B. Turn on VPC Flow Logs and carry out the penetration test
- C. Submit a request to AWS Support
- D. Use a custom AWS Marketplace solution for conducting the penetration test

Answer: C

Explanation:

This concept is given in the AWS Documentation

How do I submit a penetration testing request for my AWS resources? Issue

I want to run a penetration test or other simulated event on my AWS architecture. How do I get permission from AWS to do that?

Resolution

Before performing security testing on AWS resources, you must obtain approval from AWS. After you submit your request AWS will reply in about two business days.

AWS might have additional questions about your test which can extend the approval process, so plan accordingly and be sure that your initial request is as detailed as possible.

If your request is approved, you'll receive an authorization number.

Option A,B and D are all invalid because the first step is to get prior authorization from AWS for penetration tests

For more information on penetration testing, please visit the below URL

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

* <https://aws.amazon.com/premiumsupport/knowledge-center/penetration-testing/> (

The correct answer is: Submit a request to AWS Support Submit your Feedback/Queries to our Experts

NEW QUESTION 24

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 encryption 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 25

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 29

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 33

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 34

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 39

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 40

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 uni
- 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 m assigne
- 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/UserGi 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 41

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 44

A company is deploying a new web application on AWS. Based on their other web applications, they anticipate being the target of frequent DDoS attacks. Which steps can the company use to protect their application? Select 2 answers from the options given below.

Please select:

- A. Associate the EC2 instances with a security group that blocks traffic from blacklisted IP addresses.
- B. Use an ELB Application Load Balancer and Auto Scaling group to scale to absorb application layer traffic.
- C. Use Amazon Inspector on the EC2 instances to examine incoming traffic and discard malicious traffic.
- D. Use CloudFront and AWS WAF to prevent malicious traffic from reaching the application
- E. Enable GuardDuty to block malicious traffic from reaching the application

Answer: BD

Explanation:

The below diagram from AWS shows the best case scenario for avoiding DDos attacks using services such as AWS Cloudfront WAF, ELB and Autoscaling

Option A is invalid because by default security groups don't allow access Option C is invalid because AWS Inspector cannot be used to examine traffic Option E is invalid because this can be used for attacks on EC2 Instances but not against DDos attacks on the entire application For more information on DDos mitigation from AWS, please visit the below URL:

<https://aws.amazon.com/answers/networking/aws-ddos-attack-mitigation/>

The correct answers are: Use an ELB Application Load Balancer and Auto Scaling group to scale to absorb application layer traffic., Use CloudFront and AWS WAF to prevent malicious traffic from reaching the application

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 IAM 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.

IAM 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 IAM 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 IAM and assign this role to an EC2 instance when you first create it

Submit your Feedback/Queries to our Experts

NEW QUESTION 52

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/userguide/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 IAM 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-accessexample3.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-sharint>
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 61

Your company has confidential documents stored in the simple storage service. Due to compliance requirements, you have to ensure that the data in the S3 bucket is available in a different geographical location. As an architect what is the change you would make to comply with this requirement.
Please select:

- A. Apply Multi-AZ for the underlying S3 bucket
- B. Copy the data to an EBS Volume in another Region
- C. Create a snapshot of the S3 bucket and copy it to another region
- D. Enable Cross region replication for the S3 bucket

Answer: D

Explanation:

This is mentioned clearly as a use case for S3 cross-region replication

You might configure cross-region replication on a bucket for various reasons, including the following:

- Compliance requirements - Although, by default Amazon S3 stores your data across multiple geographically distant Availability Zones, compliance requirements might dictate that you store data at even further distances. Cross-region replication allows you to replicate data between distant AWS Regions to satisfy these compliance requirements.

Option A is invalid because Multi-AZ cannot be used to S3 buckets

Option B is invalid because copying it to an EBS volume is not a recommended practice Option C is invalid because creating snapshots is not possible in S3

For more information on S3 cross-region replication, please visit the following URL: <https://docs.aws.amazon.com/AmazonS3/latest/dev/crr.html>

The correct answer is: Enable Cross region replication for the S3 bucket Submit your Feedback/Queries to our Experts

NEW QUESTION 64

When managing permissions for the API gateway, what can be used to ensure that the right level of permissions are given to developers, IT admins and users?
These permissions should be easily managed.
Please select:

- A. Use the secure token service to manage the permissions for the different users
- B. Use IAM Policies to create different policies for the different types of users.
- C. Use the AWS Config tool to manage the permissions for the different users
- D. Use IAM Access Keys to create sets of keys for the different types of user

Answer: B

Explanation:

The AWS Documentation mentions the following

You control access to Amazon API Gateway with IAM permissions by controlling access to the following two API Gateway component processes:

* To create, deploy, and manage an API in API Gateway, you must grant the API developer permissions to perform the required actions supported by the API management component of API Gateway.

* To call a deployed API or to refresh the API caching, you must grant the API caller permissions to perform required IAM actions supported by the API execution component of API Gateway.

Option A, C and D are invalid because these cannot be used to control access to AWS services. This needs to be done via policies. For more information on permissions with the API gateway, please visit the following URL: <https://docs.aws.amazon.com/apigateway/latest/developerguide/permissions.html>

The correct answer is: Use IAM Policies to create different policies for the different types of users. Submit your Feedback/Queries to our Experts

NEW QUESTION 65

Company policy requires that all insecure server protocols, such as FTP, Telnet, HTTP, etc be disabled on all servers. The security team would like to regularly check all servers to ensure compliance with this requirement by using a scheduled CloudWatch event to trigger a review of the current infrastructure. What process will check compliance of the company's EC2 instances?
Please select:

- A. Trigger an AWS Config Rules evaluation of the restricted-common-ports rule against every EC2 instance.
- B. Query the Trusted Advisor API for all best practice security checks and check for "action recommended" status.
- C. Enable a GuardDuty threat detection analysis targeting the port configuration on every EC2 instance.
- D. Run an Amazon inspector assessment using the Runtime Behavior Analysis rules package against every EC2 instance.

Answer: D

Explanation:

Option B is incorrect because querying Trusted Advisor API's are not possible

Option C is incorrect because GuardDuty should be used to detect threats and not check the compliance of security protocols.

Option D states that Run Amazon Inspector using runtime behavior analysis rules which will analyze the behavior of your instances during an assessment run, and provide guidance about how to make your EC2 instances more secure.

Insecure Server Protocols

This rule helps determine whether your EC2 instances allow support for insecure and unencrypted ports/services such as FTP, Telnet HTTP, IMAP, POP version 3, SMTP, SNMP versions 1 and 2, rsh, and rlogin.

For more information, please refer to below URL: https://docs.aws.amazon.com/mspector/latest/userguide/inspector_runtime-behavioranalysis.html#insecure-protocols

(

The correct answer is: Run an Amazon Inspector assessment using the Runtime Behavior Analysis rules package against every EC2 instance.

Submit your Feedback/Queries to our Experts

NEW QUESTION 69

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 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 72

A company is planning on extending their on-premise AWS Infrastructure to the AWS Cloud. They need to have a solution that would give core benefits of traffic encryption and ensure latency is kept to a minimum. Which of the following would help fulfil this requirement? Choose 2 answers from the options given below Please select:

A. AWS VPN

B. AWS VPC Peering

C. AWS NAT gateways

D. AWS Direct Connect

Answer: AD

Explanation:

The AWS Document mention the following which supports the requirement

Option B is invalid because VPC peering is only used for connection between VPCs and cannot be used to connect On-premise infrastructure to the AWS Cloud.

Option C is invalid because NAT gateways is used to connect instances in a private subnet to the internet For more information on VPN Connections, please visit the following url <https://docs.aws.amazon.com/AmazonVPC/latest/UserGuideA/pn-connections.html>

The correct answers are: AWS VPN, AWS Direct Connect Submit your Feedback/Queries to our Experts

NEW QUESTION 75

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 79

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 83

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 85

Your company currently has a set of EC2 Instances hosted in a VPC. The IT Security department is suspecting a possible DDos attack on the instances. What can you do to zero in on the IP addresses which are receiving a flurry of requests. Please select:

- A. Use VPC Flow logs to get the IP addresses accessing the EC2 Instances
- B. Use AWS Cloud trail to get the IP addresses accessing the EC2 Instances
- C. Use AWS Config to get the IP addresses accessing the EC2 Instances
- D. Use AWS Trusted Advisor to get the IP addresses accessing the EC2 Instances

Answer: A

Explanation:

With VPC Flow logs you can get the list of IP addresses which are hitting the Instances in your VPC You can then use the information in the logs to see which external IP addresses are sending a flurry of requests which could be the potential threat for a DDos attack.

Option B is incorrect Cloud Trail records AWS API calls for your account. VPC FLOWlogs logs network traffic for VPC, subnets. Network interfaces etc.

As per AWS,

VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC where as AWS

CloudTrail, is a service that captures API calls and delivers the log files to an Amazon S3 bucket that you specify.

Option C is invalid this is a config service and will not be able to get the IP addresses

Option D is invalid because this is a recommendation service and will not be able to get the IP addresses

For more information on VPC Flow Logs, please visit the following URL: <https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/flow-logs.html>
The correct answer is: Use VPC Flow logs to get the IP addresses accessing the EC2 Instances Submit your Feedback/Queries to our Experts

NEW QUESTION 89

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 92

You have a requirement to conduct penetration testing on the AWS Cloud for a couple of EC2 Instances. How could you go about doing this? Choose 2 right answers from the options given below. Please select:

- A. Get prior approval from AWS for conducting the test
- B. Use a pre-approved penetration testing tool.
- C. Work with an AWS partner and no need for prior approval request from AWS
- D. Choose any of the AWS instance type

Answer: AB

Explanation:

You can use a pre-approved solution from the AWS Marketplace. But till date the AWS Documentation still mentions that you have to get prior approval before conducting a test on the AWS Cloud for EC2 Instances.

Option C and D are invalid because you have to get prior approval first. AWS Docs Provides following details:

"For performing a penetration test on AWS resources first of all we need to take permission from AWS and complete a requisition form and submit it for approval. The form should contain information about the instances you wish to test identify the expected start and end dates/times of your test and requires you to read and agree to Terms and Conditions specific to penetration testing and to the use of appropriate tools for testing. Note that the end date may not be more than 90 days from the start date."

(

At this time, our policy does not permit testing small or micro RDS instance types. Testing of ml

.small, t1 .micro or t2.nano EC2 instance types is not permitted.

For more information on penetration testing please visit the following URL: <https://aws.amazon.com/security/penetration-test/>

The correct answers are: Get prior approval from AWS for conducting the test Use a pre-approved penetration testing tool. Submit your Feedback/Queries to our Experts

NEW QUESTION 97

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 101

A company is using a Redshift cluster to store their data warehouse. There is a requirement from the Internal IT Security team to ensure that data gets encrypted for the Redshift database. How can this be achieved?

Please select:

- A. Encrypt the EBS volumes of the underlying EC2 Instances

- B. Use AWS KMS Customer Default master key
- C. Use SSL/TLS for encrypting the data
- D. Use S3 Encryption

Answer: B

Explanation:

The AWS Documentation mentions the following

Amazon Redshift uses a hierarchy of encryption keys to encrypt the database. You can use either

AWS Key Management Service (AWS KMS) or a hardware security module (HSM) to manage the top-level

encryption keys in this hierarchy. The process that Amazon Redshift uses for encryption differs depending on how you manage keys.

Option A is invalid because it's the cluster that needs to be encrypted

Option C is invalid because this encrypts objects in transit and not objects at rest. Option D is invalid because this is used only for objects in S3 buckets

For more information on Redshift encryption, please visit the following URL: <https://docs.aws.amazon.com/redshift/latest/mgmt/work-with-db-encryption.html>

The correct answer is: Use AWS KMS Customer Default master key. Submit your Feedback/Queries to our Experts

NEW QUESTION 102

A company has resources hosted in their AWS Account. There is a requirement to monitor all API activity for all regions. The audit needs to be applied for future regions as well. Which of the following can be used to fulfill this requirement?

Please select:

- A. Ensure CloudTrail for each region
- B. Then enable for each future region.
- C. Ensure one CloudTrail trail is enabled for all regions.
- D. Create a CloudTrail for each region
- E. Use CloudFormation to enable the trail for all future regions.
- F. Create a CloudTrail for each region
- G. Use AWS Config to enable the trail for all future region

Answer: B

Explanation:

The AWS Documentation mentions the following

You can now turn on a trail across all regions for your AWS account. CloudTrail will deliver log files from all regions to the Amazon S3 bucket and an optional

CloudWatch Logs log group you specified. Additionally, when AWS launches a new region, CloudTrail will create the same trail in the new region. As a result, you will receive log files containing API activity for the new region without taking any action.

Option A and C are invalid because this would be a maintenance overhead to enable CloudTrail for every region

Option D is invalid because this AWS Config cannot be used to enable trails. For more information on this feature, please visit the following URL:

<https://aws.amazon.com/about-aws/whats-new/2015/12/turn-on-cloudtrail-across-all-regions-and-support-for-multiple-trails>

The correct answer is: Ensure one CloudTrail trail is enabled for all regions. Submit your Feedback/Queries to our Experts

NEW QUESTION 106

A company hosts data in S3. There is now a mandate that going forward all data in the S3 bucket needs to be encrypted at rest. How can this be achieved?

Please select:

- A. Use AWS Access keys to encrypt the data
- B. Use SSL certificates to encrypt the data
- C. Enable server-side encryption on the S3 bucket
- D. Enable MFA on the S3 bucket

Answer: C

Explanation:

The AWS Documentation mentions the following

Server-side encryption is about data encryption at rest—that is, Amazon S3 encrypts your data at the object level as it writes it to disks in its data centers and decrypts it for you when you access it. As long as you authenticate your request and you have access permissions, there is no difference in the way you access encrypted or unencrypted objects.

Options A and B are invalid because neither Access Keys nor SSL certificates can be used to encrypt data.

Option D is invalid because MFA is just used as an extra level of security for S3 buckets. For more information on S3 server-side encryption, please refer to the below link: <https://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html>

Submit your Feedback/Queries to our Experts

NEW QUESTION 107

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 the 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 112

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 117

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 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 bucket 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 122

Your company has just started using AWS and created an AWS account. They are aware of the potential issues when root access is enabled. How can they best safeguard the account when it comes to root access? Choose 2 answers from the options given below
Please select:

- A. Delete the root access account
- B. Create an Admin IAM user with the necessary permissions
- C. Change the password for the root account.
- D. Delete the root access keys

Answer: BD

Explanation:

The AWS Documentation mentions the following
All AWS accounts have root user credentials (that is, the credentials of the account owner). These credentials allow full access to all resources in the account. Because you can't restrict permissions for root user credentials, we recommend that you delete your root user access keys. Then create AWS Identity and Access Management (IAM) user credentials for everyday interaction with AWS. Option A is incorrect since you cannot delete the root access account
Option C is partially correct but cannot be used as the ideal solution for safeguarding the account For more information on root access vs admin IAM users, please refer to below URL: <https://docs.aws.amazon.com/iam/latest/userguide/root-vs-iam.html>
The correct answers are: Create an Admin IAM user with the necessary permissions. Delete the root access keys Submit your Feedback/Queries to our Experts

NEW QUESTION 124

You have just developed a new mobile application that handles analytics workloads on large scale datasets that are stored on Amazon Redshift. Consequently, the application needs to access Amazon Redshift tables. Which of the below methods would be the best both practically and security-wise, to access the tables?
Choose the correct answer from the options below
Please select:

- A. Create an IAM user and generate encryption keys for that use

- B. Create a policy for Redshift readonly acces
- C. Embed th keys in the application.
- D. Create an HSM client certificate in Redshift and authenticate using this certificate.
- E. Create a Redshift read-only access policy in 1AM and embed those credentials in the application.
- F. Use roles that allow a web identity federated user to assume a role that allows access to the Redshift table by providing temporary credentials.

Answer: D

Explanation:

The AWS Documentation mentions the following

"When you write such an app, you'll make requests to AWS services that must be signed with an AWS access key. However, we strongly recommend that you do not embed or distribute long-term AWS credentials with apps that a user downloads t device, even in an encrypted store. Instead, build your app so that it requests temporary AWS security credentials dynamica when needed using web identify federation. The supplied temporary credentials map to an AWS role that has only the permissioi needed to perform the tasks required by the mobile app". Option A.B and C are all automatically incorrect because you need to use 1AM Roles for Secure access to services For more information on web identity federation please refer to the below Link: http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_oidc.html

The correct answer is: Use roles that allow a web identity federated user to assume a role that allows access to the RedShift table by providing temporary credentials.

Submit your Feedback/Queries to our Experts

NEW QUESTION 126

A company has hired a third-party security auditor, and the auditor needs read-only access to all AWS resources and logs of all VPC records and events that have occurred on AWS. How can the company meet the auditor's requirements without comprising security in the AWS environment? Choose the correct answer from the options below

Please select:

- A. Create a role that has the required permissions for the auditor.
- B. Create an SNS notification that sends the CloudTrail log files to the auditor's email when CloudTrail delivers the logs to S3, but do not allow the auditor access to the AWS environment.
- C. The company should contact AWS as part of the shared responsibility model, and AWS will grant required access to th^ third-party auditor.
- D. Enable CloudTrail logging and create an 1AM user who has read-only permissions to the required AWS resources, including the bucket containing the CloudTrail logs.

Answer: D

Explanation:

AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain events related to API calls across your AWS infrastructure. CloudTrail provides a history of AWS API calls for your account including API calls made through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This history simplifies security analysis, resource change tracking, and troubleshooting.

Option A and C are incorrect since Cloudtrail needs to be used as part of the solution Option B is incorrect since the auditor needs to have access to Cloudtrail For more information on cloudtrail, please visit the below URL: <https://aws.amazon.com/cloudtrail>

The correct answer is: Enable CloudTrail logging and create an 1AM user who has read-only permissions to the required AWS resources, including the bucket containing the CloudTrail logs. Submit your Feedback/Queries to our Experts

NEW QUESTION 131

An auditor needs access to logs that record all API events on AWS. The auditor only needs read-only access to the log files and does not need access to each AWS account. The company has multiple AWS accounts, and the auditor needs access to all the logs for all the accounts. What is the best way to configure access for the auditor to view event logs from all accounts? Choose the correct answer from the options below

Please select:

- A. Configure the CloudTrail service in each AWS account, and have the logs delivered to an AWS bucket on each account, while granting the auditor permissions to the bucket via roles in the secondary accounts and a single primary 1AM account that can assume a read-only role in the secondary AWS accounts.
- B. Configure the CloudTrail service in the primary AWS account and configure consolidated billing for all the secondary account
- C. Then grant the auditor access to the S3 bucket that receives theCloudTrail log files.
- D. Configure the CloudTrail service in each AWS account and enable consolidated logging inside of CloudTrail.
- E. Configure the CloudTrail service in each AWS account and have the logs delivered to a single AWS bucket in the primary account and erant the auditor access to that single bucket in the orimarvaccoun

Answer: D

Explanation:

Given the current requirements, assume the method of "least privilege" security design and only allow the auditor access to the minimum amount of AWS resources as possibli

AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain events related to API calls across your AWS infrastructure. CloudTrail provides a history of AWS API calls for your account including API calls made through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This history simplifies security analysis, resource change tracking, and troubleshooting

only be granted access in one location

Option Option A is incorrect since the auditor should B is incorrect since consolidated billing is not a key requirement as part of the question

Option C is incorrect since there is not consolidated logging

For more information on Cloudtrail please refer to the below URL: <https://aws.amazon.com/cloudtrail>

(

The correct answer is: Configure the CloudTrail service in each AWS account and have the logs delivered to a single AWS bud in the primary account and grant the auditor access to that single bucket in the primary account.

Submit your Feedback/Queries to our Experts

NEW QUESTION 133

You are planning on using the AWS KMS service for managing keys for your application. For which of the following can the KMS CMK keys be used for

encrypting? Choose 2 answers from the options given below
Please select:

- A. Image Objects
- B. Large files
- C. Password
- D. RSA Keys

Answer: CD

Explanation:

The CMK keys themselves can only be used for encrypting data that is maximum 4KB in size. Hence it can be used for encrypting information such as passwords and RSA keys.

Option A and B are invalid because the actual CMK key can only be used to encrypt small amounts of data and not large amounts of data

A\ You have to generate the data key from the CMK key in order to encrypt high amounts of data

For more information on the concepts for KMS, please visit the following URL: <https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html>

The correct answers are: Password, RSA Keys Submit your Feedback/Queries to our Experts

NEW QUESTION 134

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 key
- B. The cluster key encrypts the database key
- C. The database key encrypts the data encryption keys.
- D. The master keys encrypts the database key
- 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 136

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 138

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 143

The correct answers are: Enable versioning on the S3 bucket Enable MFA Delete in the bucket policy Submit your Feedback/Queries to our Experts

You company has mandated that all data in AWS be encrypted at rest. How can you achieve this for EBS volumes? Choose 2 answers from the options given below

Please select:

- A. Use Windows bit locker for EBS volumes on Windows instances
- B. Use TrueEncrypt for EBS volumes on Linux instances
- C. Use AWS Systems Manager to encrypt the existing EBS volumes
- D. Boot EBS volume can be encrypted during launch without using custom AMI

Answer: AB

Explanation:

EBS encryption can also be enabled when the volume is created and not for existing volumes. One can use existing tools for OS level encryption.

Option C is incorrect.

AWS Systems Manager is a management service that helps you automatically collect software inventory, apply OS patches, create system images, and configure Windows and Linux operating systems.

Option D is incorrect

You cannot choose to encrypt a non-encrypted boot volume on instance launch. To have encrypted boot volumes during launch, your custom AMI must have its boot volume encrypted before launch. For more information on the Security Best practices, please visit the following URL:

[.com/whit Security Practices](#).

The correct answers are: Use Windows bit locker for EBS volumes on Windows instances. Use TrueEncrypt for EBS volumes on Linux instances

Submit your Feedback/Queries to our Experts

NEW QUESTION 144

You are designing a connectivity solution between on-premises infrastructure and Amazon VPC. Your server's on-premises will be communicating with your VPC instances. You will be establishing IPSec

tunnels over the internet. You will be using VPN gateways and terminating the IPsec tunnels on AWS-supported customer gateways. Which of the following objectives would you achieve by

implementing an IPsec tunnel as outlined above? Choose 4 answers from the options below Please select:

- A. End-to-end protection of data in transit
- B. End-to-end Identity authentication
- C. Data encryption across the internet
- D. Protection of data in transit over the Internet
- E. Peer identity authentication between VPN gateway and customer gateway
- F. Data integrity protection across the Internet

Answer: CDEF

Explanation:

Since the Web server needs to talk to the database server on port 3306 that means that the database server should allow incoming traffic on port 3306. The below table from the AWS documentation shows how the security groups should be set up.

Option B is invalid because you need to allow incoming access for the database server from the WebSecGrp security group.

Options C and D are invalid because you need to allow Outbound traffic and not inbound traffic For more information on security groups please visit the below

Link: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2.html

The correct answer is: Allow Inbound on port 3306 for Source Web Server Security Group WebSecGrp. Submit your Feedback/Queries to our Experts

NEW QUESTION 146

A user has enabled versioning on an S3 bucket. The user is using server side encryption for data at

Rest. If the user is supplying his own keys for encryption SSE-C, which of the below mentioned statements is true?

Please select:

- A. The user should use the same encryption key for all versions of the same object
- B. It is possible to have different encryption keys for different versions of the same object
- C. AWS S3 does not allow the user to upload his own keys for server side encryption
- D. The SSE-C does not work when versioning is enabled

Answer: B

Explanation:

Managing your own encryption keys, you

You can encrypt the object and send it across to S3

Option A is invalid because ideally you should use different encryption keys Option C is invalid because you can use your own encryption keys Option D is invalid because encryption works even if versioning is enabled For more information on client side encryption please visit the below Link: [""Keys.html](#)

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

The correct answer is: It is possible to have different encryption keys for different versions of the same object Submit your Feedback/Queries to our Experts

NEW QUESTION 150

Your company has an external web site. This web site needs to access the objects in an S3 bucket. Which of the following would allow the web site to access the objects in the most secure manner? Please select:

- A. Grant public access for the bucket via the bucket policy
- B. Use the aws:Referer key in the condition clause for the bucket policy
- C. Use the aws:sites key in the condition clause for the bucket policy
- D. Grant a role that can be assumed by the web site

Answer: B

Explanation:

An example of this is given in the AWS Documentatio Restricting Access to a Specific HTTP Referrer

Suppose you have a website with domain name (www.example.com or example.com) with links to photos and videos stored in your S3 bucket examplebucket. By default, all the S3 resources are private, so only the AWS account that created the resources can access them. To allow read access to these objects from your website, you can add a bucket policy that allows s3:GetObject permission with a condition, using the aws:referer key, that the get request must originate from specific webpages. The following policy specifies the StringLike condition with the aws:Referer condition key.

Option A is invalid because giving public access is not a secure way to provide access Option C is invalid because aws:sites is not a valid condition key Option D is invalid because IAM roles will not be assigned to web sites

For more information on example bucket policies please visit the below Link:

1 <https://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies.html>

The correct answer is: Use the aws:Referer key in the condition clause for the bucket policy Submit your Feedback/Queries to our Experts

NEW QUESTION 151

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 IAM policy which allows access to specific tags

Submit your Feedback/Queries to our Experts

NEW QUESTION 153

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 154

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 159

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 163

An organization has setup multiple 1AM users. The organization wants that each 1AM user accesses the 1AM console only within the organization and not from outside. How can it achieve this? Please select:

- A. Create an 1AM policy with the security group and use that security group for AWS console login
- B. Create an 1AM policy with a condition which denies access when the IP address range is not from the organization
- C. Configure the EC2 instance security group which allows traffic only from the organization's IP range
- D. Create an 1AM policy with VPC and allow a secure gateway between the organization and AWS Console

Answer: B

Explanation:

You can actually use a Deny condition which will not allow the person to log in from outside. The below example shows the Deny condition to ensure that any address specified in the source address is not allowed to access the resources in aws.

Option A is invalid because you don't mention the security group in the 1AM policy Option C is invalid because security groups by default don't allow traffic

Option D is invalid because the 1AM policy does not have such an option For more information on 1AM policy conditions, please visit the URL:

http://docs.aws.amazon.com/IAM/latest/UserGuide/access_pol_examples.htm #iam-policy-example-ec2-two-condition!

The correct answer is: Create an IAM policy with a condition which denies access when the IP address range is not from the organization

Submit your Feedback/Queries to our Experts

NEW QUESTION 165

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 170

A company has a requirement to create a DynamoDB table. The company's software architect has provided the following CLI command for the DynamoDB table:

Which of the following has been taken into account from a security perspective from the above command? Please select:

- A. Since the ID is hashed, it ensures security of the underlying table.
- B. The above command ensures data encryption at rest for the Customer table.
- C. The above command ensures data encryption in transit for the Customer table.
- D. The right throughput has been specified from a security perspective.

Answer: B

Explanation:

The above command with the "-sse-specification Enabled=true" parameter ensures that the data for the DynamoDB table is encrypted at rest.

Options A, C, and D are all invalid because this command is specifically used to ensure data encryption at rest.

For more information on DynamoDB encryption, please visit the URL:

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/encryption.tutorial.html> The correct answer is: The above command ensures data encryption at rest for the Customer table.

NEW QUESTION 171

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 are 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 174

What is the result of the following bucket policy?

Choose the correct answer

Please select:

- A. It will allow all access to the bucket mybucket
- B. It will allow the user mark from AWS account number 111111111 all access to the bucket but deny everyone else all access to the bucket
- C. It will deny all access to the bucket mybucket
- D. None of these

Answer: C

Explanation:

The policy consists of 2 statements, one is the allow for the user mark to the bucket and the next is the deny policy for all other users. The deny permission will override the allow and hence all users will not have access to the bucket.

Options A,B and D are all invalid because this policy is used to deny all access to the bucket mybucket For examples on S3 bucket policies, please refer to the below Link: <http://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies.html>

The correct answer is: It will deny all access to the bucket mybucket Submit your Feedback/Quenes to our Experts

NEW QUESTION 178

Your company is planning on using AWS EC2 and ELB for deployment for their web applications. The security policy mandates that all traffic should be encrypted. Which of the following options will ensure that this requirement is met. Choose 2 answers from the options below.

Please select:

- A. Ensure the load balancer listens on port 80
- B. Ensure the load balancer listens on port 443
- C. Ensure the HTTPS listener sends requests to the instances on port 443
- D. Ensure the HTTPS listener sends requests to the instances on port 80

Answer: BC

Explanation:

The AWS Documentation mentions the following

You can create a load balancer that listens on both the HTTP (80) and HTTPS (443) ports. If you specify that the HTTPS listener sends requests to the instances on port 80, the load balancer terminates the requests and communication from the load balancer to the instances is not encrypted, if the HTTPS listener sends requests to the instances on port 443, communication from the load balancer to the instances is encrypted.

Option A is invalid because there is a need for secure traffic, so port 80 should not be used Option D is invalid because for the HTTPS listener you need to use port 443

For more information on HTTPS with ELB, please refer to the below Link: <https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-create-https-ssl-loadbalancer.html>

The correct answers are: Ensure the load balancer listens on port 443, Ensure the HTTPS listener sends requests to the instances on port 443

Submit your Feedback/Queries to our Experts

NEW QUESTION 183

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 184

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 185

Your company is planning on developing an application in AWS. This is a web based application. The application users will use their facebook or google identities for authentication. You want to have the ability to manage user profiles without having to add extra coding to manage this. Which of the below would assist in this. Please select:

- A. Create an OIDC identity provider in AWS
- B. Create a SAML provider in AWS
- C. Use AWS Cognito to manage the user profiles
- D. Use 1AM users to manage the user profiles

Answer: B

Explanation:

The AWS Documentation mentions the following The AWS Documentation mentions the following

OIDC identity providers are entities in 1AM that describe an identity provider (IdP) service that supports the OpenID Connect (OIDC) standard. You use an OIDC identity provider when you want to establish trust between an OIDC-compatible IdP—such as Google, Salesforce, and many others—and your AWS account This is useful if you are creating a mobile app or web application that requires access to AWS resources, but you don't want to create custom sign-in code or manage your own user identities

Option A is invalid because in the security groups you would not mention this information/ Option C is invalid because SAML is used for federated authentication

Option D is invalid because you need to use the OIDC identity provider in AWS For more information on ODIC identity providers, please refer to the below Link:

<https://docs.aws.amazon.com/IAM/latest/UserGuide/id roles providers create oidc.html>! The correct answer is: Create an OIDC identity provider in AWS

NEW QUESTION 189

A company has set up EC2 instances on the AW5 Cloud. There is a need to see all the IP addresses which are accessing the EC2 Instances. Which service can help achieve this?

Please select:

- A. Use the AWS Inspector service
- B. Use AWS VPC Flow Logs
- C. Use Network ACL's
- D. Use Security Groups

Answer: B

Explanation:

The AWS Documentation mentions the foil

A flow log record represents a network flow in your flow log. Each record captures the network flow for a specific 5-tuple, for a specific capture window. A 5-tuple is a set of five different values that specify the source, destination, and protocol for an internet protocol (IP) flow.

Options A,C and D are all invalid because these services/tools cannot be used to get the the IP addresses which are accessing the EC2 Instances

For more information on VPC Flow Logs please visit the URL <https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/flow-logs.html>

The correct answer is: Use AWS VPC Flow Logs Submit your Feedback/Queries to our Experts

NEW QUESTION 193

You have a set of 100 EC2 Instances in an AWS account. You need to ensure that all of these instances are patched and kept to date. All of the instances are in a private subnet. How can you achieve this. Choose 2 answers from the options given below

Please select:

- A. Ensure a NAT gateway is present to download the updates
- B. Use the Systems Manager to patch the instances
- C. Ensure an internet gateway is present to download the updates
- D. Use the AWS inspector to patch the updates

Answer: AB

Explanation:

Option C is invalid because the instances need to remain in the private: Option D is invalid because AWS inspector can only detect the patches

One of the AWS Blogs mentions how patching of Linux servers can be accomplished. Below is the diagram representation of the architecture setup

For more information on patching Linux workloads in AWS, please refer to the Lin. <https://aws.amazon.com/blogs/security/how-to-patch-linux-workloads-on-aws/>

The correct answers are: Ensure a NAT gateway is present to download the updates. Use the Systems Manager to patch the instances

Submit your Feedback/Queries to our Experts

NEW QUESTION 197

You have an EC2 instance with the following security configured:

1. ICMP inbound allowed on Security Group
2. ICMP outbound not configured on Security Group
3. ICMP inbound allowed on Network ACL
4. ICMP outbound denied on Network ACL

If Flow logs is enabled for the instance, which of the following flow records will be recorded? Choose 3 answers from the options give below

Please select:

- A. An ACCEPT record for the request based on the Security Group
- B. An ACCEPT record for the request based on the NACL
- C. A REJECT record for the response based on the Security Group
- D. A REJECT record for the response based on the NACL

Answer: ABD

Explanation:

This example is given in the AWS documentation as well

For example, you use the ping command from your home computer (IP address is 203.0.113.12) to your instance (the network interface's private IP address is 172.31.16.139). Your security group's inbound rules allow ICMP traffic and the outbound rules do not allow ICMP traffic however, because security groups are stateful, the response ping from your instance is allowed. Your network ACL permits inbound ICMP traffic but does not permit outbound ICMP traffic. Because network ACLs are stateless, the response ping is dropped and will not reach your home computer. In a flow log, this is displayed as 2 flow log records:

An ACCEPT record for the originating ping that was allowed by both the network ACL and the security group, and therefore was allowed to reach your instance.

A REJECT record for the response ping that the network ACL denied.

Option C is invalid because the REJECT record would not be present For more information on Flow Logs, please refer to the below URL:

<http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/flow-logs.html>

The correct answers are: An ACCEPT record for the request based on the Security Group, An ACCEPT record for the request based on the NACL, A REJECT record for the response based on the NACL Submit your Feedback/Queries to our Experts

NEW QUESTION 198

Your company looks at the gaming domain and hosts several Ec2 Instances as game servers. The servers each experience user loads in the thousands. There is a concern of DDos attacks on the EC2 Instances which could cause a huge revenue loss to the company. Which of the following can help mitigate this security concern and also ensure minimum downtime for the servers.

Please select:

- A. Use VPC Flow logs to monitor the VPC and then implement NACL's to mitigate attacks
- B. Use AWS Shield Advanced to protect the EC2 Instances
- C. Use AWS Inspector to protect the EC2 Instances
- D. Use AWS Trusted Advisor to protect the EC2 Instances

Answer: B

Explanation:

Below is an excerpt from the AWS Documentation on some of the use cases for AWS Shield

NEW QUESTION 200

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

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

100% Actual & Verified — Instant Download, Please Click
[Order The AWS-Certified-Security-Specialty Practice Test Here](#)