Exam Questions SCS-C01

AWS Certified Security- Specialty

https://www.2passeasy.com/dumps/SCS-C01/

NEW QUESTION 1
- (Exam Topic 1)
A security engineer is designing an incident response plan to address the risk of a compromised Amazon EC2 instance. The plan must recommend a solution to meet the following requirements:
• A trusted forensic environment must be provisioned
• Automated response processes must be orchestrated
Which AWS services should be included in the plan? {Select TWO)

A. AWS CloudFormation
B. Amazon GuardDuty
C. Amazon Inspector
D. Amazon Macie
E. AWS Step Functions

Answer: AE

NEW QUESTION 2
- (Exam Topic 1)
A company uses HTTP Live Streaming (HLS) to stream live video content to paying subscribers by using Amazon CloudFront. HLS splits the video content into chunks so that the user can request the right chunk based on different conditions Because the video events last for several hours, the total video is made up of thousands of chunks
The origin URL is not disclosed and every user is forced to access the CloudFront URL The company has a web application that authenticates the paying users against an internal repository and a CloudFront key pair that is already issued.
What is the simplest and MOST effective way to protect the content?

A. Develop the application to use the CloudFront key pair to create signed URLs that users will use to access the content.
B. Develop the application to use the CloudFront key pair to set the signed cookies that users will use to access the content.
C. Develop the application to issue a security token that Lambda@Edge will receive to authenticate and authorize access to the content
D. Keep the CloudFront URL encrypted inside the application, and use AWS KMS to resolve the URL on-the-fly after the user is authenticated.

Answer: B

NEW QUESTION 3
- (Exam Topic 1)
A global company that deals with International finance is investing heavily in cryptocurrencies and wants to experiment with mining technologies using AWS. The company's security team has enabled Amazon
GuardDuty and is concerned by the number of findings being generated by the accounts. The security team wants to minimize the possibility of GuardDuty finding false negatives for compromised instances that are performing mining
How can the security team continue using GuardDuty while meeting these requirements?

A. In the GuardDuty console, select the CryptoCurrency:EC2/BitcoinTool B'DNS finding and use the suppress findings option
B. Create a custom AWS Lambda function to process newly detected GuardDuty alerts Process the CryptoCurrency EC2/BitcoinTool BIDNS alert and filter outthe high-severity finding types only.
C. When creating a new Amazon EC2 Instance, provide the instance with a specific tag that indicates it is performing mining operations Create a custom AWS Lambda function to process newly detected GuardDuty alerts and filter for the presence of this tag
D. When GuardDuty produces a cryptocurrency finding, process the finding with a custom AWS Lambda function to extract the instance ID from the finding Then use the AWS Systems Manager Run Command to check for a running process performing mining operations

Answer: A

NEW QUESTION 4
- (Exam Topic 1)
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: B

NEW QUESTION 5
- (Exam Topic 1)
A Solutions Architect is designing a web application that uses Amazon CloudFront, an Elastic Load Balancing Application Load Balancer, and an Auto Scaling group of Amazon EC2 instances. The load balancer and EC2 instances are in the US West (Oregon) region. It has been decided that encryption in transit is necessary by using a customer-branded domain name from the client to CloudFront and from CloudFront to the load balancer.
Assuming that AWS Certificate Manager is used, how many certificates will need to be generated?

A. One in the US West (Oregon) region and one in the US East (Virginia) region.
B. Two in the US West (Oregon) region and none in the US East (Virginia) region.
C. One in the US West (Oregon) region and none in the US East (Virginia) region.
D. Two in the US East (Virginia) region and none in the US West (Oregon) region.

Answer: B

NEW QUESTION 6
- (Exam Topic 1)
A company is using AWS Organizations to manage multiple AWS member accounts. All of these accounts have Amazon GuardDuty enabled in all Regions. The company's AW5 Security Operations Center has a centralized security account for logging and monitoring. One of the member accounts has received an excessively high bill A security engineer discovers that a compromised Amazon EC2 instance is being used to mine crypto currency. The Security Operations Center did not receive a GuardDuty finding in the central security account.
but there was a GuardDuty finding in the account containing the compromised EC2 instance. The security engineer needs to ensure an GuardDuty finding are available in the security account.
What should the security engineer do to resolve this issue?

A. Set up an Amazon CloudWatch Event rule to forward ail GuardDuty findings to the security account Use an AWS Lambda function as a target to raise findings
B. Set up an Amazon CloudWatch Events rule to forward all GuardDuty findings to the security account Use an AWS Lambda function as a target to raise findings in AWS Security Hub
C. Check that GuardDuty in the security account is able to assume a role in the compromised account using the GuardDuty fast findings permission Schedule an Amazon CloudWatch Events rule and an AWS Lambda function to periodically check for GuardDuty findings
D. Use the aws GuardDuty get-members AWS CLI command m the security account to see if the account is listed Send an invitation from GuardDuty m the security account to GuardDuty in the compromised account Accept the invitation to forward all future GuardDuty findings

Answer: D

NEW QUESTION 7
- (Exam Topic 1)
A company has several production AWS accounts and a central security AWS account. The security account is used for centralized monitoring and has IAM privileges to all resources in every corporate account. All of the company's Amazon S3 buckets are tagged with a value denoting the data classification of their contents.
A Security Engineer is deploying a monitoring solution in the security account that will enforce bucket policy compliance. The system must monitor S3 buckets in all production accounts and confirm that any policy change is in accordance with the bucket's data classification. If any change is out of compliance; the Security team must be notified quickly.
Which combination of actions would build the required solution? (Choose three.)

A. Configure Amazon CloudWatch Events in the production accounts to send all S3 events to the security account event bus.
B. Enable Amazon GuardDuty in the security accoun
C. and join the production accounts as members.
D. Configure an Amazon CloudWatch Events rule in the security account to detect S3 bucket creation or modification events.
E. Enable AWS Trusted Advisor and activate email notifications for an email address assigned to the security contact.
F. Invoke an AWS Lambda function in the security account to analyze S3 bucket settings in response to S3 events, and send non-compliance notifications to the Security team.
G. Configure event notifications on S3 buckets for PUT; POST, and DELETE events.

Answer: DEF

NEW QUESTION 8
- (Exam Topic 1)
A convoys data lake uses Amazon S3 and Amazon Athena. The company's security engineer has been asked to design an encryption solution that meets the company's data protection requirements. The encryption solution must work with Amazon S3 and keys managed by the company. The encryption solution must be protected in a hardware security module that is validated id Federal information Processing Standards (FPS) 140-2 Level 3.
Which solution meets these requirements?

A. Use client-side encryption with an AWS KMS customer-managed key implemented with the AWS Encryption SDK
B. Use AWS CloudHSM to store the keys and perform cryptographic operations Save the encrypted text inAmazon S3
C. Use an AWS KMS customer-managed key that is backed by a custom key store using AWS CloudHSM
D. Use an AWS KMS customer-managed key with the bring your own key (BYOK) feature to import a key stored in AWS CloudHSM

Answer: B

NEW QUESTION 9
- (Exam Topic 1)
A Security Engineer discovered a vulnerability in an application running on Amazon ECS. The vulnerability allowed attackers to install malicious code. Analysis of the code shows it exfiltrates data on port 5353 in batches at random time intervals.
While the code of the containers is being patched, how can Engineers quickly identify all compromised hosts and stop the egress of data on port 5353?

A. Enable AWS Shield Advanced and AWS WA
B. Configure an AWS WAF custom filter for egress traffic on port 5353
C. Enable Amazon Inspector on Amazon ECS and configure a custom assessment to evaluate containers that have port 5353 ope
D. Update the NACLs to block port 5353 outbound.
E. Create an Amazon CloudWatch custom metric on the VPC Flow Logs identifying egress traffic on port 5353. Update the NACLs to block port 5353 outbound.
F. Use Amazon Athena to query AWS CloudTrail logs in Amazon S3 and look for any traffic on port 5353. Update the security groups to block port 5353 outbound.

Answer: C

NEW QUESTION 10
- (Exam Topic 1)
A company is operating an open-source software platform that is internet facing. The legacy software platform no longer receives security updates. The software platform operates using Amazon route 53 weighted load balancing to send traffic to two Amazon EC2 instances that connect to an Amazon POS cluster a recent report suggests this software platform is vulnerable to SQL injection attacks. with samples of attacks provided. The company's security engineer must secure this system against SQL injection attacks within 24 hours. The secure, engineer's solution involve the least amount of effort and maintain normal operations during implementation.
What should the security engineer do to meet these requirements?

A. Create an Application Load Balancer with the existing EC2 instances as a target group Create an AWS WAF web ACL containing rules mat protect the application from this attac
B. then apply it to the ALB Test to ensure me vulnerability has been mitigated, then redirect thee Route 53 records to point to the ALB Update security groups on the EC 2 instances to prevent direct access from the internet
C. Create an Amazon CloudFront distribution specifying one EC2 instance as an origin Create an AWS WAF web ACL containing rules that protect the application from this attack, then apply it to me distribution Test to ensure the vulnerability has mitigated, then redirect the Route 53 records to point toCloudFront
D. Obtain me latest source code for the platform and make ire necessary updates Test me updated code to ensure that the vulnerability has been irrigated, then deploy me patched version of the platform to the EC2 instances
E. Update the security group mat is attached to the EC2 instances, removing access from the internet to the TCP port used by the SQL database Create an AWS WAF web ACL containing rules mat protect me application from this attack, men apply it to the EC2 instances Test to ensure me vulnerability has been mitigate
F. then restore the security group to me onginal setting

Answer: A

NEW QUESTION 10
- (Exam Topic 1)
An company is using AWS Secrets Manager to store secrets that are encrypted using a CMK and are stored in the security account 111122223333. One of the company's production accounts. 444455556666, must to retrieve the secret values from the security account 111122223333. A security engineer needs to apply a policy to the secret in the security account based on least privilege access so the production account can retrieve the secret value only.
Which policy should the security engineer apply?

A.
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "secretsmanager:*",
            "Principal": {"AWS": "444455556666"},
            "Resource": "*"
        }
    ]
}
```

B.
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "secretsmanager:*",
            "Principal": {"AWS": "111122223333"},
            "Resource": "*"
        }
    ]
}
```

C.
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "secretsmanager:GetSecretValue",
            "Principal": {"AWS": "111122223333"},
            "Resource": "*"
        }
    ]
}
```

D.
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "secretsmanager:GetSecretValue",
            "Principal": {"AWS": "444455556666"},
            "Resource": "*"
        }
    ]
```

A. Option A
B. Option B
C. Option C
D. Option D

Answer: A

NEW QUESTION 15
- (Exam Topic 1)
After a recent security audit involving Amazon S3, a company has asked assistance reviewing its S3 buckets to determine whether data is properly secured. The first S3 bucket on the list has the following bucket policy.

Is this bucket policy sufficient to ensure that the data is not publicity accessible?

A. Yes, the bucket policy makes the whole bucket publicly accessible despite now the S3 bucket ACL orobject ACLs are configured.
B. Yes, none of the data in the bucket is publicity accessible, regardless of how the S3 bucket ACL and object ACLs are configured.
C. No, the IAM user policy would need to be examined first to determine whether any data is publicly accessible.
D. No, the S3 bucket ACL and object ACLs need to be examined first to determine whether any data is publicly accessible.

Answer: A

NEW QUESTION 17
- (Exam Topic 1)
After multiple compromises of its Amazon EC2 instances, a company's Security Officer is mandating that memory dumps of compromised instances be captured for further analysis. A Security Engineer just received an EC2 abuse notification report from AWS stating that an EC2 instance running the most recent Windows Server 2019 Base AMI is compromised.
How should the Security Engineer collect a memory dump of the EC2 instance for forensic analysis?

A. Give consent to the AWS Security team to dump the memory core on the compromised instance and provide it to AWS Support for analysis.
B. Review memory dump data that the AWS Systems Manager Agent sent to Amazon CloudWatch Logs.
C. Download and run the EC2Rescue for Windows Server utility from AWS.
D. Reboot the EC2 Windows Server, enter safe mode, and select memory dump.

Answer: B

NEW QUESTION 19
- (Exam Topic 1)
A company is outsourcing its operational support 1o an external company. The company’s security officer must implement an access solution fen delegating operational support that minimizes overhead.
Which approach should the security officer take to meet these requirements?

A. implement Amazon Cognito identity pools with a role that uses a policy that denies the actions related to Amazon Cognito API management Allow the external company to federate through its identity provider
B. Federate AWS identity and Access Management (IAM) with the external company's identity provider Create an IAM role and attach a policy with the necessary permissions
C. Create an IAM group for me external company Add a policy to the group that denies IAM modifications Securely provide the credentials to the eternal company.
D. Use AWS SSO with the external company's identity provide
E. Create an IAM group to map to the identity provider user group, and attach a policy with the necessary permissions.

Answer: B

NEW QUESTION 20
- (Exam Topic 1)
A company's Security Engineer has been asked to monitor and report all AWS account root user activities. Which of the following would enable the Security Engineer to monitor and report all root user activities?
(Select TWO)

A. Configuring AWS Organizations to monitor root user API calls on the paying account
B. Creating an Amazon CloudWatch Events rule that will trigger when any API call from the root user isreported
C. Configuring Amazon Inspector to scan the AWS account for any root user activity
D. Configuring AWS Trusted Advisor to send an email to the Security team when the root user logs in to the console
E. Using Amazon SNS to notify the target group

Answer: BE

NEW QUESTION 22
- (Exam Topic 1)
A company has an application hosted in an Amazon EC2 instance and wants the application to access secure strings stored in AWS Systems Manager Parameter Store When the application tries to access the secure string key value, it fails.
Which factors could be the cause of this failure? (Select TWO.)

A. The EC2 instance role does not have decrypt permissions on the AWS Key Management Sen/ice (AWS KMS) key used to encrypt the secret
B. The EC2 instance role does not have read permissions to read the parameters In Parameter Store
C. Parameter Store does not have permission to use AWS Key Management Service (AWS KMS) to decrypt the parameter
D. The EC2 instance role does not have encrypt permissions on the AWS Key Management Service (AWS KMS) key associated with the secret

E. The EC2 instance does not have any tags associated.

Answer: CE

NEW QUESTION 27
- (Exam Topic 1)
Unapproved changes were previously made to a company's Amazon S3 bucket. A security engineer configured AWS Config to record configuration changes made to the company's S3 buckets. The engineer discovers there are S3 configuration changes being made, but no Amazon SNS notifications are being sent. The engineer has already checked the configuration of the SNS topic and has confirmed the configuration is valid.
Which combination of steps should the security engineer take to resolve the issue? (Select TWO.)

A. Configure the S3 bucket ACLs to allow AWS Config to record changes to the buckets.
B. Configure policies attached to S3 buckets to allow AWS Config to record changes to the buckets.
C. Attach the AmazonS3ReadOnryAccess managed policy to the IAM user.
D. Verify the security engineer's IAM user has an attached policy that allows all AWS Config actions.
E. Assign the AWSConfigRole managed policy to the AWS Config role

Answer: BE

NEW QUESTION 28
- (Exam Topic 1)
A company's architecture requires that its three Amazon EC2 instances run behind an Application Load Balancer (ALB). The EC2 instances transmit sensitive data between each other Developers use SSL certificates to encrypt the traffic between the public users and the ALB However the Developers are unsure of how to encrypt the data in transit between the ALB and the EC2 instances and the traffic between the EC2 instances
Which combination of activities must the company implement to meet its encryption requirements'? (Select TWO)

A. Configure SSLTLS on the EC2 instances and configure the ALB target group to use HTTPS
B. Ensure that all resources are in the same VPC so the default encryption provided by the VPC is used to encrypt the traffic between the EC2 instances.
C. In the AL
D. select the default encryption to encrypt the traffic between the ALB and the EC2 instances
E. In the code for the application, include a cryptography library and encrypt the data before sending it between the EC2 instances
F. Configure AWS Direct Connect to provide an encrypted tunnel between the EC2 instances

Answer: BC

NEW QUESTION 32
- (Exam Topic 1)
A Developer signed in to a new account within an AWS Organizations organizations unit (OU) containing multiple accounts. Access to the Amazon S3 service is restricted with the following SCP:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "s3:*",
            "Resource": "*"
        }
    ]
}
```

How can the Security Engineer provide the Developer with Amazon S3 access without affecting other accounts?

A. Move the SCP to the root OU of Organizations to remove the restriction to access Amazon S3.
B. Add an IAM policy for the Developer, which grants S3 access.
C. Create a new OU without applying the SCP restricting S3 acces
D. Move the Developer account to this new OU.
E. Add an allow list for the Developer account for the S3 service.

Answer: B

NEW QUESTION 34
- (Exam Topic 1)
A Security Engineer manages AWS Organizations for a company. The Engineer would like to restrict AWS usage to allow Amazon S3 only in one of the organizational units (OUs). The Engineer adds the following SCP to the OU:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowS3",
            "Effect": "Allow",
            "Action": "s3:*",
            "Resource": "*"
        }
    ]
}
```

The next day. API calls to AWS IAM appear in AWS CloudTrail logs In an account under that OU. How should the Security Engineer resolve this issue?

A. Move the account to a new OU and deny IAM:* permissions.
B. Add a Deny policy for all non-S3 services at the account level.
C. Change the policy to:{“Version”: “2012-10-17”,“Statement”: [{“Sid”: “AllowS3”,"Effect": "Allow","Action": "s3:*","Resource": "*/*»}]}
D. Detach the default FullAWSAccess SCP

Answer: C

NEW QUESTION 35
- (Exam Topic 1)
A company is collecting AWS CloudTrail log data from multiple AWS accounts by managing individual trails in each account and forwarding log data to a centralized Amazon S3 bucket residing in a log archive account. After CloudTrail introduced support for AWS Organizations trails, the company decided to further centralize management and automate deployment of the CloudTrail logging capability across all of its AWS accounts.
The company's security engineer created an AWS Organizations trail in the master account, enabled
server-side encryption with AWS KMS managed keys (SSE-KMS) for the log files, and specified the same bucket as the storage location. However, the engineer noticed that logs recorded by the new trail were not delivered to the bucket.
Which factors could cause this issue? (Select TWO.)

A. The CMK key policy does not allow CloudTrail to make encrypt and decrypt API calls against the key.
B. The CMK key policy does not allow CloudTrail to make GenerateDataKey API calls against the key.
C. The IAM role used by the CloudTrail trail does not have permissions to make PutObject API calls against a folder created for the Organizations trail.
D. The S3 bucket policy does not allow CloudTrail to make PutObject API calls against a folder created for the Organizations trail.
E. The CMK key policy does not allow the IAM role used by the CloudTrail trail to use the key for crypto graphical operations.

Answer: AD

NEW QUESTION 36
- (Exam Topic 1)
A company’s security engineer is configuring Amazon S3 permissions to ban all current and future public buckets However, the company hosts several websites directly off S3 buckets with public access enabled
The engineer needs to bock me pubic S3 buckets without causing any outages on me easting websites The
engineer has set up an Amazon CloudFrom distribution (or each website Which set or steps should the security engineer implement next?

A. Configure an S3 bucket as the origin an origin access identity (OAI) for the CloudFront distribution Switch the DNS records from websites to point to the CloudFront distribution Enable Nock public access settings at the account level
B. Configure an S3 bucket as the origin with an origin access identity (OAI) for the CloudFront distribution Switch the ONS records tor the websites to point to the CloudFront disinfection Then, tor each S3 bucket enable block public access settings
C. Configure an S3 bucket as the origin with an origin access identity (OAI) for the CloudFront distribution Enable block public access settings at the account level
D. Configure an S3 bucket as the origin for me CloudFront distribution Configure the S3 bucket policy to accept connections from the CloudFront points of presence only Switch the DNS records for the websites to point to the CloudFront distribution Enable block public access settings at me account level

Answer: A

NEW QUESTION 39
- (Exam Topic 1)
A Security Engineer accidentally deleted the imported key material in an AWS KMS CMK. What should the Security Engineer do to restore the deleted key material?

A. Create a new CM
B. Download a new wrapping key and a new import token to import the original key material
C. Create a new CMK Use the original wrapping key and import token to import the original key material.
D. Download a new wrapping key and a new import token Import the original key material into the existing CMK.
E. Use the original wrapping key and import token Import the original key material into the existing CMK

Answer: C

NEW QUESTION 43
- (Exam Topic 1)
An external Auditor finds that a company's user passwords have no minimum length. The company is currently using two identity providers:
• AWS IAM federated with on-premises Active Directory
• Amazon Cognito user pools to accessing an AWS Cloud application developed by the company Which combination o1 actions should the Security Engineer take to solve this issue? (Select TWO.)

A. Update the password length policy In the on-premises Active Directory configuration.
B. Update the password length policy In the IAM configuration.
C. Enforce an IAM policy In Amazon Cognito and AWS IAM with a minimum password length condition.
D. Update the password length policy in the Amazon Cognito configuration.
E. Create an SCP with AWS Organizations that enforces a minimum password length for AWS IAM and Amazon Cognito.

Answer: AD

NEW QUESTION 46
- (Exam Topic 1)
A company has a serverless application for internal users deployed on AWS. The application uses AWS Lambda for the front end and for business logic. The Lambda function accesses an Amazon RDS database inside a VPC The company uses AWS Systems Manager Parameter Store for storing database credentials.
A recent security review highlighted the following issues

- The Lambda function has internet access.
- The relational database is publicly accessible.
- The database credentials are not stored in an encrypted state.

Which combination of steps should the company take to resolve these security issues? (Select THREE)

A. Disable public access to the RDS database inside the VPC
B. Move all the Lambda functions inside the VPC.
C. Edit the IAM role used by Lambda to restrict internet access.
D. Create a VPC endpoint for Systems Manage
E. Store the credentials as a string paramete
F. Change the parameter type to an advanced parameter.
G. Edit the IAM role used by RDS to restrict internet access.
H. Create a VPC endpoint for Systems Manage
I. Store the credentials as a SecureString parameter.

Answer: ABE

NEW QUESTION 50
- (Exam Topic 1)
A security engineer has noticed that VPC Flow Logs are getting a lot REJECT traffic originating from a single Amazon EC2 instance in an Auto Scaling group. The security engineer is concerned that this EC2 instance may be compromised.
What immediate action should the security engineer take? What immediate action should the security engineer take?

A. Remove me instance from the Auto Seating group Close me security group mm ingress only from a single forensic P address to perform an analysis.
B. Remove me instance from the Auto Seating group Change me network ACL rules to allow traffic only from a single forensic IP address to perform en analysis Add a rule to deny all other traffic.
C. Remove the instance from the Auto Scaling group Enable Amazon GuardDuty in that AWS account Install the Amazon Inspector agent cm the suspicious EC 2 instance to perform a scan.
D. Take a snapshot of the suspicious EC2 instanc
E. Create a new EC2 instance from me snapshot in a closed security group with ingress only from a single forensic IP address to perform an analysis

Answer: B

NEW QUESTION 54
- (Exam Topic 1)
A security engineer is responsible for providing secure access to AWS resources for thousands of developer in a company's corporate identity provider (idp). The developers access a set of AWS services from the corporate premises using IAM credential. Due to the velum of require for provisioning new IAM users, it is taking a long time to grant access permissions. The security engineer receives reports that developer are sharing their IAM credentials with others to avoid provisioning delays. The causes concern about overall security for the security engineer.
Which actions will meet the program requirements that address security?

A. Create an Amazon CloudWatch alarm for AWS CloudTrail Events Create a metric filter to send a notification when me same set of IAM credentials is used by multiple developer
B. Create a federation between AWS and the existing corporate IdP Leverage IAM roles to provide federated access to AWS resources
C. Create a VPN tunnel between the corporate premises and the VPC Allow permissions to all AWS services only if it originates from corporate premises.
D. Create multiple IAM rotes for each IAM user Ensure that users who use the same IAM credentials cannot assume the same IAM role at the same time.

Answer: B

NEW QUESTION 56
- (Exam Topic 1)
A large government organization is moving to the cloud and has specific encryption requirements. The first workload to move requires that a customer's data be immediately destroyed when the customer makes that request.
Management has asked the security team to provide a solution that will securely store the data, allow only authorized applications to perform encryption and decryption and allow for immediate destruction of the data
Which solution will meet these requirements?

A. Use AWS Secrets Manager and an AWS SDK to create a unique secret for the customer-specific data
B. Use AWS Key Management Service (AWS KMS) and the AWS Encryption SDK to generate and store a data encryption key for each customer.
C. Use AWS Key Management Service (AWS KMS) with service-managed keys to generate and store customer-specific data encryption keys
D. Use AWS Key Management Service (AWS KMS) and create an AWS CloudHSM custom key store Use CloudHSM to generate and store a new CMK for each customer.

Answer: A

NEW QUESTION 60
- (Exam Topic 1)
A company recently performed an annual security assessment of its AWS environment. The assessment showed that audit logs are not available beyond 90 days and that unauthorized changes to IAM policies are made without detection.
How should a security engineer resolve these issues?

A. Create an Amazon S3 lifecycle policy that archives AWS CloudTrail trail logs to Amazon S3 Glacier after 90 day
B. Configure Amazon Inspector to provide a notification when a policy change is made to resources.
C. Configure AWS Artifact to archive AWS CloudTrail logs Configure AWS Trusted Advisor to provide a notification when a policy change is made to resources.
D. Configure Amazon CloudWatch to export log groups to Amazon S3. Configure AWS CloudTrail to provide a notification when a policy change is made to resources.
E. Create an AWS CloudTrail trail that stores audit logs in Amazon S3. Configure an AWS Config rule to provide a notif cation when a policy change is made to resources.

Answer: A

NEW QUESTION 62
- (Exam Topic 1)
Two Amazon EC2 instances in different subnets should be able to connect to each other but cannot. It has been confirmed that other hosts in the same subnets are able to communicate successfully, and that security groups have valid ALLOW rules in place to permit this traffic.
Which of the following troubleshooting steps should be performed?

A. Check inbound and outbound security groups, looking for DENY rules.
B. Check inbound and outbound Network ACL rules, looking for DENY rules.
C. Review the rejected packet reason codes in the VPC Flow Logs.
D. Use AWS X-Ray to trace the end-to-end application flow

Answer: C

NEW QUESTION 65
- (Exam Topic 2)
You have a web site that is sitting behind AWS Cloudfront. You need to protect the web site against threats such as SQL injection and Cross site scripting attacks.
Which of the following service can help in such a scenario
Please select:

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

Answer: B

Explanation:
The AWS Documentation mentions the following
AWS WAF is a web application firewall that helps detect and block malicious web requests targeted at your web applications. AWS WAF allows you to create rules that can help protect against common web exploits like SQL injection and cross-site scripting. With AWS WAF you first identify the resource (either an Amazon CloudFront distribution or an Application Load Balancer) that you need to protect.
Option A is invalid because this will only give advise on how you can better the security in your AWS account but not protect against threats mentioned in the question.
Option C is invalid because this can be used to scan EC2 Instances for vulnerabilities but not protect against threats mentioned in the question.
Option D is invalid because this can be used to check config changes but not protect against threats mentioned in the quest
For more information on AWS WAF, please visit the following URL: https://aws.amazon.com/waf/details;
The correct answer is: AWS WAF
Submit your Feedback/Queries to our Experts

NEW QUESTION 66
- (Exam Topic 2)
An organization is using AWS CloudTrail, Amazon CloudWatch Logs, and Amazon CloudWatch to send alerts when new access keys are created. However, the alerts are no longer appearing in the Security Operations mail box.
Which of the following actions would resolve this issue?

A. In CloudTrail, verify that the trail logging bucket has a log prefix configured.
B. In Amazon SNS, determine whether the “Account spend limit” has been reached for this alert.
C. In SNS, ensure that the subscription used by these alerts has not been deleted.
D. In CloudWatch, verify that the alarm threshold “consecutive periods” value is equal to, or greater than 1.

Answer: C

NEW QUESTION 68
- (Exam Topic 2)
A company will store sensitive documents in three Amazon S3 buckets based on a data classification scheme of “Sensitive,” “Confidential,” and “Restricted.”
The security solution must meet all of the following requirements:
- Each object must be encrypted using a unique key.
- Items that are stored in the “Restricted” bucket require two-factor authentication for decryption.
- AWS KMS must automatically rotate encryption keys annually.

Which of the following meets these requirements?

A. Create a Customer Master Key (CMK) for each data classification type, and enable the rotation of it annuall
B. For the “Restricted” CMK, define the MFA policy within the key polic
C. Use S3 SSE-KMS to encrypt the objects.
D. Create a CMK grant for each data classification type with EnableKeyRotation and MultiFactorAuthPresent set to tru
E. S3 can then use the grants to encrypt each object with a unique CMK.
F. Create a CMK for each data classification type, and within the CMK policy, enable rotation of it annually, and define the MFA polic
G. S3 can then create DEK grants to uniquely encrypt each object within the S3 bucket.
H. Create a CMK with unique imported key material for each data classification type, and rotate them annuall
I. For the “Restricted” key material, define the MFA policy in the key polic
J. Use S3 SSE-KMS to encrypt the objects.

Answer: A

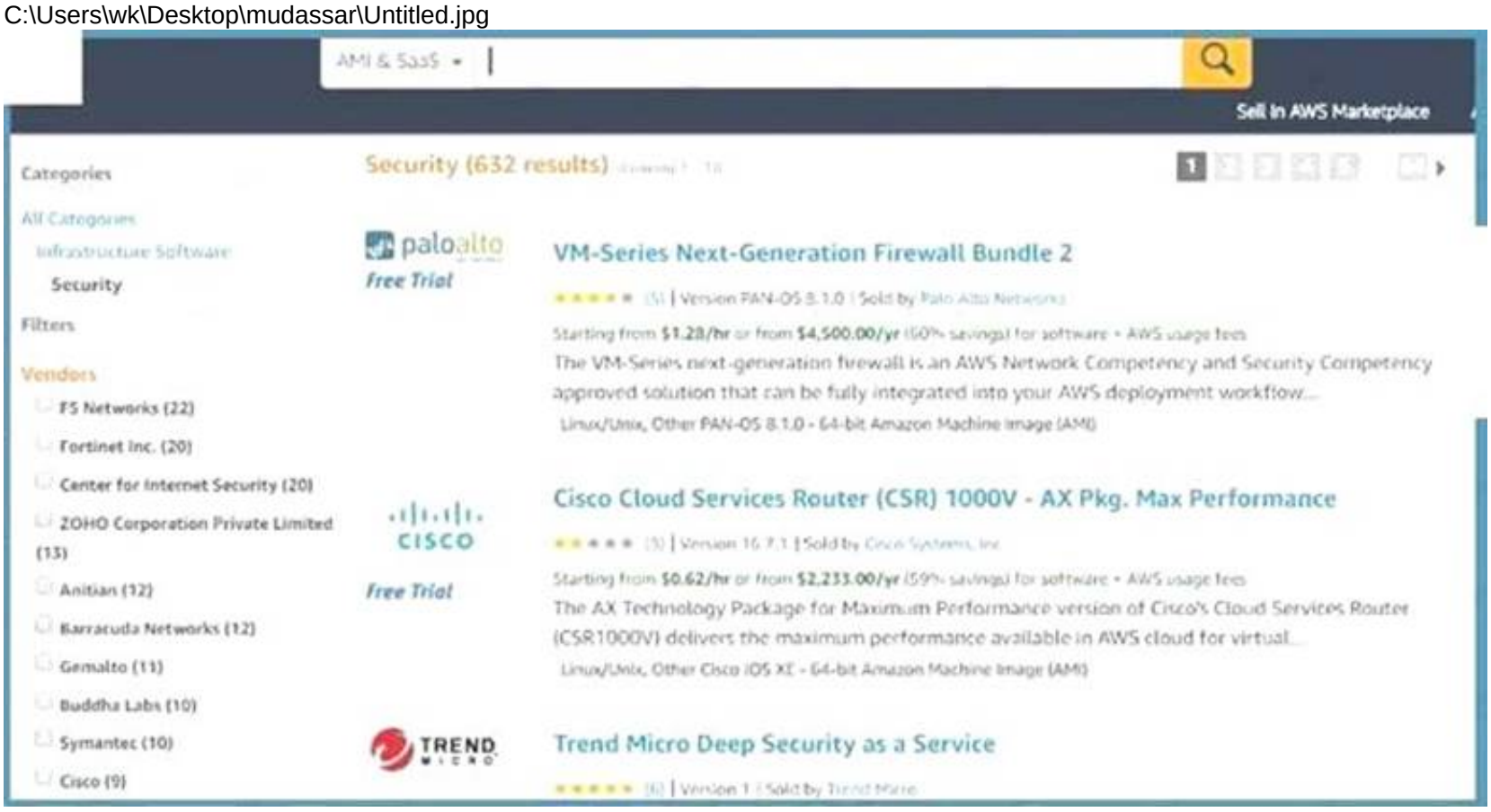
Explanation:
CMKs that are not eligible for automatic key rotation, including asymmetric CMKs, CMKs in custom key stores, and CMKs with imported key material.

NEW QUESTION 71
- (Exam Topic 2)
A company wants to have an Intrusion detection system available for their VPC in AWS. They want to have complete control over the system. Which of the following would be ideal to implement?
Please select:

A. Use AWS WAF to catch all intrusions occurring on the systems in the VPC
B. Use a custom solution available in the AWS Marketplace
C. Use VPC Flow logs to detect the issues and flag them accordingly.
D. Use AWS Cloudwatch to monitor all traffic

Answer: B

Explanation:
Sometimes companies want to have custom solutions in place for monitoring Intrusions to their systems. In such a case, you can use the AWS Marketplace for looking at custom solutions.
C:\Users\wk\Desktop\mudassar\Untitled.jpg



Option A.C and D are all invalid because they cannot be used to conduct intrusion detection or prevention. For more information on using custom security solutions please visit the below URL https://d1.awsstatic.com/Marketplace/security/AWSMP_Security_Solution%200verview.pdf
For more information on using custom security solutions please visit the below URL: https://d1 .awsstatic.com/Marketplace/security/AWSMP Security Solution%20Overview.pd1
The correct answer is: Use a custom solution available in the AWS Marketplace Submit your Feedback/Queries to our Experts

NEW QUESTION 73
- (Exam Topic 2)
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:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam: : 123456789012: user/alice"},
      "Action": "s3:*",
      "Resource": ["arn:aws:s3: : :bucket1", "arn:aws:s3: : :bucket1/*"]
    }
  ]
}
```

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

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "s3:*",
    "Resource": ["arn:aws:s3: : :bucket2", "arn:aws:s3: : :bucket2/*"]
    }
  ]
}
```

Which buckets can user "alice" access?

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

Answer: C

Explanation:
Both S3 policies and IAM policies can be used to grant access to buckets. IAM policies specify what actions are allowed or denied on what AWS resources (e.g. allow ec2:TerminateInstance on the EC2 instance with instance_id=i-8b3620ec). You attach IAM policies to IAM users, groups, or roles, which are then subject to the permissions you've defined. In other words, IAM policies define what a principal can do in your AWS environment. S3 bucket policies, on the other hand, are attached only to S3 buckets. S3 bucket policies specify what actions are allowed or denied for which principals on the bucket that the bucket policy is attached to (e.g. allow user Alice to PUT but not DELETE objects in the bucket).
https://aws.amazon.com/blogs/security/iam-policies-and-bucket-policies-and-acls-oh-my-controlling-access-to-s

NEW QUESTION 76
- (Exam Topic 2)
A company wants to have a secure way of generating, storing and managing cryptographic exclusive access for the keys. Which of the following can be used for this purpose?
Please select:

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

Answer: D

Explanation:
The AWS Documentation mentions the following
The AWS CloudHSM service helps you meet corporate, contractual and regulatory compliance requirements for data security by using dedicated Hardware Security Module (HSM) instances within the AWS cloud. AWS and AWS Marketplace partners offer a variety of solutions for protecting sensitive data within the AWS platform, but for some applications and data subject to contractual or regulatory mandates for managing cryptographic keys, additional protection may be necessary. CloudHSM complements existing data protection solutions and allows you to protect your encryption keys within HSMs that are desigr and validated to government standards for secure key management. CloudHSM allows you to securely generate, store and manage cryptographic keys used for data encryption in a way that keys are accessible only by you.
Option A.B and Care invalid because in all of these cases, the management of the key will be with AWS. Here the question specifically mentions that you want to have exclusive access over the keys. This can be achieved with Cloud HSM
For more information on CloudHSM, please visit the following URL: https://aws.amazon.com/cloudhsm/faq:
The correct answer is: Use Cloud HSM Submit your Feedback/Queries to our Experts

NEW QUESTION 78
- (Exam Topic 2)
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

Explanation:
https://docs.aws.amazon.com/elasticloadbalancing/latest/application/create-https-listener.html

NEW QUESTION 80
- (Exam Topic 2)
You have a vendor that needs access to an AWS resource. You create an AWS user account. You want to restrict access to the resource using a policy for just

that user over a brief period. Which of the following would be an ideal policy to use?
Please select:

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

Answer: B

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

NEW QUESTION 82
- (Exam Topic 2)
The Security Engineer implemented a new vault lock policy for 10TB of data and called initiate-vault-lock 12 hours ago. The Audit team identified a typo that is allowing incorrect access to the vault.
What is the MOST cost-effective way to correct this?

A. Call the abort-vault-lock operation, fix the typo, and call the initiate-vault-lock again.
B. Copy the vault data to Amazon S3, delete the vault, and create a new vault with the data.
C. Update the policy, keeping the vault lock in place.
D. Update the policy and call initiate-vault-lock again to apply the new policy.

Answer: A

Explanation:
Initiate the lock by attaching a vault lock policy to your vault, which sets the lock to an in-progress state and returns a lock ID. While in the in-progress state, you have 24 hours to validate your vault lock policy before the lock ID expires. Use the lock ID to complete the lock process. If the vault lock policy doesn't work as expected, you can abort the lock and restart from the beginning. For information on how to use the S3 Glacier API to lock a vault, see Locking a Vault by Using the Amazon S3 Glacier API. https://docs.aws.amazon.com/amazonglacier/latest/dev/vault-lock-policy.html

NEW QUESTION 83
- (Exam Topic 2)
An organization receives an alert that indicates that an EC2 instance behind an ELB Classic Load Balancer has been compromised.
What techniques will limit lateral movement and allow evidence gathering?

A. Remove the instance from the load balancer and terminate it.
B. Remove the instance from the load balancer, and shut down access to the instance by tightening the security group.
C. Reboot the instance and check for any Amazon CloudWatch alarms.
D. Stop the instance and make a snapshot of the root EBS volume.

Answer: B

Explanation:
https://d1.awsstatic.com/whitepapers/aws_security_incident_response.pdf

NEW QUESTION 87
- (Exam Topic 2)
A company uses AWS Organization to manage 50 AWS accounts. The finance staff members log in as AWS IAM users in the FinanceDept AWS account. The staff members need to read the consolidated billing information in the MasterPayer AWS account. They should not be able to view any other resources in the MasterPayer AWS account. IAM access to billing has been enabled in the MasterPayer account.
Which of the following approaches grants the finance staff the permissions they require without granting any unnecessary permissions?

A. Create an IAM group for the finance users in the FinanceDept account, then attach the AWS managed ReadOnlyAccess IAM policy to the group.
B. Create an IAM group for the finance users in the MasterPayer account, then attach the AWS managed ReadOnlyAccess IAM policy to the group.
C. Create an AWS IAM role in the FinanceDept account with the ViewBilling permission, then grant the finance users in the MasterPayer account the permission to assume that role.
D. Create an AWS IAM role in the MasterPayer account with the ViewBilling permission, then grant the finance users in the FinanceDept account the permission to assume that role.

Answer: D

Explanation:
AWS Region that You Request a Certificate In (for AWS Certificate Manager) If you want to require HTTPS between viewers and CloudFront, you must change the AWS region to US East (N. Virginia) in the AWS Certificate Manager console before you request or import a certificate. If you want to require HTTPS between CloudFront and your origin, and you're using an ELB load balancer as your origin, you can request or import a certificate in any region.
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/cnames-and-https-requirements.html

NEW QUESTION 89
- (Exam Topic 2)

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: B

Explanation:
https://docs.aws.amazon.com/kms/latest/developerguide/key-policies.html#key-policy-default-allow-root-enable

NEW QUESTION 94
- (Exam Topic 2)
Your IT Security team has advised to carry out a penetration test on the resources in their company's AWS Account. This is as part of their capability to analyze the security of the Infrastructure. What should be done first in this regard?
Please select:

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

Answer: C

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

NEW QUESTION 98
- (Exam Topic 2)
What is the function of the following AWS Key Management Service (KMS) key policy attached to a customer master key (CMK)?

```
{
   "Effect": "Allow",
   "Principal": {
    "AWS": "arn:aws:iam::111122223333:user/ExampleUser"
   },
   "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms: GenerateDataKey*",
    "kms:CreateGrant",
    "kms:ListGrants"

   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "kms:ViaService": [
      "workmail.us-west-2.amazonaws.com",
      "ses.us-west-2.amazonaws.com"
     ]
    }
   }
}
```

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 the request 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 100
- (Exam Topic 2)
An application outputs logs to a text file. The logs must be continuously monitored for security incidents.
Which design will meet the requirements with MINIMUM effort?

A. Create a scheduled process to copy the component's logs into Amazon S3. Use S3 events to trigger a Lambda function that updates Amazon CloudWatch metrics with the log dat
B. Set up CloudWatch alerts based on the metrics.
C. Install and configure the Amazon CloudWatch Logs agent on the application's EC2 instanc
D. Create a CloudWatch metric filter to monitor the application log
E. Set up CloudWatch alerts based on the metrics.
F. Create a scheduled process to copy the application log files to AWS CloudTrai
G. Use S3 events to trigger Lambda functions that update CloudWatch metrics with the log dat
H. Set up CloudWatch alerts based on the metrics.
I. Create a file watcher that copies data to Amazon Kinesis when the application writes to the log file.Have Kinesis trigger a Lambda function to update Amazon CloudWatch metrics with the log dat
J. Set up CloudWatch alerts based on the metrics.

Answer: B

Explanation:
https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/QuickStartEC2Instance.html

NEW QUESTION 104
- (Exam Topic 2)
The Security Engineer is given the following requirements for an application that is running on Amazon EC2 and managed by using AWS CloudFormation templates with EC2 Auto Scaling groups:
-Have the EC2 instances bootstrapped to connect to a backend database.
-Ensure that the database credentials are handled securely.
-Ensure that retrievals of database credentials are logged.
Which of the following is the MOST efficient way to meet these requirements?

A. Pass databases credentials to EC2 by using CloudFormation stack parameters with the property set to tru
B. Ensure that the instance is configured to log to Amazon CloudWatch Logs.
C. Store database passwords in AWS Systems Manager Parameter Store by using SecureString parameters.Set the IAM role for the EC2 instance profile to allow access to the parameters.
D. Create an AWS Lambda that ingests the database password and persists it to Amazon S3 with server-side encryptio
E. Have the EC2 instances retrieve the S3 object on startup, and log all script invocations to syslog.
F. Write a script that is passed in as UserData so that it is executed upon launch of the EC2 instance.Ensure that the instance is configured to log to Amazon CloudWatch Logs.

Answer: B

NEW QUESTION 105
- (Exam Topic 2)
You want to get a list of vulnerabilities for an EC2 Instance as per the guidelines set by the Center of Internet Security. How can you go about doing this?
Please select:

A. Enable AWS Guard Duty for the Instance
B. Use AWS Trusted Advisor
C. Use AWS inspector
D. UseAWSMacie

Answer: C

Explanation:
The AWS Inspector service can inspect EC2 Instances based on specific Rules. One of the rules packages is based on the guidelines set by the Center of Internet Security
Center for Internet security (CIS) Benchmarks
The CIS Security Benchmarks program provides well-defined, un-biased and consensus-based industry best practices to help organizations assess and improve their security. Amazon Web Services is a CIS Security Benchmarks Member company and the list of Amazon Inspector certifications can be viewed nere.
Option A is invalid because this can be used to protect an instance but not give the list of vulnerabilities Options B and D are invalid because these services cannot give a list of vulnerabilities For more information
on the guidelines, please visit the below URL:
* https://docs.aws.amazon.com/inspector/latest/userguide/inspector_cis.html The correct answer is: Use AWS Inspector
Submit your Feedback/Queries to our Experts

NEW QUESTION 109
- (Exam Topic 2)
A Security Engineer is implementing a solution to allow users to seamlessly encrypt Amazon S3 objects without having to touch the keys directly. The solution

must be highly scalable without requiring continual management. Additionally, the organization must be able to immediately delete the encryption keys.
Which solution meets these requirements?

A. Use AWS KMS with AWS managed keys and the ScheduleKeyDeletion API with a PendingWindowInDays set to 0 to remove the keys if necessary.
B. Use KMS with AWS imported key material and then use the DeleteImportedKeyMaterial API to remove the key material if necessary.
C. Use AWS CloudHSM to store the keys and then use the CloudHSM API or the PKCS11 library to delete the keys if necessary.
D. Use the Systems Manager Parameter Store to store the keys and then use the service API operations to delete the key if necessary.

Answer: C

Explanation:
https://docs.aws.amazon.com/kms/latest/developerguide/importing-keys-delete-key-material.html

NEW QUESTION 111
- (Exam Topic 2)
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

Explanation:
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3

NEW QUESTION 116
- (Exam Topic 2)
A Security Administrator has a website hosted in Amazon S3. The Administrator has been given the following requirements:
- Users may access the website by using an Amazon CloudFront distribution.
- Users may not access the website directly by using an Amazon S3 URL.

Which configurations will support these requirements? (Choose two.)

A. Associate an origin access identity with the CloudFront distribution.
B. Implement a “Principal”: “cloudfront.amazonaws.com” condition in the S3 bucket policy.
C. Modify the S3 bucket permissions so that only the origin access identity can access the bucket contents.
D. Implement security groups so that the S3 bucket can be accessed only by using the intended CloudFront distribution.
E. Configure the S3 bucket policy so that it is accessible only through VPC endpoints, and place the CloudFront distribution into the specified VPC.

Answer: AC

NEW QUESTION 118
- (Exam Topic 2)
A Security Architect is evaluating managed solutions for storage of encryption keys. The requirements are:
-Storage is accessible by using only VPCs.
-Service has tamper-evident controls.
-Access logging is enabled.
-Storage has high availability.
Which of the following services meets these requirements?

A. Amazon S3 with default encryption
B. AWS CloudHSM
C. Amazon DynamoDB with server-side encryption
D. AWS Systems Manager Parameter Store

Answer: B

NEW QUESTION 120
- (Exam Topic 2)
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

Explanation:

Follow the link:
https://docs.aws.amazon.com/dynamodb-encryption-client/latest/devguide/what-is-ddb-encrypt.html

NEW QUESTION 122
- (Exam Topic 2)
Which of the following are valid event sources that are associated with web access control lists that trigger AWS WAF rules? (Choose two.)

A. Amazon S3 static web hosting
B. Amazon CloudFront distribution
C. Application Load Balancer
D. Amazon Route 53
E. VPC Flow Logs

Answer: BC

Explanation:
A web access control list (web ACL) gives you fine-grained control over the web requests that your Amazon API Gateway API, Amazon CloudFront distribution or Application Load Balancer responds to.

NEW QUESTION 127
- (Exam Topic 2)
A security team is responsible for reviewing AWS API call activity in the cloud environment for security violations. These events must be recorded and retained in a centralized location for both current and future AWS regions.
What is the SIMPLEST way to meet these requirements?

A. Enable AWS Trusted Advisor security checks in the AWS Console, and report all security incidents for all regions.
B. Enable AWS CloudTrail by creating individual trails for each region, and specify a single Amazon S3 bucket to receive log files for later analysis.
C. Enable AWS CloudTrail by creating a new trail and applying the trail to all region
D. Specify a single Amazon S3 bucket as the storage location.
E. Enable Amazon CloudWatch logging for all AWS services across all regions, and aggregate them to a single Amazon S3 bucket for later analysis.

Answer: C

NEW QUESTION 128
- (Exam Topic 2)
Which approach will generate automated security alerts should too many unauthorized AWS API requests be identified?

A. Create an Amazon CloudWatch metric filter that looks for API call error codes and then implement an alarm based on that metric’s rate.
B. Configure AWS CloudTrail to stream event data to Amazon Kinesi
C. Configure an AWS Lambda function on the stream to alarm when the threshold has been exceeded.
D. Run an Amazon Athena SQL query against CloudTrail log file
E. Use Amazon QuickSight to create an operational dashboard.
F. Use the Amazon Personal Health Dashboard to monitor the account’s use of AWS services, and raise an alert if service error rates increase.

Answer: A

Explanation:
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail.html#cloudwatch- Open the CloudWatch console at https://console.aws.amazon.com/cloudwatch/. In the navigation pane, choose Logs. In the list of log groups, select the check box next to the log group that you created for CloudTrail log events. Choose Create Metric Filter. On the Define Logs Metric Filter screen, choose Filter Pattern and then type the following: { ($.errorCode = "*UnauthorizedOperation") || ($.errorCode = "AccessDenied*") } Choose Assign Metric. For Filter Name, type AuthorizationFailures. For Metric Namespace, type CloudTrailMetrics. For Metric Name, type AuthorizationFailureCount.

NEW QUESTION 131
- (Exam Topic 2)
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

Explanation:
https://docs.aws.amazon.com/config/latest/developerguide/cloudtrail-enabled.html https://docs.aws.amazon.com/config/latest/developerguide/iam-root-access-key-check.html

NEW QUESTION 133
- (Exam Topic 2)

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

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

Answer: D

Explanation:
The AWS Documentation states the following
• AWS managed CM Ks: You cannot manage key rotation for AWS managed CMKs. AWS KMS
automatically rotates AWS managed keys every three years (1095 days).
Note: AWS-managed CMKs are rotated every 3yrs, Customer-Managed CMKs are rotated every 365-days from when rotation is enabled.
Option A, B, C are invalid because the dettings for automatic key rotation is not changeable. For more information on key rotation please visit the below URL
https://docs.aws.amazon.com/kms/latest/developereuide/rotate-keys.html
AWS managed CMKs are CMKs in your account that are created, managed, and used on your behalf by an AWS service that is integrated with AWS KMS. This CMK is unique to your AWS account and region. Only the service that created the AWS managed CMK can use it
You can login to you IAM dashbaord . Click on "Encryption Keys" You will find the list based on the services you are using as follows:
• aws/elasticfilesystem 1 aws/lightsail
• aws/s3
• aws/rds and many more Detailed Guide: KMS
You can recognize AWS managed CMKs because their aliases have the format aws/service-name, such as aws/redshift. Typically, a service creates its AWS managed CMK in your account when you set up the service or the first time you use the CMfC
The AWS services that integrate with AWS KMS can use it in many different ways. Some services create AWS managed CMKs in your account. Other services require that you specify a customer managed CMK that you have created. And, others support both types of CMKs to allow you the ease of an AWS managed CMK or the control of a customer-managed CMK
Rotation period for CMKs is as follows:
• AWS managed CMKs: 1095 days
• Customer managed CMKs: 365 days
Since question mentions about "CMK where backing keys is managed by AWS", its Amazon(AWS) managed and its rotation period turns out to be 1095 days{every 3 years)
For more details, please check below AWS Docs: https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html The correct answer is: After 3 years
Submit your Feedback/Queries to our Experts

NEW QUESTION 135
- (Exam Topic 2)
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

Explanation:
https://docs.aws.amazon.com/ses/latest/DeveloperGuide/smtp-connect.html

NEW QUESTION 139
- (Exam Topic 2)
A company uses identity federation to authenticate users into an identity account (987654321987) where the users assume an IAM role named IdentityRole. The users then assume an IAM role named JobFunctionRole in the target AWS account (123456789123) to perform their job functions.
A user is unable to assume the IAM role in the target account. The policy attached to the role in the identity account is:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/JobFunctionRole"
            ],
            "Effect": "Allow"
        }
    ]
}
```

What should be done to enable the user to assume the appropriate role in the target account?

A Update the IAM policy attached to the role in the identity account to be:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": [
                "arn:aws:iam::123456789123:role/JobFunctionRole"
            ],
            "Effect": "Allow"
        }
    ]
}
```

B Update the trust policy on the role in the target account to be:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::987654321987:role/IdentityRole"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

C Update the trust policy on the role in the identity account to be:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": { "AWS": "arn:aws:iam::987654321987:root"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

D Update the IAM policy attached to the role in the target account to be:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1502946463000",
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::123456789123:role/JobFunctionRole"
        }
    ]
}
```

A. Option A
B. Option B
C. Option C
D. Option D

Answer: A

NEW QUESTION 144
- (Exam Topic 2)

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

Explanation:
https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/permissions-reference-cw.html

NEW QUESTION 146
- (Exam Topic 2)
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

Explanation:
https://docs.aws.amazon.com/vpc/latest/userguide/vpc-dns.html

NEW QUESTION 149
- (Exam Topic 2)
An Amazon EC2 instance is denied access to a newly created AWS KMS CMK used for decrypt actions. The environment has the following configuration:
- The instance is allowed the kms:Decrypt action in its IAM role for all resources
- The AWS KMS CMK status is set to enabled
- The instance can communicate with the KMS API using a configured VPC endpoint What is causing the issue?

A. The kms:GenerateDataKey permission is missing from the EC2 instance's IAM role
B. The ARN tag on the CMK contains the EC2 instance's ID instead of the instance's ARN
C. The kms:Encrypt permission is missing from the EC2 IAM role
D. The KMS CMK key policy that enables IAM user permissions is missing

Answer: A

Explanation:
In a key policy, you use "*" for the resource, which means "this CMK." A key policy applies only to the CMK it is attached to
References:

NEW QUESTION 152
- (Exam Topic 2)
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 IAM 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 IAM 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 IAM 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 IAM role (execution role) associated with it. You specify the IAM 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 IAM 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 IAM 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 IAM 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 156
- (Exam Topic 2)
A company hosts a critical web application on the AWS Cloud. This is a key revenue generating application for the company. The IT Security team is worried about potential DDos attacks against the web site. The senior management has also specified that immediate action needs to be taken in case of a potential DDos attack. What should be done in this regard?
Please select:

A. Consider using the AWS Shield Service
B. Consider using VPC Flow logs to monitor traffic for DDos attack and quickly take actions on a trigger of a potential attack.
C. Consider using the AWS Shield Advanced Service
D. Consider using Cloudwatch logs to monitor traffic for DDos attack and quickly take actions on a trigger of a potential attack.

Answer: C

Explanation:
Option A is invalid because the normal AWS Shield Service will not help in immediate action against a DDos attack. This can be done via the AWS Shield Advanced Service
Option B is invalid because this is a logging service for VPCs traffic flow but cannot specifically protect against DDos attacks.
Option D is invalid because this is a logging service for AWS Services but cannot specifically protect against DDos attacks.
The AWS Documentation mentions the following
AWS Shield Advanced provides enhanced protections for your applications running on Amazon EC2. Elastic Load Balancing (ELB), Amazon CloudFront and Route 53 against larger and more sophisticated attacks. AWS Shield Advanced is available to AWS Business Support and AWS Enterprise Support customers. AWS Shield Advanced protection provides always-on, flow-based monitoring of network traffic and active application monitoring to provide near real-time notifications of DDoS attacks. AWS Shield Advanced also gives customers highly flexible controls over attack mitigations to take actions instantly. Customers can also engage the DDoS Response Team (DRT) 24X7 to manage and mitigate their application layer DDoS attacks.
For more information on AWS Shield, please visit the below URL: https://aws.amazon.com/shield/faqs;
The correct answer is: Consider using the AWS Shield Advanced Service Submit your Feedback/Queries to our Experts

NEW QUESTION 157
- (Exam Topic 2)
A company has contracted with a third party to audit several AWS accounts. To enable the audit,
cross-account IAM roles have been created in each account targeted for audit. The Auditor is having trouble accessing some of the accounts.
Which of the following may be causing this problem? (Choose three.)

A. The external ID used by the Auditor is missing or incorrect.
B. The Auditor is using the incorrect password.
C. The Auditor has not been granted sts:AssumeRole for the role in the destination account.
D. The Amazon EC2 role used by the Auditor must be set to the destination account role.
E. The secret key used by the Auditor is missing or incorrect.
F. The role ARN used by the Auditor is missing or incorrect.

Answer: ACF

Explanation:
Using IAM to grant access to a Third-Party Account 1) Create a role to provide access to the require resources 1.1) Create a role policy that specifies the AWS Account ID to be accessed, "sts:AssumeRole" as action, and "sts:ExternalID" as condition 1.2) Create a role using the role policy just created 1.3) Assign a resouce policy to the role. This will provide permission to access resource ARNs to the auditor 2) Repeat steps 1 and 2 on all AWS accounts 3) The auditor connects to the AWS account AWS Security Token Service (STS). The auditor must provide its ExternalID from step 1.2, the ARN of the role he is trying to assume from step 1.3, sts:ExternalID 4) STS provide the auditor with temporary credentials that provides the role access from step 1
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-user_externalid.html
https://aws.amazon.com/blogs/security/how-to-audit-cross-account-roles-using-aws-cloudtrail-and-amazon-clou

NEW QUESTION 162
- (Exam Topic 2)
An application has a requirement to be resilient across not only Availability Zones within the application's primary region but also be available within another region altogether.
Which of the following supports this requirement for AWS resources that are encrypted by AWS KMS?

A. Copy the application's AWS KMS CMK from the source region to the target region so that it can be used to decrypt the resource after it is copied to the target region.
B. Configure AWS KMS to automatically synchronize the CMK between regions so that it can be used to decrypt the resource in the target region.
C. Use AWS services that replicate data across regions, and re-wrap the data encryption key created in the source region by using the CMK in the target region so that the target region's CMK can decrypt the database encryption key.
D. Configure the target region's AWS service to communicate with the source region's AWS KMS so that it can decrypt the resource in the target region.

Answer: C

NEW QUESTION 167
- (Exam Topic 2)
An organization wants to be alerted when an unauthorized Amazon EC2 instance in its VPC performs a network port scan against other instances in the VPC. When the Security team performs its own internal tests in a separate account by using pre-approved third-party scanners from the AWS Marketplace, the Security team also then receives multiple Amazon GuardDuty events from Amazon CloudWatch alerting on its test activities.
How can the Security team suppress alerts about authorized security tests while still receiving alerts about the unauthorized activity?

A. Use a filter in AWS CloudTrail to exclude the IP addresses of the Security team's EC2 instances.
B. Add the Elastic IP addresses of the Security team's EC2 instances to a trusted IP list in Amazon GuardDuty.
C. Install the Amazon Inspector agent on the EC2 instances that the Security team uses.
D. Grant the Security team's EC2 instances a role with permissions to call Amazon GuardDuty API operations.

Answer: B

Explanation:
Trusted IP lists consist of IP addresses that you have whitelisted for secure communication with your AWS infrastructure and applications. GuardDuty does not generate findings for IP addresses on trusted IP lists. At any given time, you can have only one uploaded trusted IP list per AWS account per region. Threat lists consist of known malicious IP addresses. GuardDuty generates findings based on threat lists. At any given time, you can have up to six uploaded threat lists per AWS account per region. https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_upload_lists.html

NEW QUESTION 172
- (Exam Topic 3)
A company has a web-based application using Amazon CloudFront and running on Amazon Elastic Container Service (Amazon ECS) behind an Application Load Balancer (ALB). The ALB is terminating TLS and balancing load across ECS service tasks A security engineer needs to design a solution to ensure that application content is accessible only through CloudFront and that I is never accessible directly.
How should the security engineer build the MOST secure solution?

A. Add an origin custom header Set the viewer protocol policy to HTTP and HTTPS Set the origin protocol pokey to HTTPS only Update the application to validate the CloudFront custom header
B. Add an origin custom header Set the viewer protocol policy to HTTPS only Set the origin protocol policy to match viewer Update the application to validate the CloudFront custom header.
C. Add an origin custom header Set the viewer protocol policy to redirect HTTP to HTTPS Set the origin protocol policy to HTTP only Update the application to validate the CloudFront custom header.
D. Add an origin custom header Set the viewer protocol policy to redirect HTTP to HTTP
E. Set the origin protocol policy to HTTPS only Update the application to validate the CloudFront custom header

Answer: D

NEW QUESTION 174
- (Exam Topic 3)
A company uses a third-party application to store encrypted data in Amazon S3. The company uses another third-party application trial decrypts the data from Amazon S3 to ensure separation of duties Between the applications A Security Engineer warns to separate the permissions using IAM roles attached to Amazon EC2 instances. The company prefers to use native AWS services.
Which encryption method will meet these requirements?

A. Use encrypted Amazon EBS volumes with Amazon default keys (AWS EBS)
B. Use server-side encryption with customer-provided keys (SSE-C)
C. Use server-side encryption with AWS KMS managed keys (SSE-KMS)
D. Use server-side encryption with Amazon S3 managed keys (SSE-S3)

Answer: C

NEW QUESTION 177
- (Exam Topic 3)
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 179
- (Exam Topic 3)
A company uses Amazon RDS for MySQL as a database engine for its applications. A recent security audit revealed an RDS instance that is not compliant with company policy for encrypting data at rest. A security engineer at the company needs to ensure that all existing RDS databases are encrypted using server-side encryption and that any future deviations from the policy are detected.
Which combination of steps should the security engineer take to accomplish this? (Select TWO.)

A. Create an AWS Config rule to detect the creation of unencrypted RDS database
B. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to trigger on the AWS Config rules compliance state change and use Amazon Simple Notification Service (Amazon SNS) to notify the security operations team.
C. Use AWS System Manager State Manager to detect RDS database encryption configuration drif
D. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to track state changes and use Amazon Simple Notification Service (Amazon SNS) to notify

the security operations team.
E. Create a read replica for the existing unencrypted RDS database and enable replica encryption in the proces
F. Once the replica becomes active, promote it into a standalone database instance and terminate the unencrypted database instance.
G. Take a snapshot of the unencrypted RDS databas
H. Copy the snapshot and enable snapshot encryption in the proces
I. Restore the database instance from the newly created encrypted snapsho
J. Terminate the unencrypted database instance.
K. Enable encryption for the identified unencrypted RDS instance by changing the configurations of the existing database

Answer: AD

NEW QUESTION 182
- (Exam Topic 3)
A development team is using an AWS Key Management Service (AWS KMS) CMK to try to encrypt and decrypt a secure string parameter from AWS Systems Manager Parameter Store. However, the development team receives an error message on each attempt.
Which issues that are related to the CMK could be reasons for the error? (Select TWO.)

A. The CMK that is used in the attempt does not exist.
B. The CMK that is used in the attempt needs to be rotated.
C. The CMK that is used in the attempt is using the CMK's key ID instead of the CMK ARN.
D. The CMK that is used in the attempt is not enabled.
E. The CMK that is used in the attempt is using an alias.

Answer: AD

NEW QUESTION 187
- (Exam Topic 3)
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 IAM user with the necessary permissions
C. Change the password for the root account.
D. Delete the root access keys

Answer: BD

Explanation:
The AWS Documentation mentions the following
All AWS accounts have root user credentials (that is, the credentials of the account owner). These credentials allow full access to all resources in the account. Because you cant restrict permissions for root user credentials, we recommend that you delete your root user access keys. Then create AWS Identity and Access Management (IAM) user credentials for everyday interaction with AWS.
Option A is incorrect since you cannot delete the root access account
Option C is partially correct but cannot be used as the ideal solution for safeguarding the account For more information on root access vs admin IAM users, please refer to below URL: https://docs.aws.amazon.com/eeneral/latest/er/root-vs-iam.html
The correct answers are: Create an Admin IAM user with the necessary permissions. Delete the root access keys Submit your Feedback/Queries to our Experts

NEW QUESTION 191
- (Exam Topic 3)
A company wants to ensure that its AWS resources can be launched only in the us-east-1 and us-west-2 Regions.
What is the MOST operationally efficient solution that will prevent developers from launching Amazon EC2 instances in other Regions?

A. Enable Amazon GuardDuty in all Region
B. Create alerts to detect unauthorized activity outside us-east-1 and us-west-2.
C. Use an organization in AWS Organization
D. Attach an SCP that allows all actions when the aws: Requested Region condition key is either us-east-1 or us-west-2. Delete the FullAWSAccess policy.
E. Provision EC2 resources by using AWS Cloud Formation templates through AWS CodePipelin
F. Allow only the values of us-east-1 and us-west-2 in the AWS CloudFormation template's parameters.
G. Create an AWS Config rule to prevent unauthorized activity outside us-east-1 and us-west-2.

Answer: C

NEW QUESTION 194
- (Exam Topic 3)
A company has multiple Amazon S3 buckets encrypted with customer-managed CMKs Due to regulatory requirements the keys must be rotated every year. The company's Security Engineer has enabled automatic key rotation for the CMKs; however the company wants to verity that the rotation has occurred.
What should the Security Engineer do to accomplish this?

A. Filter AWS CloudTrail logs for KeyRotaton events
B. Monitor Amazon CloudWatcn Events for any AWS KMS CMK rotation events
C. Using the AWS CL
D. run the aws kms gel-key-relation-status operation with the --key-id parameter to check the CMK rotation date
E. Use Amazon Athena to query AWS CloudTrail logs saved in an S3 bucket to filter Generate New Key events

Answer: C

NEW QUESTION 197

- (Exam Topic 3)
A company is operating a website using Amazon CloudFornt. CloudFront servers some content from Amazon S3 and other from web servers running EC2 instances behind an Application. Load Balancer (ALB). Amazon DynamoDB is used as the data store. The company already uses AWS Certificate Manager (ACM) to store a public TLS certificate that can optionally secure connections between the website users and CloudFront. The company has a new requirement to enforce end-to-end encryption in transit.
Which combination of steps should the company take to meet this requirement? (Select THREE.)

A. Update the CloudFront distributio
B. configuring it to optionally use HTTPS when connecting to origins on Amazon S3
C. Update the web application configuration on the web servers to use HTTPS instead of HTTP when connecting to DynamoDB
D. Update the CloudFront distribution to redirect HTTP corrections to HTTPS
E. Configure the web servers on the EC2 instances to listen using HTTPS using the public ACM TLS certificate Update the ALB to connect to the target group using HTTPS
F. Update the ALB listen to listen using HTTPS using the public ACM TLS certificat
G. Update the CloudFront distribution to connect to the HTTPS listener.
H. Create a TLS certificate Configure the web servers on the EC2 instances to use HTTPS only with that certificat
I. Update the ALB to connect to the target group using HTTPS.

Answer: BCE

NEW QUESTION 198
- (Exam Topic 3)
A new application will be deployed on EC2 instances in private subnets. The application will transfer sensitive data to and from an S3 bucket. Compliance requirements state that the data must not traverse the public internet. Which solution meets the compliance requirement?
Please select:

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

Answer: C

Explanation:
The AWS Documentation mentions the following
A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink without requiring an internet gateway, NAT device, VPN connection, or
AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network.
Option A is invalid because using a proxy server is not sufficient enough
Option B and D are invalid because you need secure communication which should not traverse the internet For more information on VPC endpoints please see the below link https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-endpoints.htmll
The correct answer is: Access the S3 bucket through a VPC endpoint for S3 Submit your Feedback/Queries to our Experts

NEW QUESTION 201
- (Exam Topic 3)
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 203
- (Exam Topic 3)
A company deployed AWS Organizations to help manage its increasing number of AWS accounts. A security engineer wants to ensure only principals in the Organization structure can access a specic Amazon S3 bucket. The solution must also minimize operational overhead
Which solution will meet these requirements?

A. 1 Put all users into an IAM group with an access policy granting access to the J bucket.
B. Have the account creation trigger an AWS Lambda function that manages the bucket policy, allowing access to accounts listed in the policy only.
C. Add an SCP to the Organizations master account, allowing all principals access to the bucket.
D. Specify the organization ID in the global key condition element of a bucket policy, allowing all principals access.

Answer: D

NEW QUESTION 206
- (Exam Topic 3)
A company hosts data in S3. There is a requirement to control access to the S3 buckets. Which are the 2 ways in which this can be achieved?
Please select:

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

Answer: AC

Explanation:
The AWS Documentation mentions the following
Amazon S3 offers access policy options broadly categorized as resource-based policies and user policies. Access policies you attach to your resources (buckets and objects) are referred to as resource-based policies. For example, bucket policies and access control lists (ACLs) are resource-based policies. You can also attach access policies to users in your account. These are called user policies. You may choose to use resource-based policies, user policies, or some combination of these to manage permissions to your Amazon S3 resources.
Option B and D are invalid because these cannot be used to control access to S3 buckets For more information on S3 access control, please refer to the below
Link: https://docs.aws.amazon.com/AmazonS3/latest/dev/s3-access-control.htmll
The correct answers are: Use Bucket policies. Use IAM user policies Submit your Feedback/Queries to our Experts

NEW QUESTION 210
- (Exam Topic 3)
Your company has been using AWS for the past 2 years. They have separate S3 buckets for logging the various AWS services that have been used. They have hired an external vendor for analyzing their log files. They have their own AWS account. What is the best way to ensure that the partner account can access the log files in the company account for analysis. Choose 2 answers from the options given below
Please select:

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

Answer: BD

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

NEW QUESTION 212

- (Exam Topic 3)
A company's application team needs to host a MySQL database on AWS. According to the company's security policy, all data that is stored on AWS must be encrypted at rest. In addition, all cryptographic material must be compliant with FIPS 140-2 Level 3 validation.
The application team needs a solution that satisfies the company's security requirements and minimizes operational overhead.
Which solution will meet these requirements?

A. Host the database on Amazon RD
B. Use Amazon Elastic Block Store (Amazon EBS) for encryption.Use an AWS Key Management Service (AWS KMS) custom key store that is backed by AWS CloudHSM for key management.
C. Host the database on Amazon RD
D. Use Amazon Elastic Block Store (Amazon EBS) for encryption.Use an AWS managed CMK in AWS Key Management Service (AWS KMS) for key management.
E. Host the database on an Amazon EC2 instanc
F. Use Amazon Elastic Block Store (Amazon EBS) for encryptio
G. Use a customer managed CMK in AWS Key Management Service (AWS KMS) for key management.
H. Host the database on an Amazon EC2 instanc
I. Use Transparent Data Encryption (TDE) for encryption and key management.

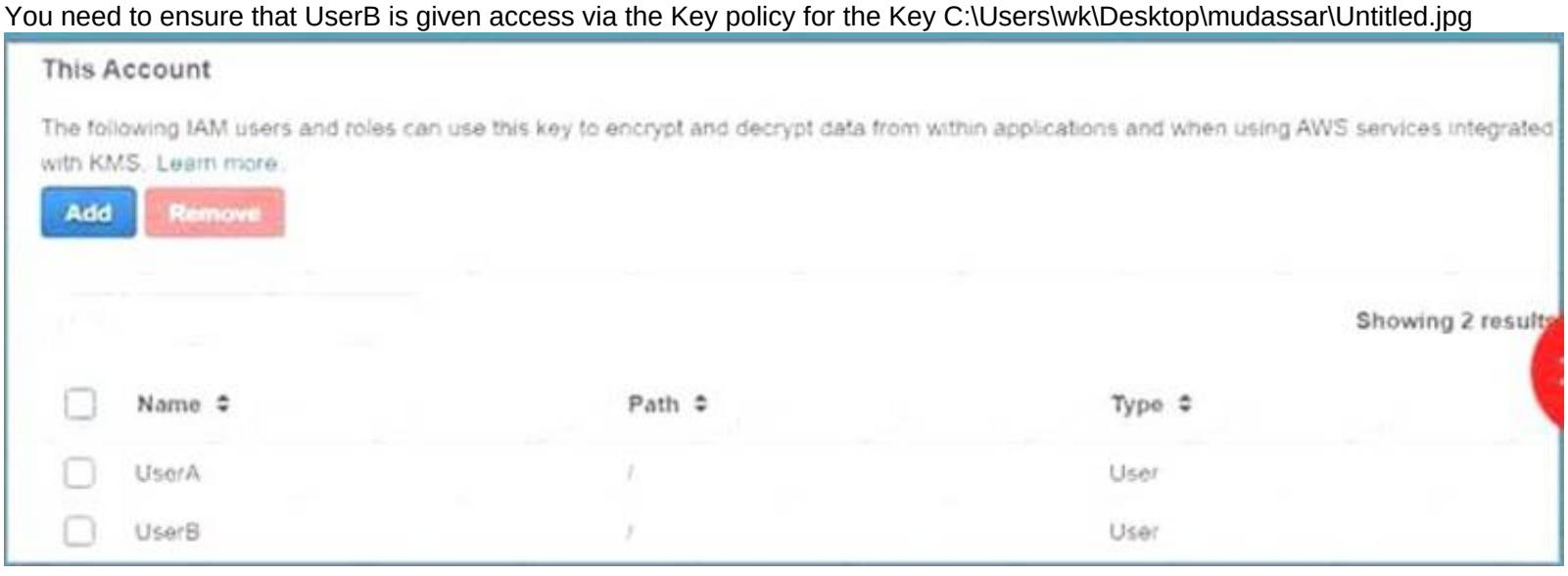
Answer: B

NEW QUESTION 216
- (Exam Topic 3)
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



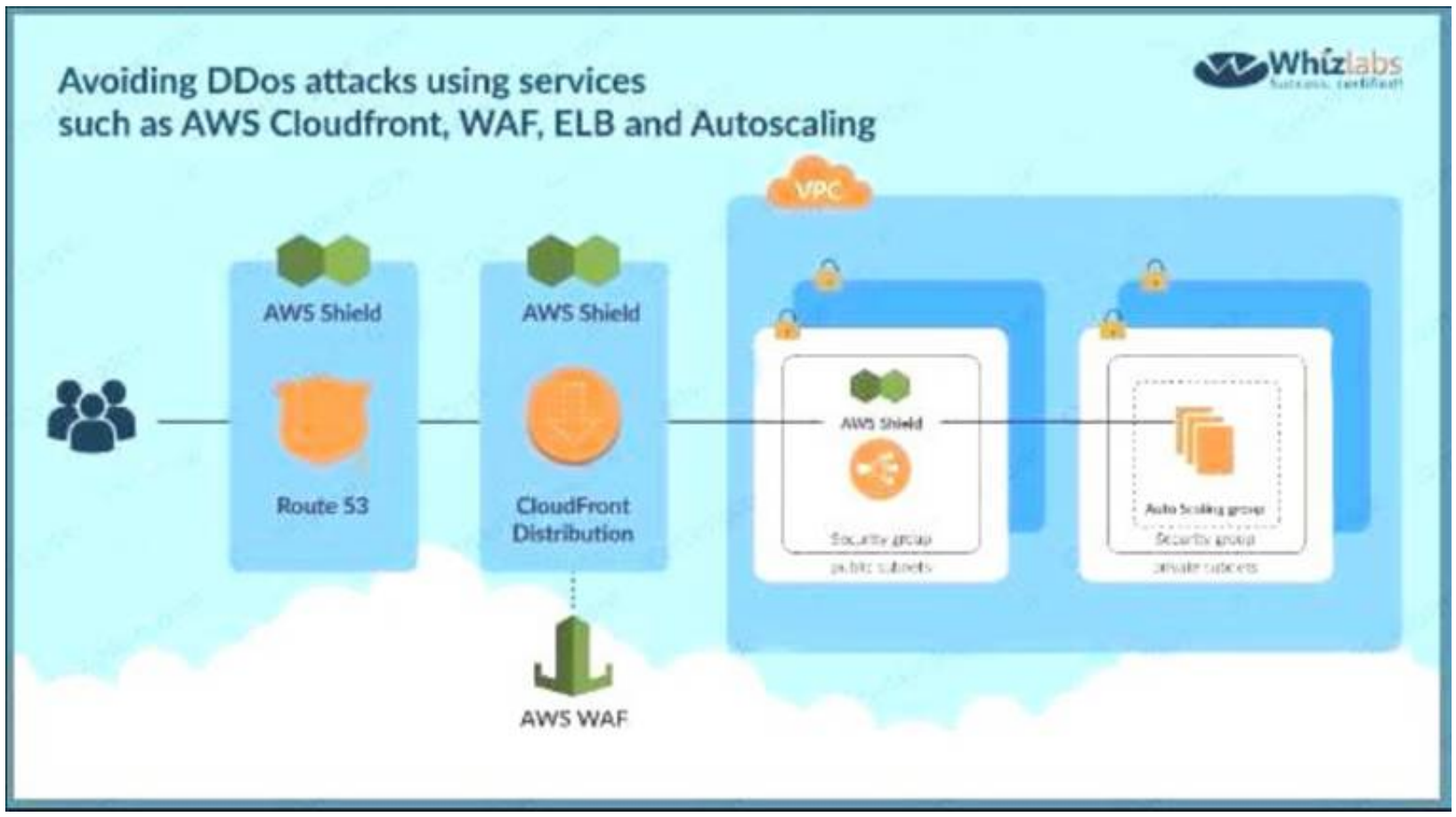
Option is invalid because you don't assign roles to IAM users
For more information on Key policies please visit the below Link: https://docs.aws.amazon.com/kms/latest/developerguide/key-poli
The correct answer is: Ensure that UserB is given the right permissions in the Key policy

NEW QUESTION 218
- (Exam Topic 3)
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 layer traffic.
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 221
- (Exam Topic 3)
Your IT Security team has identified a number of vulnerabilities across critical EC2 Instances in the company's AWS Account. Which would be the easiest way to ensure these vulnerabilities are remediated?
Please select:

A. Create AWS Lambda functions to download the updates and patch the servers.
B. Use AWS CLI commands to download the updates and patch the servers.
C. Use AWS inspector to patch the servers
D. Use AWS Systems Manager to patch the servers

Answer: D

Explanation:
The AWS Documentation mentions the following
You can quickly remediate patch and association compliance issues by using Systems Manager Run Command. You can tat either instance IDs or Amazon EC2 tags and execute the AWS-RefreshAssociation document or the AWS-RunPatchBaseline document. If refreshing the association or re-running the patch baseline fails to resolve the compliance issue, then you need to investigate your associations, patch baselines, or instance configurations to understand why the Run Command executions did not resolve the problem
Options A and B are invalid because even though this is possible, still from a maintenance perspective it would be difficult to maintain the Lambda functions
Option C is invalid because this service cannot be used to patch servers
For more information on using Systems Manager for compliance remediation please visit the below Link: https://docs.aws.amazon.com/systems-manaeer/latest/usereuide/sysman-compliance-fixing.html
The correct answer is: Use AWS Systems Manager to patch the servers Submit your Feedback/Queries to our Experts

NEW QUESTION 226
- (Exam Topic 3)
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. IAM 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 IAM User Guide.

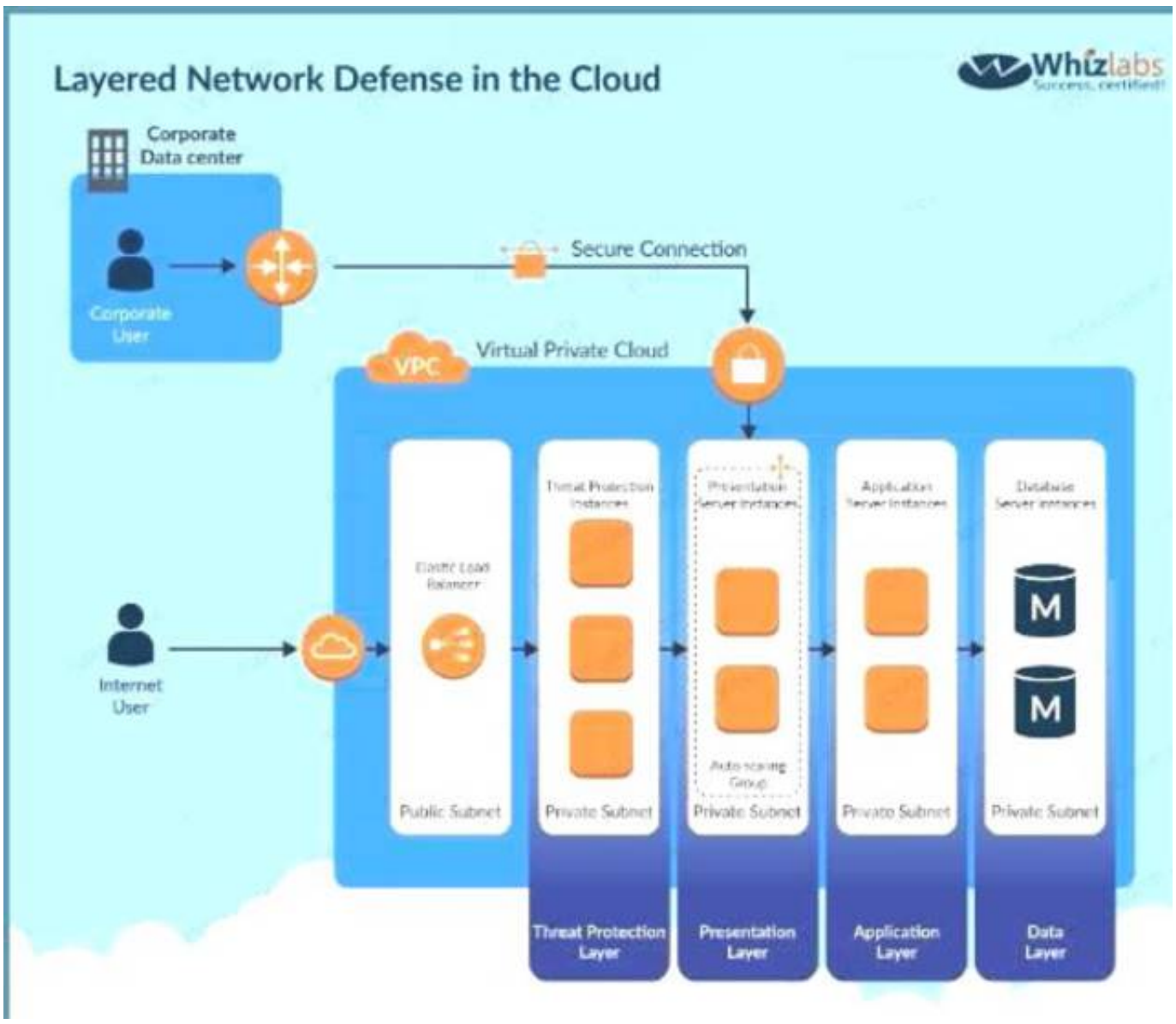
C:\Users\wk\Desktop\mudassar\Untitled.jpg
Option B is invalid because just enabling bucket versioning will not guarantee replication of objects Option D is invalid because the condition for the bucket policy needs to be set accordingly For more information on example bucket policies, please visit the 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 230
- (Exam Topic 3)
Your company has a set of EC2 Instances defined in AWS. They need to ensure that all traffic packets are monitored and inspected for any security threats. How can this be achieved? Choose 2 answers from the options given below
Please select:

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

Answer: AB

Explanation:
If you want to inspect the packets themselves, then you need to use custom based software A diagram representation of this is given in the AWS Security best practices C:\Users\wk\Desktop\mudassar\Untitled.jpg



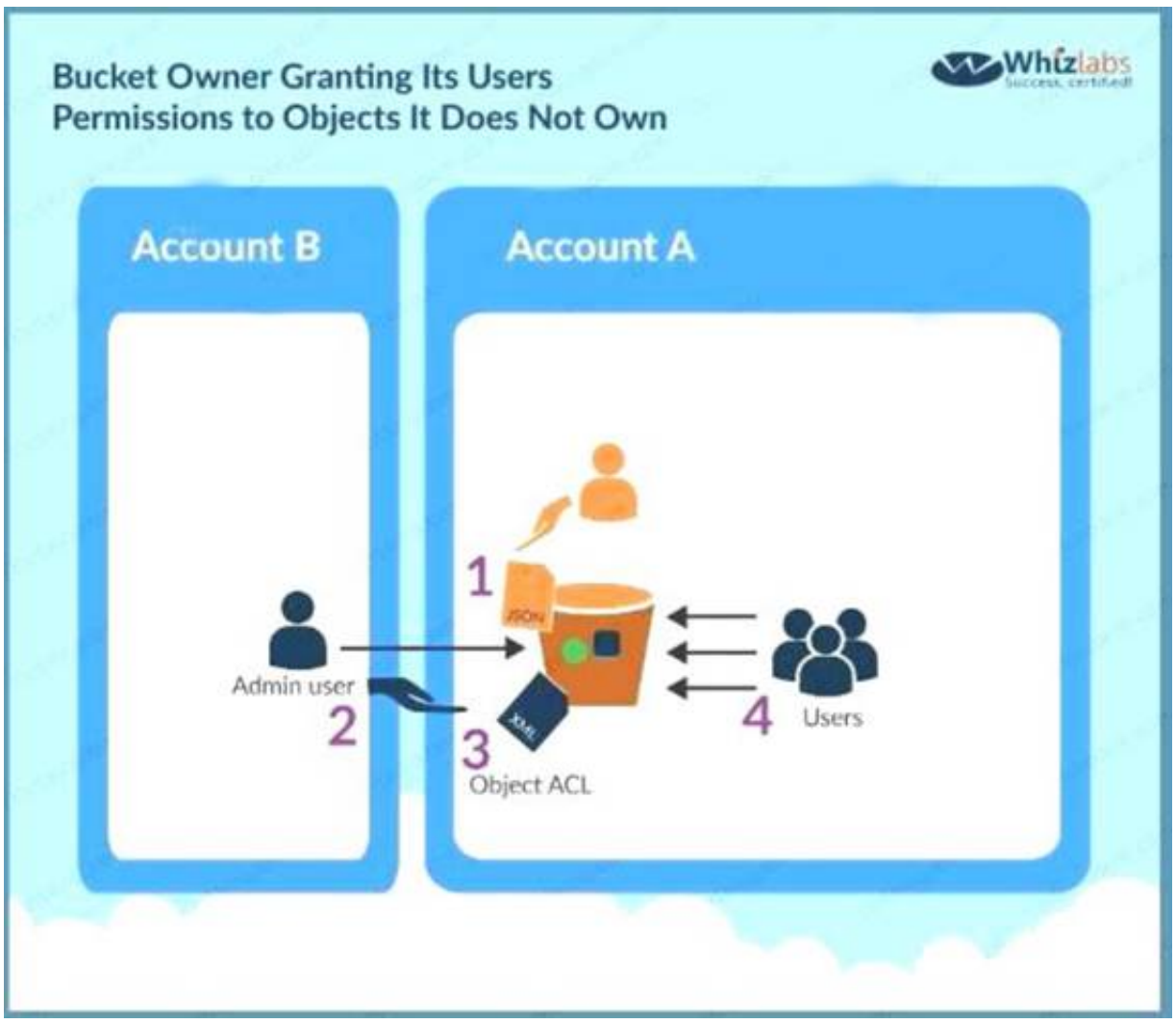
Option C is invalid because VPC Flow logs cannot conduct packet inspection.
For more information on AWS Security best practices, please refer to below URL:
The correct answers are: Use a host based intrusion detection system. Use a third party firewall installed on a central EC2
Submit your Feedback/Queries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

NEW QUESTION 234
- (Exam Topic 3)
A company has external vendors that must deliver files to the company. These vendors have cross-account that gives them permission to upload objects to one of the company's S3 buckets.
What combination of steps must the vendor follow to successfully deliver a file to the company? Select 2 answers from the options given below
Please select:

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

Answer: BE

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



Option A and D are invalid because bucket ACL's are used to give grants to bucket Option C is not required since encryption is not part of the requirement For more information on this scenario please see the below Link:
https://docs.aws.amazon.com/AmazonS3/latest/dev/example-walkthroushs-manaeing-access-example3.htmll The correct answers are: Add a grant to the objects ACL giving full permissions to bucket owner., Upload the
file to the company's S3 bucket
Submit your Feedback/Queries to our Experts

NEW QUESTION 239
- (Exam Topic 3)
Your company has an external web site. This web site needs to access the objects in an S3 bucket. Which of the following would allow the web site to access the objects in the most secure manner?
Please select:

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

Answer: B

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

```
{
 "Version":"2012-10-17",
 "Id":"http referer policy example",
 "Statement":[
  {
   "Sid":"Allow get requests originating from www.example.com and example.com.",
   "Effect":"Allow",
   "Principal":"*",
   "Action":"s3:GetObject",
   "Resource":"arn:aws:s3:::examplebucket/*",
   "Condition":{
    "StringLike":{"aws:Referer":["http://www.example.com/*","http://example.com/*"]}
   }
  }
 ]
}
```

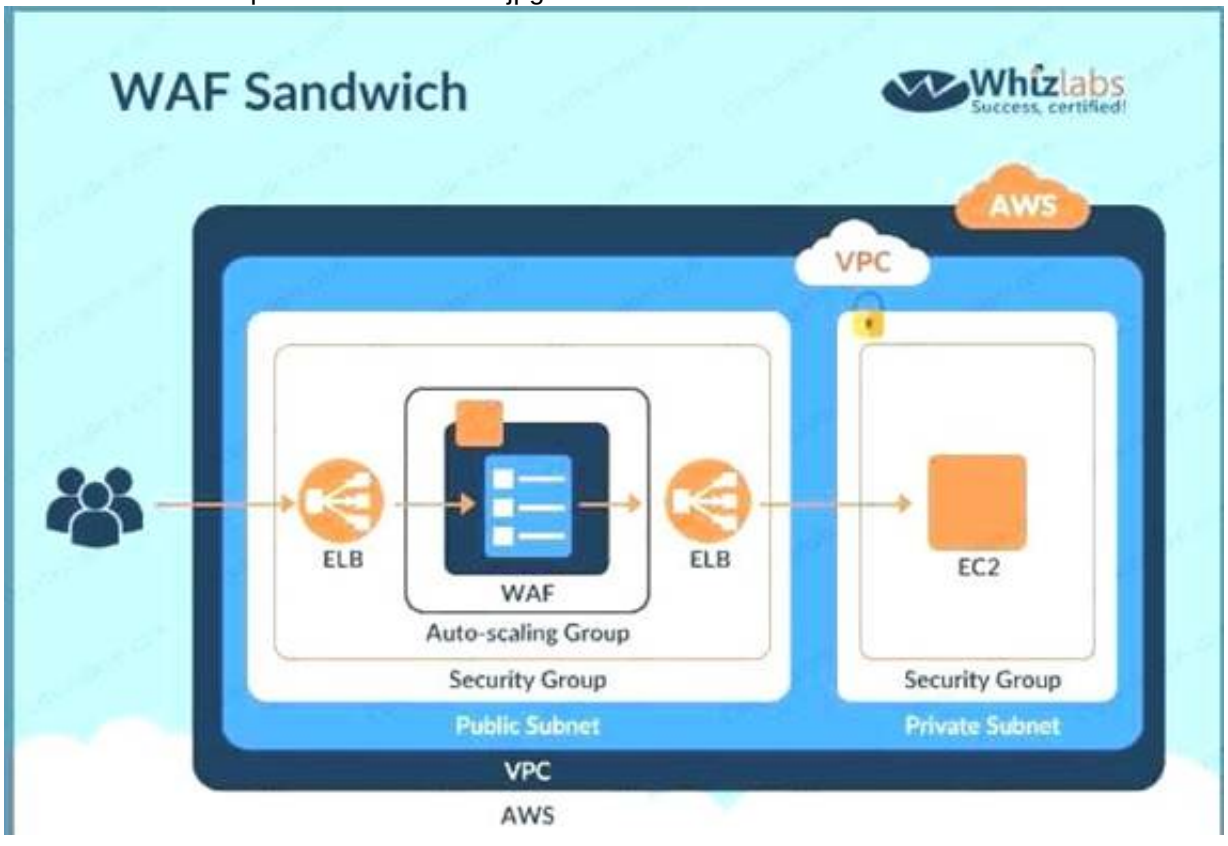
Option A is invalid because giving public access is not a secure way to provide access Option C is invalid because aws:sites is not a valid condition key Option D is invalid because IAM roles will not be assigned to web sites
For more information on example bucket policies please visit the below Link: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

NEW QUESTION 243
- (Exam Topic 3)
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 244
- (Exam Topic 3)
A company plans to create individual child accounts within an existing organization in AWS Organizations for each of its DevOps teams. AWS CloudTrail has been enabled and configured on all accounts to write audit logs to an Amazon S3 bucket in a centralized AWS account. A security engineer needs to ensure that DevOps team members are unable to modify or disable this configuration.
How can the security engineer meet these requirements?

A. Create an 1AM policy that prohibits changes to the specific CloudTrail trail and apply the policy to the AWS account root user.
B. Create an S3 bucket policy in the specified destination account for the CloudTrail trail that prohibits configuration changes from the AWS account root user in the source account.
C. Create an SCP that prohibits changes to the specific CloudTrail trail and apply the SCP to the appropriate organizational unit or account in Organizations.
D. Create an 1AM policy that prohibits changes to the specific CloudTrail trail and apply the policy to a new 1AM grou
E. Have team members use individual 1AM accounts that are members of the new 1AM group.

Answer: D

NEW QUESTION 248
- (Exam Topic 3)
A company is using AWS Organizations. The company wants to restrict AWS usage to the eu-west-1 Region for all accounts under an OU that is named "development." The solution must persist restrictions to existing and new AWS accounts under the development OU.

A. Include the following SCP on the development OU:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyNonDefaultRegions",
            "Effect": "Deny",
            "NotAction": [
                <Desired Global Services> ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                        "eu-west-1"
                    ]
                },
                "ArnNotLike": {
                    "aws:PrincipalARN": "arn:aws:iam::*:role/ANSExecution"
                }
            }
        }
    ]
}
```

B. Include the following SCP on the development account

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyNonDefaultRegions",
            "Effect": "Deny",
            "NotAction": [
                <Desired Global Services> ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                        "eu-west-1"
                    ]
                },
                "ArnNotLike": {
                    "aws:PrincipalARN": "arn:aws:iam::*:role/AWSExecution"
                }
            }
        }
    ]
}
```

C. Include the following SCP on the development OU

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyNonDefaultRegions",
            "Effect": "Deny",
            "NotAction": [
                <Desired Global Services> ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestedRegion": [
                        "eu-west-1"
                    ]
                },
                "ArnNotLike": {
                    "aws:PrincipalARN": "arn:aws:iam::*:role/AWSExecution"
                }
            }
        }
    ]
}
```

D. Include the following SCP on the development OU

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyNonDefaultRegions",
            "Effect": "Allow",
            "NotAction": [
                <Desired Global Services> ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                        "us-east-1"
                    ]
                },
                "ArnNotLike": {
                    "aws:PrincipalARN": "arn:aws:iam::*:role/AWSExecution"
                }
            }
        }
    ]
}
```

A. Option A
B. Option B
C. Option C
D. Option D

Answer: A

NEW QUESTION 253
- (Exam Topic 3)
A company uses an Amazon S3 bucket to store reports Management has mandated that all new objects stored in this bucket must be encrypted at rest using server-side encryption with a client-specified AWS Key Management Service (AWS KMS) CMK owned by the same account as the S3 bucket. The AWS account number is 111122223333, and the bucket name Is report bucket. The company's security specialist must write the S3 bucket policy to ensure the mandate can be Implemented
Which statement should the security specialist include in the policy?

A.
```
{
    "Effect": "Deny",
    "Principal": "*",
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::reportbucket/*",
    "Condition": {
        "StringEquals": {
            "s3:x-amz-server-side-encryption": "AES256"
        }
    }
}
```

B.
```
{
    "Effect": "Deny",
    "Principal": "*",
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::reportbucket/*",
    "Condition": {
        "StringNotLike": {
            "s3:x-amz-server-side-encryption-aws-kms-key-id": "arn:aws:kms:*:111122223333:key/*"
        }
    }
}
```

C.
```
{
    "Effect": "Deny",
    "Principal": "*",
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::reportbucket/*",
    "Condition": {
        "StringNotLike": {
            "s3:x-amz-server-side-encryption": "aws:kms"
        }
    }
}
```

D.

```
{
    "Effect": "Deny",
    "Principal": "*",
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::reportbucket/*",
    "Condition": {
        "StringNotLikeIfExists": {
            "s3:x-amz-server-side-encryption-aws-kms-key-id": "arn:aws:kms:*:111122223333:key/*"
        }
    }
}
```

Answer: A

NEW QUESTION 256
- (Exam Topic 3)
Your company has an EC2 Instance hosted in AWS. This EC2 Instance hosts an application. Currently this application is experiencing a number of issues. You need to inspect the network packets to see what the type of error that is occurring? Which one of the below steps can help address this issue?
Please select:

A. Use the VPC Flow Logs.
B. Use a network monitoring tool provided by an AWS partner.
C. Use another instanc
D. Setup a port to "promiscuous mode" and sniff the traffic to analyze the packet
E. Use Cloudwatch metric

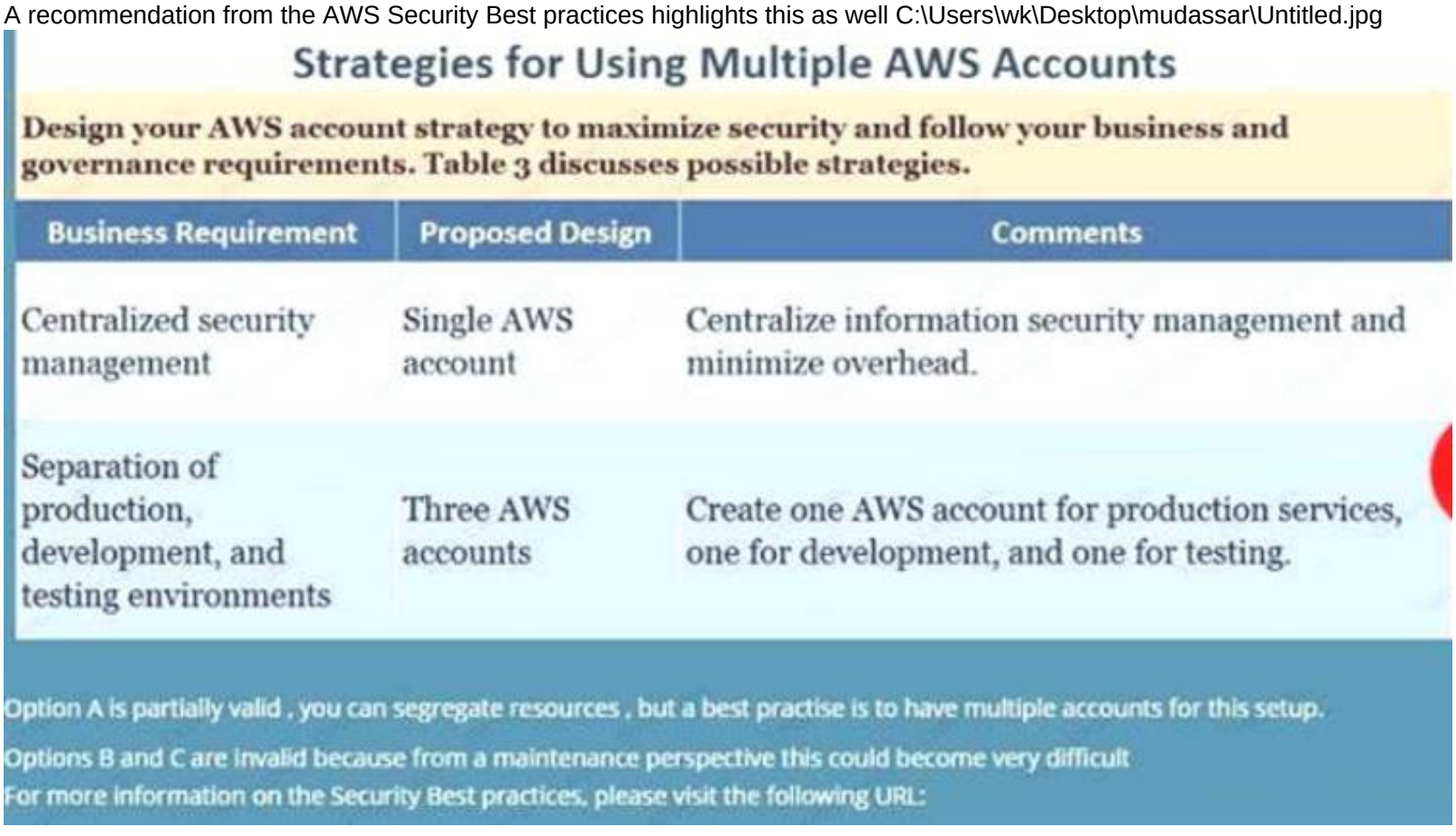
Answer: B

NEW QUESTION 259
- (Exam Topic 3)
A company is planning on using AWS for hosting their applications. They want complete separation and isolation of their production , testing and development environments. Which of the following is an ideal way to design such a setup?
Please select:

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

Answer: D

Explanation:
A recommendation from the AWS Security Best practices highlights this as well 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 261
- (Exam Topic 3)
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 264
- (Exam Topic 3)
A company is undergoing a layer 3 and layer 4 DDoS attack on its web servers running on AWS.
Which combination of AWS services and features will provide protection in this scenario? (Select THREE).

A. Amazon Route 53
B. AWS Certificate Manager (ACM)
C. Amazon S3
D. AWS Shield
E. Elastic Load Balancer
F. Amazon GuardDuty

Answer: DEF

NEW QUESTION 265
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SCS-C01 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SCS-C01 Product From:

https://www.2passeasy.com/dumps/SCS-C01/

Money Back Guarantee

SCS-C01 Practice Exam Features:

* SCS-C01 Questions and Answers Updated Frequently

* SCS-C01 Practice Questions Verified by Expert Senior Certified Staff

* SCS-C01 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SCS-C01 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year