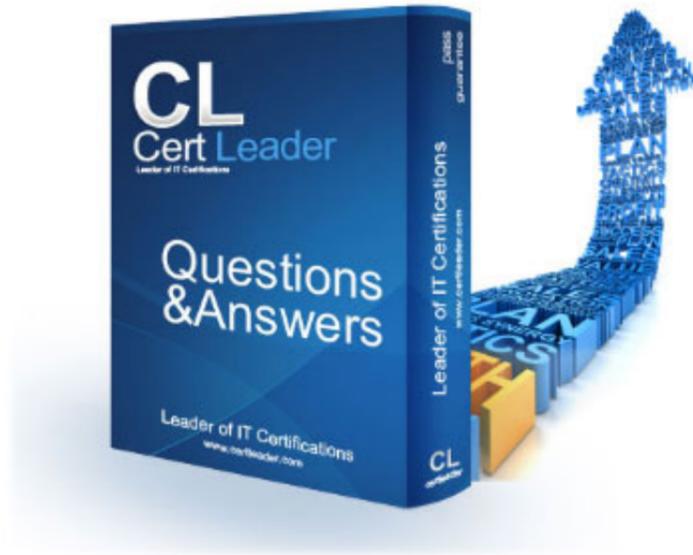# SCS-C01 Dumps

AWS Certified Security- Specialty

https://www.certleader.com/SCS-C01-dumps.html

NEW QUESTION 1
Your developer is using the KMS service and an assigned key in their Java program. They get the below error when running the code
arn:aws:iam::113745388712:user/UserB is not authorized to perform: kms:DescribeKey Which of the following could help resolve the issue?
Please select:

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

Answer: C

Explanation:
You need to ensure that UserB is given access via the Key policy for the Key C:\Users\wk\Desktop\mudassar\Untitled.jpg

Option is invalid because you don't assign roles to 1AM users
For more information on Key policies please visit the below Link: https://docs.aws.amazon.com/kms/latest/developerguide/key-poli
The correct answer is: Ensure that UserB is given the right permissions in the Key policy

NEW QUESTION 2
A company has several Customer Master Keys (CMK), some of which have imported key material. Each CMK must be rotated annually.
What two methods can the security team use to rotate each key? Select 2 answers from the options given below
Please select:

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

Answer: AD

Explanation:
The AWS Documentation mentions the following
Automatic key rotation is available for all customer managed CMKs with KMS-generated key material. It is not available for CMKs that have imported key material (the value of the Origin field is External), but you can rotate these CMKs manually.
Rotating Keys Manually
You might want to create a newCMKand use it in place of a current CMK instead of enabling automatic key rotation. When the new CMK has different cryptographic material than the current CMK, using the new CMK has the same effect as changing the backing key in an existing CMK. The process of replacing one CMK with another is known as manual key rotation.
When you begin using the new CMK, be sure to keep the original CMK enabled so that AWS KMS can decrypt data that the original CMK encrypted. When decrypting data, KMS identifies the CMK that was used to encrypt the data, and it uses the sam CMK to decrypt the data. As long as you keep both the original and new CMKs enabled, AWS KMS can decrypt any data that was encrypted by either CMK.
Option B is invalid because you also need to point the key alias to the new key Option C is invalid because existing CMK keys cannot be rotated as they are
Option E is invalid because deleting existing keys will not guarantee the creation of a new default CMK key For more information on Key rotation please see the below Link: https://docs.aws.amazon.com/kms/latest/developereuide/rotate-keys.html
The correct answers are: Enable automatic key rotation for a CMK, Import new key material to a new CMK;
Point the key alias to the new CMK.

Submit your Feedback/Queries to our Experts

NEW QUESTION 3
A Development team has asked for help configuring the IAM roles and policies in a new AWS account. The team using the account expects to have hundreds of master keys and therefore does not want to manage access control for customer master keys (CMKs).
Which of the following will allow the team to manage AWS KMS permissions in IAM without the complexity of editing individual key policies?

A. The account's CMK key policy must allow the account's IAM roles to perform KMS EnableKey.
B. Newly created CMKs must have a key policy that allows the root principal to perform all actions.
C. Newly created CMKs must allow the root principal to perform the kms CreateGrant API operation.
D. Newly created CMKs must mirror the IAM policy of the KMS key administrator.

Answer: C

NEW QUESTION 4
A Security Administrator is configuring an Amazon S3 bucket and must meet the following security requirements:

Encryption at rest
Logging of all object retrievals in AWS CloudTrail
Which of the following meet these security requirements? (Choose three.)

A. Specify "aws:SecureTransport": "true" within a condition in the S3 bucket policy.
B. Enable a security group for the S3 bucket that allows port 443, but not port 80.
C. Set up default encryption for the S3 bucket.
D. Enable Amazon CloudWatch Logs for the AWS account.
E. Enable API logging of data events for all S3 objects.
F. Enable S3 object versioning for the S3 bucket.

Answer: ACE

NEW QUESTION 5
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 6
A company uses user data scripts that contain sensitive information to bootstrap Amazon EC2 instances. A Security Engineer discovers that this sensitive information is viewable by people who should not have access to it.
What is the MOST secure way to protect the sensitive information used to bootstrap the instances?

A. Store the scripts in the AMI and encrypt the sensitive data using AWS KMS Use the instance role profile to control access to the KMS keys needed to decrypt the data.
B. Store the sensitive data in AWS Systems Manager Parameter Store using the encrypted string parameter and assign the GetParameters permission to the EC2 instance role.
C. Externalize the bootstrap scripts in Amazon S3 and encrypt them using AWS KM
D. Remove the scripts from the instance and clear the logs after the instance is configured.
E. Block user access of the EC2 instance's metadata service using IAM policie
F. Remove all scripts and clear the logs after execution.

Answer: A

NEW QUESTION 7
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-load-balancer.htmll
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 8
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 randomly-generated AES-256 key. These keys are encrypted by using the database key for the cluster.
The database key encrypts data encryption keys in the cluster. The database key is a randomly-generated AES-256 key. It is stored on disk in a separate network from the Amazon Redshift cluster and passed to the cluster across a secure channel.
The cluster key encrypts the database key for the Amazon Redshift cluster.
Option B is incorrect because the master key encrypts the cluster key and not the database key
Option C is incorrect because the master key encrypts the cluster key and not the data encryption keys Option D is incorrect because the master key encrypts the cluster key only
For more information on how keys are used in Redshift, please visit the following URL: https://docs.aws.amazon.com/kms/latest/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 9
Your company manages thousands of EC2 Instances. There is a mandate to ensure that all servers don't have any critical security flaws. Which of the following

can be done to ensure this? Choose 2 answers from the options given below.
Please select:

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

Answer: BD

Explanation:
The AWS Documentation mentions the following on AWS Inspector
Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for vulnerabilities or deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity. These findings can be reviewed directly or as part of detailed assessment reports which are available via the Amazon Inspector console or API.
Option A is invalid because the AWS Config service is not used to check the vulnerabilities on servers Option C is invalid because the AWS Inspector service is not used to patch servers
For more information on AWS Inspector, please visit the following URL: https://aws.amazon.com/inspector>
Once you understand the list of servers which require critical updates, you can rectify them by installing the required patches via the SSM tool.
For more information on the Systems Manager, please visit the following URL: https://docs.aws.amazon.com/systems-manager/latest/APIReference/Welcome.html
The correct answers are: Use AWS Inspector to ensure that the servers have no critical flaws.. Use AWS SSM to patch the servers

NEW QUESTION 10
Compliance requirements state that all communications between company on-premises hosts and EC2 instances be encrypted in transit. Hosts use custom proprietary protocols for their communication, and EC2 instances need to be fronted by a load balancer for increased availability.
Which of the following solutions will meet these requirements?

A. Offload SSL termination onto an SSL listener on a Classic Load Balancer, and use a TCP connection between the load balancer and the EC2 instances.
B. Route all traffic through a TCP listener on a Classic Load Balancer, and terminate the TLS connection on the EC2 instances.
C. Create an HTTPS listener using an Application Load Balancer, and route all of the communication through that load balancer.
D. Offload SSL termination onto an SSL listener using an Application Load Balancer, and re-spawn and SSL connection between the load balancer and the EC2 instances.

Answer: B

NEW QUESTION 10
You have an EC2 instance with the following security configured:
a: ICMP inbound allowed on Security Group
b: ICMP outbound not configured on Security Group
c: ICMP inbound allowed on Network ACL
d: ICMP outbound denied on Network ACL
If Flow logs is enabled for the instance, which of the following flow records will be recorded? Choose 3 answers from the options give below
Please select:

A. An ACCEPT record for the request based on the Security Group
B. An ACCEPT record for the request based on the NACL
C. A REJECT record for the response based on the Security Group
D. A REJECT record for the response based on the NACL

Answer: ABD

Explanation:
This example is given in the AWS documentation as well
For example, you use the ping command from your home computer (IP address is 203.0.113.12) to your instance (the network interface's private IP address is 172.31.16.139). Your security group's inbound rules allow ICMP traffic and the outbound rules do not allow ICMP traffic however, because security groups are stateful, the response ping from your instance is allowed. Your network ACL permits inbound ICMP traffic but does not permit outbound ICMP traffic. Because network ACLs are stateless, the response ping is dropped and will not reach your home computer. In a flow log, this is displayed as 2 flow log records:
An ACCEPT record for the originating ping that was allowed by both the network ACL and the security group, and therefore was allowed to reach your instance.
A REJECT record for the response ping that the network ACL denied.
Option C is invalid because the REJECT record would not be present For more information on Flow Logs, please refer to the below URL:
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/flow-loes.html
The correct answers are: An ACCEPT record for the request based on the Security Group, An ACCEPT record for the request based on the NACL, A REJECT record for the response based on the NACL
Submit your Feedback/Queries to our Experts

NEW QUESTION 15
You have a set of 100 EC2 Instances in an AWS account. You need to ensure that all of these instances are patched and kept to date. All of the instances are in a private subnet. How can you achieve this. Choose 2 answers from the options given below
Please select:

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

Answer: AB

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

One of the AWS Blogs mentions how patching of Linux servers can be accomplished. Below is the diagram representation of the architecture setup
C:\Users\wk\Desktop\mudassar\Untitled.jpg

For more information on patching Linux workloads in AWS, please refer to the Lin. https://aws.amazon.com/blogs/security/how-to-patch-linux-workloads-on-awsj
The correct answers are: Ensure a NAT gateway is present to download the updates. Use the Systems Manager to patch the instances
Submit your Feedback/Queries to our Experts

NEW QUESTION 20

An organization has launched 5 instances: 2 for production and 3 for testing. The organization wants that one particular group of 1AM users should only access the test instances and not the production ones. How can the organization set that as a part of the policy?
Please select:

A. Launch the test and production instances in separate regions and allow region wise access to the group
B. Define the 1AM policy which allows access based on the instance ID
C. Create an 1AM policy with a condition which allows access to only small instances
D. Define the tags on the test and production servers and add a condition to the 1AM policy which allows access to specification tags

Answer: D

Explanation:
Tags enable you to categorize your AWS resources in different ways, for example, by purpose, owner, or environment. This is useful when you have many resources of the same type — you can quickly identify a specific resource based on the tags you've assigned to it
Option A is invalid because this is not a recommended practices
Option B is invalid because this is an overhead to maintain this in policies Option C is invalid because the instance type will not resolve the requirement For information on resource tagging, please visit the below URL: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Usine_Tags.htmll
The correct answer is: Define the tags on the test and production servers and add a condition to the 1AM policy which allows access to specific tags
Submit your Feedback/Queries to our Experts

NEW QUESTION 23

An organization is moving non-business-critical applications to AWS while maintaining a mission-critical application in an on-premises data center. An on-premises application must share limited confidential information with the applications in AWS. The internet performance is unpredictable.
Which configuration will ensure continued connectivity between sites MOST securely?

A. VPN and a cached storage gateway
B. AWS Snowball Edge

C. VPN Gateway over AWS Direct Connect
D. AWS Direct Connect

Answer: C

NEW QUESTION 27
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 29
A company hosts a popular web application that connects to an Amazon RDS MySQL DB instance running in a private VPC subnet that was created with default ACL settings. The IT Security department has a suspicion that a DDos attack is coming from a suspecting IP. How can you protect the subnets from this attack?
Please select:

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

Answer: C

Explanation:
Option A and B are invalid because by default the Security Groups already block traffic. You can use NACL's as an additional security layer for the subnet to deny traffic.
Option D is invalid since just changing the Inbound Rules is sufficient The AWS Documentation mentions the following
A network access control list (ACLJ is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC.
The correct answer is: Change the Inbound NACL to deny access from the suspecting IP

NEW QUESTION 32
A company's database developer has just migrated an Amazon RDS database credential to be stored and managed by AWS Secrets Manager. The developer has also enabled rotation of the credential within the Secrets Manager console and set the rotation to change every 30 days.
After a short period of time, a number of existing applications have failed with authentication errors. What is the MOST likely cause of the authentication errors?

A. Migrating the credential to RDS requires that all access come through requests to the Secrets Manager.
B. Enabling rotation in Secrets Manager causes the secret to rotate immediately, and the applications are using the earlier credential.
C. The Secrets Manager IAM policy does not allow access to the RDS database.
D. The Secrets Manager IAM policy does not allow access for the applications.

Answer: B

NEW QUESTION 35
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 C:\Users\wk\Desktop\mudassar\Untitled.jpg

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 36
An application makes calls to AWS services using the AWS SDK. The application runs on Amazon EC2 instances with an associated IAM role. When the application attempts to access an object within an Amazon S3 bucket; the Administrator receives the following error message: HTTP 403: Access Denied. Which combination of steps should the Administrator take to troubleshoot this issue? (Select three.)

A. Confirm that the EC2 instance's security group authorizes S3 access.
B. Verify that the KMS key policy allows decrypt access for the KMS key for this IAM principle.
C. Check the S3 bucket policy for statements that deny access to objects.
D. Confirm that the EC2 instance is using the correct key pair.
E. Confirm that the IAM role associated with the EC2 instance has the proper privileges.
F. Confirm that the instance and the S3 bucket are in the same Region.

Answer: ABC

NEW QUESTION 37
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 40
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 42
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 46
An application has been written that publishes custom metrics to Amazon CloudWatch. Recently, IAM changes have been made on the account and the metrics are no longer being reported.
Which of the following is the LEAST permissive solution that will allow the metrics to be delivered?

A. Add a statement to the IAM policy used by the application to allow logs:putLogEvents and logs:createLogStream
B. Modify the IAM role used by the application by adding the CloudWatchFullAccess managed policy.
C. Add a statement to the IAM policy used by the application to allow cloudwatch:putMetricData.
D. Add a trust relationship to the IAM role used by the application for cloudwatch.amazonaws.com.

Answer: C

NEW QUESTION 47
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 data and management 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-data-events-with-cloudtr 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 50
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 54
Your company has a set of EC2 Instances defined in AWS. These Ec2 Instances have strict security groups attached to them. You need to ensure that changes to the Security groups are noted and acted on accordingly. How can you achieve this?
Please select:

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

Answer: D

Explanation:
The below diagram from an AWS blog shows how security groups can be monitored
C:\Users\wk\Desktop\mudassar\Untitled.jpg

Option A is invalid because you need to use Cloudwatch Events to check for chan, Option B is invalid because you need to use Cloudwatch Events to check for chang
Option C is invalid because AWS inspector is not used to monitor the activity on Security Groups For more information on monitoring security groups, please visit the below URL:
Ihttpsy/aws.amazon.com/blogs/security/how-to-automatically-revert-and-receive-notifications-about-changes-to 'pc-security-groups/
The correct answer is: Use Cloudwatch events to be triggered for any changes to the Security Groups. Configure the Lambda function for email notification as well.
Submit your Feedback/Queries to our Experts

NEW QUESTION 59
A Security Engineer must implement mutually authenticated TLS connections between containers that communicate inside a VPC.
Which solution would be MOST secure and easy to maintain?

A. Use AWS Certificate Manager to generate certificates from a public certificate authority and deploy them to all the containers.
B. Create a self-signed certificate in one container and use AWS Secrets Manager to distribute the certificate to the other containers to establish trust.
C. Use AWS Certificate Manager Private Certificate Authority (ACM PCA) to create a subordinate certificate authority, then create the private keys in the containers and sign them using the ACM PCA API.
D. Use AWS Certificate Manager Private Certificate Authority (ACM PCA) to create a subordinate certificate authority, then use AWS Certificate Manager to generate the private certificates and deploy them to all the containers.

Answer: C

NEW QUESTION 61
A company is deploying a new web application on AWS. Based on their other web applications, they anticipate being the target of frequent DDoS attacks. Which steps can the company use to protect their application? Select 2 answers from the options given below.
Please select:

A. Associate the EC2 instances with a security group that blocks traffic from blacklisted IP addresses.
B. Use an ELB Application Load Balancer and Auto Scaling group to scale to absorb application layertraffic.
C. Use Amazon Inspector on the EC2 instances to examine incoming traffic and discard malicious traffic.
D. Use CloudFront and AWS WAF to prevent malicious traffic from reaching the application
E. Enable GuardDuty to block malicious traffic from reaching the application

Answer: BD

Explanation:
The below diagram from AWS shows the best case scenario for avoiding DDos attacks using services such as AWS Cloudfro WAF, ELB and Autoscaling
C:\Users\wk\Desktop\mudassar\Untitled.jpg

Option A is invalid because by default security groups don't allow access Option C is invalid because AWS Inspector cannot be used to examine traffic
Option E is invalid because this can be used for attacks on EC2 Instances but not against DDos attacks on the entire application For more information on DDos mitigation from AWS, please visit the below URL:
https://aws.amazon.com/answers/networking/aws-ddos-attack-mitieationi
The correct answers are: Use an ELB Application Load Balancer and Auto Scaling group to scale to absorb application layer traffic., Use CloudFront and AWS WAF to prevent malicious traffic from reaching the application
Submit your Feedback/Queries to our Experts

NEW QUESTION 62
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 65
You need to have a cloud security device which would allow to generate encryption keys based on FIPS 140-2 Level 3. Which of the following can be used for this purpose.
Please select:

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

Answer: AD

Explanation:
AWS Key Management Service (KMS) now uses FIPS 140-2 validated hardware security modules (HSM) and supports FIPS 140-2 validated endpoints, which provide independent assurances about the confidentiality and integrity of your keys.
All master keys in AWS KMS regardless of their creation date or origin are automatically protected using FIPS 140-2 validated
HSMs. defines four levels of security, simply named "Level 1" to "Level 4". It does not specify in detail what level of security is required by any particular application.
• FIPS 140-2 Level 1 the lowest, imposes very limited requirements; loosely, all components must be "production-grade" anc various egregious kinds of insecurity must be absent
• FIPS 140-2 Level 2 adds requirements for physical tamper-evidence and role-based authentication.
• FIPS 140-2 Level 3 adds requirements for physical tamper-resistance (making it difficult for attackers to gain access to sensitive information contained in the module) and identity-based authentication, and for a physical or logical separation between the interfaces by which "critical security parameters" enter and leave the module, and its other interfaces.
• FIPS 140-2 Level 4 makes the physical security requirements more stringent and requires robustness against environmental attacks.
AWSCIoudHSM provides you with a FIPS 140-2 Level 3 validated single-tenant HSM cluster in your Amazon Virtual Private Cloud (VPQ to store and use your keys. You have exclusive control over how your keys are used via an authentication mechanism independent from AWS. You interact with keys in your AWS CloudHSM cluster similar to the way you interact with your applications running in Amazon EC2.
AWS KMS allows you to create and control the encryption keys used by your applications and supported AWS services in multiple regions around the world from a single console. The service uses a FIPS 140-2 validated HSM to protect the security of your keys. Centralized management of all your keys in AWS KMS lets you enforce who can use your keys under which conditions, when they get rotated, and who can manage them.
AWS KMS HSMs are validated at level 2 overall and at level 3 in the following areas:
• Cryptographic Module Specification
• Roles, Services, and Authentication
• Physical Security
• Design Assurance
So I think that we can have 2 answers for this question. Both A & D.
• https://aws.amazon.com/blo15s/security/aws-key-management-service- now-ffers-flps-140-2-validated-cryptographic-m<
enabling-easier-adoption-of-the-service-for-regulated-workloads/
• https://a ws.amazon.com/cloudhsm/faqs/
• https://aws.amazon.com/kms/faqs/
• https://en.wikipedia.org/wiki/RPS
The AWS Documentation mentions the following
AWS CloudHSM is a cloud-based hardware security module (HSM) that enables you to easily generate and use your own encryption keys on the AWS Cloud. With CloudHSM, you can manage your own encryption keys using FIPS 140-2 Level 3 validated HSMs. CloudHSM offers you the flexibility to integrate with your applications using industry-standard APIs, such as PKCS#11, Java Cryptography Extensions)CE). and Microsoft CryptoNG (CNG) libraries. CloudHSM is also standards-compliant and enables you to export all of your keys to most other commercially-available HSMs. It is a fully-managed service that automates time-consuming administrative tasks for you, such as hardware provisioning, software patching,
high-availability, and backups. CloudHSM also enables you to scale quickly by adding and removing HSM capacity on-demand, with no up-front costs.
All other options are invalid since AWS Cloud HSM is the prime service that offers FIPS 140-2 Level 3 compliance
For more information on CloudHSM, please visit the following url https://aws.amazon.com/cloudhsm;
The correct answers are: AWS KMS, AWS Cloud HSM Submit your Feedback/Queries to our Experts

NEW QUESTION 70
A Systems Engineer is troubleshooting the connectivity of a test environment that includes a virtual security appliance deployed inline. In addition to using the virtual security appliance, the Development team wants to use security groups and network ACLs to accomplish various security requirements in the environment.
What configuration is necessary to allow the virtual security appliance to route the traffic?

A. Disable network ACLs.
B. Configure the security appliance's elastic network interface for promiscuous mode.
C. Disable the Network Source/Destination check on the security appliance's elastic network interface
D. Place the security appliance in the public subnet with the internet gateway

Answer: B

NEW QUESTION 73
A company is planning on using AWS for hosting their applications. They want complete separation and isolation of their production , testing and development environments. Which of the following is an ideal way to design such a setup?
Please select:

A. Use separate VPCs for each of the environments
B. Use separate 1AM Roles for each of the environments
C. Use separate 1AM Policies for each of the environments
D. Use separate AWS accounts for each of the environments

Answer: D

Explanation:
A recommendation from the AWS Security Best practices highlights this as well C:\Users\wk\Desktop\mudassar\Untitled.jpg

option A is partially valid, you can segregate resources, but a best practise is to have multiple accounts for this setup.
Options B and C are invalid because from a maintenance perspective this could become very difficult For more information on the Security Best practices, please visit the following URL:
https://dl.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf
The correct answer is: Use separate AWS accounts for each of the environments Submit your
Feedback/Queries to our Experts

NEW QUESTION 76
A company is building a data lake on Amazon S3. The data consists of millions of small files containing sensitive information. The Security team has the following requirements for the architecture:
• Data must be encrypted in transit.
• Data must be encrypted at rest.
• The bucket must be private, but if the bucket is accidentally made public, the data must remain confidential. Which combination of steps would meet the requirements? (Choose two.)

A. Enable AES-256 encryption using server-side encryption with Amazon S3-managed encryption keys (SSE-S3) on the S3 bucket.
B. Enable default encryption with server-side encryption with AWS KMS-managed keys (SSE-KMS) on the S3 bucket.
C. Add a bucket policy that includes a deny if a PutObject request does not include aws:SecureTransport.
D. Add a bucket policy with aws:SourceIp to Allow uploads and downloads from the corporate intranet only.
E. Add a bucket policy that includes a deny if a PutObject request does not include s3:x-amz-server-side-encryption: "aws:kms".
F. Enable Amazon Macie to monitor and act on changes to the data lake's S3 bucket.

Answer: BC

Explanation:
Bucket encryption using KMS will protect both in case disks are stolen as well as if the bucket is public. This is because the KMS key would need to have privileges granted to it for users outside of AWS.

NEW QUESTION 79
A company stores critical data in an S3 bucket. There is a requirement to ensure that an extra level of security is added to the S3 bucket. In addition , it should be ensured that objects are available in a secondary region if the primary one goes down. Which of the following can help fulfil these requirements? Choose 2 answers from the options given below

Please select:

A. Enable bucket versioning and also enable CRR
B. Enable bucket versioning and enable Master Pays
C. For the Bucket policy add a condition for {"Null": {"aws:MultiFactorAuthAge": true}} i
D. Enable the Bucket ACL and add a condition for {"Null": {"aws:MultiFactorAuthAge": true}}

Answer: AC

Explanation:
The AWS Documentation mentions the following Adding a Bucket Policy to Require MFA
Amazon S3 supports MFA-protected API access, a feature that can enforce multi-factor authentication (MFA) for access to your Amazon S3 resources. Multi-factor authentication provides an extra level of security you can apply to your AWS environment. It is a security feature that requires users to prove physical possession of an MFA device by providing a valid MFA code. For more information, go to AWS Multi-Factor Authentication. You can require MFA authentication for any requests to access your Amazoi. S3 resources.
You can enforce the MFA authentication requirement using the aws:MultiFactorAuthAge key in a bucket policy. 1AM users car access Amazon S3 resources by using temporary credentials issued by the AWS Security Token Service (STS). You provide the MFA code at the time of the STS request.
When Amazon S3 receives a request with MFA authentication, the aws:MultiFactorAuthAge key provides a numeric value indicating how long ago (in seconds) the temporary credential was created. If the temporary credential provided in the request was not created using an MFA device, this key value is null (absent). In a bucket policy, you can add a condition to check this value, as shown in the following example bucket policy. The policy denies any Amazon S3 operation on the /taxdocuments folder in the examplebucket bucket if the request is not MFA authenticated. To learn more about MFA authentication, see Using Multi-Factor Authentication (MFA) in AWS in the 1AM User Guide.

C:\Users\wk\Desktop\mudassar\Untitled.jpg
Option B is invalid because just enabling bucket versioning will not guarantee replication of objects Option D is invalid because the condition for the bucket policy needs to be set accordingly For more information on example bucket policies, please visit the following URL: •
https://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies.html
Also versioning and Cross Region replication can ensure that objects will be available in the destination region in case the primary region fails.
For more information on CRR, please visit the following URL: https://docs.aws.amazon.com/AmazonS3/latest/dev/crr.html
The correct answers are: Enable bucket versioning and also enable CRR, For the Bucket policy add a condition for {"Null": { "aws:MultiFactorAuthAge": true}}
Submit your Feedback/Queries to our Experts

NEW QUESTION 80
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 table.Attach the poll to the DynamoDB table.
D. Create an 1AM user with permissions to write to the DynamoDB tabl
E. Store an access key for that user in the Lambda environment variables.
F. Create an 1AM service role with permissions to write to the DynamoDB tabl
G. 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 84

Due to new compliance requirements, a Security Engineer must enable encryption with customer-provided keys on corporate data that is stored in DynamoDB.

The company wants to retain full control of the encryption keys.

Which DynamoDB feature should the Engineer use to achieve compliance'?

A. Use AWS Certificate Manager to request a certificat
B. Use that certificate to encrypt data prior to uploading it to DynamoDB.
C. Enable S3 server-side encryption with the customer-provided key
D. Upload the data to Amazon S3, and then use S3Copy to move all data to DynamoDB
E. Create a KMS master ke
F. Generate per-record data keys and use them to encrypt data prior to uploading it to DynamoD
G. Dispose of the cleartext and encrypted data keys after encryption without storing.
H. Use the DynamoDB Java encryption client to encrypt data prior to uploading it to DynamoDB.

Answer: D

NEW QUESTION 89

A Systems Engineer has been tasked with configuring outbound mail through Simple Email Service (SES) and requires compliance with current TLS standards.

The mail application should be configured to connect to which of the following endpoints and corresponding ports?

A. email.us-east-1.amazonaws.com over port 8080
B. email-pop3.us-east-1.amazonaws.com over port 995
C. email-smtp.us-east-1.amazonaws.com over port 587
D. email-imap.us-east-1.amazonaws.com over port 993

Answer: C

NEW QUESTION 92

The Information Technology department has stopped using Classic Load Balancers and switched to
Application Load Balancers to save costs. After the switch, some users on older devices are no longer able to connect to the website.

What is causing this situation?

A. Application Load Balancers do not support older web browsers.
B. The Perfect Forward Secrecy settings are not configured correctly.
C. The intermediate certificate is installed within the Application Load Balancer.
D. The cipher suites on the Application Load Balancers are blocking connections.

Answer: D

NEW QUESTION 94

An organization is using Amazon CloudWatch Logs with agents deployed on its Linux Amazon EC2 instances. The agent configuration files have been checked and the application log files to be pushed are configured correctly. A review has identified that logging from specific instances is missing.

Which steps should be taken to troubleshoot the issue? (Choose two.)

A. Use an EC2 run command to confirm that the "awslogs" service is running on all instances.
B. Verify that the permissions used by the agent allow creation of log groups/streams and to put log events.
C. Check whether any application log entries were rejected because of invalid time stamps by reviewing/var/cwlogs/rejects.log.
D. Check that the trust relationship grants the service "cwlogs.amazonaws.com" permission to write objects to the Amazon S3 staging bucket.
E. Verify that the time zone on the application servers is in UTC.

Answer: AB

NEW QUESTION 99

A web application runs in a VPC on EC2 instances behind an ELB Application Load Balancer. The application stores data in an RDS MySQL DB instance. A Linux bastion host is used to apply schema updates to the database - administrators connect to the host via SSH from a corporate workstation. The following security groups are applied to the infrastructure-

* sgLB - associated with the ELB
* sgWeb - associated with the EC2 instances.
* sgDB - associated with the database
* sgBastion - associated with the bastion host Which security group configuration will allow the application to be secure and functional?

Please select:

A. sgLB :allow port 80 and 443 traffic from 0.0.0.0/0sgWeb :allow port 80 and 443 traffic from 0.0.0.0/0 sgDB :allow port 3306 traffic from sgWeb and sgBastionsgBastion: allow port 22 traffic from the corporate IP address range
B. sgLB :allow port 80 and 443 traffic from 0.0.0.0/0 sgWeb :allow port 80 and 443 traffic from sgLB sgDB :allow port 3306 traffic from sgWeb and sgLBsgBastion: allow port 22 traffic from the VPC IP address range
C. sgLB :allow port 80 and 443 traffic from 0.0.0.0/0 sgWeb :allow port 80 and 443 traffic from sgLBsgDB :allow port 3306 traffic from sgWeb and sgBastion sgBastion: allow port 22 traffic from the VPC IP address range
D. sgLB :allow port 80 and 443 traffic from 0.0.0.0/0 sgWeb :allow port 80 and 443 traffic from sgLBsgDB :al!ow port 3306 traffic from sgWeb and sgBastion sgBastion: allow port 22 traffic from the corporate IP address range

Answer: D

Explanation:
The Load Balancer should accept traffic on ow port 80 and 443 traffic from 0.0.0.0/0 The backend EC2 Instances should accept traffic from the Load Balancer
The database should allow traffic from the Web server
And the Bastion host should only allow traffic from a specific corporate IP address range Option A is incorrect because the Web group should only allow traffic from the Load balancer For more information on AWS Security Groups, please refer to below URL: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/usins-network-security.htmll
The correct answer is: sgLB :allow port 80 and 443 traffic from 0.0.0.0/0 sgWeb :allow port 80 and 443 traffic from sgLB
sgDB :allow port 3306 traffic from sgWeb and sgBastion sgBastion: allow port 22 traffic from the corporate IP address range Submit your Feedback/Queries to our Experts

NEW QUESTION 104
During a recent internal investigation, it was discovered that all API logging was disabled in a production account, and the root user had created new API keys that appear to have been used several times.
What could have been done to detect and automatically remediate the incident?

A. Using Amazon Inspector, review all of the API calls and configure the inspector agent to leverage SNS topics to notify security of the change to AWS CloudTrail, and revoke the new API keys for the root user.
B. Using AWS Config, create a config rule that detects when AWS CloudTrail is disabled, as well as any calls to the root user create-api-ke
C. Then use a Lambda function to re-enable CloudTrail logs and deactivate the root API keys.
D. Using Amazon CloudWatch, create a CloudWatch event that detects AWS CloudTrail deactivation and a separate Amazon Trusted Advisor check to automatically detect the creation of root API key
E. Then use a Lambda function to enable AWS CloudTrail and deactivate the root API keys.
F. Using Amazon CloudTrail, create a new CloudTrail event that detects the deactivation of CloudTrail logs, and a separate CloudTrail event that detects the creation of root API key
G. Then use a Lambda function to enable CloudTrail and deactivate the root API keys.

Answer: B

NEW QUESTION 108
A company maintains sensitive data in an Amazon S3 bucket that must be protected using an AWS KMS CMK. The company requires that keys be rotated automatically every year.
How should the bucket be configured?

A. Select server-side encryption with Amazon S3-managed keys (SSE-S3) and select an AWS-managed CMK.
B. Select Amazon S3-AWS KMS managed encryption keys (S3-KMS) and select a customer-managed CMK with key rotation enabled.
C. Select server-side encryption with Amazon S3-managed keys (SSE-S3) and select a customer-managed CMK that has imported key material.
D. Select server-side encryption with AWS KMS-managed keys (SSE-KMS) and select an alias to an AWS-managed CMK.

Answer: B

NEW QUESTION 110
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 usershave 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 113
An AWS account includes two S3 buckets: bucket1 and bucket2. The bucket2 does not have a policy defined, but bucket1 has the following bucket policy:

In addition, the same account has an IAM User named "alice", with the following IAM policy.

Which buckets can user "alice" access?

A. Bucket1 only
B. Bucket2 only
C. Both bucket1 and bucket2
D. Neither bucket1 nor bucket2

Answer: C

NEW QUESTION 116
The Security Engineer created a new AWS Key Management Service (AWS KMS) key with the following key policy:

What are the effects of the key policy? (Choose two.)

A. The policy allows access for the AWS account 111122223333 to manage key access though IAM policies.
B. The policy allows all IAM users in account 111122223333 to have full access to the KMS key.
C. The policy allows the root user in account 111122223333 to have full access to the KMS key.
D. The policy allows the KMS service-linked role in account 111122223333 to have full access to the KMS key.
E. The policy allows all IAM roles in account 111122223333 to have full access to the KMS key.

Answer: BE

NEW QUESTION 121
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:

C:\Users\wk\Desktop\mudassar\Untitled.jpg
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 125
A company has hired a third-party security auditor, and the auditor needs read-only access to all AWS resources and logs of all VPC records and events that have

occurred on AWS. How can the company meet the auditor's requirements without comprising security in the AWS environment? Choose the correct answer from the options below
Please select:

A. Create a role that has the required permissions for the auditor.
B. Create an SNS notification that sends the CloudTrail log files to the auditor's email when CloudTrail delivers the logs to S3, but do not allow the auditor access to the AWS environment.
C. The company should contact AWS as part of the shared responsibility model, and AWS will grant required access to th^ third-party auditor.
D. Enable CloudTrail logging and create an 1AM user who has read-only permissions to the required AWS resources, including the bucket containing the CloudTrail logs.

Answer: D

Explanation:
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.
Option A and C are incorrect since Cloudtrail needs to be used as part of the solution Option B is incorrect since the auditor needs to have access to Cloudtrail
For more information on cloudtrail, please visit the below URL: https://aws.amazon.com/cloudtraiL
The correct answer is: Enable CloudTrail logging and create an 1AM user who has read-only permissions to the required AWS resources, including the bucket containing the CloudTrail logs.
Submit your Feedback/Queries to our Experts

NEW QUESTION 130
An application is currently secured using network access control lists and security groups. Web servers are located in public subnets behind an Application Load Balancer (ALB); application servers are located in private subnets.
How can edge security be enhanced to safeguard the Amazon EC2 instances against attack? (Choose two.)

A. Configure the application's EC2 instances to use NAT gateways for all inbound traffic.
B. Move the web servers to private subnets without public IP addresses.
C. Configure AWS WAF to provide DDoS attack protection for the ALB.
D. Require all inbound network traffic to route through a bastion host in the private subnet.
E. Require all inbound and outbound network traffic to route through an AWS Direct Connect connection.

Answer: BC

NEW QUESTION 135
What is the function of the following AWS Key Management Service (KMS) key policy attached to a customer master key (CMK)?

A. The Amazon WorkMail and Amazon SES services have delegated KMS encrypt and decrypt permissions to the ExampleUser principal in the 111122223333 account.
B. The ExampleUser principal can transparently encrypt and decrypt email exchanges specifically between ExampleUser and AWS.
C. The CMK is to be used for encrypting and decrypting only when the principal is ExampleUser and therequest comes from WorkMail or SES in the specified region.
D. The key policy allows WorkMail or SES to encrypt or decrypt on behalf of the user for any CMK in the account.

Answer: C

NEW QUESTION 139
There are currently multiple applications hosted in a VPC. During monitoring it has been noticed that multiple port scans are coming in from a specific IP Address block. The internal security team has requested that all offending IP Addresses be denied for the next 24 hours. Which of the following is the best method to quickly
and temporarily deny access from the specified IP Address's. Please select:

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

Answer: B

Explanation:
NACL acts as a firewall at the subnet level of the VPC and we can deny the offending IP address block at the subnet level using NACL rules to block the incoming traffic to the VPC instances. Since NACL rules are applied as per the Rule numbers make sure that this rule number should take precedence over other rule numbers if there are any such rules that will allow traffic from these IP ranges. The lowest rule number has more precedence over a rule that has a higher number.
The AWS Documentation mentions the following as a best practices for 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 a unique authentication code (a one-time password, or OTP). Users must provide both their normal credentials (like their user name and password) and the OTP. The MFA device can either be a special piece of hardware, or it can be a virtual device (for example, it can run in an app on a smartphone).

Options C is invalid because these options are not available Option D is invalid because there is not root access for users
For more information on 1AM best practices, please visit the below URL: https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html
The correct answer is: Modify the Network ACLs associated with all public subnets in the VPC to deny access from the IP Address block.
omit your Feedback/Queries to our Experts

NEW QUESTION 142
You have an S3 bucket hosted in AWS. This is used to host promotional videos uploaded by yourself. You need to provide access to users for a limited duration of time. How can this be achieved?
Please select:

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

Answer: B

Explanation:
The AWS Documentation mentions the following
All objects by default are private. Only the object owner has permission to access these objects. However, the object owner can optionally share objects with others by creating a pre-signed URL using their own security credentials, to grant time-limited permission to download the objects.
Option A is invalid because this can be used to prevent accidental deletion of objects Option C is invalid because timestamps are not possible for Roles
Option D is invalid because policies is not the right way to limit access based on time For more information on pre-signed URL's, please visit the URL:
https://docs.aws.ama2on.com/AmazonS3/latest/dev/ShareObiectPreSisnedURL.html
The correct answer is: Use Pre-signed URL's Submit your Feedback/Queries to our Experts

NEW QUESTION 146
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 151
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 156
A Security Administrator is restricting the capabilities of company root user accounts. The company uses AWS Organizations and has enabled it for all feature sets, including consolidated billing. The top-level account is used for billing and administrative purposes, not for operational AWS resource purposes.
How can the Administrator restrict usage of member root user accounts across the organization?

A. Disable the use of the root user account at the organizational roo
B. Enable multi-factor authentication of the root user account for each organizational member account.
C. Configure IAM user policies to restrict root account capabilities for each Organizations member account.
D. Create an organizational unit (OU) in Organizations with a service control policy that controls usage of the root use
E. Add all operational accounts to the new OU.
F. Configure AWS CloudTrail to integrate with Amazon CloudWatch Logs and then create a metric filter for RootAccountUsage.

Answer: C

NEW QUESTION 161
Which technique can be used to integrate AWS 1AM (Identity and Access Management) with an on-premise LDAP (Lightweight Directory Access Protocol) directory service?
Please select:

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

Answer: B

Explanation:
On the AWS Blog site the following information is present to help on this context
The newly released whitepaper. Single Sign-On: Integrating AWS, OpenLDAP, and Shibboleth, will help you integrate your existing LDAP-based user directory with AWS. When you integrate your existing directory with AWS, your users can access AWS by using their existing credentials. This means that your users don't need to maintain yet another user name and password just to access AWS resources.
Option A.C and D are all invalid because in this sort of configuration, you have to use SAML to enable single sign on.
For more information on integrating AWS with LDAP for Single Sign-On, please visit the following URL: https://aws.amazon.eom/blogs/security/new-whitepaper-sinEle-sign-on-inteErating-aws-openldap-and-shibbolet The correct answer is: Use SAML (Security Assertion Markup Language) to enable single sign-on between AWS and LDAP. Submit your Feedback/Queries to our Experts

NEW QUESTION 163
Your application currently use AWS Cognito for authenticating users. Your application consists of different types of users. Some users are only allowed read access to the application and others are given contributor access. How wou you manage the access effectively?
Please select:

A. Create different cognito endpoints, one for the readers and the other for the contributors.
B. Create different cognito groups, one for the readers and the other for the contributors.
C. You need to manage this within the application itself
D. This needs to be managed via Web security tokens

Answer: B

Explanation:
The AWS Documentation mentions the following
You can use groups to create a collection of users in a user pool, which is often done to set the permissions for those users. For example, you can create separate groups for users who are readers, contributors, and editors of your website and app.
Option A is incorrect since you need to create cognito groups and not endpoints
Options C and D are incorrect since these would be overheads when you can use AWS Cognito For more information on AWS Cognito user groups please refer to the below Link: https://docs.aws.amazon.com/coenito/latest/developersuide/cognito-user-pools-user-groups.htmll
The correct answer is: Create different cognito groups, one for the readers and the other for the contributors. Submit your Feedback/Queries to our Experts

NEW QUESTION 166
A Security Engineer is defining the logging solution for a newly developed product. Systems Administrators and Developers need to have appropriate access to event log files in AWS CloudTrail to support and troubleshoot the product.
Which combination of controls should be used to protect against tampering with and unauthorized access to log files? (Choose two.)

A. Ensure that the log file integrity validation mechanism is enabled.
B. Ensure that all log files are written to at least two separate Amazon S3 buckets in the same account.
C. Ensure that Systems Administrators and Developers can edit log files, but prevent any other access.
D. Ensure that Systems Administrators and Developers with job-related need-to-know requirements only are capable of viewing—but not modifying—the log files.
E. Ensure that all log files are stored on Amazon EC2 instances that allow SSH access from the internal corporate network only.

Answer: AD

NEW QUESTION 171
A user has created a VPC with the public and private subnets using the VPC wizard. The VPC has CIDR 20.0.0.0/16. The public subnet uses CIDR 20.0.1.0/24.
The user is planning to host a web server in the public subnet with port 80 and a Database server in the private subnet with port 3306. The user is configuring a
security group for the public subnet (WebSecGrp) and the private subnet (DBSecGrp). which of the below mentioned entries is required in the private subnet
database security group DBSecGrp?
Please select:

A. Allow Inbound on port 3306 for Source Web Server Security Group WebSecGrp.
B. Allow Inbound on port 3306 from source 20.0.0.0/16
C. Allow Outbound on port 3306 for Destination Web Server Security Group WebSecGrp.
D. Allow Outbound on port 80 for Destination NAT Instance IP

Answer: A

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.
C:\Users\wk\Desktop\mudassar\Untitled.jpg

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 172
During a recent security audit, it was discovered that multiple teams in a large organization have placed restricted data in multiple Amazon S3 buckets, and the
data may have been exposed. The auditor has requested that the organization identify all possible objects that contain personally identifiable information (PII) and
then determine whether this information has been accessed.
What solution will allow the Security team to complete this request?

A. Using Amazon Athena, query the impacted S3 buckets by using the PII query identifier functio
B. Then, create a new Amazon CloudWatch metric for Amazon S3 object access to alert when the objects are accessed.
C. Enable Amazon Macie on the S3 buckets that were impacted, then perform data classificatio
D. For identified objects that contain PII, use the research function for auditing AWS CloudTrail logs and S3 bucket logs for GET operations.
E. Enable Amazon GuardDuty and enable the PII rule set on the S3 buckets that were impacted, then perform data classificatio
F. Using the PII findings report from GuardDuty, query the S3 bucket logs by using Athena for GET operations.
G. Enable Amazon Inspector on the S3 buckets that were impacted, then perform data classificatio
H. For identified objects that contain PII, query the S3 bucket logs by using Athena for GET operations.

Answer: B

NEW QUESTION 176
A company has deployed a custom DNS server in AWS. The Security Engineer wants to ensure that Amazon EC2 instances cannot use the Amazon-provided
DNS.
How can the Security Engineer block access to the Amazon-provided DNS in the VPC?

A. Deny access to the Amazon DNS IP within all security groups.
B. Add a rule to all network access control lists that deny access to the Amazon DNS IP.
C. Add a route to all route tables that black holes traffic to the Amazon DNS IP.

D. Disable DNS resolution within the VPC configuration.

Answer: D

NEW QUESTION 178
In response to the past DDoS attack experiences, a Security Engineer has set up an Amazon CloudFront distribution for an Amazon S3 bucket. There is concern that some users may bypass the CloudFront distribution and access the S3 bucket directly.
What must be done to prevent users from accessing the S3 objects directly by using URLs?

A. Change the S3 bucket/object permission so that only the bucket owner has access.
B. Set up a CloudFront origin access identity (OAI), and change the S3 bucket/object permission so that only the OAI has access.
C. Create IAM roles for CloudFront, and change the S3 bucket/object permission so that only the IAM role has access.
D. Redirect S3 bucket access to the corresponding CloudFront distribution.

Answer: B

NEW QUESTION 183
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

C:\Users\wk\Desktop\mudassar\Untitled.jpg
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 187
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 192
While analyzing a company's security solution, a Security Engineer wants to secure the AWS account root user.
What should the Security Engineer do to provide the highest level of security for the account?

A. Create a new IAM user that has administrator permissions in the AWS accoun

B. Delete the password for the AWS account root user.
C. Create a new IAM user that has administrator permissions in the AWS accoun
D. Modify the permissions for the existing IAM users.
E. Replace the access key for the AWS account root use
F. Delete the password for the AWS account root user.
G. Create a new IAM user that has administrator permissions in the AWS accoun
H. Enable multi-factor authentication for the AWS account root user.

Answer: D

Explanation:
If you continue to use the root user credentials, we recommend that you follow the security best practice to enable multi-factor authentication (MFA) for your account. Because your root user can perform sensitive operations in your account, adding an additional layer of authentication helps you to better secure your account. Multiple types of MFA are available.

NEW QUESTION 194
When managing permissions for the API gateway, what can be used to ensure that the right level of permissions are given to developers, IT admins and users? These permissions should be easily managed.
Please select:

A. Use the secure token service to manage the permissions for the different users
B. Use 1AM Policies to create different policies for the different types of users.
C. Use the AWS Config tool to manage the permissions for the different users
D. Use 1AM Access Keys to create sets of keys for the different types of users.

Answer: B

Explanation:
The AWS Documentation mentions the following
You control access to Amazon API Gateway with 1AM permissions by controlling access to the following two API Gateway component processes:
* To create, deploy, and manage an API in API Gateway, you must grant the API developer permissions to perform the required actions supported by the API management component of API Gateway.
* To call a deployed API or to refresh the API caching, you must grant the API caller permissions to perform required 1AM actions supported by the API execution component of API Gateway.
Option A, C and D are invalid because these cannot be used to control access to AWS services. This needs to be done via policies. For more information on permissions with the API gateway, please visit the following URL:
https://docs.aws.amazon.com/apisateway/latest/developerguide/permissions.html
The correct answer is: Use 1AM Policies to create different policies for the different types of users. Submit your Feedback/Queries to our Experts

NEW QUESTION 195
Your team is experimenting with the API gateway service for an application. There is a need to implement a custom module which can be used for authentication/authorization for calls made to the API gateway. How can this be achieved?
Please select:

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

Answer: B

Explanation:
The AWS Documentation mentions the following
An Amazon API Gateway Lambda authorizer (formerly known as a custom authorize?) is a Lambda function that you provide to control access to your API methods. A Lambda authorizer uses bearer token authentication strategies, such as OAuth or SAML. It can also use information described by headers, paths, query strings, stage variables, or context variables request parameters.
Options A,C and D are invalid because these cannot be used if you need a custom authentication/authorization for calls made to the API gateway
For more information on using the API gateway Lambda authorizer please visit the URL:
https://docs.aws.amazon.com/apisateway/latest/developerguide/apieateway-use-lambda-authorizer.htmll The correct answer is: Use a Lambda authorizer
Submit your Feedback/Queries to our Experts

NEW QUESTION 199
You have an instance setup in a test environment in AWS. You installed the required application and the promoted the server to a production environment. Your IT Security team has advised that there maybe traffic flowing in from an unknown IP address to port 22. How can this be mitigated immediately?
Please select:

A. Shutdown the instance
B. Remove the rule for incoming traffic on port 22 for the Security Group
C. Change the AMI for the instance
D. Change the Instance type for the instance

Answer: B

Explanation:
In the test environment the security groups might have been opened to all IP addresses for testing purpose. Always to ensure to remove this rule once all testing is completed.
Option A, C and D are all invalid because this would affect the application running on the server. The easiest way is just to remove the rule for access on port 22.
For more information on authorizing access to an instance, please visit the below URL: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/authorizing-access-to-an-instance.htmll
The correct answer is: Remove the rule for incoming traffic on port 22 for the Security Group Submit your Feedback/Queries to our Experts

NEW QUESTION 202
DDoS attacks that happen at the application layer commonly target web applications with lower volumes of traffic compared to infrastructure attacks. To mitigate these types of attacks, you should probably want to include a WAF (Web Application Firewall) as part of your infrastructure. To inspect all HTTP requests, WAFs sit in-line with your application traffic. Unfortunately, this creates a scenario where WAFs can become a point of failure or bottleneck. To mitigate this problem, you need the ability to run multiple WAFs on demand during traffic spikes. This type of scaling for WAF is done via a "WAF sandwich." Which of the following statements best describes what a "WAF sandwich" is? Choose the correct answer from the options below
Please select:

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

Answer: D

Explanation:
The below diagram shows how a WAF sandwich is created. Its the concept of placing the Ec2 instance which hosts the WAF software in between 2 elastic load balancers.
C:\Users\wk\Desktop\mudassar\Untitled.jpg

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 207
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/
The correct answers are: Enable versioning on the S3 bucket Enable MFA Delete in the bucket policy Submit your Feedback/Queries to our Experts

NEW QUESTION 212

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

A. Use AWS Inspector to inspect all the security Groups
B. Use the AWS Trusted Advisor to see which security groups have compromised access.
C. Use AWS Config to see which security groups have compromised access.
D. Use the AWS CLI to query the security groups and then filter for the rules which have unrestricted accessd

Answer: B

Explanation:
The AWS Trusted Advisor can check security groups for rules that allow unrestricted access to a resource. Unrestricted access increases opportunities for malicious activity (hacking, denial-of-service attacks, loss of data).
If you go to AWS Trusted Advisor, you can see the details C:\Users\wk\Desktop\mudassar\Untitled.jpg

Option A is invalid because AWS Inspector is used to detect security vulnerabilities in instances and not for security groups.
Option C is invalid because this can be used to detect changes in security groups but not show you security groups that have compromised access.
Option Dis partially valid but would just be a maintenance overhead
For more information on the AWS Trusted Advisor, please visit the below URL: https://aws.amazon.com/premiumsupport/trustedadvisor/best-practices;
The correct answer is: Use the AWS Trusted Advisor to see which security groups have compromised access. Submit your Feedback/Queries to our Experts

NEW QUESTION 213
A Security Administrator is performing a log analysis as a result of a suspected AWS account compromise. The Administrator wants to analyze suspicious AWS CloudTrail log files but is overwhelmed by the volume of audit logs being generated.
What approach enables the Administrator to search through the logs MOST efficiently?

A. Implement a "write-only" CloudTrail event filter to detect any modifications to the AWS account resources.
B. Configure Amazon Macie to classify and discover sensitive data in the Amazon S3 bucket that contains the CloudTrail audit logs.
C. Configure Amazon Athena to read from the CloudTrail S3 bucket and query the logs to examine account activities.
D. Enable Amazon S3 event notifications to trigger an AWS Lambda function that sends an email alarm when there are new CloudTrail API entries.

Answer: C

NEW QUESTION 216
A Security Engineer received an AWS Abuse Notice listing EC2 instance IDs that are reportedly abusing other hosts.
Which action should the Engineer take based on this situation? (Choose three.)

A. Use AWS Artifact to capture an exact image of the state of each instance.
B. Create EBS Snapshots of each of the volumes attached to the compromised instances.
C. Capture a memory dump.
D. Log in to each instance with administrative credentials to restart the instance.
E. Revoke all network ingress and egress except for to/from a forensics workstation.
F. Run Auto Recovery for Amazon EC2.

Answer: BCE

NEW QUESTION 218
A company has a set of EC2 Instances hosted in AWS. The EC2 Instances have EBS volumes which is used to store critical information. There is a business continuity requirement to ensure high availability for the EBS volumes. How can you achieve this?

A. Use lifecycle policies for the EBS volumes
B. Use EBS Snapshots
C. Use EBS volume replication
D. Use EBS volume encryption

Answer: B

Explanation:
Data stored in Amazon EBS volumes is redundantly stored in multiple physical locations as part of normal operation of those services and at no additional charge. However, Amazon EBS replication is stored within the same availability zone, not across multiple zones; therefore, it is highly recommended that you conduct regular snapshots to Amazon S3 for long-term data durability Option A is invalid because there is no lifecycle policy for EBS volumes Option C is invalid because there is no EBS volume replication Option D is invalid because EBS volume encryption will not ensure business continuity For information on security for Compute Resources, please visit the below URL: https://d1.awsstatic.com/whitepapers/Security/Security_Compute_Services_Whitepaper.pdf

NEW QUESTION 219
Your company has been using AWS for the past 2 years. They have separate S3 buckets for logging the various AWS services that have been used. They have hired an external vendor for analyzing their log files. They have their own AWS account. What is the best way to ensure that the partner account can access the log files in the company account for analysis. Choose 2 answers from the options given below
Please select:

A. Create an 1AM user in the company account
B. Create an 1AM Role in the company account
C. Ensure the 1AM user has access for read-only to the S3 buckets
D. Ensure the 1AM Role has access for read-only to the S3 buckets

Answer: BD

Explanation:
The AWS Documentation mentions the following
To share log files between multiple AWS accounts, you must perform the following general steps. These steps are explained in detail later in this section.
Create an 1AM role for each account that you want to share log files with.
For each of these 1AM roles, create an access policy that grants read-only access to the account you want to share the log files with.
Have an 1AM user in each account programmatically assume the appropriate role and retrieve the log files. Options A and C are invalid because creating an 1AM user and then sharing the 1AM user credentials with the
vendor is a direct 'NO' practise from a security perspective.
For more information on sharing cloudtrail logs files, please visit the following URL https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-sharine-loes.htmll
The correct answers are: Create an 1AM Role in the company account Ensure the 1AM Role has access for read-only to the S3 buckets
Submit your Feedback/Queries to our Experts

NEW QUESTION 223
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

C:\Users\wk\Desktop\mudassar\Untitled.jpg
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 224
A company is hosting sensitive data in an AWS S3 bucket. It needs to be ensured that the bucket always remains private. How can this be ensured continually?
Choose 2 answers from the options given below
Please select:

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

Answer: AD

Explanation:
One of the AWS Blogs mentions the usage of AWS Config and Lambda to achieve this. Below is the diagram representation of this
C:\Users\wk\Desktop\mudassar\Untitled.jpg

ption C is invalid because the Trusted Advisor API cannot be used to monitor changes to the AWS Bucket Option B doesn't seems to be the most appropriate.
1. If the object is in a bucket in which all the objects need to be private and the object is not private anymore, the Lambda function makes a PutObjectAcI call to S3 to make the object private.

|https://aws.amazon.com/blogs/security/how-to-detect-and-automatically-remediate-unintended-permissions-in-a The following link also specifies that
Create a new Lambda function to examine an Amazon S3 buckets ACL and bucket policy. If the bucket ACL is found to al public access, the Lambda function overwrites it to be private. If a bucket policy is found, the Lambda function creatt an SNS message, puts the policy in the message body, and publishes it to the Amazon SNS topic we created. Bucket policies can be complex, and overwriting your policy may cause unexpected loss of access, so this Lambda function doesn't attempt to alter your policy in any way.
https://aws.amazon.com/blogs/security/how-to-use-aws-config-to-monitor-for-and-respond-to-amazon-s3-bucke Based on these facts Option D seems to be more appropriate then Option B.
For more information on implementation of this use case, please refer to the Link:
https://aws.amazon.com/blogs/security/how-to-use-aws-config-to-monitor-for-and-respond-to-amazon-s3-bucke
The correct answers are: Use AWS Config to monitor changes to the AWS Bucket Use AWS Lambda function to change the bucket ACL

NEW QUESTION 228
A Security Engineer is looking for a way to control access to data that is being encrypted under a CMK. The Engineer is also looking to use additional authenticated data (AAD) to prevent tampering with ciphertext.
Which action would provide the required functionality?

A. Pass the key alias to AWS KMS when calling Encrypt and Decrypt API actions.
B. Use IAM policies to restrict access to Encrypt and Decrypt API actions.
C. Use kms:EncryptionContext as a condition when defining IAM policies for the CMK.
D. Use key policies to restrict access to the appropriate IAM groups.

Answer: D

NEW QUESTION 233
You have an S3 bucket defined in AWS. You want to ensure that you encrypt the data before sending it across the wire. What is the best way to achieve this.
Please select:

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

Answer: B

Explanation:
One can use the AWS Encryption CLI to encrypt the data before sending it across to the S3 bucket. Options A and C are invalid because this would still mean that data is transferred in plain text Option D is invalid because you cannot just enable client side encryption for the S3 bucket For more information on Encrypting and Decrypting data, please visit the below URL:
https://aws.amazonxom/blogs/securirv/how4o-encrvpt-and-decrypt-your-data-with-the-aws-encryption-cl
The correct answer is: Use the AWS Encryption CLI to encrypt the data first Submit your Feedback/Queries to our Experts

NEW QUESTION 236
A company had one of its Amazon EC2 key pairs compromised. A Security Engineer must identify which current Linux EC2 instances were deployed and used the compromised key pair.
How can this task be accomplished?

A. Obtain the list of instances by directly querying Amazon EC2 using: aws ec2 describe-instances --fi1ters "Name=key-name,Values=KEYNAMEHERE".
B. Obtain the fingerprint for the key pair from the AWS Management Console, then search for the fingerprint in the Amazon Inspector logs.
C. Obtain the output from the EC2 instance metadata using: curl http://169.254.169.254/latest/meta-data/public- keys/0/.
D. Obtain the fingerprint for the key pair from the AWS Management Console, then search for the fingerprint in Amazon CloudWatch Logs using: aws logs filter-log-events.

Answer: D

NEW QUESTION 237
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 242
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-remote-commands.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 243
In your LAMP application, you have some developers that say they would like access to your logs. However, since you are using an AWS Auto Scaling group, your instances are constantly being re-created. What would you do to make sure that these developers can access these log files? Choose the correct answer from the options below
Please select:

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

Answer: D

Explanation:
One important security aspect is to never give access to actual servers, hence Option A.B and C are just totally wrong from a security perspective.
The best option is to have a central logging server that can be used to archive logs. These logs can then be stored in S3.
Options A,B and C are all invalid because you should not give access to the developers on the Apache se For more information on S3, please refer to the below link
https://aws.amazon.com/documentation/s3j
The correct answer is: Set up a central logging server that you can use to archive your logs; archive these logs to an S3 bucket for developer-access.
Submit vour Feedback/Queries to our Experts

NEW QUESTION 247
Your company is planning on developing an application in AWS. This is a web based application. The application user will use their facebook or google identities for authentication. You want to have the ability to manage user profiles without having to add extra coding to manage this. Which of the below would assist in this.
Please select:

A. Create an OIDC identity provider in AWS
B. Create a SAML provider in AWS
C. Use AWS Cognito to manage the user profiles
D. Use 1AM users to manage the user profiles

Answer: C

Explanation:
The AWS Documentation mentions the following
A user pool is a user directory in Amazon Cognito. With a user pool, your users can sign in to your web or mobile app through Amazon Cognito. Your users can also sign in through social identity providers like Facebook or Amazon, and through SAML identity providers. Whether your users sign in directly or through a third party, all members of the user pool have a directory profile that you can access through an SDK.
User pools provide:
Sign-up and sign-in services.
A built-in, customizable web UI to sign in users.
Social sign-in with Facebook, Google, and Login with Amazon, as well as sign-in with SAML identity providers from your user pool.
User directory management and user profiles.
Security features such as multi-factor authentication (MFA), checks for compromised credentials, account takeover protection, and phone and email verification.
Customized workflows and user migration through AWS Lambda triggers. Options A and B are invalid because these are not used to manage users Option D is invalid because this would be a maintenance overhead
For more information on Cognito User Identity pools, please refer to the below Link: https://docs.aws.amazon.com/coenito/latest/developerguide/cognito-user-identity-pools.html
The correct answer is: Use AWS Cognito to manage the user profiles Submit your Feedback/Queries to our Experts

NEW QUESTION 249
A pharmaceutical company has digitized versions of historical prescriptions stored on premises. The company would like to move these prescriptions to AWS and perform analytics on the data in them. Any operation with this data requires that the data be encrypted in transit and at rest.
Which application flow would meet the data protection requirements on AWS?

A. Digitized files -> Amazon Kinesis Data Analytics
B. Digitized files -> Amazon Kinesis Data Firehose -> Amazon S3 -> Amazon Athena
C. Digitized files -> Amazon Kinesis Data Streams -> Kinesis Client Library consumer -> Amazon S3 -> Athena
D. Digitized files -> Amazon Kinesis Data Firehose -> Amazon Elasticsearch

Answer: B

NEW QUESTION 252
A company is planning to run a number of Admin related scripts using the AWS Lambda service. There is a need to understand if there are any errors encountered when the script run. How can this be accomplished in the most effective manner.
Please select:

A. Use Cloudwatch metrics and logs to watch for errors
B. Use Cloudtrail to monitor for errors
C. Use the AWS Config service to monitor for errors
D. Use the AWS inspector service to monitor for errors

Answer: A

Explanation:
The AWS Documentation mentions the following
AWS Lambda automatically monitors Lambda functions on your behalf, reporting metrics through Amazon CloudWatch. To help you troubleshoot failures in a function. Lambda logs all requests handled by your function and also automatically stores logs generated by your code through Amazon CloudWatch Logs.
Option B,C and D are all invalid because these services cannot be used to monitor for errors. I For more information on Monitoring Lambda functions, please visit the following URL: https://docs.aws.amazon.com/lambda/latest/dg/monitorine-functions-loes.htmll
The correct answer is: Use Cloudwatch metrics and logs to watch for errors Submit your Feedback/Queries to our Experts

NEW QUESTION 256
A company is planning on extending their on-premise AWS Infrastructure to the AWS Cloud. They need to have a solution that would give core benefits of traffic encryption and ensure latency is kept to a minimum. Which of the following would help fulfil this requirement? Choose 2 answers from the options given below
Please select:

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

Answer: AD

Explanation:
The AWS Document mention the following which supports the requirement C:\Users\wk\Desktop\mudassar\Untitled.jpg

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

NEW QUESTION 259
......

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your SCS-C01 Exam with Our Prep Materials Via below:

https://www.certleader.com/SCS-C01-dumps.html