

Amazon

Exam Questions AWS-Certified-Security-Specialty

Amazon AWS Certified Security - Specialty



NEW QUESTION 1

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

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

Answer: C

Explanation:

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

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

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

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

NEW QUESTION 2

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

A.

B.

C.

D.

A.

Answer: A

Explanation:

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

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

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

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

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

NEW QUESTION 3

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

Please select:

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

Answer: D

Explanation:

The AWS Documentation mentions the following

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

Option A,B and C are invalid because in all of these cases, the management of the key will be with AWS. Here the question specifically mentions that you want to

have exclusive access over the keys. This can be achieved with Cloud HSM

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

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

NEW QUESTION 4

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

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

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

- A. Create a VPC endpoint for DynamoDB within a VP
- B. Configure the Lambda function to access resources in the VPC.
- C. Create a resource policy that grants the Lambda function permissions to write to the DynamoDB tabl
- D. Attach the poll to the DynamoDB table.
- E. Create an 1AM user with permissions to write to the DynamoDB tabl
- F. Store an access key for that user in the Lambda environment variables.
- G. Create an 1AM service role with permissions to write to the DynamoDB tabl
- H. Associate that role with the Lambda function.

Answer: D

Explanation:

The ideal way is to create an 1AM role which has the required permissions and then associate it with the Lambda function

The AWS Documentation additionally mentions the following

Each Lambda function has an 1AM role (execution role) associated with it. You specify the 1AM role when you create your Lambda function. Permissions you grant to this role determine what AWS Lambda can do when it assumes the role. There are two types of permissions that you grant to the 1AM role:

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

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

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

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

Option C is invalid because AWS Roles should be used and not 1AM Users

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

The correct answer is: Create an 1AM service role with permissions to write to the DynamoDB table. Associate that role with the Lambda function.

Submit your Feedback/Queries to our Exp

NEW QUESTION 5

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

authentication for these users. How can this be accomplished?

Please select:

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

Answer: A

Explanation:

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

Option B,C and D are invalid because no such security options are available in AWS For more information on 1AM best practices, please visit the below URL

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

Submit your Feedback/Queries to our Experts

NEW QUESTION 6

An application running on EC2 instances must use a username and password to access a database. The developer has stored those secrets in the SSM

Parameter Store with type SecureString using the default KMS CMK. Which combination of configuration steps will allow the application to access the secrets via the API? Select 2 answers from the options below

Please select:

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

Answer: CD

Explanation:

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

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

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

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

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

Submit your Feedback/Queries to our Experts

NEW QUESTION 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

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 accessd

Answer: B

Explanation:

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

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

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

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

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

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

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

NEW QUESTION 10

You have just received an email from AWS Support stating that your AWS account might have been compromised. Which of the following steps would you look to

carry out immediately. Choose 3 answers from the options below.
Please select:

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

Answer: ABD

Explanation:

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

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

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

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

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

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

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

NEW QUESTION 10

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

Please select:

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

Answer: B

Explanation:

The AWS Documentation mentions the following.

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

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

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

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

NEW QUESTION 15

A security team is creating a response plan in the event an employee executes unauthorized actions on AWS infrastructure. They want to include steps to determine if the employee's 1AM permissions changed as part of the incident.

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

- A. Use AWS Config to examine the employee's 1AM permissions prior to the incident and compare them to the employee's current 1AM permissions.
- B. Use Made to examine the employee's 1AM permissions prior to the incident and compare them to the employee's A current 1AM permissions.
- C. Use CloudTrail to examine the employee's 1AM permissions prior to the incident and compare them to the employee's current 1AM permissions.
- D. Use Trusted Advisor to examine the employee's 1AM permissions prior to the incident and compare them to the employee's current 1AM permissions.

Answer: A

Explanation:

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

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

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

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/TrackineChanees.html> The correct answer is: Use AWS Config to examine the employee's 1AM permissions prior to the incident and compare them the employee's current 1AM permissions.

Submit your Feedback/Queries to our Experts

NEW QUESTION 17

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

Please select:

- A. Delete the AWS keys for the root account
- B. Create 1AM Groups
- C. Create 1AM Roles
- D. Restrict access using 1AM policies

Answer: A

Explanation:

The first level or measure that should be taken is to delete the keys for the 1AM root user
When you log into your account and go to your Security Access dashboard, this is the first step that can be seen

Option B and C are wrong because creation of 1AM groups and roles will not change the impact of leakage of AWS root access keys
Option D is wrong because the first key aspect is to protect the access keys for the root account For more information on best practises for Security Access keys, please visit the below URL: <https://docs.aws.amazon.com/eeneral/latest/gr/aws-access-keys-best-practices.html>
The correct answer is: Delete the AWS keys for the root account Submit your Feedback/Queries to our Experts

NEW QUESTION 20

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

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

NEW QUESTION 23

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 26

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

Please select:

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

Answer: B

Explanation:

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

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

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

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

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

Submit your Feedback/Queries to our Experts

NEW QUESTION 30

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

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

Answer: B

Explanation:

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

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

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

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

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

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

NEW QUESTION 31

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 an 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-content-restricting-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 32

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

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

A. As long as you keep both

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

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

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

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

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

Submit your Feedback/Queries to our Experts

NEW QUESTION 35

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 40

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

Please select:

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

Answer: D

Explanation:

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

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

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

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

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

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

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

NEW QUESTION 43

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

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

Answer: AD

Explanation:

The AWS Documentation mentions the following about these services

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

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

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

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

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

The correct answers are: Amazon Cloudwatch Logs, Amazon Cloudtrail

NEW QUESTION 45

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 thfl 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/developereuide/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 49

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

Please select:

- A. AWS VPN
- B. AWS VPC Peering
- C. AWS NAT gateways
- D. AWS Direct Connect

Answer: AD

Explanation:

The AWS Document mention the following which supports the requirement

Option B is invalid because VPC peering is only used for connection between VPCs and cannot be used to connect On-premise infrastructure to the AWS Cloud. Option C is invalid because NAT gateways is used to connect instances in a private subnet to the internet For more information on VPN Connections, please visit the following url <https://docs.aws.amazon.com/AmazonVPC/latest/UserGuideA/pn-connections.html>

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

NEW QUESTION 54

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

Please select:

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

Answer: B

Explanation:

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

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

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

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

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

NEW QUESTION 59

A windows machine in one VPC needs to join the AD domain in another VPC. VPC Peering has been established. But the domain join is not working. What is the other step that needs to be followed to ensure that the AD domain join can work as intended
Please select:

- A. Change the VPC peering connection to a VPN connection
- B. Change the VPC peering connection to a Direct Connect connection
- C. Ensure the security groups for the AD hosted subnet has the right rule for relevant subnets
- D. Ensure that the AD is placed in a public subnet

Answer: C

Explanation:

In addition to VPC peering and setting the right route tables, the security groups for the AD EC2 instance needs to ensure the right rules are put in place for allowing incoming traffic.

Option A and B is invalid because changing the connection type will not help. This is a problem with the Security Groups.

Option D is invalid since the AD should not be placed in a public subnet

For more information on allowing ingress traffic for AD, please visit the following url

[|https://docs.aws.amazon.com/quickstart/latest/active-directory-ds/ingress.html|](https://docs.aws.amazon.com/quickstart/latest/active-directory-ds/ingress.html)

The correct answer is: Ensure the security groups for the AD hosted subnet has the right rule for relevant subnets Submit your Feedback/Queries to our Experts

NEW QUESTION 60

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 63

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

Please select:

- A. Use AWS Config to ensure that the servers have no critical flaws.

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

Answer: BD

Explanation:

The AWS Documentation mentions the following on AWS Inspector

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

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

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

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

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

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

(

NEW QUESTION 65

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

Please select:

- A. Check to see if the right role has been assigned to the EC2 instances
- B. Check to see if the 1AM user has the right permissions for EC2
- C. Ensure that agent is running on the instances.
- D. Check the Instance status by using the Health AP

Answer: ACD

Explanation:

For ensuring that the instances are configured properly you need to ensure the followi .

1) You installed the latest version of the SSM Agent on your instance

2) Your instance is configured with an AWS Identity and Access Management (IAM) role that enables the instance to communicate with the Systems Manager API

3) You can use the Amazon EC2 Health API to quickly determine the following information about Amazon EC2 instances The status of one or more instances

The last time the instance sent a heartbeat value The version of the SSM Agent

The operating system

The version of the EC2Config service (Windows) The status of the EC2Config service (Windows)

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

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

Submit your Feedback/Queries to our Experts

NEW QUESTION 69

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

Please select:

- A. Ensure that the SSM agent is running on the target machine
- B. Check the /var/log/amazon/ssm/errors.log file
- C. Ensure the right AMI is used for the Instance
- D. Ensure the security groups allow outbound communication for the instance

Answer: AB

Explanation:

The AWS Documentation mentions the following

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

View Agent Logs

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

On Windows

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

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

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

On Linux

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

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

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

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

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

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

Submit your Feedback/Queries to our Experts

NEW QUESTION 72

You are working for a company and been allocated the task for ensuring that there is a federated authentication mechanism setup between AWS and their On-

premise Active Directory. Which of the following are important steps that need to be covered in this process? Choose 2 answers from the options given below. Please select:

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

Answer: AD

Explanation:

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

One is the Groups configuration in AD Active Directory Configuration

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

One approach for creating the AD groups that uniquely identify the AWS 1AM role mapping is by selecting a common group naming convention. For example, your AD groups would start with an identifier, for example, AWS-, as this will distinguish your AWS groups from others within the organization. Next include the 12-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 76

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

Please select:

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

Answer: B

Explanation:

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

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

A is incorrect because Creating a new CMK and attaching it to the exiting volume will not allow the data to be decrypted, you cannot attach customer master keys after the volume is encrypted

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

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

NEW QUESTION 78

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/awsccloudtrail/latest/userguide/how-cloudtrail-works.html>

Note:

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

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

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

NEW QUESTION 79

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

Please select:

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

Answer: D

Explanation:

Option A is invalid because keys cannot be exported and imported across regions. Option B is invalid because key rotation cannot be used to export keys Option C is invalid because the backing key cannot be used to export keys This is mentioned in the AWS documentation

What geographic region are my keys stored in?

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

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

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

NEW QUESTION 80

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

Please select:

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

Answer: ACD

Explanation:

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

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

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

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

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

NEW QUESTION 81

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

Please select:

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

Answer: BC

Explanation:

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

Option A is invalid because databases should not be placed in the public subnet

Option D is invalid because the database security group should not allow traffic from the internet For more information on this type of setup, please refer to the below URL: https://docs.aws.amazon.com/AmazonVPC/latest/UserGuideA/PC_Scenario2.

The correct answers are: Place the EC2 Instance with the Oracle database in a separate private subnet Create a database security group and ensure the web security group to allowed incoming access

Submit your Feedback/Queries to our Experts

NEW QUESTION 84

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 88

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 93

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

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

Answer: B

Explanation:

The AWS Documentation mentions the following on lifecycle policies

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

Transition actions - In which you define when objects transition to another . For example, you may choose to transition objects to the STANDARD_IA (IA, for infrequent access) storage class 30 days after creation, or archive objects to the GLACIER storage class one year after creation.

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

Option A and C are invalid because neither bucket policies 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:

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

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

NEW QUESTION 98

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

Please select:

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

Answer: B

Explanation:

The AWS Documentation mentions the following

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

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

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

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

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

NEW QUESTION 100

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

Please select:

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

Answer: C

Explanation:

The AWS Documentation mentions the following

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

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

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

Submit your Feedback/Queries to our Experts

NEW QUESTION 103

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 104

One of your company's EC2 Instances have been compromised. The company has strict po thorough investigation on finding the culprit for the security breach.

What would you do in from the options given below.

Please select:

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

Answer: ABC

Explanation:

Some of the important aspects in such a situation are

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

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

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

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

Note:

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

The correct answers are: Take a snapshot of the EBS volume. Isolate the machine from the network. Make sure that logs are stored securely for auditing and troubleshooting purpose
Submit your Feedback/Queries to our Experts

NEW QUESTION 105

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

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

Answer: D

Explanation:

Since there are applications which work on legacy protocols, you need to ensure that the ELB can be used at the network layer as well and hence you should choose the Classic ELB. Since the traffic needs to be secure till the EC2 Instances, the SSL termination should occur on the EC2 Instances. Option A and C are invalid because you need to use a Classic Load balancer since this is a legacy application.

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

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

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

Submit your Feedback/Queries to our Experts

NEW QUESTION 107

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

Please select:

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

Answer: B

Explanation:

The AWS Documentation mentions the following

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

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

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

NEW QUESTION 108

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

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

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

Answer: B

Explanation:

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

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

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

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

NEW QUESTION 113

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 117

In order to encrypt data in transit for a connection to an AWS RDS instance, which of the following would you implement
Please select:

- A. Transparent data encryption
- B. SSL from your application
- C. Data keys from AWS KMS
- D. Data Keys from CloudHSM

Answer: B

Explanation:

This is mentioned in the AWS Documentation

You can use SSL from your application to encrypt a connection to a DB instance running MySQL MariaDB, Amazon Aurora, SQL Server, Oracle, or PostgreSQL. Option A is incorrect since Transparent data encryption is used for data at rest and not in transit Options C and D are incorrect since keys can be used for encryption of data at rest

For more information on working with RDS and SSL, please refer to below URL:

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.SSL.html>

The correct answer is: SSL from your application Submit your Feedback/Queries to our Experts

NEW QUESTION 119

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

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

Answer: BC

Explanation:

Below is the snapshot of the Shared Responsibility Model

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

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

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

NEW QUESTION 121

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

Please select:

- A. Delete the root access account
- B. Create an Admin 1AM user with the necessary permissions
- C. Change the password for the root account.
- D. Delete the root access keys

Answer: BD

Explanation:

The AWS Documentation mentions the following

All AWS accounts have root user credentials (that is, the credentials of the account owner). These credentials allow full access to all resources in the account.

Because you cant restrict permissions for root user credentials, we recommend that you delete your root user access keys. Then create AWS Identity and Access Management (IAM) user credentials for everyday interaction with AWS. Option A is incorrect since you cannot delete the root access account

Option C is partially correct but cannot be used as the ideal solution for safeguarding the account For more information on root access vs admin IAM users, please refer to below URL: <https://docs.aws.amazon.com/eeneral/latest/er/root-vs-iam.html>

The correct answers are: Create an Admin IAM user with the necessary permissions. Delete the root access keys Submit your Feedback/Queries to our Experts

NEW QUESTION 123

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

Please select:

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

Answer: A

Explanation:

The AWS Documentation mentions the following

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

Option B is incorrect since this is used for identity federation

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

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

The correct answer is: AWS Cognito

Submit your Feedback/Queries to our Experts

NEW QUESTION 128

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

Please select:

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

Answer: D

Explanation:

The below diagram shows how a WAF sandwich is created. It's the concept of placing the EC2 instance which hosts the WAF software in between 2 elastic load balancers.

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

The correct answer is: The EC2 instance running your WAF software is included in an Auto Scaling group and placed in between two Elastic load balancers.

Submit your Feedback/Queries to our Experts

NEW QUESTION 129

An employee keeps terminating EC2 instances on the production environment. You've determined the best way to ensure this doesn't happen is to add an extra layer of defense against terminating the instances. What is the best method to ensure the employee does not terminate the production instances? Choose the 2 correct answers from the options below

Please select:

- A. Tag the instance with a production-identifying tag and add resource-level permissions to the employee user with an explicit deny on the terminate API call to instances with the production tag.
- B. Tag the instance with a production-identifying tag and modify the employee's group to allow only start, stop, and reboot API calls and not the terminate instance call.
- C. Modify the IAM policy on the user to require MFA before deleting EC2 instances and disable MFA access to the employee
- D. Modify the IAM policy on the user to require MFA before deleting EC2 instances

Answer: AB

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. Each tag consists of a key and an optional value, both of which you define

Options C & D are incorrect because it will not ensure that the employee cannot terminate the instance.

For more information on tagging AWS resources please refer to the below URL: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html

The correct answers are: Tag the instance with a production-identifying tag and add resource-level permissions to the employee user with an explicit deny on the terminate API call to instances with the production tag. Tag the instance with a production-identifying tag and modify the employee's group to allow only start, stop, and reboot API calls and not the terminate instance

Submit your Feedback/Queries to our Experts

NEW QUESTION 133

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

Please select:

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

Answer: A

Explanation:

This is mentioned in the AWS Documentation

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

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

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

and passed to the cluster across a secure channel.

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

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

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

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

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

NEW QUESTION 138

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

Please select:

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

Answer: D

Explanation:

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

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

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

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

NEW QUESTION 140

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

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, y

You can encrypt the object and send it across to S3

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

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

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

NEW QUESTION 144

You are planning to use AWS Config to check the configuration of the resources in your AWS account. You are planning on using an existing IAM role and using it for the AWS Config resource. Which of the following is required to ensure the AWS Config service can work as required?

Please select:

- A. Ensure that there is a trust policy in place for the AWS Config service within the role
- B. Ensure that there is a grant policy in place for the AWS Config service within the role
- C. Ensure that there is a user policy in place for the AWS Config service within the role
- D. Ensure that there is a group policy in place for the AWS Config service within the role

Answer: A

Explanation:

Options B,C and D are invalid because you need to ensure a trust policy is in place and not a grant, user or group policy or more information on the IAM role permissions please visit the below Link: <https://docs.aws.amazon.com/config/latest/developerguide/iamrole-permissions.html>

The correct answer is: Ensure that there is a trust policy in place for the AWS Config service within the role

Submit your Feedback/Queries to our Experts

NEW QUESTION 149

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

Please select:

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

Answer: C

Explanation:

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

NEW QUESTION 150

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

Choose the correct answer

Please select:

- A. Upload data to S3 and use lifecycle policies to move the data into Glacier for long-term archiving.
- B. Upload the data on EBS, use lifecycle policies to move EBS snapshots into S3 and later into Glacier for long-term archiving.
- C. Use Direct Connect to upload data to S3 and use 1AM policies to move the data into Glacier for long-term archiving.
- D. Use Storage Gateway to store data to S3 and use lifecycle policies to move the data into Redshift for long-term archiving.

Answer: A

Explanation:

amazon Glacier is a secure, durable, and extremely low-cost cloud storage service for data archiving and long-term backup. Customers can reliably store large or small amounts of data for as little as \$0,004 per gigabyte per month, a significant savings compared to on-premises solutions. With Amazon lifecycle policies you can create transition actions in which you define when objects transition to another Amazon S3 storage class. For example, you may choose to transition objects to the STANDARDIA (IA, for infrequent access) storage class 30 days after creation, or archive objects to the GLACIER storage class one year after creation. Option B is invalid because lifecycle policies are not available for EBS volumes Option C is invalid because 1AM policies cannot be used to move data to Glacier Option D is invalid because lifecycle policies is not used to move data to Redshift For more information on S3 lifecycle policies, please visit the URL: <http://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html> The correct answer is: Upload data to S3 and use lifecycle policies to move the data into Glacier for long-term archiving. Submit your Feedback/Queries to our Experts

NEW QUESTION 154

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

Please select:

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

Answer: D

Explanation:

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

NEW QUESTION 158

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

- A. How can we ensure that all the users in the AWS organisation have access to this bucket? Please select:
- B. Ensure the bucket policy has a condition which involves aws:PrincipalOrgID
- C. Ensure the bucket policy has a condition which involves aws:AccountNumber
- D. Ensure the bucket policy has a condition which involves aws:PrincipalID
- E. Ensure the bucket policy has a condition which involves aws:OrgID

Answer: A

Explanation:

The AWS Documentation mentions the following AWS Identity and Access Management (IAM) now makes it easier for you to control access to your AWS resources by using the AWS organization of IAM principals (users and roles). For some services, you grant permissions using resource-based policies to specify the accounts and principals that can access the resource and what actions they can perform on it. Now, you can use a new condition key, aws:PrincipalOrgID, in these policies to require all principals accessing the resource to be from an account in the organization Option B.C and D are invalid because the condition in the bucket policy has to mention aws:PrincipalOrgID For more information on controlling access via Organizations, please refer to the below Link: <https://aws.amazon.com/blogs/security/control-access-to-aws-resources-by-usins-the-awsorganization- of-iam-principal> (The correct answer is: Ensure the bucket policy has a condition which involves aws:PrincipalOrgID Submit your Feedback/Queries to our Experts

NEW QUESTION 163

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 165

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

Please select:

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

Answer: AB

Explanation:

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

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

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

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

Submit your Feedback/Queries to our Experts

NEW QUESTION 169

An enterprise wants to use a third-party SaaS application. The SaaS application needs to have access to issue several API commands to discover Amazon EC2 resources running within the enterprise's account. The enterprise has internal security policies that require any outside access to their environment must conform to the principles of least privilege and there must be controls in place to ensure that the credentials used by the SaaS vendor cannot be used by any other third party. Which of the following would meet all of these conditions?

Please select:

- A. From the AWS Management Console, navigate to the Security Credentials page and retrieve the access and secret key for your account.
- B. Create an IAM user within the enterprise account assign a user policy to the IAM user that allows only the actions required by the SaaS applicatio
- C. Create a new access and secret key for the user and provide these credentials to the SaaS provider.
- D. Create an IAM role for cross-account access allows the SaaS provider's account to assume the role and assign it a policy that allows only the actions required by the SaaS application.
- E. Create an IAM role for EC2 instances, assign it a policy that allows only the actions required for the SaaS application to work, provide the role ARN to the SaaS provider to use when launching their application instances.

Answer: C

Explanation:

The below diagram from an AWS blog shows how access is given to other accounts for the services in your own account

Options A and B are invalid because you should not user IAM users or IAM Access keys Options D is invalid because you need to create a role for cross account access

For more information on Allowing access to external accounts, please visit the below URL:

<https://aws.amazon.com/blogs/apn/how-to-best-architect-your-aws-marketplace-saassubscription-across-multiple-aws-accounts/>

The correct answer is: Create an IAM role for cross-account access allows the SaaS provider's account to assume the role and assign it a policy that allows only the actions required by the SaaS application.

Submit your Feedback/Queries to our Experts

NEW QUESTION 170

.....

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](#)