Exam Questions AWS-Certified-Security-Specialty

Amazon AWS Certified Security - Specialty

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

NEW QUESTION 1
You are designing a custom 1AM policy that would allow uses 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 onl if the user has been MFA activated, that means it is true, then allow access.
Option D is invalid because the "boor 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 boot attribute in the condition element will return a value True for option A which will ensure that access is allowed on S3 resources.
For more information on an example on such a policy, please visit the following URL:

NEW QUESTION 2
You are hosting a web site via website hosting on an S3 bucket - http://demo.s3-website-us-east-l
.amazonaws.com. You have some web pages that use Javascript that access resources in another bucket which has web site hosting also enabled. But when users access the web pages , they are getting a blocked Javascript error. How can you rectify this?
Please select:

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

Answer: A

Explanation:
Your answer is incorrect Answer-A

Such a scenario is also given in the AWS Documentation Cross-Origin Resource Sharing:
Use-case Scenarios
The following are example scenarios for using CORS:
• Scenario 1: Suppose that you are hosting a website in an Amazon S3 bucket named website as described in Hosting a Static Website on Amazon S3. Your users load the website endpoint http://website.s3-website-us-east-1 .amazonaws.com. Now you want to use JavaScript on the webpages that are stored in this bucket to be able to make authenticated GET and PUT requests against the same bucket by using the Amazon S3 API endpoint for the bucket website.s3.amazonaws.com. A browser would normally block JavaScript from allowing those requests, but with CORS you can configure your bucket to explicitly enable cross-origin requests from website.s3-website-us-east-1 .amazonaws.com.
• Scenario 2: Suppose that you want to host a web font from your S3 bucket. Again, browsers require a CORS check (also called a preflight check) for loading web fonts. You would configure the bucket that is hosting the web font to allow any origin to make these requests.
Option Bis invalid because versioning is only to create multiple versions of an object and can help in accidental deletion of objects
Option C is invalid because this is used as an extra measure of caution for deletion of objects Option D is invalid because this is used for Cross region replication of objects
For more information on Cross Origin Resource sharing, please visit the following URL
• ittps://docs.aws.amazon.com/AmazonS3/latest/dev/cors.html
The correct answer is: Enable CORS for the bucket
Submit your Feedback/Queries to our Experts

NEW QUESTION 3
You have a vendor that needs access to an AWS resource. You create an AWS user account. You want to restrict access to the resource using a policy for just that user over a brief period. Which of the following would be an ideal policy to use?
Please select:

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

Answer: B

Explanation:
The AWS Documentation gives an example on such a case
Inline policies are useful if you want to maintain a strict one-to-one relationship between a policy and the principal entity that if s applied to. For example, you want to be sure that the permissions in a policy are not inadvertently assigned to a principal entity other than the one they're intended for. When you use an inline policy, the permissions in the policy cannot be inadvertently attached to the wrong principal entity. In addition, when you use the AWS Management Console to delete that principal entit the policies embedded in the principal entity are deleted as well. That's because they are part of the principal entity.
Option A is invalid because AWS Managed Polices are ok for a group of users, but for individual users,
inline policies are better.
Option C and D are invalid because they are specifically meant for access to S3 buckets For more information on policies, please visit the following URL:
https://docs.aws.amazon.com/IAM/latest/UserGuide/access managed-vs-inline
The correct answer is: An Inline Policy Submit your Feedback/Queries to our Experts

NEW QUESTION 4
Your company has a requirement to monitor all root user activity by notification. How can this best be achieved? Choose 2 answers from the options given below. Each answer forms part of the solution
Please select:

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

Answer: AC

Explanation:
Below is a snippet from the AWS blogs on a solution

Option B is invalid because you need to create a Cloudwatch Events Rule and there is such thing as a Cloudwatch Logs Rule Option D is invalid because Cloud Trail API calls can be recorded but cannot be used to send across notifications For more information on this blog article, please visit the following URL:
https://aws.amazon.com/blogs/mt/monitor-and-notify-on-aws-account-root-user-activityy
The correct answers are: Create a Cloudwatch Events Rule, Use a Lambda function Submit your Feedback/Queries to our Experts

NEW QUESTION 5
Your company has an EC2 Instance that is hosted in an AWS VPC. There is a requirement to ensure that logs files from the EC2 Instance are stored accordingly. The access should also be limited for the destination of the log files. How can this be accomplished? Choose 2 answers from the options given below. Each answer forms part of the solution
Please select:

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

Answer: BD

Explanation:
You can create a Log group and send all logs from the EC2 Instance to that group. You can then limit the access to the Log groups via an 1AM policy.
Option A is invalid because Cloudtrail is used to record API activity and not for storing log files Option C is invalid because Cloudtrail is the wrong service to be used for this requirement
For more information on Log Groups and Log Streams, please visit the following URL:

* https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/Workinj
For more information on Access to Cloudwatch logs, please visit the following URL:
* https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/auth-and-access-control-cwl.html The correct answers are: Stream the log files to a separate Cloudwatch Log group. Create an 1AM policy that gives the desired level of access to the Cloudwatch Log group
Submit your Feedback/Queries to our Experts

NEW QUESTION 6
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 7
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 8
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.htmll
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 9
You have a 2 tier application hosted in AWS. It consists of a web server and database server (SQL Server) hosted on separate EC2 Instances. You are devising the security groups for these EC2 Instances. The Web tier needs to be accessed by users across the Internet. You have created a web security group(wg-123) and database security group(db-345). Which combination of the following security group rules will allow the application to be secure and functional. Choose 2 answers from the options given below.
Please select:

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

Answer: AB

Explanation:
The Web security groups should allow access for ports 80 and 443 for HTTP and HTTPS traffic to all users from the internet.
The database security group should just allow access from the web security group from port 1433. Option C is invalid because this is not a valid configuration
Option D is invalid because database security should not be allowed on the internet For more information on Security Groups please visit the below URL:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/usins-network-security.htmll
The correct answers are: wg-123 - Allow ports 80 and 443 from 0.0.0.0/0, db-345 - Allow port 1433 from wg-123
Submit your Feedback/Queries to our Experts

NEW QUESTION 10
Your company has mandated that all calls to the AWS KMS service be recorded. How can this be achieved?
Please select:

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

Answer: B

Explanation:
The AWS Documentation states the following
AWS KMS is integrated with CloudTrail, a service that captures API calls made by or on behalf of AWS KMS in your AWS account and delivers the log files to an Amazon S3 bucket that you specify. CloudTrail captures API calls from the AWS KMS console or from the AWS KMS API. Using the information collected by CloudTrail, you can determine what request was made, the source IP
address from which the request was made, who made the request when it was made, and so on. Option A is invalid because logging is not possible in the KMS service
Option C and D are invalid because Cloudwatch cannot be used to monitor API calls For more information on logging using Cloudtrail please visit the below URL
https://docs.aws.amazon.com/kms/latest/developerguide/loeeing-usine-cloudtrail.html The correct answer is: Enable a trail in Cloudtrail
Jubmit your Feedback/Queries to our Experts

NEW QUESTION 10
Your IT Security team has advised to carry out a penetration test on the resources in their company's AWS Account. This is as part of their capability to analyze the security of the Infrastructure. What should be done first in this regard?
Please select:

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

Answer: C

Explanation:
This concept is given in the AWS Documentation
How do I submit a penetration testing request for my AWS resources? Issue
I want to run a penetration test or other simulated event on my AWS architecture. How do I get permission from AWS to do that?
Resolution
Before performing security testing on AWS resources, you must obtain approval from AWS. After you submit your request AWS will reply in about two business days.
AWS might have additional questions about your test which can extend the approval process, so plan accordingly and be sure that your initial request is as detailed as possible.
If your request is approved, you'll receive an authorization number.
Option A.B and D are all invalid because the first step is to get prior authorization from AWS for penetration tests
For more information on penetration testing, please visit the below URL
* https://aws.amazon.com/security/penetration-testing/
* https://aws.amazon.com/premiumsupport/knowledge-center/penetration-testing/ (
The correct answer is: Submit a request to AWS Support Submit your Feedback/Queries to our Experts

NEW QUESTION 12
You have just recently set up a web and database tier in a VPC and hosted the application. When testing the app , you are not able to reach the home page for the app. You have verified the security groups. What can help you diagnose the issue.
Please select:

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

Answer: B

Explanation:
Option A is invalid because this can be used to check for security issues in your account, but not verify as to why you cannot reach the home page for your application
Option C is invalid because this used to protect your app against application layer attacks, but not verify as to why you cannot reach the home page for your application
Option D is invalid because this used to protect your instance against attacks, but not verify as to why you cannot reach the home page for your application
The AWS Documentation mentions the following
VPC Flow Logs capture network flow information for a VPC, subnet or network interface and stores it in Amazon CloudWatch Logs. Flow log data can help customers troubleshoot network issues; for example, to diagnose why specific traffic is not reaching an instance, which might be a result of overly restrictive security group rules. Customers can also use flow logs as a security toi to monitor the traffic that reaches their instances, to profile network traffic, and to look for abnormal traffic behaviors.
For more information on AWS Security, please visit the following URL: https://aws.amazon.com/answers/networking/vpc-security-capabilities>
The correct answer is: Use VPC Flow logs to diagnose the traffic Submit your Feedback/Queries to our Experts

NEW QUESTION 17
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.htmll 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 19
Which of the following is not a best practice for carrying out a security audit? Please select:

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

Answer: A

Explanation:
A year's time is generally too long a gap for conducting security audits The AWS Documentation mentions the following
You should audit your security configuration in the following situations: On a periodic basis.
If there are changes in your organization, such as people leaving.
If you have stopped using one or more individual AWS services. This is important for removing permissions that users in your account no longer need.
If you've added or removed software in your accounts, such as applications on Amazon EC2 instances, AWS OpsWor stacks, AWS CloudFormation templates, etc.
If you ever suspect that an unauthorized person might have accessed your account.
Option B, C and D are all the right ways and recommended best practices when it comes to conducting audits For more information on Security Audit guideline, please visit the below URL: https://docs.aws.amazon.com/eeneral/latest/gr/aws-security-audit-euide.html
The correct answer is: Conduct an audit on a yearly basis Submit your Feedback/Queries to our Experts

NEW QUESTION 21
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 25
Every application in a company's portfolio has a separate AWS account for development and production. The security team wants to prevent the root user and all 1AM users in the production accounts from accessing a specific set of unneeded services. How can they control this functionality? Please select:

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

Answer: A

Explanation:
As an administrator of the master account of an organization, you can restrict which AWS services and individual API actions the users and roles in each member account can access. This restriction even overrides the administrators of member accounts in the organization. When AWS Organizations blocks access to a service or API action for a member account a user or role in that account can't access any prohibited service or API action, even if an administrator of a member account explicitly grants such permissions in an 1AM policy. Organization permissions overrule account permissions. Option B is invalid because service policies cannot be assigned to the root account at the account
level.
Option C and D are invalid because 1AM policies alone at the account level would not be able to suffice the requirement
For more information, please visit the below URL id=docs_orgs_console https://docs.aws.amazon.com/IAM/latest/UserGi manage attach-policy.html
The correct answer is: Create a Service Control Policy that denies access to the services. Assemble all production accounts in an organizational unit. Apply the policy to that organizational unit
Submit your Feedback/Queries to our Experts

NEW QUESTION 28
An application running on EC2 instances in a VPC must call an external web service via TLS (port 443). The instances run in public subnets.
Which configurations below allow the application to function and minimize the exposure of the instances? Select 2 answers from the options given below
Please select:

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

Answer: BD

Explanation:
Since here the traffic needs to flow outbound from the Instance to a web service on Port 443, the outbound rules on both the Network and Security Groups need to allow outbound traffic. The Incoming traffic should be allowed on ephermal ports for the Operating System on the Instance to allow a connection to be established on any desired or available port.
Option A is invalid because this rule alone is not enough. You also need to ensure incoming traffic on ephemeral ports
Option C is invalid because need to ensure incoming traffic on ephemeral ports and not only port 443 Option E and F are invalid since here you are allowing additional ports on Security groups which are not required
For more information on VPC Security Groups, please visit the below URL:
https://docs.aws.amazon.com/AmazonVPC/latest/UserGuideA/PC_SecurityGroups.htmll
The correct answers are: A network ACL with rules that allow outgoing traffic on port 443 and incoming traffic on ephemeral ports, A security group with a rule that allows outgoing traffic on port 443
Submit your Feedback/Queries to our Experts

NEW QUESTION 31
Your company has a set of 1000 EC2 Instances defined in an AWS Account. They want to effectively automate several administrative tasks on these instances.
Which of the following would be an effective way to achieve this?
Please select:

A. Use the AWS Systems Manager Parameter Store
B. Use the AWS Systems Manager Run Command
C. Use the AWS Inspector
D. Use AWS Config

Answer: B

Explanation:
The AWS Documentation mentions the following
AWS Systems Manager Run Command lets you remotely and securely manage the configuration of your managed instances. A managed instance is any Amazon EC2 instance or on-premises machine in your hybrid environment that has been configured for Systems Manager. Run Command enables you to automate common administrative tasks and perform ad hoc configuration changes at scale. You can use Run Command from the AWS console, the AWS Command Line Interface, AWS Tools for Windows PowerShell, or the AWS SDKs. Run Command is offered at no additional cost.
Option A is invalid because this service is used to store parameter Option C is invalid because this service is used to scan vulnerabilities in an EC2 Instance.
Option D is invalid because this service is used to check for configuration changes For more information on executing remote commands, please visit the below U
https://docs.aws.amazon.com/systems-manaEer/latest/usereuide/execute-remote-commands.htmll (
The correct answer is: Use the AWS Systems Manager Run Command Submit your Feedback/Queries to our Experts

NEW QUESTION 36
You want to launch an EC2 Instance with your own key pair in AWS. How can you achieve this?
Choose 3 answers from the options given below. Please select:

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

Answer: ABC

Explanation:
This is given in the AWS Documentation Creating a Key Pair
You can use Amazon EC2 to create your key pair. For more information, see Creating a Key Pair Using Amazon EC2.
Alternatively, you could use a third-party tool and then import the public key to Amazon EC2. For more information, see Importing Your Own Public Key to Amazon EC2.
Option B is Correct, because you can use the AWS CLI to create a new key pair 1 https://docs.aws.amazon.com/cli/latest/userguide/cli-ec2-keypairs.html
Option D is invalid because the public key needs to be stored in the EC2 Instance For more information on EC2 Key pairs, please visit the below URL:
* https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs
The correct answers are: Use a third party tool to create the Key pair. Create a new key pair using the AWS CLI, Import the public key into EC2
Submit your Feedback/Queries to our Experts

NEW QUESTION 38
You are building a large-scale confidential documentation web server on AWSand all of the documentation for it will be stored on S3. One of the requirements is that it cannot be publicly accessible from S3 directly, and you will need to use Cloud Front to accomplish this. Which of the methods listed below would satisfy the requirements as outlined? Choose an answer from the options below
Please select:

A. Create an Identity and Access Management (1AM) user for CloudFront and grant access to the objects in your S3 bucket to that 1AM 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 ace logs are less useful because they're incomplete.
Option A is invalid because you need to create a Origin Access Identity for Cloudfront and not an 1AM 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-contentrestrictine- access-to-s3.htmll
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 39
Your company makes use of S3 buckets for storing dat

A. There is a company policy that all services should have logging enable
B. How can you ensure thatlogging is always enabled for created S3 buckets in the AWS Account? Please select:
C. Use AWS Inspector to inspect all S3 buckets and enable logging for those where it is not enabled
D. Use AWS Config Rules to check whether logging is enabled for buckets
E. Use AWS Cloudwatch metrics to check whether logging is enabled for buckets
F. Use AWS Cloudwatch logs to check whether logging is enabled for buckets

Answer: B

Explanation:
This is given in the AWS Documentation as an example rule in AWS Config Example rules with triggers
Example rule with configuration change trigger
1. You add the AWS Config managed rule, S3_BUCKET_LOGGING_ENABLED, to your account to check whether your Amazon S3 buckets have logging enabled.
2. The trigger type for the rule is configuration changes. AWS Config runs the evaluations for the rule when an Amazon S3 bucket is created, changed, or deleted.
3. When a bucket is updated, the configuration change triggers the rule and AWS Config evaluates whether the bucket is compliant against the rule.
Option A is invalid because AWS Inspector cannot be used to scan all buckets
Option C and D are invalid because Cloudwatch cannot be used to check for logging enablement for buckets.

For more information on Config Rules please see the below Link: https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config-rules.html
The correct answer is: Use AWS Config Rules to check whether logging is enabled for buckets Submit your Feedback/Queries to our Experts

NEW QUESTION 44
A company has external vendors that must deliver files to the company. These vendors have crossaccount that gives them permission to upload objects to one of the company's S3 buckets.
What combination of steps must the vendor follow to successfully deliver a file to the company? Select 2 answers from the options given below
Please select:

A. Attach an 1AM role to the bucket that grants the bucket owner full permissions to the object
B. Add a grant to the objects ACL giving full permissions to bucket owner.
C. Encrypt the object with a KMS key controlled by the company.
D. Add a bucket policy to the bucket that grants the bucket owner full permissions to the object
E. Upload the file to the company's S3 bucket

Answer: BE

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

Option A and D are invalid because bucket ACL's are used to give grants to bucket Option C is not required since encryption is not part of the requirement For more information on this scenario please see the below Link:
https://docs.aws.amazon.com/AmazonS3/latest/dev/example-walkthroushs-manaeing-accessexample3. html
The correct answers are: Add a grant to the objects ACL giving full permissions to bucket owner., Upload the file to the company's S3 bucket
Submit your Feedback/Queries to our Experts

NEW QUESTION 47
An application running on EC2 instances in a VPC must access sensitive data in the data center. The access must be encrypted in transit and have consistent low latency. Which hybrid architecture will meet these requirements?
Please select:

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

Answer: B

Explanation:
Since this is required over a consistency low latency connection, you should use Direct Connect. For encryption, you can make use of a VPN
Option A is invalid because exposing an HTTPS endpoint will not help all traffic to flow between a VPC and the data center.
Option C is invalid because low latency is a key requirement Option D is invalid because only Direct Connect will not suffice
For more information on the connection options please see the below Link: https://aws.amazon.com/answers/networking/aws-multiple-vpc-vpn-connection-sharint
The correct answer is: A VPN between the VPC and the data center over a Direct Connect connection Submit your Feedback/Queries to our Experts

NEW QUESTION 52
Your current setup in AWS consists of the following architecture. 2 public subnets, one subnet which has the web servers accessed by users across the internet and the other subnet for the database server. Which of the following changes to the architecture would add a better security boundary to the resources hosted in your setup
Please select:

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

Answer: B

Explanation:

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

Option A and C are invalid because if you move the web server to a private subnet, then it cannot be accessed by users Option D is invalid because NAT instances should be present in the public subnet For more information on public and private subnets in AWS, please visit the following url .com/AmazonVPC/latest/UserGuide/VPC Scenario2.
The correct answer is: Consider moving the database server to a private subnet Submit your Feedback/Queries to our Experts

NEW QUESTION 55
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 53 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.htmll
The correct answer is: Enable Cross region replication for the S3 bucket Submit your Feedback/Queries to our Experts

NEW QUESTION 56
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.htmll
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 58
Company policy requires that all insecure server protocols, such as FTP, Telnet, HTTP, etc be disabled on all servers. The security team would like to regularly check all servers to ensure compliance with this requirement by using a scheduled CloudWatch event to trigger a review of the current infrastructure. What process will check compliance of the company's EC2 instances?
Please select:

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

Answer: D

Explanation:
Option B is incorrect because querying Trusted Advisor API's are not possible
Option C is incorrect because GuardDuty should be used to detect threats and not check the compliance of security protocols.
Option D states that Run Amazon Inspector using runtime behavior analysis rules which will analyze the behavior of your instances during an assessment run, and provide guidance about how to make your EC2 instances more secure.
Insecure Server Protocols
This rule helps determine whether your EC2 instances allow support for insecure and unencrypted ports/services such as FTP, Telnet HTTP, IMAP, POP version 3, SMTP, SNMP versions 1 and 2, rsh, and rlogin.
For more information, please refer to below URL: https://docs.aws.amazon.eom/mspector/latest/userguide/inspector_runtime-behavioranalysis. html#insecure-protocols
(
The correct answer is: Run an Amazon Inspector assessment using the Runtime Behavior Analysis rules package against every EC2 instance.
Submit your Feedback/Queries to our Experts

NEW QUESTION 61
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|
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 63
You need to inspect the running processes on an EC2 Instance that may have a security issue. How can you achieve this in the easiest way possible. Also you need to ensure that the process does not interfere with the continuous running of the instance.
Please select:

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

Answer: C

Explanation:
The SSM Run command can be used to send OS specific commands to an Instance. Here you can check and see the running processes on an instance and then send the output to an S3 bucket. Option A is invalid because this is used to record API activity and cannot be used to record running processes.
Option B is invalid because Cloudwatch is a logging and metric service and cannot be used to record running processes.
Option D is invalid because AWS Config is a configuration service and cannot be used to record running processes.
For more information on the Systems Manager Run command, please visit the following URL: https://docs.aws.amazon.com/systems-manaEer/latest/usereuide/execute-remote-commands.htmll The correct answer is: Use the SSM Run command to send the list of running processes information to

an S3 bucket. Submit your Feedback/Queries to our Experts

NEW QUESTION 66
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 (1AM) 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 1AM 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 70
You are trying to use the AWS Systems Manager run command on a set of Instances. The run command on a set of Instances. What can you do to diagnose the issue? Choose 2 answers from the options given
Please select:

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

Answer: AB

Explanation:
The AWS Documentation mentions the following
If you experience problems executing commands using Run Command, there might be a problem with the SSM Agent. Use the following information to help you troubleshoot the agent
View Agent Logs
The SSM Agent logs information in the following files. The information in these files can help you troubleshoot problems.
On Windows
%PROGRAMDATA%\Amazon\SSM\Logs\amazon-ssm-agent.log
%PROGRAMDATA%\Amazon\SSM\Logs\error.log
The default filename of the seelog is seelog-xml.template. If you modify a seelog, you must rename the file to seelog.xml.
On Linux
/var/log/amazon/ssm/amazon-ssm-agentlog /var/log/amazon/ssm/errors.log
Option C is invalid because the right AMI has nothing to do with the issues. The agent which is used to execute run commands can run on a variety of AMI'S
Option D is invalid because security groups does not come into the picture with the communication between the agent and the SSM service
For more information on troubleshooting AWS SSM, please visit the following URL: https://docs.aws.amazon.com/systems-manaeer/latest/userguide/troubleshootine-remotecommands. htmll
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 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 77
You have a requirement to serve up private content using the keys available with Cloudfront. How can this be achieved?
Please select:

A. Add the keys to the backend distribution.
B. Add the keys to the S3 bucket
C. Create pre-signed URL's
D. Use AWS Access keys

Answer: C

Explanation:
Option A and B are invalid because you will not add keys to either the backend distribution or the S3 bucket.
Option D is invalid because this is used for programmatic access to AWS resources
You can use Cloudfront key pairs to create a trusted pre-signed URL which can be distributed to users Specifying the AWS Accounts That Can Create Signed URLs and Signed Cookies (Trusted Signers) Topics
• Creating CloudFront Key Pairs for Your Trusted Signers
• Reformatting the CloudFront Private Key (.NET and Java Only)
• Adding Trusted Signers to Your Distribution
• Verifying that Trusted Signers Are Active (Optional) 1 Rotating CloudFront Key Pairs
To create signed URLs or signed cookies, you need at least one AWS account that has an active CloudFront key pair. This accou is known as a trusted signer.
The trusted signer has two purposes:
• As soon as you add the AWS account ID for your trusted signer to your distribution, CloudFront starts to require that users us signed URLs or signed cookies to access your objects.
' When you create signed URLs or signed cookies, you use the private key from the trusted signer's key pair to sign a portion of the URL or the cookie. When someone requests a restricted object CloudFront compares the signed portion of the URL or cookie with the unsigned portion to verify that the URL or cookie hasn't been tampered with. CloudFront also verifies that the URL or cookie is valid, meaning, for example, that the expiration date and time hasn't passed.
For more information on Cloudfront private trusted content please visit the following URL:
• https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-contenttrusted- s
The correct answer is: Create pre-signed URL's Submit your Feedback/Queries to our Experts

NEW QUESTION 82
You are building a system to distribute confidential training videos to employees. Using CloudFront, what method could be used to serve content that is stored in S3, but not publicly accessible from S3 directly?
Please select:

A. Create an Origin Access Identity (OAI) for CloudFront and grant access to the objects in your S3 bucket to that OAI.
B. Add the CloudFront account security group "amazon-cf/amazon-cf-sg" to the appropriate S3 bucket policy.
C. Create an Identity and Access Management (1AM) User for CloudFront and grant access to the objects in your S3 bucket to that 1AM User.
D. Create a S3 bucket policy that lists the CloudFront distribution ID as the Principal and the target bucket as the Amazon Resource Name (ARN).

Answer: AExplanation:

Explanation:
You can optionally secure the content in your Amazon S3 bucket so users can access it through
CloudFront but cannot access it directly by using Amazon S3 URLs. This prevents anyone from bypassing CloudFront and using the Amazon S3 URL to get content that you want to restrict access to. This step isn't required to use signed URLs, but we recommend it
To require that users access your content through CloudFront URLs, you perform the following tasks: Create a special CloudFront user called an origin access identity.
Give the origin access identity permission to read the objects in your bucket. Remove permission for anyone else to use Amazon S3 URLs to read the objects.
Option B,C and D are all automatically invalid, because the right way is to ensure to create Origin Access Identity (OAI) for CloudFront and grant access accordingly.
For more information on serving private content via Cloudfront, please visit the following URL:
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/PrivateContent.htmll
The correct answer is: Create an Origin Access Identity (OAI) for CloudFront and grant access to the objects in your S3 bucket t that OAI.
You can optionally secure the content in your Amazon S3 bucket so users can access it through CloudFront but cannot access it directly by using Amazon S3 URLs. This prevents anyone from bypassing CloudFront and using the Amazon S3 URL to get content that you want to restrict access to. This step isn't required to use signed URLs, but we recommend it
To require that users access your content through CloudFront URLs, you perform the following tasks: Create a special CloudFront user called an origin access identity.
Give the origin access identity permission to read the objects in your bucket. Remove permission for anyone else to use Amazon S3 URLs to read the objects.
Option B,C and D are all automatically invalid, because the right way is to ensure to create Origin Access Identity (OAI) for CloudFront and grant access accordingly.
For more information on serving private content via Cloudfront, please visit the following URL:
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/PrivateContent.htmll
The correct answer is: Create an Origin Access Identity (OAI) for CloudFront and grant access to the objects in your S3 bucket t that OAI.
Submit your Feedback/Queries to our Experts Submit your Feedback/Queries to our Experts

NEW QUESTION 86
You have a requirement to conduct penetration testing on the AWS Cloud for a couple of EC2 Instances. How could you go about doing this? Choose 2 right answers from the options given below. Please select:

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

D. Choose any of the AWS instance type

Answer: AB

Explanation:
You can use a pre-approved solution from the AWS Marketplace. But till date the AWS Documentation still mentions that you have to get prior approval before conducting a test on the AWS Cloud for EC2 Instances.
Option C and D are invalid because you have to get prior approval first. AWS Docs Provides following details:
"For performing a penetration test on AWS resources first of all we need to take permission from AWS and complete a requisition form and submit it for approval. The form should contain information about the instances you wish to test identify the expected start and end dates/times of your test and requires you to read and agree to Terms and Conditions specific to penetration testing and to the use of appropriate tools for testing. Note that the end date may not be more than 90 days from the start date."
(
At this time, our policy does not permit testing small or micro RDS instance types. Testing of ml
.small, t1 .micro or t2.nano EC2 instance types is not permitted.
For more information on penetration testing please visit the following URL: https://aws.amazon.eom/security/penetration-testine/l
The correct answers are: Get prior approval from AWS for conducting the test Use a pre-approved penetration testing tool. Submit your Feedback/Queries to our Experts

NEW QUESTION 87
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
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.ama2on.com/about-aws/whats-new/20l5/l2/turn-on-cloudtrail-across-all-reeions-andsupport- for-multiple-trails
The correct answer is: Ensure one Cloudtrail trail is enabled for all regions. Submit your Feedback/Queries to our Experts

NEW QUESTION 93
A customer has an instance hosted in the AWS Public Cloud. The VPC and subnet used to host the Instance have been created with the default settings for the Network Access Control Lists. They need to provide an IT Administrator secure access to the underlying instance. How can this be accomplished.
Please select:

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

Answer: C

Explanation:
Options A & B are invalid as default NACL rule will allow all inbound and outbound traffic.
The requirement is that the IT administrator should be able to access this EC2 instance from his workstation. For that we need to enable the Security Group of

EC2 instance to allow traffic from the IT administrator's workstation. Hence option C is correct.
Option D is incorrect as we need to enable the Inbound SSH traffic on the EC2 instance Security Group since the traffic originate' , from the IT admin's workstation.
The correct answer is: Ensure that the security group allows Inbound SSH traffic from the IT Administrator's Workstation Submit your Feedback/Queries to our Experts

NEW QUESTION 96
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 97
Your company has a requirement to work with a DynamoDB table. There is a security mandate that all data should be encrypted at rest. What is the easiest way to accomplish this for DynamoDB. Please select:

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

Answer: B

Explanation:
The most easiest option is to enable encryption when the DynamoDB table is created. The AWS Documentation mentions the following
Amazon DynamoDB offers fully managed encryption at rest. DynamoDB encryption at rest provides enhanced security by encrypting your data at rest using an AWS Key Management Service (AWS KMS) managed encryption key for DynamoDB. This functionality eliminates the operational burden and complexity involved in protecting sensitive data.
Option A is partially correct, you can use the AWS SDK to encrypt the data, but the easier option would be to encrypt the table before hand.
Option C is invalid because you cannot encrypt the table after it is created
Option D is invalid because encryption for S3 buckets is for the objects in S3 only.
For more information on securing data at rest for DynamoDB please refer to below URL:
https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/EncryptionAtRest.htmll The correct answer is: Encrypt the DynamoDB table using KMS during its creation Submit your Feedback/Queries to our Experts

NEW QUESTION 98
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.ama20n.com/elasticloadbalancing/latest/classic/elb-https-load-balancers.htmll 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 100
A company has set up the following structure to ensure that their S3 buckets always have logging enabled

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

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

Answer: B

Explanation:
The most probable cause is that you have not allowed the Lambda functions to have the appropriate permissions on the S3 bucket to make the relevant changes.
Option A is invalid because this is more of a permission instead of a configuration rule issue. Option C is invalid because changing the language will not be the core solution.
Option D is invalid because you don't necessarily need to use the API gateway service
For more information on accessing resources from a Lambda function, please refer to below URL https://docs.aws.amazon.com/lambda/latest/ds/accessing-resources.htmll
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 101
Your company has a set of EC2 Instances defined in AWS. They need to ensure that all traffic packets are monitored and inspected for any security threats. How can this be achieved? Choose 2 answers from the options given below
Please select:

A. Use a host based intrusion detection system
B. Use a third party firewall installed on a central EC2 instance
C. Use VPC Flow logs
D. Use Network Access control lists logging

Answer: AB

Explanation:
If you want to inspect the packets themselves, then you need to use custom based software A diagram representation of this is given in the AWS Security best practices

Option C is invalid because VPC Flow logs cannot conduct packet inspection. For more information on AWS Security best practices, please refer to below URL:
The correct answers are: Use a host based intrusion detection system. Use a third party firewall installed on a central EC2
Submit your Feedback/Queries to our Experts

NEW QUESTION 105
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.pd1
The correct answer is: AWS Cloudformation Submit your Feedback/Queries to our Experts

NEW QUESTION 109
Your company has a set of EBS volumes defined in AWS. The security mandate is that all EBS volumes are encrypted. What can be done to notify the IT admin staff if there are any unencrypted volumes in the account.
Please select:

A. Use AWS Inspector to inspect all the EBS volumes
B. Use AWS Config to check for unencrypted EBS volumes
C. Use AWS Guard duty to check for the unencrypted EBS volumes
D. Use AWS Lambda to check for the unencrypted EBS volumes

Answer: B

Explanation:
The enc config rule for AWS Config can be used to check for unencrypted volumes. encrypted-volurrn
5 volumes that are in an attached state are encrypted. If you specify the ID of a KMS key for encryptio using the kmsld parameter, the rule checks if the EBS volumes in an attached state are encrypted
with that KMS key*1.
Options A and C are incorrect since these services cannot be used to check for unencrypted EBS volumes
Option D is incorrect because even though this is possible, trying to implement the solution alone with just the Lambda servk
would be too difficult
For more information on AWS Config and encrypted volumes, please refer to below URL:
https://docs.aws.amazon.com/config/latest/developerguide/encrypted-volumes.html Submit your Feedback/Queries to our Experts

NEW QUESTION 112
Your company use AWS KMS for management of its customer keys. From time to time, there is a requirement to delete existing keys as part of housekeeping activities. What can be done during the deletion process to verify that the key is no longer being used.
Please select:

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

Answer: A

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

NEW QUESTION 116
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 117
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 corn/whitepapers/Security/AWS Practices.
The correct answers are: Encryption of data at rest Protection of data in transit Submit your Feedback/Queries to our Experts

NEW QUESTION 119
You want to track access requests for a particular S3 bucket. How can you achieve this in the easiest possible way?
Please select:

A. Enable server access logging for the bucket
B. Enable Cloudwatch metrics for the bucket
C. Enable Cloudwatch logs for the bucket
D. Enable AWS Config for the S3 bucket

Answer: A

Explanation:
The AWS Documentation mentions the foil
To track requests for access to your bucket you can enable access logging. Each access log record provides details about a single access request, such as the requester, bucket name, request time, request action, response status, and error code, if any.
Options B and C are incorrect Cloudwatch is used for metrics and logging and cannot be used to track access requests.
Option D is incorrect since this can be used for Configuration management but for not for tracking S3 bucket requests.
For more information on S3 server logs, please refer to below UF https://docs.aws.amazon.com/AmazonS3/latest/dev/ServerLoes.html
The correct answer is: Enable server access logging for the bucket Submit your Feedback/Queries to our Experts

NEW QUESTION 124
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 (1AM) 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 1AM 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 1AM user with the necessary permissions. Delete the root access keys Submit your Feedback/Queries to our Experts

NEW QUESTION 126
You need to create a Linux EC2 instance in AWS. Which of the following steps is used to ensure secure authentication the EC2 instance from a windows machine. Choose 2 answers from the options given below.
Please select:

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

Answer: BC

Explanation:
The AWS Documentation mentions the following
You can use Amazon EC2 to create your key pair. Alternatively, you could use a third-party tool and then import the public key to Amazon EC2. Each key pair requires a name. Be sure to choose a name that is easy to remember. Amazon EC2 associates the public key with the name that you specify as the key name. Amazon EC2 stores the public key only, and you store the private key. Anyone who possesses your private key can decrypt login information, so it's important that you store your private keys in a secure place.
Options A and D are incorrect since you should use key pairs for secure access to Ec2 Instances For more information on EC2 key pairs, please refer to below URL: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html
The correct answers are: Create a key pair using putty. Use the private key to log into the instance Submit your Feedback/Queries to our Experts

NEW QUESTION 128
Your 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 1AM
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 ca 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/coenito/latest/developerguide/what-is-amazon-cognito.html
The correct answer is: AWS Cognito
Submit your Feedback/Queries to our Experts

NEW QUESTION 132
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. he EC2 instance running your WAF software is included in an Auto Scaling group and placed in between two Elastic load balancers.

Answer: D

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

Option A.B and C are incorrect since the EC2 Instance with the WAF software needs to be placed in an Autoscaling Group For more information on a WAF sandwich please refer to the below Link: https://www.cloudaxis.eom/2016/11/2l/waf-sandwich/l
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 137
An auditor needs access to logs that record all API events on AWS. The auditor only needs read-only access to the log files and does not need access to each AWS account. The company has multiple AWS accounts, and the auditor needs access to all the logs for all the accounts. What is the best way to configure access for the auditor to view event logs from all accounts? Choose the correct answer from the options below
Please select:

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

Answer: D

Explanation:
Given the current requirements, assume the method of "least privilege" security design and only allow the auditor access to the minimum amount of AWS resources as possibli
AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain events
related to API calls across your AWS infrastructure. CloudTrail provides a history of AWS API calls for your account including API calls made through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This history simplifies security analysis, resource change tracking, and troubleshooting
only be granted access in one location
Option Option A is incorrect since the auditor should B is incorrect since consolidated billing is not a key requirement as part of the question
Option C is incorrect since there is not consolidated logging
For more information on Cloudtrail please refer to the below URL: https://aws.amazon.com/cloudtraiL
(
The correct answer is: Configure the CloudTrail service in each AWS account and have the logs delivered to a single AWS bud in the primary account and grant the auditor access to that single bucket in the primary account.
Submit your Feedback/Queries to our Experts

NEW QUESTION 142

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

A. Ensure that the on-premise servers are running on Hyper-V.
B. Ensure that an 1AM service role is created
C. Ensure that an 1AM User is created
D. Ensure that an 1AM Group is created for the on-premise servers

Answer: B

Explanation:
You need to ensure that an 1AM service role is created for allowing the on-premise servers to communicate with the AWS Systems Manager.
Option A is incorrect since it is not necessary that servers should only be running Hyper-V Options C and D are incorrect since it is not necessary that 1AM users and groups are created For more information on the Systems Manager role please refer to the below URL:
.com/systems-rnanaeer/latest/usereuide/sysman-!
The correct answer is: Ensure that an 1AM service role is created Submit your Feedback/Queries to our Experts

NEW QUESTION 143
You have several S3 buckets defined in your AWS account. You need to give access to external AWS accounts to these S3 buckets. Which of the following can allow you to define the permissions for the external accounts? Choose 2 answers from the options given below
Please select:

A. 1AM policies
B. Buckets ACL's
C. 1AM users
D. Bucket policies

Answer: BD

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

Options A and C are incorrect since for external access to buckets, you need to use either Bucket policies or Bucket ACL's or more information on Security for storage services role please refer to the below URL:
https://d1.awsstatic.com/whitepapers/Security/Security Storage Services Whitepaper.pdf The correct answers are: Buckets ACL's, Bucket policies
Submit your Feedback/Queries to our Experts

NEW QUESTION 145
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 employees group to allow only start stop, and reboot API calls and not the terminate instance call.
C. Modify the 1AM policy on the user to require MFA before deleting EC2 instances and disable MFA access to the employee
D. Modify the 1AM 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 answer resources please refer to the below URL: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Usins_Tags.htmll
The correct answers are: Tag the instance with a production-identifying tag and add resource-level permissions to the employe 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 employees group to allow only start stop, and reboot API calls and not the terminate instance
Submit your Feedback/Queries to our Experts

NEW QUESTION 147
You have been given a new brief from your supervisor for a client who needs a web application set up on AWS. The a most important requirement is that MySQL must be used as the database, and this database must not be hosted in t« public cloud, but rather at the client's data center due to security risks. Which of the following solutions would be the ^ best to assure that the client's requirements are met? Choose the correct answer from the options below
Please select:

A. Build the application server on a public subnet and the database at the client's data cente
B. Connect them with a VPN connection which uses IPsec.

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

Answer: A

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

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

NEW QUESTION 150
Which of the following is the correct sequence of how KMS manages the keys when used along with the Redshift cluster service
Please select:

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

Answer: A

Explanation:
This is mentioned in the AWS Documentation
Amazon Redshift uses a four-tier, key-based architecture for encryption. The architecture consists of data encryption keys, a database key, a cluster key, and a master key.
Data encryption keys encrypt data blocks in the cluster. Each data block is assigned a randomlygenerated 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 randomlygenerated 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/developereuide/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 152
A company wants to use Cloudtrail for logging all API activity. They want to segregate the logging of data events and management events. How can this be achieved? Choose 2 answers from the options given below
Please select:

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

Answer: BC

Explanation:
The AWS Documentation mentions the following
You can configure multiple trails differently so that the trails process and log only the events that you specify. For example, one trail can log read-only data and management events, so that all read-only events are delivered to one S3 bucket. Another trail can log only write-only data and management events, so that all write-only events are delivered to a separate S3 bucket
Options A and D are invalid because you have to create a trail and not a log group
For more information on managing events with cloudtrail, please visit the following URL:
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/loHEing-manasement-and-dataevents- with-cloudtrai
The correct answers are: Create one trail that logs data events to an S3 bucket. Create another trail that logs management events to another S3 bucket
Submit your Feedback/Queries to our Experts

NEW QUESTION 153
Your company has been using AWS for hosting EC2 Instances for their web and database applications. They want to have a compliance check to see the following
Whether any ports are left open other than admin ones like SSH and RDP
Whether any ports to the database server other than ones from the web server security group are
open Which of the following can help achieve this in the easiest way possible. You don't want to carry out an extra configuration changes?
Please select:

A. AWS Config
B. AWS Trusted Advisor
C. AWS Inspector D.AWSGuardDuty

Answer: B

Explanation:
Trusted Advisor checks for compliance with the following security recommendations:
Limited access to common administrative ports to only a small subset of addresses. This includes ports 22 (SSH), 23 (Telnet) 3389 (RDP), and 5500 (VNQ.
Limited access to common database ports. This includes ports 1433 (MSSQL Server), 1434 (MSSQL Monitor), 3306 (MySQL), Oracle (1521) and 5432 (PostgreSQL).
Option A is partially correct but then you would need to write custom rules for this. The AWS trusted advisor can give you all o these checks on its dashboard
Option C is incorrect. Amazon Inspector needs a software agent to be installed on all EC2 instances that are included in th.
assessment target, the security of which you want to evaluate with Amazon Inspector. It monitors the behavior of the EC2
instance on which it is installed, including network, file system, and process activity, and collects a wide set of behavior and
configuration data (telemetry), which it then passes to the Amazon Inspector service.
Our question's requirement is to choose a choice that is easy to implement. Hence Trusted Advisor is more appropriate for this)
question.
Options D is invalid because this service dont provide these details.
For more information on the Trusted Advisor, please visit the following URL https://aws.amazon.com/premiumsupport/trustedadvisor>
The correct answer is: AWS Trusted Advisor Submit your Feedback/Queries to our Experts

NEW QUESTION 155
An application is designed to run on an EC2 Instance. The applications needs to work with an S3 bucket. From a security perspective , what is the ideal way for the EC2 instance/ application to be configured?
Please select:

A. Use the AWS access keys ensuring that they are frequently rotated.
B. Assign an 1AM user to the application that has specific access to only that S3 bucket
C. Assign an 1AM Role and assign it to the EC2 Instance
D. Assign an 1AM group and assign it to the EC2 Instance

Answer: C

Explanation:
The below diagram from the AWS whitepaper shows the best security practicse of allocating a role that has access to the S3 bucket

Options A,B and D are invalid because using users, groups or access keys is an invalid security practise when giving access to resources from other AWS resources.
For more information on the Security Best practices, please visit the following URL: https://d1.awsstatic.com/whitepapers/Security/AWS Security Best Practices.pdl
The correct answer is: Assign an 1AM Role and assign it to the EC2 Instance Submit your Feedback/Queries to our Experts

NEW QUESTION 156
A company hosts critical data in an S3 bucket. Even though they have assigned the appropriate permissions to the bucket, they are still worried about data deletion. What measures can be taken to restrict the risk of data deletion on the bucket. Choose 2 answers from the options given below Please select:

A. Enable versioning on the S3 bucket
B. Enable data at rest for the objects in the bucket
C. Enable MFA Delete in the bucket policy

D. Enable data in transit for the objects in the bucket

Answer: AC

Explanation:
One of the AWS Security blogs mentions the followinj
Versioning keeps multiple versions of an object in the same bucket. When you enable it on a bucket Amazon S3 automatically adds a unique version ID to every object stored in the bucket. At that point, a simple DELETE action does not permanently delete an object version; it merely associates a delete marker with the object. If you want to permanently delete an object version, you must specify its version ID in your DELETE request.
You can add another layer of protection by enabling MFA Delete on a versioned bucket. Once you do so, you must provide your AWS accounts access keys and a valid code from the account's MFA device in order to permanently delete an object version or suspend or reactivate versioning on the bucket. Option B is invalid because enabling encryption does not guarantee risk of data deletion.
Option D is invalid because this option does not guarantee risk of data deletion.
For more information on AWS S3 versioning and MFA please refer to the below URL: https://aws.amazon.com/blogs/security/securing-access-to-aws-using-mfa-part-3/

NEW QUESTION 161
The correct answers are: Enable versioning on the S3 bucket Enable MFA Delete in the bucket policy Submit your Feedback/Queries to our Experts
You company has mandated that all data in AWS be encrypted at rest. How can you achieve this for EBS volumes? Choose 2 answers from the options given below
Please select:

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

Answer: AB

Explanation:
EBS encryption can also be enabled when the volume is created and not for existing volumes. One can use existing tools for OS level encryption.
Option C is incorrect.
AWS Systems Manager is a management service that helps you automatically collect software inventory, apply OS patches, create system images, and configure Windows and Linux operating systems.
Option D is incorrect
You cannot choose to encrypt a non-encrypted boot volume on instance launch. To have encrypted boot volumes during launch , your custom AMI must have it's boot volume encrypted before launch. For more information on the Security Best practices, please visit the following URL:
.com/whit Security Practices.
The correct answers are: Use Windows bit locker for EBS volumes on Windows instances. Use TrueEncrypt for EBS volumes on Linux instances
Submit your Feedback/Queries to our Experts

NEW QUESTION 164
You are designing a connectivity solution between on-premises infrastructure and Amazon VPC. Your server's on-premises will be communicating with your VPC instances. You will be establishing IPSec
tunnels over the internet. Yo will be using VPN gateways and terminating the IPsec tunnels on AWSsupported customer gateways. Which of the following objectives would you achieve by
implementing an IPSec tunnel as outlined above? Choose 4 answers form the options below Please select:

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

Answer: CDEF

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

Option B is invalid because you need to allow incoming access for the database server from the WebSecGrp security group.
Options C and D are invalid because you need to allow Outbound traffic and not inbound traffic For more information on security groups please visit the below Link: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC Scenario2.html
The correct answer is: Allow Inbound on port 3306 for Source Web Server Security Group WebSecGrp. Submit your Feedback/Queries to our Experts

NEW QUESTION 168
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:
.anaging 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 you 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.ama2on.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 169
You are planning to use AWS Configto check the configuration of the resources in your AWS account. You are planning on using an existing 1AM 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 1AM role permissions please visit the below Link: https://docs.aws.amazon.com/config/latest/developerguide/iamrole-permissions.htmll
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 173
Your company has an external web site. This web site needs to access the objects in an S3 bucket. Which of the following would allow the web site to access the objects in the most secure manner? Please select:

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

Answer: B

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

Option A is invalid because giving public access is not a secure way to provide access Option C is invalid because aws:sites is not a valid condition key Option D is invalid because 1AM roles will not be assigned to web sites
For more information on example bucket policies please visit the below Link:
1 https://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies.html
The correct answer is: Use the aws:Referer key in the condition clause for the bucket policy Submit your Feedback/Queries to our Experts

NEW QUESTION 175
Your company is planning on AWS on hosting its AWS resources. There is a company policy which mandates that all security keys are completely managed within the company itself. Which of the following is the correct measure of following this policy?
Please select:

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

Answer: B

Explanation:
y ensuring that you generate the key pairs for EC2 Instances, you will have complete control of the access keys.
Options A,C and D are invalid because all of these processes means that AWS has ownership of the keys. And the question specifically mentions that you need ownership of the keys
For information on security for Compute Resources, please visit the below URL: https://d1.awsstatic.com/whitepapers/Security/Security Compute Services Whitepaper.pdfl
The correct answer is: Generating the key pairs for the EC2 Instances using puttygen Submit your Feedback/Queries to our Experts

NEW QUESTION 177
The CFO of a company wants to allow one of his employees to view only the AWS usage report page. Which of the below mentioned 1AM policy statements allows the user to have access to the AWS usage report page?
Please select:

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

Answer: C

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

NEW QUESTION 180
Your company has the following setup in AWS

A. A set of EC2 Instances hosting a web application
B. An application load balancer placed in front of the EC2 InstancesThere seems to be a set of malicious requests coming from a set of IP addresse
C. Which of the following can be used to protect against these requests?Please select:
D. Use Security Groups to block the IP addresses
E. Use VPC Flow Logs to block the IP addresses
F. Use AWS inspector to block the IP addresses
G. Use AWS WAF to block the IP addresses

Answer: D

Explanation:
Your answer is incorrect Answer -D
The AWS Documentation mentions the following on AWS WAF which can be used to protect Application Load Balancers and Cloud front
A web access control list (web ACL) gives you fine-grained control over the web requests that your Amazon CloudFront distributions or Application Load Balancers respond to. You can allow or block the following types of requests:
Originate from an IP address or a range of IP addresses Originate from a specific country or countries
Contain a specified string or match a regular expression (regex) pattern in a particular part of requests
Exceed a specified length
Appear to contain malicious SQL code (known as SQL injection)
Appear to contain malicious scripts (known as cross-site scripting)
Option A is invalid because by default Security Groups have the Deny policy
Options B and C are invalid because these services cannot be used to block IP addresses For information on AWS WAF, please visit the below URL: https://docs.aws.amazon.com/waf/latest/developerguide/web-acl.html
The correct answer is: Use AWS WAF to block the IP addresses Submit your Feedback/Queries to our Experts

NEW QUESTION 185
An organization has setup multiple 1AM users. The organization wants that each 1AM user accesses the 1AM console only within the organization and not from outside. How can it achieve this? Please select:

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

Answer: B

Explanation:
You can actually use a Deny condition which will not allow the person to log in from outside. The below example shows the Deny condition to ensure that any address specified in the source address is not allowed to access the resources in aws.
Option A is invalid because you don't mention the security group in the 1AM policy Option C is invalid because security groups by default don't allow traffic
Option D is invalid because the 1AM policy does not have such an option For more information on 1AM policy conditions, please visit the URL:
http://docs.aws.amazon.com/IAM/latest/UserGuide/access pol examples.htm l#iam-policy-example-ec2-two-condition!
The correct answer is: Create an 1AM policy with a condition which denies access when the IP address range is not from the organization
Submit your Feedback/Queries to our Experts

NEW QUESTION 188
You are creating a Lambda function which will be triggered by a Cloudwatch Event. The data from these events needs to be stored in a DynamoDB table. How should the Lambda function be given access to the DynamoDB table?
Please select:

A. Put the AWS Access keys in the Lambda function since the Lambda function by default is secure
B. Use an 1AM role which has permissions to the DynamoDB table and attach it to the Lambda function.
C. Use the AWS Access keys which has access to DynamoDB and then place it in an S3 bucket.
D. Create a VPC endpoint for the DynamoDB tabl
E. Access the VPC endpoint from the Lambda function.

Answer: B

Explanation:
AWS Lambda functions uses roles to interact with other AWS services. So use an 1AM role which has permissions to the DynamoDB table and attach it to the Lambda function.
Options A and C are all invalid because you should never use AWS keys for access. Option D is invalid because the VPC endpoint is used for VPCs
For more information on Lambda function Permission model, please visit the URL https://docs.aws.amazon.com/lambda/latest/dg/intro-permission-model.html
The correct answer is: Use an 1AM role which has permissions to the DynamoDB table and attach it to the Lambda function. Submit your Feedback/Queries to our Experts

NEW QUESTION 192
A company has a requirement to create a DynamoDB table. The company's software architect has provided the following CLI command for the DynamoDB table

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

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

Answer: B

Explanation:
The above command with the "-sse-specification Enabled=true" parameter ensures that the data for the DynamoDB table is encrypted at rest.
Options A,C and D are all invalid because this command is specifically used to ensure data encryption at rest
For more information on DynamoDB encryption, please visit the URL:
https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/encryption.tutorial.html The correct answer is: The above command ensures data encryption at rest for the Customer table

NEW QUESTION 196
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 STANDARDJA (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 Redshif For more information on S3 lifecycle policies, please visit the URL:
http://docs.aws.amazon.com/AmazonS3/latest/dev/obiect-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 199
What is the result of the following bucket policy?

Choose the correct answer
Please select:

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

Answer: C

Explanation:
The policy consists of 2 statements, one is the allow for the user mark to the bucket and the next is the deny policy for all other users. The deny permission will override the allow and hence all users
will not have access to the bucket.
Options A,B and D are all invalid because this policy is used to deny all access to the bucket mybucket For examples on S3 bucket policies, please refer to the below Link: http://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies.htmll
The correct answer is: It will deny all access to the bucket mybucket Submit your FeedbacK/Quenes to our Experts

NEW QUESTION 203
Your company is planning on using AWS EC2 and ELB for deployment for their web applications. The security policy mandates that all traffic should be encrypted.
Which of the following options will ensure that this requirement is met. Choose 2 answers from the options below.
Please select:

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

Answer: BC

Explanation:
The AWS Documentation mentions the following
You can create a load balancer that listens on both the HTTP (80) and HTTPS (443) ports. If you specify that the HTTPS listener sends requests to the instances on port 80, the load balancer terminates the requests and communication from the load balancer to the instances is not encrypted, if the HTTPS listener sends requests to the instances on port 443, communication from the load balancer to the instances is encrypted.
Option A is invalid because there is a need for secure traffic, so port 80 should not be used Option D is invalid because for the HTTPS listener you need to use port 443
For more information on HTTPS with ELB, please refer to the below Link: https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-create-https-ssl-loadbalancer. html
The correct answers are: Ensure the load balancer listens on port 443, Ensure the HTTPS listener sends requests to the instances on port 443

Submit your Feedback/Queries to our Experts

NEW QUESTION 207
You have an Amazon VPC that has a private subnet and a public subnet in which you have a NAT instance server. You have created a group of EC2 instances that configure themselves at startup by downloading a bootstrapping script
from S3 that deploys an application via GIT.
Which one of the following setups would give us the highest level of security? Choose the correct answer from the options given below.
Please select:

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

Answer: D

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

Options A and B are invalid because the instances need to be in the private subnet
Option C is invalid because since the instance needs to be in the private subnet, you should not attach an EIP to the instance
For more information on NAT instance, please refer to the below Link: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuideA/PC lnstance.html!
The correct answer is: EC2 instances in our private subnet no EIPs, route outgoing traffic via the NAT Submit your Feedback/Queries to our Experts

NEW QUESTION 208
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

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

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

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

Money Back Guarantee

AWS-Certified-Security-Specialty Practice Exam Features:

* AWS-Certified-Security-Specialty Questions and Answers Updated Frequently

* AWS-Certified-Security-Specialty Practice Questions Verified by Expert Senior Certified Staff

* AWS-Certified-Security-Specialty Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* AWS-Certified-Security-Specialty Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year