



Amazon

Exam Questions AWS-Certified-Security-Specialty

Amazon AWS Certified Security - Specialty

About ExamBible

Your Partner of IT Exam

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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 have a vendor that needs access to an AWS resource. You create an AWS user account. You want to restrict access to the resource using a policy for just that user over a brief period. Which of the following would be an ideal policy to use?

Please select:

- A. An AWS Managed Policy
- B. An Inline Policy
- C. A Bucket Policy
- D. A bucket ACL

Answer: B

Explanation:

The AWS Documentation gives an example on such a case

Inline policies are useful if you want to maintain a strict one-to-one relationship between a policy and the principal entity that it's applied to. For example, you want to be sure that the permissions in a policy are not inadvertently assigned to a principal entity other than the one they're intended for. When you use an inline policy, the permissions in the policy cannot be inadvertently attached to the wrong principal entity. In addition, when you use the AWS Management Console to delete that principal entity, the policies embedded in the principal entity are deleted as well. That's because they are part of the principal entity.

Option A is invalid because AWS Managed Policies are OK for a group of users, but for individual users, inline policies are better.

Option C and D are invalid because they are specifically meant for access to S3 buckets. For more information on policies, please visit the following URL:

<https://docs.aws.amazon.com/IAM/latest/UserGuide/access-managed-vs-inline>

The correct answer is: An Inline Policy. Submit your Feedback/Queries to our Experts

NEW QUESTION 3

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

Please select:

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

Answer: AC

Explanation:

Below is a snippet from the AWS blogs on a solution

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

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

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

NEW QUESTION 4

A company wants to have a secure way of generating, storing and managing cryptographic exclusive access for the keys. Which of the following can be used for this purpose?

Please select:

- A. Use KMS and the normal KMS encryption keys
- B. Use KMS and use an external key material
- C. Use S3 Server Side encryption
- D. Use Cloud HSM

Answer: D

Explanation:

The AWS Documentation mentions the following

The AWS CloudHSM service helps you meet corporate, contractual and regulatory compliance requirements for data security by using dedicated Hardware Security Module (HSM) instances within the AWS cloud. AWS and AWS Marketplace partners offer a variety of solutions for protecting sensitive data within the AWS platform, but for some applications and data subject to contractual or regulatory mandates for managing cryptographic keys, additional protection may be necessary. CloudHSM complements existing data protection solutions and allows you to protect your encryption keys within HSMs that are design and validated to government standards for secure key management. CloudHSM allows you to securely generate, store and manage cryptographic keys used for data encryption in a way that keys are accessible only by you.

Option A,B and Care invalid because in all of these cases, the management of the key will be with AWS. Here the question specifically mentions that you want to have exclusive access over the keys. This can be achieved with Cloud HSM

For more information on CloudHSM, please visit the following URL: <https://aws.amazon.com/cloudhsm/faq>:

The correct answer is: Use Cloud HSM Submit your Feedback/Queries to our Experts

NEW QUESTION 5

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

Please select:

- A. Stream the log files to a separate Cloudtrail trail
- B. Stream the log files to a separate Cloudwatch Log group
- C. Create an 1AM policy that gives the desired level of access to the Cloudtrail trail
- D. Create an 1AM 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 1AM 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/Workinj>

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 1AM policy that gives the desired level of access to the Cloudwatch Log group

Submit your Feedback/Queries to our Experts

NEW QUESTION 6

You have a web site that is sitting behind AWS Cloudfront. You need to protect the web site against threats such as SQL injection and Cross site scripting attacks. Which of the following service can help in such a scenario

Please select:

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

Answer: B

Explanation:

The AWS Documentation mentions the following

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

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

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

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

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

The correct answer is: AWS WAF

Submit your Feedback/Queries to our Experts

NEW QUESTION 7

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 CL
- B. Query for all resources with the tag of production.
- C. Create a bash shell script with the AWS CL
- 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 now 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 resou For more information on AWS Config, please visit the below URL: <https://docs.aws.amazon.com/config/latest/developereuide/how-does-confie-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 8

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 VP
- 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 tabl
- D. Attach the poll to the DynamoDB table.
- E. Create an 1AM user with permissions to write to the DynamoDB tabl
- F. Store an access key for that user in the Lambda environment variables.
- G. Create an 1AM service role with permissions to write to the DynamoDB tabl
- H. Associate that role with the Lambda function.

Answer: D

Explanation:

The ideal way is to create an 1AM 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 1AM role (execution role) associated with it. You specify the 1AM 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 1AM 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 resources 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 1AM 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 1AM service role with permissions to write to the DynamoDB table. Associate that role with the Lambda function.

Submit your Feedback/Queries to our Exp

NEW QUESTION 9

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

You are devising a policy to allow users to have the ability to access objects in a bucket called appbucket. You define the below custom bucket policy

But when you try to apply the policy you get the error "Action does not apply to any resource(s) in statement." What should be done to rectify the error Please select:

- A. Change the 1AM permissions by applying PutBucketPolicy permissions.
- B. Verify that the policy has the same name as the bucket nam
- C. If no
- D. make it the same.
- E. Change the Resource section to "arn:aws:s3:::appbucket/*".
- F. Create the bucket "appbucket" and then apply the polic

Answer: C

Explanation:

When you define access to objects in a bucket you need to ensure that you specify to which objects in the bucket access needs to be given to. In this case, the * can be used to assign the permission to all objects in the bucket

Option A is invalid because the right permissions are already provided as per the question requirement

Option B is invalid because it is not necessary that the policy has the same name as the bucket Option D is invalid because this should be the default flow for applying the policy

For more information on bucket policies please visit the below URL: <https://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies.html>
The correct answer is: Change the Resource section to "arn:aws:s3:::appbucket/" 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 12

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

Please select:

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

Answer: C

Explanation:

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

Center for Internet security (CIS) Benchmarks

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

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

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

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

Submit your Feedback/Queries to our Experts

NEW QUESTION 15

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 17

You have just received an email from AWS Support stating that your AWS account might have been compromised. Which of the following steps would you look to carry out immediately. Choose 3 answers from the options below.

Please select:

- A. Change the root account password.
- B. Rotate all 1AM access keys
- C. Keep all resources running to avoid disruption
- D. Change the password for all 1AM user

Answer: ABD

Explanation:

One of the articles from AWS mentions what should be done in such a scenario

If you suspect that your account has been compromised, or if you have received a notification from AWS that the account has been compromised, perform the following tasks:

Change your AWS root account password and the passwords of any 1AM users. Delete or rotate all root and AWS Identity and Access Management (1AM) access keys.

Delete any resources on your account you didn't create, especially running EC2 instances, EC2 spot bids, or 1AM users.

Respond to any notifications you received from AWS Support through the AWS Support Center. Option C is invalid because there could be compromised instances or resources running on your environment. They should be shutdown or stopped immediately.

For more information on the article, please visit the below URL: <https://aws.amazon.com/premiumsupport/knowledge-center/potential-account-compromise>

The correct answers are: Change the root account password. Rotate all 1AM access keys. Change the password for all 1AM users. Submit your Feedback/Queries to our Experts

NEW QUESTION 20

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 lo 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/awsccloudtrail/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 21

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 toi 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 26

Which of the following is not a best practice for carrying out a security audit? Please select:

- A. Conduct an audit on a yearly basis
- B. Conduct an audit if application instances have been added to your account
- C. Conduct an audit if you ever suspect that an unauthorized person might have accessed your account
- D. Whenever there are changes in your organization

Answer: A

Explanation:

A year's time is generally too long a gap for conducting security audits. The AWS Documentation mentions the following:

You should audit your security configuration in the following situations: On a periodic basis.

If there are changes in your organization, such as people leaving.

If you have stopped using one or more individual AWS services. This is important for removing permissions that users in your account no longer need.

If you've added or removed software in your accounts, such as applications on Amazon EC2 instances, AWS OpsWorks stacks, AWS CloudFormation templates, etc.

If you ever suspect that an unauthorized person might have accessed your account.

Option B, C and D are all the right ways and recommended best practices when it comes to conducting audits. For more information on Security Audit guideline, please visit the below URL: <https://docs.aws.amazon.com/eeneral/latest/gr/aws-security-audit-euide.html>

The correct answer is: Conduct an audit on a yearly basis. Submit your Feedback/Queries to our Experts

NEW QUESTION 31

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

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

Answer: B

Explanation:

The AWS Documentation mentions the following:

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

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

The correct answer is: Key pairs

Submit your Feedback/Queries to our Experts

NEW QUESTION 32

A company hosts a critical web application on the AWS Cloud. This is a key revenue generating application for the company. The IT Security team is worried about potential DDoS attacks against the web site. The senior management has also specified that immediate action needs to be taken in case of a potential DDoS attack. What should be done in this regard?

Please select:

- A. Consider using the AWS Shield Service
- B. Consider using VPC Flow logs to monitor traffic for DDoS attack and quickly take actions on a trigger of a potential attack.
- C. Consider using the AWS Shield Advanced Service
- D. Consider using Cloudwatch logs to monitor traffic for DDoS attack and quickly take actions on a trigger of a potential attack.

Answer: C

Explanation:

Option A is invalid because the normal AWS Shield Service will not help in immediate action against a DDoS attack. This can be done via the AWS Shield Advanced Service.

Option B is invalid because this is a logging service for VPCs traffic flow but cannot specifically protect against DDoS attacks.

Option D is invalid because this is a logging service for AWS Services but cannot specifically protect against DDoS attacks.

The AWS Documentation mentions the following:

AWS Shield Advanced provides enhanced protections for your applications running on Amazon EC2, Elastic Load Balancing (ELB), Amazon CloudFront and Route 53 against larger and more sophisticated attacks. AWS Shield Advanced is available to AWS Business Support and AWS Enterprise Support customers.

AWS Shield Advanced protection provides always-on, flow-based monitoring of network traffic and active application monitoring to provide near real-time notifications of DDoS attacks. AWS Shield Advanced also gives customers highly flexible controls over attack mitigations to take actions instantly. Customers can also engage the DDoS Response Team (DRT) 24x7 to manage and mitigate their application layer DDoS attacks.

For more information on AWS Shield, please visit the below URL: <https://aws.amazon.com/shield/faqs>;

The correct answer is: Consider using the AWS Shield Advanced Service. Submit your Feedback/Queries to our Experts

NEW QUESTION 35

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

Please select:

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

Answer: D

Explanation:

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

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

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

<https://docs.aws.amazon.com/AmazonVPC/latest/Peeri>

The correct answer is: Check the Route tables for the VPCs. 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 unit
- C. Apply the policy to that organizational unit.
- D. Create a Service Control Policy that denies access to the service
- E. Apply the policy to the root account.
- F. Create an 1AM policy that denies access to the service
- G. Associate the policy with an 1AM group and enlist all users and the root users in this group.
- H. Create an 1AM policy that denies access to the service
- I. Create a Config Rule that checks that all users have the policy assigned
- J. Trigger a Lambda function that adds the policy when found missing.

Answer: A

Explanation:

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

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

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

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

Submit your Feedback/Queries to our Experts

NEW QUESTION 41

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 43

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

Please select:

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

Answer: B

Explanation:

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

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

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

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

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

Submit your Feedback/Queries to our Experts

NEW QUESTION 46

You have a set of Keys defined using the AWS KMS service. You want to stop using a couple of keys, but are not sure of which services are currently using the keys. Which of the following would be a safe option to stop using the keys from further usage. Please select:

- A. Delete the keys since anyway there is a 7 day waiting period before deletion
- B. Disable the keys
- C. Set an alias for the key
- D. Change the key material for the key

Answer: B

Explanation:

Option A is invalid because once you schedule the deletion and waiting period ends, you cannot come back from the deletion process.

Option C and D are invalid because these will not check to see if the keys are being used or not. The AWS Documentation mentions the following

Deleting a customer master key (CMK) in AWS Key Management Service (AWS KMS) is destructive and potentially dangerous. It deletes the key material and all metadata associated with the CMK, and is irreversible. After a CMK is deleted you can no longer decrypt the data that was encrypted under that CMK, which means that data becomes unrecoverable. You should delete a CMK only when you are sure that you don't need to use it anymore. If you are not sure, consider disabling the CMK

instead of deleting it. You can re-enable a disabled CMK if you need to use it again later, but you cannot recover a deleted CMK.

For more information on deleting keys from KMS, please visit the below URL: <https://docs.aws.amazon.com/kms/latest/developerguide/deleting-keys.html>

The correct answer is: Disable the keys. Submit your Feedback/Queries to our Experts

NEW QUESTION 50

You are building a large-scale confidential documentation web server on AWS and all of the documentation for it will be stored on S3. One of the requirements is that it cannot be publicly accessible from S3 directly, and you will need to use CloudFront to accomplish this. Which of the methods listed below would satisfy the requirements as outlined? Choose an answer from the options below

Please select:

- A. Create an Identity and Access Management (IAM) user for CloudFront and grant access to the objects in your S3 bucket to that IAM User.
- B. Create an Origin Access Identity (OAI) for CloudFront and grant access to the objects in your S3 bucket to that OAI.
- C. Create individual policies for each bucket the documents are stored in and in that policy grant access to only CloudFront.
- D. Create an S3 bucket policy that lists the CloudFront distribution ID as the Principal and the target bucket as the Amazon Resource Name (ARN).

Answer: B

Explanation:

If you want to use CloudFront signed URLs or signed cookies to provide access to objects in your Amazon S3 bucket you probably also want to prevent users from accessing your Amazon S3 objects using Amazon S3 URLs. If users access your objects directly in Amazon S3, they bypass the controls provided by CloudFront signed URLs or signed cookies, for example, control over the date and time that a user can no longer access your content and control over which IP addresses can be used to access content. In addition, if user's access objects both through CloudFront and directly by using Amazon S3 URLs, CloudFront access logs are less useful because they're incomplete.

Option A is invalid because you need to create a Origin Access Identity for CloudFront and not an IAM user

Option C and D are invalid because using policies will not help fulfil the requirement. For more information on Origin Access Identity please see the below Link:

<http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-contentrestrictions-access-to-s3.html>

The correct answer is: Create an Origin Access Identity (OAI) for CloudFront and grant access to the objects in your S3 bucket to that OAI.

(

Submit your Feedback/Queries to our Experts

NEW QUESTION 54

A company has several Customer Master Keys (CMK), some of which have imported key material.

Each CMK must be rotated annually.

What two methods can the security team use to rotate each key? Select 2 answers from the options given below

Please select:

- A. Enable automatic key rotation for a CMK
- B. Import new key material to an existing CMK
- C. Use the CLI or console to explicitly rotate an existing CMK
- D. Import new key material to a new CMK; Point the key alias to the new CMK.
- E. Delete an existing CMK and a new default CMK will be created

Answer: AD

Explanation:

The AWS Documentation mentions the following

Automatic key rotation is available for all customer managed CMKs with KMS-generated key material. It is not available for CMKs that have imported key material (the value of the Origin field is External), but you can rotate these CMKs manually.

Rotating Keys Manually

You might want to create a new CMK and use it in place of a current CMK instead of enabling automatic key rotation. When the new CMK has different cryptographic material than the current CMK, using the new CMK has the same effect as changing the backing key in an existing CMK. The process of replacing one CMK with another is known as manual key rotation.

When you begin using the new CMK, be sure to keep the original CMK enabled so that AWS KMS can decrypt data that the original CMK encrypted. When decrypting data, KMS identifies the CMK that was used to encrypt the data, and it uses the same CMK to decrypt the data

A. As long as you keep both

the original and new CMKs enabled, AWS KMS can decrypt any data that was encrypted by either CMK.

Option B is invalid because you also need to point the key alias to the new key. Option C is invalid because existing CMK keys cannot be rotated as they are

Option E is invalid because deleting existing keys will not guarantee the creation of a new default CMK key

For more information on Key rotation please see the below Link: <https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html>

The correct answers are: Enable automatic key rotation for a CMK, Import new key material to a new CMK; Point the key alias to the new CMK.

Submit your Feedback/Queries to our Experts

NEW QUESTION 58

A new application will be deployed on EC2 instances in private subnets. The application will transfer sensitive data to and from an S3 bucket. Compliance requirements state that the data must not traverse the public internet. Which solution meets the compliance requirement? Please select:

- A. Access the S3 bucket through a proxy server
- B. Access the S3 bucket through a NAT gateway.
- C. Access the S3 bucket through a VPC endpoint for S3
- D. Access the S3 bucket through the SSL protected S3 endpoint

Answer: C

Explanation:

The AWS Documentation mentions the following

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

Option A is invalid because using a proxy server is not sufficient enough

Option B and D are invalid because you need secure communication which should not traverse the internet

For more information on VPC endpoints please see the below link <https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-endpoints.html>

The correct answer is: Access the S3 bucket through a VPC endpoint for S3 Submit your Feedback/Queries to our Experts

NEW QUESTION 59

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 60

You are responsible to deploying a critical application onto AWS. Part of the requirements for this application is to ensure that the controls set for this application met PCI compliance. Also there is a need to monitor web application logs to identify any malicious activity. Which of the following services can be used to fulfil this requirement. Choose 2 answers from the options given below Please select:

- A. Amazon Cloudwatch Logs
- B. Amazon VPC Flow Logs
- C. Amazon AWS Config
- D. Amazon Cloudtrail

Answer: AD

Explanation:

The AWS Documentation mentions the following about these services

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 account activity related to actions across your AWS infrastructure. CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting.

Option B is incorrect because VPC flow logs can only check for flow to instances in a VPC Option C is incorrect because this can check for configuration changes only

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

You can use Amazon CloudWatch Logs to monitor, store, and access your log files from Amazon Elastic Compute Cloud (Amazon EC2) instances, AWS CloudTrail, Amazon Route 53, and other sources. You can then retrieve the associated log data from CloudWatch Logs.

For more information on Cloudwatch logs, please refer to below URL: <http://docs.aws.amazon.com/AmazonCloudWatch/latest/loes/WhatIsCloudWatchLoES.html>

The correct answers are: Amazon Cloudwatch Logs, Amazon Cloudtrail

NEW QUESTION 61

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 65

Your company manages thousands of EC2 Instances. There is a mandate to ensure that all servers don't have any critical security flaws. Which of the following can be done to ensure this? Choose 2 answers from the options given below. Please select:

- A. Use AWS Config to ensure that the servers have no critical flaws.
- B. Use AWS inspector to ensure that the servers have no critical flaws.
- C. Use AWS inspector to patch the servers
- D. Use AWS SSM to patch the servers

Answer: BD

Explanation:

The AWS Documentation mentions the following on AWS Inspector
Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for vulnerabilities or deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity. These findings can be reviewed directly or as part of detailed assessment reports which are available via the Amazon Inspector console or API.

Option A is invalid because the AWS Config service is not used to check the vulnerabilities on servers Option C is invalid because the AWS Inspector service is not used to patch servers

For more information on AWS Inspector, please visit the following URL: <https://aws.amazon.com/inspector>

Once you understand the list of servers which require critical updates, you can rectify them by installing the required patches via the SSM tool.

For more information on the Systems Manager, please visit the following URL: <https://docs.aws.amazon.com/systems-manager/latest/APIReference/Welcome.html>

The correct answers are: Use AWS Inspector to ensure that the servers have no critical flaws.. Use AWS SSM to patch the servers

(

NEW QUESTION 70

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

- A. Use AWS Cloudtrail to record the processes running on the server to an S3 bucket.
- B. Use AWS Cloudwatch to record the processes running on the server
- C. Use the SSM Run command to send the list of running processes information to an S3 bucket.
- D. Use AWS Config to see the changed process information on the server

Answer: C

Explanation:

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

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

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

For more information on the Systems Manager Run command, please visit the following URL: <https://docs.aws.amazon.com/systems-manager/latest/userguide/execute-remote-commands.html> The correct answer is: Use the SSM Run command to send the list of running processes information to an S3 bucket. Submit your Feedback/Queries to our Experts

NEW QUESTION 72

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. CloudTrail 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, whereas 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 73

You are building a system to distribute confidential training videos to employees. Using CloudFront, what method could be used to serve content that is stored in S3, but not publicly accessible from S3 directly?

Please select:

- A. Create an Origin Access Identity (OAI) for CloudFront and grant access to the objects in your S3 bucket to that OAI.
- B. Add the CloudFront account security group "amazon-cf/amazon-cf-sg" to the appropriate S3 bucket policy.
- C. Create an Identity and Access Management (IAM) User for CloudFront and grant access to the objects in your S3 bucket to that IAM User.
- D. Create a S3 bucket policy that lists the CloudFront distribution ID as the Principal and the target bucket as the Amazon Resource Name (ARN).

Answer: A

Explanation:

You can optionally secure the content in your Amazon S3 bucket so users can access it through CloudFront but cannot access it directly by using Amazon S3 URLs. This prevents anyone from bypassing CloudFront and using the Amazon S3 URL to get content that you want to restrict access to. This step isn't required to use signed URLs, but we recommend it.

To require that users access your content through CloudFront URLs, you perform the following tasks: Create a special CloudFront user called an origin access identity.

Give the origin access identity permission to read the objects in your bucket. Remove permission for anyone else to use Amazon S3 URLs to read the objects.

Option B, C, and D are all automatically invalid, because the right way is to ensure to create Origin Access Identity (OAI) for CloudFront and grant access accordingly.

For more information on serving private content via CloudFront, please visit the following URL:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/PrivateContent.html>

The correct answer is: Create an Origin Access Identity (OAI) for CloudFront and grant access to the objects in your S3 bucket to that OAI.

You can optionally secure the content in your Amazon S3 bucket so users can access it through CloudFront but cannot access it directly by using Amazon S3 URLs. This prevents anyone from bypassing CloudFront and using the Amazon S3 URL to get content that you want to restrict access to. This step isn't required to use signed URLs, but we recommend it.

To require that users access your content through CloudFront URLs, you perform the following tasks: Create a special CloudFront user called an origin access identity.

Give the origin access identity permission to read the objects in your bucket. Remove permission for anyone else to use Amazon S3 URLs to read the objects.

Option B, C, and D are all automatically invalid, because the right way is to ensure to create Origin Access Identity (OAI) for CloudFront and grant access accordingly.

For more information on serving private content via CloudFront, please visit the following URL:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/PrivateContent.html>

The correct answer is: Create an Origin Access Identity (OAI) for CloudFront and grant access to the objects in your S3 bucket to that OAI.

Submit your Feedback/Queries to our Experts. Submit your Feedback/Queries to our Experts

NEW QUESTION 77

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

Please select:

- A. Change the access keys for all IAM users.
- B. Delete all custom created IAM policies
- C. Delete the access keys for the root account
- D. Confirm MFA to a secure device
- E. Change the password for the root account
- F. Change the password for all IAM users

Answer: CDE

Explanation:

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

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

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

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

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

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

Submit your Feedback/Queries to our Experts

NEW QUESTION 79

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

Please select:

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

Answer: C

Explanation:

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

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

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

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

NEW QUESTION 80

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

Please select:

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

Answer: D

Explanation:

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

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

What geographic region are my keys stored in?

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

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

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

NEW QUESTION 81

You have a set of Customer keys created using the AWS KMS service. These keys have been used for around 6 months. You are now trying to use the new KMS features for the existing set of key's but are not able to do so. What could be the reason for this.

Please select:

- A. You have not explicitly given access via the key policy
- B. You have not explicitly given access via the 1AM policy
- C. You have not given access via the 1AM roles
- D. You have not explicitly given access via 1AM users

Answer: A

Explanation:

By default, keys created in KMS are created with the default key policy. When features are added to KMS, you need to explicitly update the default key policy for these keys.

Option B,C and D are invalid because the key policy is the main entity used to provide access to the keys

For more information on upgrading key policies please visit the following URL: <https://docs.aws.amazon.com/kms/latest/developerguide/key-policy-upgrading.html>

(

The correct answer is: You have not explicitly given access via the key policy Submit your Feedback/Queries to our Experts

NEW QUESTION 85

A company hosts data in S3. There is now a mandate that going forward all data in the S3 bucket needs to encrypt 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 86

You have a set of application, database and web servers hosted in AWS. The web servers are placed behind an ELB. There are separate security groups for the application, database and web servers. The network security groups have been defined accordingly. There is an issue with the communication between the application and database servers. In order to troubleshoot the issue between just the application and database server, what is the ideal set of MINIMAL steps you would take?

Please select:

- A. Check the Inbound security rules for the database security group Check the Outbound security rules for the application security group
- B. Check the Outbound security rules for the database security group I Check the inbound security rules for the application security group
- C. Check the both the Inbound and Outbound security rules for the database security group Check the inbound security rules for the application security group
- D. Check the Outbound security rules for the database security group Check the both the Inbound and Outbound security rules for the application security group

Answer: A

Explanation:

Here since the communication would be established inward to the database server and outward from the application server, you need to ensure that just the Outbound rules for application server security groups are checked. And then just the Inbound rules for database server security groups are checked.

Option B can't be the correct answer. It says that we need to check the outbound security group which is not needed.

We need to check the inbound for DB SG and outbound of Application SG. Because, this two group need to communicate with each other to function properly.

Option C is invalid because you don't need to check for Outbound security rules for the database security group

Option D is invalid because you don't need to check for Inbound security rules for the application security group

For more information on Security Groups, please refer to below URL:

The correct answer is: Check the Inbound security rules for the database security group Check the Outbound security rules for the application security group

Submit your Feedback/Queries to our Experts

NEW QUESTION 89

Your company has a requirement to work with a DynamoDB table. There is a security mandate that all data should be encrypted at rest. What is the easiest way to accomplish this for DynamoDB. Please select:

- A. Use the AWS SDK to encrypt the data before sending it to the DynamoDB table
- B. Encrypt the DynamoDB table using KMS during its creation
- C. Encrypt the table using AWS KMS after it is created
- D. Use S3 buckets to encrypt the data before sending it to DynamoDB

Answer: B

Explanation:

The most easiest option is to enable encryption when the DynamoDB table is created. The AWS Documentation mentions the following Amazon DynamoDB offers fully managed encryption at rest. DynamoDB encryption at rest provides enhanced security by encrypting your data at rest using an AWS Key Management Service (AWS KMS) managed encryption key for DynamoDB. This functionality eliminates the operational burden and complexity involved in protecting sensitive data.

Option A is partially correct, you can use the AWS SDK to encrypt the data, but the easier option would be to encrypt the table before hand.

Option C is invalid because you cannot encrypt the table after it is created

Option D is invalid because encryption for S3 buckets is for the objects in S3 only.

For more information on securing data at rest for DynamoDB please refer to below URL:

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/EncryptionAtRest.html> The correct answer is: Encrypt the DynamoDB table using KMS during its creation Submit your Feedback/Queries to our Experts

NEW QUESTION 91

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

Please select:

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

Answer: ABC

Explanation:

Some of the important aspects in such a situation are

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

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

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

Option D and E are invalid because they could have adverse effects for the other IAM users. For more information on adopting a security framework, please refer to below URL [https://d1.awsstatic.com/whitepapers/compliance/NIST Cybersecurity Framework](https://d1.awsstatic.com/whitepapers/compliance/NIST%20Cybersecurity%20Framework.pdf)

Note:

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

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

Submit your Feedback/Queries to our Experts

NEW QUESTION 93

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

Please select:

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

Answer: B

Explanation:

The AWS Documentation mentions the following

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

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

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

NEW QUESTION 98

Your company uses AWS KMS for management of its customer keys. From time to time, there is a requirement to delete existing keys as part of housekeeping activities. What can be done during the deletion process to verify that the key is no longer being used.

Please select:

- A. Use CloudTrail to see if any KMS API request has been issued against existing keys
- B. Use Key policies to see the access level for the keys
- C. Rotate the keys once before deletion to see if other services are using the keys
- D. Change the IAM policy for the keys to see if other services are using the keys

Answer: A

Explanation:

The AWS documentation mentions the following

You can use a combination of AWS CloudTrail, Amazon CloudWatch Logs, and Amazon Simple Notification Service (Amazon SNS) to create an alarm that notifies you of AWS KMS API requests that attempt to use a customer master key (CMK) that is pending deletion. If you receive a notification from such an alarm, you might want to cancel deletion of the CMK to give yourself more time to determine whether you want to delete it.

Options B and D are incorrect because Key policies nor IAM policies can be used to check if the keys are being used.

Option C is incorrect since rotation will not help you check if the keys are being used. For more information on deleting keys, please refer to below URL:

<https://docs.aws.amazon.com/kms/latest/developerguide/delete-keys-create-cloudwatchalarm.html>

The correct answer is: Use CloudTrail to see if any KMS API request has been issued against existing keys Submit your Feedback/Queries to our Experts

NEW QUESTION 103

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/reference/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 108

DDoS attacks that happen at the application layer commonly target web applications with lower volumes of traffic compared to infrastructure attacks. To mitigate these types of attacks, you should probably want to include a WAF (Web Application Firewall) as part of your infrastructure. To inspect all HTTP requests, WAFs sit in-line with your application traffic. Unfortunately, this creates a scenario where WAFs can become a point of failure or bottleneck. To mitigate this problem, you need the ability to run multiple WAFs on demand during traffic spikes. This type of scaling for WAF is done via a "WAF sandwich." Which of the following statements best describes what a "WAF sandwich" is? Choose the correct answer from the options below

Please select:

- A. The EC2 instance running your WAF software is placed between your private subnets and any NATed connections to the internet.
- B. The EC2 instance running your WAF software is placed between your public subnets and your Internet Gateway.
- C. The EC2 instance running your WAF software is placed between your public subnets and your private subnets.
- D. The EC2 instance running your WAF software is included in an Auto Scaling group and placed in between two Elastic load balancers.

Answer: D

Explanation:

The below diagram shows how a WAF sandwich is created. Its the concept of placing the Ec2 instance which hosts the WAF software in between 2 elastic load balancers.

Option A,B and C are incorrect since the EC2 Instance with the WAF software needs to be placed in an Autoscaling Group For more information on a WAF sandwich please refer to the below Link: <https://www.cloudaxis.com/2016/11/21/waf-sandwich/>

The correct answer is: The EC2 instance running your WAF software is included in an Auto Scaling group and placed in between two Elastic load balancers. Submit your Feedback/Queries to our Experts

NEW QUESTION 111

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

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

Answer: BD

Explanation:

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

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

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

NEW QUESTION 114

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

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

Answer: BC

Explanation:

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

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

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

Examining CMK Permissions to Determine the Scope of Potential Usage

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

Examining AWS CloudTrail Logs to Determine Actual Usage

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

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

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

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

NEW QUESTION 118

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

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

Answer: BC

Explanation:

The AWS Documentation mentions the following

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

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

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

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

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

Submit your Feedback/Queries to our Experts

NEW QUESTION 122

An application is designed to run on an EC2 Instance. The applications 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 125

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 Documentati 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 130

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 practice

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 132

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 133

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 IAM 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 134

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 There seems to be a set of malicious requests coming from a set of IP addresses
- 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 138

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 1AM 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 STANDARDIA (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 1AM policies cannot be used to move data to Glacier

Option D is invalid because lifecycle policies is not used to move data to Redshift For more information on S3 lifecycle policies, please visit the URL:

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

The correct answer is: Upload data to S3 and use lifecycle policies to move the data into Glacier for long-term archiving.

Submit your Feedback/Queries to our Experts

NEW QUESTION 139

A company is planning on using AWS EC2 and AWS Cloudfront for their web application. For which one of the below attacks is usage of Cloudfront most suited for?

Please select:

- A. Cross side scripting
- B. SQL injection
- C. DDoS attacks
- D. Malware attacks

Answer: C

Explanation:

The below table from AWS shows the security capabilities of AWS Cloudfront AWS Cloudfront is more prominent for DDoS attacks.

Options A,B and D are invalid because Cloudfront is specifically used to protect sites against DDoS attacks For more information on security with Cloudfront, please refer to the below Link: <https://d1.awsstatic.com/whitepapers/Security/Secure content delivery with CloudFront whitepaper.pdf>

The correct answer is: DDoS attacks

Submit your Feedback/Queries to our Experts

NEW QUESTION 140

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 141

In your LAMP application, you have some developers that say they would like access to your logs. However, since you are using an AWS Auto Scaling group, your instances are constantly being recreated.

What would you do to make sure that these developers can access these log files? Choose the correct answer from the options below

Please select:

- A. Give only the necessary access to the Apache servers so that the developers can gain access to the log files.
- B. Give root access to your Apache servers to the developers.
- C. Give read-only access to your developers to the Apache servers.
- D. Set up a central logging server that you can use to archive your logs; archive these logs to an S3 bucket for developer-access.

Answer: D

Explanation:

One important security aspect is to never give access to actual servers, hence Option A,B and C are just totally wrong from a security perspective.

The best option is to have a central logging server that can be used to archive logs. These logs can then be stored in S3.

Options A,B and C are all invalid because you should not give access to the developers on the Apache server

For more information on S3, please refer to the below link <https://aws.amazon.com/documentation/s3>

The correct answer is: Set up a central logging server that you can use to archive your logs; archive these logs to an S3 bucket for developer-access.

Submit your Feedback/Queries to our Experts

NEW QUESTION 146

Your company is planning on developing an application in AWS. This is a web based application. The application user 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 IAM users to manage the user profiles

Answer: C

Explanation:

The AWS Documentation mentions the following

A user pool is a user directory in Amazon Cognito. With a user pool, your users can sign in to your web or mobile app through Amazon Cognito. Your users can also sign in through social identity providers like Facebook or Amazon, and through SAML identity providers. Whether your users sign in directly or through a third party, all members of the user pool have a directory profile that you can access through an SDK.

User pools provide:

Sign-up and sign-in services.

A built-in, customizable web UI to sign in users.

Social sign-in with Facebook, Google, and Login with Amazon, as well as sign-in with SAML identity providers from your user pool.

User directory management and user profiles.

Security features such as multi-factor authentication (MFA), checks for compromised credentials, account takeover protection, and phone and email verification.

Customized workflows and user migration through AWS Lambda triggers. Options A and B are invalid because these are not used to manage users Option D is invalid because this would be a maintenance overhead

For more information on Cognito User Identity pools, please refer to the below Link: <https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-user-identity-pools.html>

The correct answer is: Use AWS Cognito to manage the user profiles Submit your Feedback/Queries to our Experts

NEW QUESTION 148

A company has set up EC2 instances on the AWS 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 following:

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 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 149

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 153

Which of the following bucket policies will ensure that objects being uploaded to a bucket called 'demo' are encrypted.

Please select:

- A.
- B.
- C.
- D.

A.

Answer: A

Explanation:

The condition of "s3:x-amz-server-side-encryption":"aws:kms" ensures that objects uploaded need to be encrypted. Options B,C and D are invalid because you have to ensure the condition of ns3:x-amz-server-sideencryption":" aws:kms" is present For more information on AWS KMS best practices, just browse to the below URL:
<https://dl.awsstatic.com/whitepapers/aws-kms-best-practices.pdf>

Submit your Feedback/Queries to our Expert

NEW QUESTION 155

A company's AWS account consists of approximately 300 IAM users. Now there is a mandate that an access change is required for 100 IAM users to have unlimited privileges to S3.As a system administrator, how can you implement this effectively so that there is no need to apply the policy at the individual user level? Please select:

- A. Create a new role and add each user to the IAM role
- B. Use the IAM groups and add users, based upon their role, to different groups and apply the policy to group
- C. Create a policy and apply it to multiple users using a JSON script
- D. Create an S3 bucket policy with unlimited access which includes each user's AWS account ID

Answer: B

Explanation:

Option A is incorrect since you don't add a user to the 1AM Role Option C is incorrect since you don't assign multiple users to a policy Option D is incorrect since this is not an ideal approach An 1AM group is used to collectively manage users who need the same set of permissions. By having groups, it becomes easier to manage permissions. So if you change the permissions on the group scale, it will affect all the users in that group For more information on 1AM Groups, just browse to the below URL:
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_eroups.html
The correct answer is: Use the 1AM groups and add users, based upon their role, to different groups and apply the policy to group
Submit your Feedback/Queries to our Experts

NEW QUESTION 159

You need to create a policy and apply it for just an individual user. How could you accomplish this in the right way? Please select:

- A. Add an AWS managed policy for the user
- B. Add a service policy for the user
- C. Add an 1AM role for the user
- D. Add an inline policy for the user

Answer: D

Explanation:

Options A and B are incorrect since you need to add an inline policy just for the user Option C is invalid because you don't assign an 1AM role to a user The AWS Documentation mentions the following An inline policy is a policy that's embedded in a principal entity (a user, group, or role)—that is, the policy is an inherent part of the principal entity. You can create a policy and embed it in a principal entity, either when you create the principal entity or later. For more information on 1AM Access and Inline policies, just browse to the below URL: <https://docs.aws.amazon.com/IAM/latest/UserGuide/access>
The correct answer is: Add an inline policy for the user Submit your Feedback/Queries to our Experts

NEW QUESTION 160

Your CTO is very worried about the security of your AWS account. How best can you prevent hackers from completely hijacking your account? Please select:

- A. Use short but complex password on the root account and any administrators.
- B. Use AWS 1AM Geo-Lock and disallow anyone from logging in except for in your city.
- C. Use MFA on all users and accounts, especially on the root account.
- D. Don't write down or remember the root account password after creating the AWS account

Answer: C

Explanation:

Multi-factor authentication can add one more layer of security to your AWS account Even when you go to your Security Credentials dashboard one of the items is to enable MFA on your root account Option A is invalid because you need to have a good password policy Option B is invalid because there is no 1AM Geo-Lock Option D is invalid because this is not a recommended practices For more information on MFA, please visit the below URL http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa.html
The correct answer is: Use MFA on all users and accounts, especially on the root account. Submit your Feedback/Queries to our Experts

NEW QUESTION 162

There are currently multiple applications hosted in a VPC. During monitoring it has been noticed that multiple port scans are coming in from a specific IP Address block. The internal security team has requested that all offending IP Addresses be denied for the next 24 hours. Which of the following is the best method to quickly and temporarily deny access from the specified IP Address's.

Please select:

- A. Create an AD policy to modify the Windows Firewall settings on all hosts in the VPC to deny access from the IP Address block.
- B. Modify the Network ACLs associated with all public subnets in the VPC to deny access from the IP Address block.
- C. Add a rule to all of the VPC Security Groups to deny access from the IP Address block.
- D. Modify the Windows Firewall settings on all AMI'S that your organization uses in that VPC to deny access from the IP address block.

Answer: B

Explanation:

NACL acts as a firewall at the subnet level of the VPC and we can deny the offending IP address block at the subnet level using NACL rules to block the incoming traffic to the VPC instances. Since NACL rules are applied as per the Rule numbers make sure that this rule number should take precedence over other rule numbers if there are any such rules that will allow traffic from these IP ranges. The lowest rule number has more precedence over a rule that has a higher number.

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 a 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). Options C is invalid because these options are not available

Option D is invalid because there is not root access for users

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: Modify the Network ACLs associated with all public subnets in the VPC to deny access from the IP Address block.

omit your Feedback/Queries to our Experts

NEW QUESTION 165

.....

Relate Links

100% Pass Your AWS-Certified-Security-Specialty Exam with Exambible Prep Materials

<https://www.exambible.com/AWS-Certified-Security-Specialty-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>