

Exam Questions AWS-Certified-Security-Specialty

Amazon AWS Certified Security - Specialty

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



NEW QUESTION 1

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

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

Answer: C

Explanation:

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

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

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

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

NEW QUESTION 2

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

A.

B.

C.

D.

A.

Answer: A

Explanation:

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

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

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

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

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

NEW QUESTION 3

You are hosting a web site via website hosting on an S3 bucket - `http://demo.s3-website-us-east-1`

`.amazonaws.com`. You have some web pages that use Javascript that access resources in another bucket which has web site hosting also enabled. But when users access the web pages, they are getting a blocked Javascript error. How can you rectify this?

Please select:

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

Answer: A

Explanation:

Your answer is incorrect Answer-A

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

Use-case Scenarios

The following are example scenarios for using CORS:

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

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

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

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

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

The correct answer is: Enable CORS for the bucket

Submit your Feedback/Queries to our Experts

NEW QUESTION 4

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 5

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 6

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

authentication for these users. How can this be accomplished?

Please select:

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

Answer: A

Explanation:

The AWS Documentation mentions the following as a best practices for 1AM users. For extra security, enable multi-factor authentication (MFA) for privileged 1AM users (users who are allowed access to sensitive resources or APIs). With MFA, users have a device that generates unique authentication code (a one-time password, or OTP). Users must provide both their normal credentials (like their user name and password) and the OTP. The MFA device can either be a special piece of hardware, or it can be a virtual device (for example, it can run in an app on a smartphone).

Option B,C and D are invalid because no such security options are available in AWS For more information on 1AM best practices, please visit the below URL <https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html> The correct answer is: Enable MFA for these user accounts

Submit your Feedback/Queries to our Experts

NEW QUESTION 7

Your IT Security department has mandated that all data on EBS volumes created for underlying EC2 Instances need to be encrypted. Which of the following can help achieve this?

Please select:

- A. AWS KMS API
- B. AWS Certificate Manager
- C. API Gateway with STS
- D. 1AM Access Key

Answer: A

Explanation:

The AWS Documentation mentions the following on AWS KMS

AWS Key Management Service (AWS KMS) is a managed service that makes it easy for you to create and control the encryption keys used to encrypt your data

A. AWS KMS is integrated with other AWS

services including Amazon Elastic Block Store (Amazon EBS), Amazon Simple Storage Service (Amazon S3), Amazon Redshift Amazon Elastic Transcoder, Amazon WorkMail, Amazon Relational Database Service (Amazon RDS), and others to make it simple to encrypt your data with encryption keys that you manage

Option B is incorrect - The AWS Certificate manager can be used to generate SSL certificates that can be used to encrypt traffic transit, but not at rest

Option C is incorrect is again used for issuing tokens when using API gateway for traffic in transit. Option D is used for secure access to EC2 Instances

For more information on AWS KMS, please visit the following URL: <https://docs.aws.amazon.com/kms/latest/developerguide/overview.html> The correct answer is: AWS KMS API

Submit your Feedback/Queries to our Experts

NEW QUESTION 8

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

Please select:

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

Answer: B

Explanation:

The AWS Documentation mentions the following.

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

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

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

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

NEW QUESTION 9

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

Please select:

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

Answer: B

Explanation:

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

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

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

The AWS Documentation mentions the following

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

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

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

NEW QUESTION 10

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

How can the security team fulfill these requirements?

Please select:

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

Answer: B

Explanation:

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

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

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

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

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

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

NEW QUESTION 10

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

Please select:

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

Answer: A

Explanation:

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

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

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

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

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

NEW QUESTION 11

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 16

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

Please select:

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

Answer: D

Explanation:

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

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

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

[.com/AmazonVPC/latest/Peeri](https://aws.amazon.com/VPC/latest/Peering/)

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

NEW QUESTION 19

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

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

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

Answer: B

Explanation:

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

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

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

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

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

NEW QUESTION 22

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

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

Answer: A

Explanation:

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

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

For more information, please visit the below URL id=docs_orgs_console <https://docs.aws.amazon.com/IAM/latest/UserGi-manage-attach-policy.html>

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

Submit your Feedback/Queries to our Experts

NEW QUESTION 24

You want to launch an EC2 Instance with your own key pair in AWS. How can you achieve this?
Choose 3 answers from the options given below. Please select:

- A. Use a third party tool to create the Key pair
- B. Create a new key pair using the AWS CLI
- C. Import the public key into EC2
- D. Import the private key into EC2

Answer: ABC

Explanation:

This is given in the AWS Documentation Creating a Key Pair

You can use Amazon EC2 to create your key pair. For more information, see Creating a Key Pair Using Amazon EC2.

Alternatively, you could use a third-party tool and then import the public key to Amazon EC2. For more information, see Importing Your Own Public Key to Amazon EC2.

Option B is Correct, because you can use the AWS CLI to create a new key pair 1 <https://docs.aws.amazon.com/cli/latest/userguide/cli-ec2-keypairs.html>

Option D is invalid because the public key needs to be stored in the EC2 Instance For more information on EC2 Key pairs, please visit the below URL:

* <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs>

The correct answers are: Use a third party tool to create the Key pair. Create a new key pair using the AWS CLI, Import the public key into EC2

Submit your Feedback/Queries to our Experts

NEW QUESTION 29

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 Cloud Front 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 31

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 33

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

Please select:

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

Answer: D

Explanation:

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

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

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

Insecure Server Protocols

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

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

(

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

Submit your Feedback/Queries to our Experts

NEW QUESTION 36

How can you ensure that instance in an VPC does not use AWS DNS for routing DNS requests. You want to use your own managed DNS instance. How can this be achieved?

Please select:

- A. Change the existing DHCP options set
- B. Create a new DHCP options set and replace the existing one.
- C. Change the route table for the VPC
- D. Change the subnet configuration to allow DNS requests from the new DNS Server

Answer: B

Explanation:

In order to use your own DNS server, you need to ensure that you create a new custom DHCP options set with the IP of th custom DNS server. You cannot modify the existing set, so you need to create a new one.

Option A is invalid because you cannot make changes to an existing DHCP options Set.

Option C is invalid because this can only be used to work with Routes and not with a custom DNS solution.

Option D is invalid because this needs to be done at the VPC level and not at the Subnet level For more information on DHCP options set, please visit the following url <https://docs.aws.amazon.com/AmazonVPC/latest/UserGuideA/PC DHCP Options.html>

The correct answer is: Create a new DHCP options set and replace the existing one. Submit your Feedback/Queries to our Experts

NEW QUESTION 37

You need to have a cloud security device which would allow to generate encryption keys based on FIPS 140-2 Level 3. Which of the following can be used for this purpose.

Please select:

- A. AWS KMS
- B. AWS Customer Keys
- C. AWS managed keys
- D. AWS Cloud HSM

Answer: AD

Explanation:

AWS Key Management Service (KMS) now uses FIPS 140-2 validated hardware security modules (HSM) and supports FIPS 140-2 validated endpoints, which provide independent assurances about the confidentiality and integrity of your keys.

All master keys in AWS KMS regardless of their creation date or origin are automatically protected using FIPS 140-2 validated HSMs. defines four levels of security, simply named "Level 1" to "Level 4". It does not specify in detail what level of security is required by any particular application.

- FIPS 140-2 Level 1 the lowest, imposes very limited requirements; loosely, all components must be "production-grade" anc various egregious kinds of insecurity must be absent

- FIPS 140-2 Level 2 adds requirements for physical tamper-evidence and role-based authentication.

- FIPS 140-2 Level 3 adds requirements for physical tamper-resistance (making it difficult for attackers to gain access to sensitive information contained in the module) and identity-based authentication, and for a physical or logical separation between the interfaces by which "critical security parameters" enter and leave the module, and its other interfaces.

- FIPS 140-2 Level 4 makes the physical security requirements more stringent and requires robustness against environmental attacks.

AWSCloudHSM provides you with a FIPS 140-2 Level 3 validated single-tenant HSM cluster in your Amazon Virtual Private Cloud (VPQ to store and use your keys. You have exclusive control over how your keys are used via an authentication mechanism independent from AWS. You interact with keys in your AWS CloudHSM cluster similar to the way you interact with your applications running in Amazon EC2.

AWS KMS allows you to create and control the encryption keys used by your applications and supported AWS services in multiple regions around the world from a single console. The service uses a FIPS 140-2 validated HSM to protect the security of your keys. Centralized management of all your keys in AWS KMS lets you enforce who can use your keys under which conditions, when they get rotated, and who can manage them.

AWS KMS HSMs are validated at level 2 overall and at level 3 in the following areas:

- Cryptographic Module Specification

- Roles, Services, and Authentication
- Physical Security
- Design Assurance

So I think that we can have 2 answers for this question. Both A & D.

- <https://aws.amazon.com/blogs/security/aws-key-management-service-now-offers-fips-140-2-validated-cryptographic-modules-enabling-easier-adoption-of-the-service-for-regulated-workloads/>
- <https://aws.amazon.com/cloudhsm/faqs/>
- <https://aws.amazon.com/kms/faqs/>
- <https://en.wikipedia.org/wiki/RPS>

The AWS Documentation mentions the following

AWS CloudHSM is a cloud-based hardware security module (HSM) that enables you to easily generate and use your own encryption keys on the AWS Cloud.

With CloudHSM, you can manage your own encryption keys using FIPS 140-2 Level 3 validated HSMs. CloudHSM offers you the flexibility to integrate with your applications using industry-standard APIs, such as PKCS#11, Java

Cryptography Extensions (JCE), and Microsoft CryptoNG (CNG) libraries. CloudHSM is also standards-compliant and enables you to export all of your keys to most other commercially-available HSMs. It is a fully-managed service that automates time-consuming administrative tasks for you, such as hardware provisioning, software patching, high-availability, and backups. CloudHSM also enables you to scale quickly by adding and removing HSM capacity on-demand, with no up-front costs.

All other options are invalid since AWS Cloud HSM is the prime service that offers FIPS 140-2 Level 3 compliance

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

The correct answers are: AWS KMS, AWS Cloud HSM Submit your Feedback/Queries to our Experts

NEW QUESTION 38

You are trying to use the Systems Manager to patch a set of EC2 systems. Some of the systems are not getting covered in the patching process. Which of the following can be used to troubleshoot the issue? Choose 3 answers from the options given below.

Please select:

- A. Check to see if the right role has been assigned to the EC2 instances
- B. Check to see if the IAM user has the right permissions for EC2
- C. Ensure that agent is running on the instances.
- D. Check the Instance status by using the Health API

Answer: ACD

Explanation:

For ensuring that the instances are configured properly you need to ensure the following:

- 1) You installed the latest version of the SSM Agent on your instance
- 2) Your instance is configured with an AWS Identity and Access Management (IAM) role that enables the instance to communicate with the Systems Manager API
- 3) You can use the Amazon EC2 Health API to quickly determine the following information about Amazon EC2 instances:
 - The status of one or more instances
 - The last time the instance sent a heartbeat value
 - The version of the SSM Agent
 - The operating system
 - The version of the EC2Config service (Windows)
 - The status of the EC2Config service (Windows)

Option B is invalid because IAM users are not supposed to be directly granted permissions to EC2 instances. For more information on troubleshooting AWS SSM, please visit the following URL: <https://docs.aws.amazon.com/systems-manager/latest/userguide/troubleshooting-remote-commands.html>

The correct answers are: Check to see if the right role has been assigned to the EC2 instances, Ensure that agent is running on the instances., Check the Instance status by using the Health API.

Submit your Feedback/Queries to our Experts

NEW QUESTION 40

You have an EBS volume attached to an EC2 instance which uses KMS for encryption. Someone has now gone ahead and deleted the Customer Key which was used for the EBS encryption. What should be done to ensure the data can be decrypted?

Please select:

- A. Create a new Customer Key using KMS and attach it to the existing volume
- B. You cannot decrypt the data that was encrypted under the CMK, and the data is not recoverable.
- C. Request AWS Support to recover the key
- D. Use AWS Config to recover the key

Answer: B

Explanation:

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.

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

A is incorrect because creating a new CMK and attaching it to the existing volume will not allow the data to be decrypted; you cannot attach customer master keys after the volume is encrypted.

Option C and D are invalid because once the key has been deleted, you cannot recover it. For more information on EBS encryption with KMS, please visit the following URL: <https://docs.aws.amazon.com/kms/latest/developerguide/services-ebs.html>

The correct answer is: You cannot decrypt the data that was encrypted under the CMK, and the data is not recoverable. Submit your Feedback/Queries to our Experts

NEW QUESTION 41

You work as an administrator for a company. The company hosts a number of resources using AWS. There is an incident of a suspicious API activity which occurred 11 days ago. The Security Admin has asked to get the API activity from that point in time. How can this be achieved?

Please select:

- A. Search the CloudWatch logs to find for the suspicious activity which occurred 11 days ago
- B. Search the CloudTrail event history on the API events which occurred 11 days ago.
- C. Search the CloudWatch metrics to find for the suspicious activity which occurred 11 days ago

D. Use AWS Config to get the API calls which were made 11 days ago

Answer: B

Explanation:

The Cloud Trail event history allows to view events which are recorded for 90 days. So one can use a metric filter to gather the API calls from 11 days ago. Option A and C is invalid because Cloudwatch is used for logging and not for monitoring API activity Option D is invalid because AWSConfig is a configuration service and not for monitoring API activity For more information on AWS Cloudtrail, please visit the following URL:
<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/how-cloudtrail-works.html>

Note:

In this question we assume that the customer has enabled cloud trail service.

AWS CloudTrail is enabled by default for ALL CUSTOMERS and will provide visibility into the past seven days of account activity without the need for you to configure a trail in the service to get started. So for an activity that happened 11 days ago to be stored in the cloud trail we need to configure the trail manually to ensure that it is stored in the events history.

• <https://aws.amazon.com/blogs/aws/new-amazon-web-services-extends-cloudtrail-to-all-awscustomers/> The correct answer is: Search the Cloudtrail event history on the API events which occurred 11 days ago.

NEW QUESTION 44

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

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

Answer: A

Explanation:

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

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

VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC 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 45

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:

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 46

An EC2 Instance hosts a Java based application that access a DynamoDB table. This EC2 Instance is currently serving production based users. Which of the

following is a secure way of ensuring that the EC2 Instance access the Dynamo table
Please select:

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

Answer: A

Explanation:

To always ensure secure access to AWS resources from EC2 Instances, always ensure to assign a Role to the EC2 Instance Option B is invalid because KMS keys are not used as a mechanism for providing EC2 Instances access to AWS services. Option C is invalid Access keys is not a safe mechanism for providing EC2 Instances access to AWS services. Option D is invalid because there is no way access groups can be assigned to EC2 Instances. For more information on 1AM Roles, please refer to the below URL:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html

The correct answer is: Use 1AM Roles with permissions to interact with DynamoDB and assign it to the EC2 Instance Submit your Feedback/Queries to our Experts

NEW QUESTION 50

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

Please select:

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

Answer: B

Explanation:

The AWS Documentation mentions the following

You can now turn on a trail across all regions for your AWS account. CloudTrail will deliver log files from all regions to the Amazon S3 bucket and an optional CloudWatch Logs log group you specified. Additionally, when AWS launches a new region, CloudTrail will create the same trail in the new region. As a result you will receive log files containing API activity for the new region without taking any action.

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

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

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

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

NEW QUESTION 52

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

Please select:

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

Answer: C

Explanation:

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

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

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

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

NEW QUESTION 53

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 55

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

Please select:

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

Answer: C

Explanation:

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

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

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

A. Any object metadata is not encrypted. For

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

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

NEW QUESTION 56

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

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

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

Answer: B

Explanation:

The most probable cause is that you have not allowed the Lambda functions to have the appropriate permissions on the S3 bucket to make the relevant changes.

Option A is invalid because this is more of a permission instead of a configuration rule issue. Option C is invalid because changing the language will not be the core solution.

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

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

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

NEW QUESTION 57

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

Please select:

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

Answer: B

Explanation:

The AWS Security best practises mentions the following

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

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

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

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

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

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

NEW QUESTION 61

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

Please select:

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

Answer: BC

Explanation:

Below is the snapshot of the Shared Responsibility Model

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

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

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

NEW QUESTION 65

A Devops team is currently looking at the security aspect of their CI/CD pipeline. They are making use of AWS resource? for their infrastructure. They want to ensure that the EC2 Instances don't have any high security vulnerabilities. They want to ensure a complete DevSecOps process. How can this be achieved?

Please select:

- A. Use AWS Config to check the state of the EC2 instance for any sort of security issues.
- B. Use AWS Inspector API's in the pipeline for the EC2 Instances
- C. Use AWS Trusted Advisor API's in the pipeline for the EC2 Instances
- D. Use AWS Security Groups to ensure no vulnerabilities are present

Answer: B

Explanation:

Amazon Inspector offers a programmatic way to find security defects or misconfigurations in your operating systems and applications. Because you can use API calls to access both the processing of assessments and the results of your assessments, integration of the findings into workflow and notification systems is simple. DevOps teams can integrate Amazon Inspector into their CI/CD pipelines and use it to identify any pre-existing issues or when new issues are introduced. Option A.C and D are all incorrect since these services cannot check for Security Vulnerabilities. These can only be checked by the AWS Inspector service.

For more information on AWS Security best practices, please refer to below URL: [https://d1.awsstatic.com/whitepapers/Security/AWS Security Best Practices.pdf](https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf)

The correct answer is: Use AWS Inspector API's in the pipeline for the EC2 Instances Submit your Feedback/Queries to our Experts

NEW QUESTION 70

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

Choose the correct answer from the options below

Please select:

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

Answer: D

Explanation:

The AWS Documentation mentions the following

"When you write such an app, you'll make requests to AWS services that must be signed with an AWS access key. However, we strongly recommend that you do not embed or distribute long-term AWS credentials with apps that a user downloads to a device, even in an encrypted store. Instead, build your app so that it requests temporary AWS security credentials dynamically when needed using web

identity federation. The supplied temporary credentials map to an AWS role that has only the permissions needed to perform the tasks required by the mobile app".

Option A, B and C are all automatically incorrect because you need to use IAM Roles for Secure access to services. For more information on web identity

federation please refer to the below Link: http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_oidc.html

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

Submit your Feedback/Queries to our Experts

NEW QUESTION 71

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

Please select:

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

Answer: B

Explanation:

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

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

<https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-iam.html>

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

NEW QUESTION 72

You are planning on using the AWS KMS service for managing keys for your application. For which of the following can the KMS CMK keys be used for encrypting? Choose 2 answers from the options given below

Please select:

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

Answer: CD

Explanation:

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

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

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

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

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

NEW QUESTION 73

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

Please select:

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

Answer: A

Explanation:

This is mentioned in the AWS Documentation

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

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

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

and passed to the cluster across a secure channel.

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

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

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

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

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

NEW QUESTION 76

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

Please select:

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

Answer: BC

Explanation:

The AWS Documentation mentions the following

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

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

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

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

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

Submit your Feedback/Queries to our Experts

NEW QUESTION 79

Your company has been using AWS for the past 2 years. They have separate S3 buckets for logging the various AWS services that have been used. They have hired an external vendor for analyzing their log files. They have their own AWS account. What is the best way to ensure that the partner account can access the log files in the company account for analysis. Choose 2 answers from the options given below

Please select:

- A. Create an IAM user in the company account
- B. Create an IAM Role in the company account
- C. Ensure the IAM user has access for read-only to the S3 buckets
- D. Ensure the IAM Role has access for read-only to the S3 buckets

Answer: BD

Explanation:

The AWS Documentation mentions the following

To share log files between multiple AWS accounts, you must perform the following general steps. These steps are explained in detail later in this section.

Create an IAM role for each account that you want to share log files with.

For each of these IAM roles, create an access policy that grants read-only access to the account you want to share the log files with.

Have an IAM user in each account programmatically assume the appropriate role and retrieve the log files.

Options A and C are invalid because creating an IAM user and then sharing the IAM user credentials with the vendor is a direct 'NO' practise from a security perspective.

For more information on sharing cloudtrail logs files, please visit the following URL <https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-share-logs.html>

The correct answers are: Create an IAM Role in the company account Ensure the IAM Role has access for read-only to the S3 buckets

Submit your Feedback/Queries to our Experts

NEW QUESTION 81

A company is planning on using AWS for hosting their applications. They want complete separation and isolation of their production , testing and development environments. Which of the following is an ideal way to design such a setup?

Please select:

- A. Use separate VPCs for each of the environments
- B. Use separate IAM Roles for each of the environments
- C. Use separate IAM Policies for each of the environments
- D. Use separate AWS accounts for each of the environments

Answer: D

Explanation:

A recommendation from the AWS Security Best practices highlights this as well

option A is partially valid, you can segregate resources, but a best practise is to have multiple accounts for this setup.

Options B and C are invalid because from a maintenance perspective this could become very difficult For more information on the Security Best practices, please visit the following URL: https://dl.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf

The correct answer is: Use separate AWS accounts for each of the environments Submit your Feedback/Queries to our Experts

NEW QUESTION 86

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](https://d1.awsstatic.com/whitepapers/Security/AWS%20Security%20Best%20Practices.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 87

A user has enabled versioning on an S3 bucket. The user is using server side encryption for data at Rest. If the user is supplying his own keys for encryption SSE-C, which of the below mentioned statements is true? Please select:

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

Answer: B

Explanation:

Managing your own encryption keys, you

You can encrypt the object and send it across to S3

Option A is invalid because ideally you should use different encryption keys Option C is invalid because you can use your own encryption keys Option D is invalid because encryption works even if versioning is enabled For more information on client side encryption please visit the below Link: ["Keys.html](https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingClientSideEncryption.html)

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

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

NEW QUESTION 90

Your developer is using the KMS service and an assigned key in their Java program. They get the below error when running the code

arn:aws:iam::113745388712:user/UserB is not authorized to perform: kms:DescribeKey Which of the following could help resolve the issue?

Please select:

- A. Ensure that UserB is given the right IAM role to access the key
- B. Ensure that UserB is given the right permissions in the IAM policy
- C. Ensure that UserB is given the right permissions in the Key policy
- D. Ensure that UserB is given the right permissions in the Bucket policy

Answer: C

Explanation:

You need to ensure that UserB is given access via the Key policy for the Key

Option is invalid because you don't assign roles to IAM users For more information on Key policies please visit the below Link:

<https://docs.aws.amazon.com/kms/latest/developerguide/key-poli>

The correct answer is: Ensure that UserB is given the right permissions in the Key policy

NEW QUESTION 92

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

Please select:

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

Answer: B

Explanation:

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

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

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

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

NEW QUESTION 93

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

Please select:

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

Answer: A

Explanation:

The following diagram from the AWS Documentation shows how you can access the DynamoDB service from within a V without going to the Internet This can be

done with the help of a VPC endpoint

Option B is invalid because this is used for connection between an on-premise solution and AWS Option C is invalid because there is no such option
Option D is invalid because this is used to connect 2 VPCs
For more information on VPC endpoints for DynamoDB, please visit the URL:
The correct answer is: Use a VPC endpoint to the DynamoDB table Submit your Feedback/Queries to our Experts

NEW QUESTION 96

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

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

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

Answer: B

Explanation:

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

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

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

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

NEW QUESTION 98

Your company is planning on using AWS EC2 and ELB for deployment for their web applications. The security policy mandates that all traffic should be encrypted.

Which of the following options will ensure that this requirement is met. Choose 2 answers from the options below.

Please select:

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

Answer: BC

Explanation:

The AWS Documentation mentions the following

You can create a load balancer that listens on both the HTTP (80) and HTTPS (443) ports. If you specify that the HTTPS listener sends requests to the instances

on port 80, the load balancer terminates the requests and communication from the load balancer to the instances is not encrypted, if the HTTPS listener sends requests to the instances on port 443, communication from the load balancer to the instances is encrypted.

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

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

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

Submit your Feedback/Queries to our Experts

NEW QUESTION 100

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

Please select:

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

Answer: D

Explanation:

The AWS blogs mention the following to support the use of AWS GuardDuty

GuardDuty voraciously consumes multiple data streams, including several threat intelligence feeds, staying aware of malicious addresses, devious domains, and more importantly, learning to accurately identify malicious or unauthorized behavior in your AWS accounts. In combination with information gleaned from your VPC Flow Logs, AWS CloudTrail Event Logs, and DNS logs, th allows GuardDuty to

detect many different types of dangerous and mischievous behavior including probes for known vulnerabilities, port scans and probes, and access from unusual locations. On the AWS side, it looks for suspicious AWS account activity such as unauthorized deployments, unusual CloudTrail activity, patterns of access to AWS API functions, and attempts to exceed multiple service limits. GuardDuty will also look for compromised EC2 instances talking to malicious entities or services, data exfiltration attempts, and instances that are mining cryptocurrency.

Options A, B and C are invalid because these services cannot be used to detect port scans For more information on AWS Guard Duty, please refer to the below Link:

<https://aws.amazon.com/blogs/aws/amazon-guardduty-continuous-security-monitoring-threatdetection/>; (

The correct answer is: Use AWS Guard Duty to monitor any malicious port scans Submit your Feedback/Queries to our Experts

NEW QUESTION 102

Your company has many AWS accounts defined and all are managed via AWS Organizations. One AWS account has a S3 bucket that has critical dat

A. How can we ensure that all the users in the AWS organisation have access to this bucket? Please select:

- B. Ensure the bucket policy has a condition which involves aws:PrincipalOrgID
- C. Ensure the bucket policy has a condition which involves aws:AccountNumber
- D. Ensure the bucket policy has a condition which involves aws:PrincipalID
- E. Ensure the bucket policy has a condition which involves aws:OrgID

Answer: A

Explanation:

The AWS Documentation mentions the following

AWS Identity and Access Management (IAM) now makes it easier for you to control access to your AWS resources by using the AWS organization of 1AM principals (users and roles). For some services, you grant permissions using resource-based policies to specify the accounts and principals that can access the resource and what actions they can perform on it. Now, you can use a new condition key, aws:PrincipalOrgID, in these policies to require all principals accessing the resource to be from an account in the organization

Option B.C and D are invalid because the condition in the bucket policy has to mention aws:PrincipalOrgID

For more information on controlling access via Organizations, please refer to the below Link: <https://aws.amazon.com/blogs/security/control-access-to-aws-resources-by-usins-the-awsorganization-of-iam-principal/>

(

The correct answer is: Ensure the bucket policy has a condition which involves aws:PrincipalOrgID Submit your Feedback/Queries to our Experts

NEW QUESTION 105

Your organization is preparing for a security assessment of your use of AWS. In preparation for this assessment, which three 1AM best practices should you consider implementing?

Please select:

- A. Create individual 1AM users
- B. Configure MFA on the root account and for privileged 1AM users
- C. Assign 1AM users and groups configured with policies granting least privilege access
- D. Ensure all users have been assigned and dre frequently rotating a password, access ID/secret key, and X.509 certificate

Answer: ABC

Explanation:

When you go to the security dashboard, the security status will show the best practices for initiating the first level of security.

Option D is invalid because as per the dashboard, this is not part of the security recommendation For more information on best security practices please visit the URL: <https://aws.amazon.com/whitepapers/aws-security-best-practices/>;

The correct answers are: Create individual 1AM users, Configure MFA on the root account and for privileged 1AM users. Assign 1AM users and groups configured with policies granting least privilege access

Submit your Feedback/Queries to our Experts

NEW QUESTION 107

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

Please select:

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

Answer: AB

Explanation:

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

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

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

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

Submit your Feedback/Queries to our Experts

NEW QUESTION 110

Your company has a set of EC2 Instances defined in AWS. These Ec2 Instances have strict security groups attached to them. You need to ensure that changes to the Security groups are noted and acted on accordingly. How can you achieve this?

Please select:

- A. Use Cloudwatch logs to monitor the activity on the Security Group
- B. Use filters to search for the changes and use SNS for the notification.
- C. Use Cloudwatch metrics to monitor the activity on the Security Group
- D. Use filters to search for the changes and use SNS for the notification.
- E. Use AWS inspector to monitor the activity on the Security Group
- F. Use filters to search for the changes and use SNS f the notification.
- G. Use Cloudwatch events to be triggered for any changes to the Security Group
- H. Configure theLambda function for email notification as wel

Answer: D

Explanation:

The below diagram from an AWS blog shows how security groups can be monitored

Option A is invalid because you need to use Cloudwatch Events to check for chan, Option B is invalid because you need to use Cloudwatch Events to check for chang

Option C is invalid because AWS inspector is not used to monitor the activity on Security Groups For more information on monitoring security groups, please visit the below URL: <https://aws.amazon.com/blogs/security/how-to-automatically-revert-and-receive-notificationsabout-changes-to-your-amazonjpc-security-groups/>

The correct answer is: Use Cloudwatch events to be triggered for any changes to the Security Groups. Configure the Lambda function for email notification as well.

Submit your Feedback/Queries to our Experts

NEW QUESTION 113

Your company uses AWS to host its resources. They have the following requirements

- 1) Record all API calls and Transitions
 - 2) Help in understanding what resources are there in the account
 - 3) Facility to allow auditing credentials and logins
- Which services would suffice the above requirements

Please select:

- A. AWS Inspector, CloudTrail, IAM Credential Reports
- B. CloudTrai

- C. IAM Credential Reports, AWS SNS
- D. CloudTrail, AWS Config, IAM Credential Reports
- E. AWS SQS, IAM Credential Reports, CloudTrail

Answer: C

Explanation:

You can use AWS CloudTrail to get a history of AWS API calls and related events for your account. This history includes calls made with the AWS Management Console, AWS Command Line Interface, AWS SDKs, and other AWS services.

Options A,B and D are invalid because you need to ensure that you use the services of CloudTrail, AWS Config, 1AM Credential Reports

For more information on Cloudtrail, please visit the below URL: <http://docs.aws.amazon.com/awsccloudtrail/latest/userguide/cloudtrail-user-guide.html>

AWS Config is a service that enables you to assess, audit and evaluate the configurations of your AWS resources. Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. With Config, you can review changes in configurations and relationships between AWS resources, dive into detailed resource configuration histories, and determine your overall compliance against the configurations specified in your internal guidelines. This enables you to simplify compliance auditing, security analysis, char management and operational troubleshooting.

For more information on the config service, please visit the below URL <https://aws.amazon.com/config/>

You can generate and download a credential report that lists all users in your account and the status of their various credentials, including passwords, access keys, and MFA devices. You can get a credential report from the AWS Management Console, the AWS SDKs and Command Line Tools, or the 1AM API.

For more information on Credentials Report, please visit the below URL: http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_getting-report.html

The correct answer is: CloudTrail, AWS Config, 1AM Credential Reports Submit your Feedback/Queries to our Experts

NEW QUESTION 117

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 accoun

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 118

Your CTO thinks your AWS account was hacked. What is the only way to know for certain if there was unauthorized access and what they did, assuming your hackers are very sophisticated AWS engineers and doing everything they can to cover their tracks?

Please select:

- A. Use CloudTrail Log File Integrity Validation.
- B. Use AWS Config SNS Subscriptions and process events in real time.
- C. Use CloudTrail backed up to AWS S3 and Glacier.
- D. Use AWS Config Timeline forensic

Answer: A

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. You can use the AWS CLI to validate the files in the location where CloudTrail delivered them

Validated log files are invaluable in security and forensic investigations. For example, a validated log file enables you to assert positively that the log file itself has not changed, or that particular user credentials performed specific API activity. The CloudTrail log file integrity validation process also lets you know if a log file has been deleted or changed, or assert positively that no log files were delivered to your account during a given period of time.

Options B.C and D is invalid because you need to check for log File Integrity Validation for cloudtrail logs

For more information on Cloudtrail log file validation, please visit the below URL: <http://docs.aws.amazon.com/awsccloudtrail/latest/userguide/cloudtrail-log-file-validation-intro.html> The correct answer is: Use CloudTrail Log File Integrity Validation.

omit your Feedback/Queries to our Expert

NEW QUESTION 119

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 122

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

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

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

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

Money Back Guarantee

AWS-Certified-Security-Specialty Practice Exam Features:

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