



Amazon

Exam Questions AWS-Certified-Security-Specialty

Amazon AWS Certified Security - Specialty

NEW QUESTION 1

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 2

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

Please select:

A. An AWS Managed Policy

B. An Inline Policy

C. A Bucket Policy

D. A bucket ACL

Answer: B

Explanation:

The AWS Documentation gives an example on such a case

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

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

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

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

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

NEW QUESTION 3

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

Please select:

A. Create a Cloudwatch Events Rule s

B. Create a Cloudwatch Logs Rule

C. Use a Lambda function

D. Use Cloudtrail API call

Answer: AC

Explanation:

Below is a snippet from the AWS blogs on a solution

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

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

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

NEW QUESTION 4

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

Please select:

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

Answer: AD

Explanation:

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

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

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

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

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

NEW QUESTION 5

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

Please select:

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

Answer: BD

Explanation:

You can create a Log group and send all logs from the EC2 Instance to that group. You can then limit the access to the Log groups via an 1AM policy.

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

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

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

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

* <https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/auth-and-access-control-cwl.html> The correct answers are: Stream the log files to a separate Cloudwatch Log group. Create an 1AM policy that gives the desired level of access to the Cloudwatch Log group
Submit your Feedback/Queries to our Experts

NEW QUESTION 6

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

Please select:

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

Answer: D

Explanation:

The AWS Documentation states the following

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

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

Option A, B, C are invalid because the dettings for automatic key rotation is not changeable. For more information on key rotation please visit the below URL

<https://docs.aws.amazon.com/kms/latest/developereuide/rotate-keys.html>

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

You can login to you 1AM dashbaord . Click on "Encryption Keys" You will find the list based on the services you are using as follows:

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

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

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

Rotation period for CMKs is as follows:

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

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

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

Submit your Feedback/Queries to our Experts

NEW QUESTION 7

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

Please select:

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

Answer: AB

Explanation:

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

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

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

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

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

Submit your Feedback/Queries to our Experts

NEW QUESTION 8

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

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

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

Answer: C

Explanation:

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

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

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

For more information on bucket policies please visit the below URL: <https://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies.html>

The correct answer is: Change the Resource section to "arn:aws:s3:::appbucket/" Submit your Feedback/Queries to our Experts

NEW QUESTION 9

You have an S3 bucket hosted in AWS. This is used to host promotional videos uploaded by yourself. You need to provide access to users for a limited duration of time. How can this be achieved?

Please select:

- A. Use versioning and enable a timestamp for each version
- B. Use Pre-signed URL's
- C. Use 1AM Roles with a timestamp to limit the access

D. Use IAM policies with a timestamp to limit the access

Answer: B

Explanation:

The AWS Documentation mentions the following

All objects by default are private. Only the object owner has permission to access these objects. However, the object owner can optionally share objects with others by creating a pre-signed URL using their own security credentials, to grant time-limited permission to download the objects. Option A is invalid because this can be used to prevent accidental deletion of objects

Option C is invalid because timestamps are not possible for Roles

Option D is invalid because policies is not the right way to limit access based on time For more information on pre-signed URL's, please visit the URL:

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

The correct answer is: Use Pre-signed URL's Submit your Feedback/Queries to our Experts

NEW QUESTION 10

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

Please select:

A. Enable AWS Guard Duty for the Instance

B. Use AWS Trusted Advisor

C. Use AWS inspector

D. Use AWS Macie

Answer: C

Explanation:

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

Center for Internet security (CIS) Benchmarks

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

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

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

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

Submit your Feedback/Queries to our Experts

NEW QUESTION 10

You have an instance setup in a test environment in AWS. You installed the required application and then promoted the server to a production environment. Your IT Security team has advised that there maybe traffic flowing in from an unknown IP address to port 22. How can this be mitigated immediately?

Please select:

A. Shutdown the instance

B. Remove the rule for incoming traffic on port 22 for the Security Group

C. Change the AMI for the instance

D. Change the Instance type for the instance

Answer: B

Explanation:

In the test environment the security groups might have been opened to all IP addresses for testing purpose. Always to ensure to remove this rule once all testing is completed.

Option A, C and D are all invalid because this would affect the application running on the server. The easiest way is just to remove the rule for access on port 22.

For more information on authorizing access to an instance, please visit the below URL: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/authorizing-access-to-an-instance.html> The correct answer is: Remove the rule for incoming traffic on port 22 for the Security Group Submit your Feedback/Queries to our Experts

NEW QUESTION 13

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

Please select:

A. Use AWS Inspector to inspect all the security Groups

B. Use the AWS Trusted Advisor to see which security groups have compromised access.

C. Use AWS Config to see which security groups have compromised access.

D. Use the AWS CLI to query the security groups and then filter for the rules which have unrestricted access

Answer: B

Explanation:

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

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

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

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

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

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

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

NEW QUESTION 16

Your company is planning on hosting an internal network in AWS. They want machines in the VPC to authenticate using private certificates. They want to minimize the work and maintenance in working with certificates. What is the ideal way to fulfil this requirement.

Please select:

- A. Consider using Windows Server 2016 Certificate Manager
- B. Consider using AWS Certificate Manager
- C. Consider using AWS Access keys to generate the certificates
- D. Consider using AWS Trusted Advisor for managing the certificates

Answer: B

Explanation:

The AWS Documentation mentions the following

ACM is tightly linked with AWS Certificate Manager Private Certificate Authority. You can use ACM PCA to create a private certificate authority (CA) and then use ACM to issue private certificates. These are SSL/TLS X.509 certificates that identify users, computers, applications, services, servers, and other devices internally. Private certificates cannot be publicly trusted

Option A is partially invalid. Windows Server 2016 Certificate Manager can be used but since there is a requirement to "minimize the work and maintenance", AWS Certificate Manager should be used Option C and D are invalid because these cannot be used for managing certificates.

For more information on ACM, please visit the below URL: <https://docs.aws.amazon.com/acm/latest/userguide/acm-overview.html>

The correct answer is: Consider using AWS Certificate Manager Submit your Feedback/Queries to our Experts

NEW QUESTION 20

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 25

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/Peering](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 30

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

Please select:

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

Answer: A

Explanation:

Option B is partially correct but a big maintenance over head to create and maintain a script when the functionality is already available in S3
Option C is invalid because snapshots are not available in S3 Option D is invalid because versioning will not replicate objects The AWS Documentation mentions the following
Cross-region replication is a bucket-level configuration that enables automatic, asynchronous copying of objects across buck in different AWS Regions.
For more information on Cross region replication in the Simple Storage Service, please visit the below URL:
<https://docs.aws.amazon.com/AmazonS3/latest/dev/crr.html>
The correct answer is: Enable cross region replication for the bucket Submit your Feedback/Queries to our Experts

NEW QUESTION 35

You want to ensure that you keep a check on the Active EBS Volumes, Active snapshots and Elastic IP addresses you use so that you don't go beyond the service limit. Which of the below services can help in this regard?
Please select:

- A. AWS Cloudwatch
- B. AWS EC2
- C. AWS Trusted Advisor
- D. AWS SNS

Answer: C

Explanation:

Below is a snapshot of the service limits that the Trusted Advisor can monitor

Option A is invalid because even though you can monitor resources, it cannot be checked against the service limit.
Option B is invalid because this is the Elastic Compute cloud service Option D is invalid because it can be send notification but not check on service limit For more information on the Trusted Advisor monitoring, please visit the below URL:
<https://aws.amazon.com/premiumsupport/ta-faqs>> The correct answer is: AWS Trusted Advisor Submit your Feedback/Queries to our Experts

NEW QUESTION 40

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

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

Answer: A

Explanation:

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

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

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

The correct answer is: Create a Service Control Policy that denies access to the services. Assemble all production accounts in an organizational unit. Apply the policy to that organizational unit
Submit your Feedback/Queries to our Experts

NEW QUESTION 42

An application running on EC2 instances in a VPC must call an external web service via TLS (port 443). The instances run in public subnets.
Which configurations below allow the application to function and minimize the exposure of the instances? Select 2 answers from the options given below
Please select:

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

Answer: BD

Explanation:

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

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

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

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

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

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

Submit your Feedback/Queries to our Experts

NEW QUESTION 44

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

Please select:

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

Answer: B

Explanation:

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

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

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

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

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

(

Submit your Feedback/Queries to our Experts

NEW QUESTION 45

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

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

Please select:

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

Answer: BE

Explanation:

This scenario is given in the AWS Documentation

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

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

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

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

Submit your Feedback/Queries to our Experts

NEW QUESTION 48

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

Please select:

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

Answer: B

Explanation:

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

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

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

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

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

NEW QUESTION 49

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 create

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 newCMKand 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 sam CMK to decrypt the dat

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/developereuide/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 51

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

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

Answer: C

Explanation:

The AWS Documentation mentions the following

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

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

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

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

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

NEW QUESTION 53

Your current setup in AWS consists of the following architecture. 2 public subnets, one subnet which has the web servers accessed by users across the internet and the other subnet for the database server. Which of the following changes to the architecture would add a better security boundary to the resources hosted in your setup

Please select:

- A. Consider moving the web server to a private subnet
- B. Consider moving the database server to a private subnet
- C. Consider moving both the web and database server to a private subnet
- D. Consider creating a private subnet and adding a NAT instance to that subnet

Answer: B

Explanation:

The ideal setup is to ensure that the web server is hosted in the public subnet so that it can be accessed by users on the internet. The database server can be hosted in the private subnet. The below diagram from the AWS Documentation shows how this can be setup

Option A and C are invalid because if you move the web server to a private subnet, then it cannot be accessed by users Option D is invalid because NAT instances should be present in the public subnet For more information on public and private subnets in AWS, please visit the following url [.com/AmazonVPC/latest/UserGuide/VPC_Scenario2](https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2).

The correct answer is: Consider moving the database server to a private subnet Submit your Feedback/Queries to our Experts

NEW QUESTION 58

A company hosts data in S3. There is a requirement to control access to the S3 buckets. Which are the 2 ways in which this can be achieved? Please select:

- A. Use Bucket policies

- B. Use the Secure Token service
- C. Use IAM user policies
- D. Use AWS Access Keys

Answer: AC

Explanation:

The AWS Documentation mentions the following

Amazon S3 offers access policy options broadly categorized as resource-based policies and user policies. Access policies you attach to your resources (buckets and objects) are referred to as

resource-based policies. For example, bucket policies and access control lists (ACLs) are resourcebased policies. You can also attach access policies to users in your account. These are called user

policies. You may choose to use resource-based policies, user policies, or some combination of these to manage permissions to your Amazon S3 resources.

Option B and D are invalid because these cannot be used to control access to S3 buckets For more information on S3 access control, please refer to the below

Link: <https://docs.aws.amazon.com/AmazonS3/latest/dev/s3-access-control.html>

The correct answers are: Use Bucket policies. Use IAM user policies Submit your Feedback/Queries to our Experts

NEW QUESTION 62

A company continually generates sensitive records that it stores in an S3 bucket. All objects in the bucket are encrypted using SSE-KMS using one of the company's CMKs. Company compliance policies require that no more than one month of data be encrypted using the same encryption key. What solution below will meet the company's requirements?

Please select:

- A. Trigger a Lambda function with a monthly CloudWatch event that creates a new CMK and updates the S3 bucket to use the new CMK.
- B. Configure the CMK to rotate the key material every month.
- C. Trigger a Lambda function with a monthly CloudWatch event that creates a new CMK, updates the S3 bucket to use the new CMK, and deletes the old CMK.
- D. Trigger a Lambda function with a monthly CloudWatch event that rotates the key material in the CMK.

Answer: A

Explanation:

You can use a Lambda function to create a new key and then update the S3 bucket to use the new key. Remember not to delete the old key, else you will not be able to decrypt the documents stored in the S3 bucket using the older key.

Option B is incorrect because AWS KMS cannot rotate keys on a monthly basis

Option C is incorrect because deleting the old key means that you cannot access the older objects Option D is incorrect because rotating key material is not possible.

For more information on AWS KMS keys, please refer to below URL: <https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html>

The correct answer is: Trigger a Lambda function with a monthly CloudWatch event that creates a new CMK and updates the S3 bucket to use the new CMK.

Submit your Feedback/Queries to our Experts

NEW QUESTION 64

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 the 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/UserGuide/VPC_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 66

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" and 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.

AWS CloudHSM provides you with a FIPS 140-2 Level 3 validated single-tenant HSM cluster in your Amazon Virtual Private Cloud (VPC) 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 69

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

Please select:

- A. AWS KMS
- B. AWS S3 Server side encryption
- C. AWS Customer Keys
- D. AWS Cloud HSM

Answer: B

Explanation:

The AWS Documentation mentions the following

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

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

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

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

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

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

NEW QUESTION 70

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

Please select:

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

Answer: AD

Explanation:

The AWS Documentation mentions some key aspects with regards to the configuration of On-premise AD with AWS

One is the Groups configuration in AD Active Directory Configuration

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

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

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

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

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

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

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

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

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

Submit your Feedback/Queries to our Experts

NEW QUESTION 71

Which technique can be used to integrate AWS 1AM (Identity and Access Management) with an on Questions & Answers PDF P-63 premise LDAP (Lightweight Directory Access Protocol) directory service? Please select:

- A. Use an 1AM policy that references the LDAP account identifiers and the AWS credentials.
- B. Use SAML (Security Assertion Markup Language) to enable single sign-on between AWS and LDAP.
- C. Use AWS Security Token Service from an identity broker to issue short-lived AWS credentials.
- D. Use 1AM roles to automatically rotate the 1AM credentials when LDAP credentials are update

Answer: B

Explanation:

On the AWS Blog site the following information is present to help on this context

The newly released whitepaper. Single Sign-On: Integrating AWS, OpenLDAP, and Shibboleth, will help you integrate your existing LDAP-based user directory with AWS. When you integrate your existing directory with AWS, your users can access AWS by using their existing credentials. This means that your users don't need to maintain yet another user name and password just to access AWS resources.

Option A.C and D are all invalid because in this sort of configuration, you have to use SAML to enable single sign on.

For more information on integrating AWS with LDAP for Single Sign-On, please visit the following URL:

<https://aws.amazon.com/blogs/security/new-whitepaper-single-sign-on-integrating-aws-openldap-and-shibboleth/>

The correct answer is: Use SAML (Security Assertion Markup Language) to enable single sign-on between AWS and LDAP. Submit your Feedback/Queries to our Experts

NEW QUESTION 72

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 Cloud Watch 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 Cloud Watch 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 ag

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-aws-customers/> The correct answer is: Search the Cloudtrail event history on the API events which occurred 11 days ago.

NEW QUESTION 73

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

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

Answer: CDE

Explanation:

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

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

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

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

the current IAM users

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

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

Submit Your Feedback/Queries to our Experts

NEW QUESTION 75

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

Please select:

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

Answer: C

Explanation:

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

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

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

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

NEW QUESTION 76

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

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

Answer: AB

Explanation:

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

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

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

(

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

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

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

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

NEW QUESTION 79

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

Please select:

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

Answer: C

Explanation:

Option A and B are invalid because mapping keys to services cannot be done via either the IAM or bucket policy

Option D is invalid because keys for IAM users cannot be assigned to services This is mentioned in the AWS Documentation

The kms:ViaService condition key limits use of a customer-managed CMK to requests from particular AWS services. (AWS managed CMKs in your account, such as aws/s3, are always restricted to the AWS service that created them.)

For example, you can use kms:V1aService to allow a user to use a customer managed CMK only for requests that Amazon S3 makes on their behalf. Or you can use it to deny the user permission to a CMK when a request on their behalf comes from AWS Lambda.

For more information on key policy's for KMS please visit the following URL: <https://docs.aws.amazon.com/kms/latest/developerguide/policy-conditions.html>

The correct answer is: Use the kms:ViaService condition in the Key policy Submit your Feedback/Queries to our Experts

NEW QUESTION 84

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

Please select:

- A. You have not explicitly given access via the key policy

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

Answer: A

Explanation:

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

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

For more information on upgrading key policies please visit the following URL: <https://docs.aws.ama20n.com/kms/latest/developerguide/key-policy-upgrading.html> (

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

NEW QUESTION 86

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 91

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

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

Answer: D

Explanation:

The AWS Documentation mentions the followii

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

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

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

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

NEW QUESTION 96

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

- A. Adding a bucket policy on the S3 bucket.
- B. Configuring lifecycle configuration rules on the S3 bucket.
- C. Creating an 1AM policy for the S3 bucket.
- D. Enabling CORS on the S3 bucke

Answer: B

Explanation:

The AWS Documentation mentions the following on lifecycle policies

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

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

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

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

Option A and C are invalid because neither bucket policies neither 1AM policy's can control the purging of logs Option D is invalid CORS is used for accessing objects across domains and not for purging of logs For more information on AWS S3 Lifecycle policies, please visit the following URL:

[.com/AmazonS3/latest/d<](https://docs.aws.amazon.com/AmazonS3/latest/d-)

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

NEW QUESTION 100

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

Please select:

- A. Encrypt the EBS volumes of the underlying EC2 Instances
- B. Use AWS KMS Customer Default master key
- C. Use SSL/TLS for encrypting the data
- D. Use S3 Encryption

Answer: B

Explanation:

The AWS Documentation mentions the following

Amazon Redshift uses a hierarchy of encryption keys to encrypt the database. You can use either AWS Key Management Service (AWS KMS) or a hardware security module (HSM) to manage the top-level encryption keys in this hierarchy. The process that Amazon Redshift uses for encryption differs depending on how you manage keys.

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

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

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

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

NEW QUESTION 105

A company is planning to run a number of Admin-related scripts using the AWS Lambda service. There is a need to understand if there are any errors encountered when the script runs. How can this be accomplished in the most effective manner?

Please select:

- A. Use CloudWatch metrics and logs to watch for errors
- B. Use CloudTrail to monitor for errors
- C. Use the AWS Config service to monitor for errors
- D. Use the AWS Inspector service to monitor for errors

Answer: A

Explanation:

The AWS Documentation mentions the following

AWS Lambda automatically monitors Lambda functions on your behalf, reporting metrics through Amazon CloudWatch. To help you troubleshoot failures in a function, Lambda logs all requests handled by your function and also automatically stores logs generated by your code through Amazon CloudWatch Logs.

Option B, C, and D are all invalid because these services cannot be used to monitor for errors.

For more information on Monitoring Lambda functions, please visit the following URL: <https://docs.aws.amazon.com/lambda/latest/dg/monitoring-functions-logs.html>

The correct answer is: Use CloudWatch metrics and logs to watch for errors. Submit your Feedback/Queries to our Experts

NEW QUESTION 107

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

Please select:

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

Answer: C

Explanation:

The AWS Documentation mentions the following

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

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

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

Submit your Feedback/Queries to our Experts

NEW QUESTION 108

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

Please select:

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

Answer: A

Explanation:

Here, since the communication would be established inward to the database server and outward from the application server, you need to ensure that just the

Outbound rules for application server security groups are checked. And then just the Inbound rules for database server security groups are checked. Option B can't be the correct answer. It says that we need to check the outbound security group which is not needed. We need to check the inbound for DB SG and outbound of Application SG. Because, this two group need to communicate with each other to function properly. Option C is invalid because you don't need to check for Outbound security rules for the database security group. Option D is invalid because you don't need to check for Inbound security rules for the application security group. For more information on Security Groups, please refer to below URL:
The correct answer is: Check the Inbound security rules for the database security group Check the Outbound security rules for the application security group
Submit your Feedback/Queries to our Experts

NEW QUESTION 109

One of the EC2 Instances in your company has been compromised. What steps would you take to ensure that you could apply digital forensics on the Instance. Select 2 answers from the options given below
Please select:

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

Answer: BC

Explanation:

Option A is invalid because removing the role will not help completely in such a situation
Option D is invalid because terminating the instance means that you cannot conduct forensic analysis on the instance
One way to isolate an affected EC2 instance for investigation is to place it in a Security Group that only the forensic investigators can access. Close all ports except to receive inbound SSH or RDP traffic from one single IP address from which the investigators can safely examine the instance.
For more information on security scenarios for your EC2 Instance, please refer to below URL: <https://d1.awsstatic.com/Marketplace/scenarios/security/SEC 11 TSB Final.pdf>
The correct answers are: Create a separate forensic instance. Ensure that the security groups only allow communication to this forensic instance
Submit your Feedback/Queries to our Experts

NEW QUESTION 110

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 114

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

- A. Use CloudTrail to see if any KMS API request has been issued against existing keys
- B. Use Key policies to see the access level for the keys
- C. Rotate the keys once before deletion to see if other services are using the keys
- D. Change the 1AM policy for the keys to see if other services are using the keys

Answer: A

Explanation:

The AWS lertation mentions the following
You can use a combination of AWS CloudTrail, Amazon CloudWatch Logs, and Amazon Simple Notification Service (Amazon SNS) to create an alarm that notifies you of AWS KMS API requests that attempt to use a customer master key (CMK) that is pending deletion. If you receive a notification from such an alarm, you might want to cancel deletion of the CMK to give yourself more time to determine whether you want to delete it
Options B and D are incorrect because Key policies nor 1AM policies can be used to check if the keys are being used.
Option C is incorrect since rotation will not help you check if the keys are being used. For more information on deleting keys, please refer to below URL: <https://docs.aws.amazon.com/kms/latest/developereuide/deletine-keys-creatine-cloudwatchalarm.html>
The correct answer is: Use CloudTrail to see if any KMS API request has been issued against existing keys Submit your Feedback/Queries to our Experts

NEW QUESTION 116

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

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

Answer: D

Explanation:

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

The following is an example of an S3 bucket policy that restricts access to a specific bucket, examplebucket only from the VPC endpoint with the ID vpce-la2b3c4d. The policy denies all access to the bucket if the specified endpoint is not being used. The aws:sourceVpce condition is used to specify the endpoint. The aws:sourceVpce condition does not require an ARN for the VPC endpoint resource, only the VPC endpoint ID. For more information about using conditions in a policy, see Specifying Conditions in a Policy.

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

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

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

NEW QUESTION 121

A DevOps team is currently looking at the security aspect of their CI/CD pipeline. They are making use of AWS resources 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

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 126

You need to create a Linux EC2 instance in AWS. Which of the following steps is used to ensure secure authentication of the EC2 instance from a Windows machine. Choose 2 answers from the options given below.

Please select:

- A. Ensure to create a strong password for logging into the EC2 Instance
- B. Create a key pair using putty
- C. Use the private key to log into the instance
- D. Ensure the password is passed securely using SSL

Answer: BC

Explanation:

The AWS Documentation mentions the following

You can use Amazon EC2 to create your key pair. Alternatively, you could use a third-party tool and then import the public key to Amazon EC2. Each key pair requires a name. Be sure to choose a name that is easy to remember. Amazon EC2 associates the public key with the name that you specify as the key name.

Amazon EC2 stores the public key only, and you store the private key. Anyone who possesses your private key can decrypt login information, so it's important that you store your private keys in a secure place.

Options A and D are incorrect since you should use key pairs for secure access to EC2 Instances. For more information on EC2 key pairs, please refer to below URL: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html>

The correct answers are: Create a key pair using putty. Use the private key to log into the instance. Submit your Feedback/Queries to our Experts

NEW QUESTION 128

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

Please select:

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

Answer: B

Explanation:

You need to ensure that an IAM service role is created for allowing the on-premise servers to communicate with the AWS Systems Manager.
Option A is incorrect since it is not necessary that servers should only be running Hyper-V Options C and D are incorrect since it is not necessary that IAM users and groups are created For more information on the Systems Manager role please refer to the below URL:
[.com/systems-manageer/latest/userguide/sysman-!](https://aws.amazon.com/systems-manageer/latest/userguide/sysman-!)
The correct answer is: Ensure that an IAM service role is created Submit your Feedback/Queries to our Experts

NEW QUESTION 133

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

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

Answer: D

Explanation:

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

Option A is incorrect since this would be applicable for resources in a VPC Options B and C are incorrect since operationally it would be difficult to manage For more information on AWS Security best practices please refer to the below URL
https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf
The correct answer is: Use multiple AWS accounts, each account for each department Submit your Feedback/Queries to our Experts

NEW QUESTION 134

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

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

Answer: A

Explanation:

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

Option B is invalid because this is the incorrect use of the Storage gateway Option C is invalid since this is the incorrect use of the NAT instance Option D is invalid since this is an incorrect configuration For more information on VPN connections, please visit the below URL
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html
The correct answer is: Build the application server on a public subnet and the database at the client's data center. Connect them with a VPN connection which uses IPsec
Submit your Feedback/Queries to our Experts

NEW QUESTION 135

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

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

Answer: A

Explanation:

This is mentioned in the AWS Documentation
Amazon Redshift uses a four-tier, key-based architecture for encryption. The architecture consists of data encryption keys, a database key, a cluster key, and a master key.
Data encryption keys encrypt data blocks in the cluster. Each data block is assigned a randomly generated AES-256 key. These keys are encrypted by using the database key for the cluster.
The database key encrypts data encryption keys in the cluster. The database key is a randomly generated AES-256 key. It is stored on disk in a separate network from the Amazon Redshift cluster and passed to the cluster across a secure channel.
The cluster key encrypts the database key for the Amazon Redshift cluster.
Option B is incorrect because the master key encrypts the cluster key and not the database key Option C is incorrect because the master key encrypts the cluster key and not the data encryption keys
Option D is incorrect because the master key encrypts the cluster key only
For more information on how keys are used in Redshift, please visit the following URL: <https://docs.aws.amazon.com/kms/latest/developerguide/services->

redshift.html

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

NEW QUESTION 137

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 139

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

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

Answer: AC

Explanation:

The AWS documentation mentions the following on the Application Load Balancer

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

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

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

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

NEW QUESTION 141

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

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

Please select:

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

Answer: AB

Explanation:

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

Option C is incorrect.

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

Option D is incorrect

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

[.com/whit](https://aws.amazon.com/whit) Security Practices.

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

Submit your Feedback/Queries to our Experts

NEW QUESTION 142

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: <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 146

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 147

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

Please select:

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

Answer: D

Explanation:

Tags enable you to categorize your AWS resources in different ways, for example, by purpose, owner, or environment. This is useful when you have many resources of the same type — you can quickly identify a specific resource based on the tags you've assigned to it

Option A is invalid because this is not a recommended practice

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

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

Submit your Feedback/Queries to our Experts

NEW QUESTION 151

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

Please select:

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

Answer: B

Explanation:

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

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

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

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

NEW QUESTION 154

Your company has the following setup in AWS

- A. A set of EC2 Instances hosting a web application
- B. An application load balancer placed in front of the EC2 Instances There seems to be a set of malicious requests coming from a set of IP addresses

C. Which of the following can be used to protect against these requests? Please select:

- D. Use Security Groups to block the IP addresses
- E. Use VPC Flow Logs to block the IP addresses
- F. Use AWS inspector to block the IP addresses
- G. Use AWS WAF to block the IP addresses

Answer: D

Explanation:

Your answer is incorrect Answer -D

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

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

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

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

Exceed a specified length

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

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

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

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

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

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

NEW QUESTION 158

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 tabl
- E. Access the VPC endpoint from the Lambda function.

Answer: B

Explanation:

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

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

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

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

NEW QUESTION 163

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

Choose the correct answer

Please select:

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

Answer: A

Explanation:

amazon Glacier is a secure, durable, and extremely low-cost cloud storage service for data archiving and long-term backup. Customers can reliably store large or small amounts of data for as little as

\$0,004 per gigabyte per month, a significant savings compared to on-premises solutions.

With Amazon lifecycle policies you can create transition actions in which you define when objects transition to another Amazon S3 storage class. For example, you may choose to transition objects to the STANDARD_IA (IA, for infrequent access) storage class 30 days after creation, or archive objects to the GLACIER storage class one year after creation.

Option B is invalid because lifecycle policies are not available for EBS volumes Option C is invalid because IAM policies cannot be used to move data to Glacier

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

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

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

Submit your Feedback/Queries to our Experts

NEW QUESTION 165

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

Please select:

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

Answer: C

Explanation:

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

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

The correct answer is: DDoS attacks

Submit your Feedback/Queries to our Experts

NEW QUESTION 170

You have an Amazon VPC that has a private subnet and a public subnet in which you have a NAT instance server. You have created a group of EC2 instances that configure themselves at startup by downloading a bootstrapping script from S3 that deploys an application via GIT.

Which one of the following setups would give us the highest level of security? Choose the correct answer from the options given below.

Please select:

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

Answer: D

Explanation:

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

Options A and B are invalid because the instances need to be in the private subnet

Option C is invalid because since the instance needs to be in the private subnet, you should not attach an EIP to the instance

For more information on NAT instance, please refer to the below Link: <http://docs.aws.amazon.com/AmazonVPC/latest/UserGuideA/PC Instance.html>

The correct answer is: EC2 instances in our private subnet no EIPs, route outgoing traffic via the NAT Submit your Feedback/Queries to our Experts

NEW QUESTION 171

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

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

Answer: C

Explanation:

The AWS Documentation mentions the following

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

User pools provide:

Sign-up and sign-in services.

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

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

User directory management and user profiles.

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

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

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

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

NEW QUESTION 174

Your company has defined a set of S3 buckets in AWS. They need to monitor the S3 buckets and know the source IP address and the person who make requests to the S3 bucket. How can this be achieved?

Please select:

- A. Enable VPC flow logs to know the source IP addresses
- B. Monitor the S3 API calls by using Cloudtrail logging
- C. Monitor the S3 API calls by using Cloudwatch logging
- D. Enable AWS Inspector for the S3 bucket

Answer: B

Explanation:

The AWS Documentation mentions the following

Amazon S3 is integrated with AWS CloudTrail. CloudTrail is a service that captures specific API calls made to Amazon S3 from your AWS account and delivers the log files to an Amazon S3 bucket that you specify. It captures API calls made from the Amazon S3 console or from the Amazon S3 API. Using the information collected by CloudTrail, you can determine what request was made to Amazon S3, the source IP address from which the request was made, who made the request when it was

made, and so on

Options A,C and D are invalid because these services cannot be used to get the source IP address of the calls to S3 buckets

For more information on Cloudtrail logging, please refer to the below Link:

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

The correct answer is: Monitor the S3 API calls by using Cloudtrail logging Submit your Feedback/Queries to our Experts

NEW QUESTION 178

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

Please select:

- A. Create individual IAM users
- B. Configure MFA on the root account and for privileged IAM users
- C. Assign IAM users and groups configured with policies granting least privilege access
- D. Ensure all users have been assigned and are 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 IAM users, Configure MFA on the root account and for privileged IAM users. Assign IAM users and groups configured with policies granting least privilege access

Submit your Feedback/Queries to our Experts

NEW QUESTION 179

Your team is experimenting with the API gateway service for an application. There is a need to implement a custom module which can be used for authentication/authorization for calls made to the API gateway. How can this be achieved?

Please select:

- A. Use the request parameters for authorization
- B. Use a Lambda authorizer
- C. Use the gateway authorizer
- D. Use CORS on the API gateway

Answer: B

Explanation:

The AWS Documentation mentions the following

An Amazon API Gateway Lambda authorizer (formerly known as a custom authorize?) is a Lambda function that you provide to control access to your API methods. A Lambda authorizer uses bearer token authentication strategies, such as OAuth or SAML. It can also use information described by headers, paths, query strings, stage variables, or context variables request parameters.

Options A,C and D are invalid because these cannot be used if you need a custom authentication/authorization for calls made to the API gateway

For more information on using the API gateway Lambda authorizer please visit the URL:

<https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-use-lambdaauthorizer.html>

The correct answer is: Use a Lambda authorizer Submit your Feedback/Queries to our Experts

NEW QUESTION 184

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

Please select:

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

Answer: B

Explanation:

The AWS Documentation mentions the following

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

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

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

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

NEW QUESTION 188

You have private video content in S3 that you want to serve to subscribed users on the Internet. User IDs, credentials, and subscriptions are stored in an Amazon RDS database. Which configuration will allow you to securely serve private content to your users? Please select:

- A. Generate pre-signed URLs for each user as they request access to protected S3 content
- B. Create an IAM user for each subscribed user and assign the GetObject permission to each IAM user
- C. Create an S3 bucket policy that limits access to your private content to only your subscribed users' credentials
- D. Create a CloudFront Identity user for your subscribers and assign the GetObject permission to this user

Answer: A

Explanation:

All objects and buckets by default are private. The pre-signed URLs are useful if you want your user/customer to be able to upload a specific object to your bucket but you don't require them to have AWS security credentials or permissions. When you create a pre-signed URL, you must provide your security credentials, specify a bucket name, an object key, an HTTP method (PUT for uploading objects), and an expiration date and time. The pre-signed URLs are valid only for the specified duration.

Option B is invalid because this would be too difficult to implement at a user level. Option C is invalid because this is not possible

Option D is invalid because this is used to serve private content via CloudFront For more information on pre-signed URLs, please refer to the Link:

<http://docs.aws.amazon.com/AmazonS3/latest/dev/PresignedUrlUploadObject.html>

The correct answer is: Generate pre-signed URLs for each user as they request access to protected S3 content Submit your Feedback/Queries to our Experts

NEW QUESTION 189

A company is hosting sensitive data in an AWS S3 bucket. It needs to be ensured that the bucket always remains private. How can this be ensured continually? Choose 2 answers from the options given below Please select:

- A. Use AWS Config to monitor changes to the AWS Bucket
- B. Use AWS Lambda function to change the bucket policy
- C. Use AWS Trusted Advisor API to monitor the changes to the AWS Bucket
- D. Use AWS Lambda function to change the bucket ACL

Answer: AD

Explanation:

One of the AWS Blogs mentions the usage of AWS Config and Lambda to achieve this. Below is the diagram representation of this

Option C is invalid because the Trusted Advisor API cannot be used to monitor changes to the AWS Bucket Option B doesn't seem to be the most appropriate.

1. If the object is in a bucket in which all the objects need to be private and the object is not private anymore, the Lambda function makes a PutObjectAcl call to S3 to make the object private.

<https://aws.amazon.com/blogs/security/how-to-detect-and-automatically-remediate-unintended-permissions-in-amazon-s3-bucket-acls-with-cloudwatch-events/>
The following link also specifies that

Create a new Lambda function to examine an Amazon S3 bucket's ACL and bucket policy. If the bucket ACL is found to allow public access, the Lambda function overwrites it to be private. If a bucket policy is found, the Lambda function creates an SNS message, puts the policy in the message body, and publishes it to the Amazon SNS topic we created. Bucket policies can be complex, and overwriting your policy may cause unexpected loss of access, so this Lambda function doesn't attempt to alter your policy in any way.

<https://aws.amazon.com/blogs/security/how-to-use-aws-config-to-monitor-for-and-respond-to-amazon-s3-buckets-allowing-public-access/>

Based on these facts Option D seems to be more appropriate than Option B.

For more information on implementation of this use case, please refer to the Link: <https://aws.amazon.com/blogs/security/how-to-use-aws-config-to-monitor-for-and-respond-to-amazon-s3-buckets-allowing-public-access/>

The correct answers are: Use AWS Config to monitor changes to the AWS Bucket Use AWS Lambda function to change the bucket ACL

NEW QUESTION 191

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 Link: <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 196

You have an S3 bucket defined in AWS. You want to ensure that you encrypt the data before sending it across the wire. What is the best way to achieve this. Please select:

- A. Enable server side encryption for the S3 bucket

- B. This request will ensure that the data is encrypted first.
- C. Use the AWS Encryption CLI to encrypt the data first
- D. Use a Lambda function to encrypt the data before sending it to the S3 bucket.
- E. Enable client encryption for the bucket

Answer: B

Explanation:

One can use the AWS Encryption CLI to encrypt the data before sending it across to the S3 bucket. Options A and C are invalid because this would still mean that data is transferred in plain text Option D is invalid because you cannot just enable client side encryption for the S3 bucket For more information on Encrypting and Decrypting data, please visit the below URL: <https://aws.amazon.com/blogs/security/how-to-encrypt-and-decrypt-your-data-with-the-aws-encryption-cli/>

The correct answer is: Use the AWS Encryption CLI to encrypt the data first Submit your Feedback/Queries to our Experts

NEW QUESTION 199

There is a requirement for a company to transfer large amounts of data between AWS and an onpremise location. There is an additional requirement for low latency and high consistency traffic to

AWS. Given these requirements how would you design a hybrid architecture? Choose the correct answer from the options below

Please select:

- A. Provision a Direct Connect connection to an AWS region using a Direct Connect partner.
- B. Create a VPN tunnel for private connectivity, which increases network consistency and reduces latency.
- C. Create an iPSec tunnel for private connectivity, which increases network consistency and reduces latency.
- D. Create a VPC peering connection between AWS and the Customer gateway

Answer: A

Explanation:

AWS Direct Connect makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect you can establish private connectivity between AWS and your datacenter, office, or colocation environment which in many cases can reduce your network costs, increase bandwidth throughput and provide a more consistent network experience than InternetQuestions & Answers PDF P-140 based connections.

Options B and C are invalid because these options will not reduce network latency Options D is invalid because this is only used to connect 2 VPC's

For more information on AWS direct connect, just browse to the below URL: <https://aws.amazon.com/directconnect>

The correct answer is: Provision a Direct Connect connection to an AWS region using a Direct Connect partner. omit your Feedback/Queries to our Experts

NEW QUESTION 202

Your company is planning on using bastion hosts for administering the servers in AWS. Which of the following is the best description of a bastion host from a security perspective?

Please select:

- A. A Bastion host should be on a private subnet and never a public subnet due to security concerns
- B. A Bastion host sits on the outside of an internal network and is used as a gateway into the private network and is considered the critical strong point of the network
- C. Bastion hosts allow users to log in using RDP or SSH and use that session to SSH into internal network to access private subnet resources.
- D. A Bastion host should maintain extremely tight security and monitoring as it is available to the public

Answer: C

Explanation:

A bastion host is a special purpose computer on a network specifically designed and configured to withstand attacks. The computer generally hosts a single application, for example a proxy server, and all other services are removed or limited to reduce the threat to the computer.

In AWS, A bastion host is kept on a public subnet. Users log on to the bastion host via SSH or RDP and then use that session to manage other hosts in the private subnets.

Options A and B are invalid because the bastion host needs to sit on the public network. Option D is invalid because bastion hosts are not used for monitoring For more information on bastion hosts, just browse to the below URL:

<https://docs.aws.amazon.com/quickstart/latest/linux-bastion/architecture.html>

The correct answer is: Bastion hosts allow users to log in using RDP or SSH and use that session to SSH into internal network to access private subnet resources. Submit your Feedback/Queries to our Experts

NEW QUESTION 204

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. CloudTrail
- 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, IAM Credential Reports

For more information on Cloudtrail, please visit the below URL: <http://docs.aws.amazon.com/awscloudtrail/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, change 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 IAM 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, IAM Credential Reports Submit your Feedback/Queries to our Experts

NEW QUESTION 209

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

AWS-Certified-Security-Specialty Practice Exam Features:

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

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