Amazon-Web-Services

Exam Questions SCS-C01

AWS Certified Security- Specialty

NEW QUESTION 1
- (Exam Topic 1)
A company has an AWS account and allows a third-party contractor who uses another AWS account, to assume certain IAM roles. The company wants to ensure that IAM roles can be assumed by the contractor only if the contractor has multi-factor authentication enabled on their IAM user accounts
What should the company do to accomplish this?
A)

```
Add the following condition to the IAM policy attached to all IAM roles.
"Effect" : "Deny",
"Condition" : { "BoolIfExists" : { "aws:MultiFactorAuthPresent" : false } }
```

B)

```
Add the following condition to the IAM policy attached to all IAM roles:
"Effect" : "Deny",
"Condition" : { "Bool" : { "aws:MultiFactorAuthPresent" : false } }
```

C)

```
Add the following condition to the IAM policy attached to all IAM roles
"Effect" : "Allow",
"Condition" : { "Null" : { "aws:MultiFactorAuthPresent" : false } }
```

D)

```
Add the following condition to the IAM policy attached to all IAM roles
"Effect" : "Allow",
"Condition" : { "BoolIfExists" : { "aws:MultiFactorAuthPresent" : false } }
```

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

Answer: A

NEW QUESTION 2
- (Exam Topic 1)
A company has several critical applications running on a large fleet of Amazon EC2 instances. As part of a security operations review, the company needs to apply a critical operating system patch to EC2 instances within 24 hours of the patch becoming available from the operating system vendor. The company does not have a patching solution deployed on AWS, but does have AWS Systems Manager configured. The solution must also minimize administrative overhead.
What should a security engineer recommend to meet these requirements?

A. Create an AWS Config rule defining the patch as a required configuration for EC2 instances.
B. Use the AWS Systems Manager Run Command to patch affected instances.
C. Use an AWS Systems Manager Patch Manager predefined baseline to patch affected instances.
D. Use AWS Systems Manager Session Manager to log in to each affected instance and apply the patch.

Answer: B

NEW QUESTION 3
- (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 4
- (Exam Topic 1)
A company wants to encrypt the private network between its orvpremises environment and AWS. The company also wants a consistent network experience for its employees.
What should the company do to meet these requirements?

A. Establish an AWS Direct Connect connection with AWS and set up a Direct Connect gatewa
B. In the Direct Connect gateway configuration, enable IPsec and BGP, and then leverage native AWS network encryption between Availability Zones and Regions,
C. Establish an AWS Direct Connect connection with AWS and set up a Direct Connect gatewa
D. Using the Direct Connect gateway, create a private virtual interface and advertise the customer gateway private IP addresse
E. Create a VPN connection using the customer gateway and the virtual private gateway
F. Establish a VPN connection with the AWS virtual private cloud over the internet
G. Establish an AWS Direct Connect connection with AWS and establish a public virtual interfac
H. For prefixes that need to be advertised, enter the customer gateway public IP addresse

I. Create a VPN connection over Direct Connect using the customer gateway and the virtual private gateway.

Answer: C

NEW QUESTION 5
- (Exam Topic 1)
A company wants to encrypt data locally while meeting regulatory requirements related to key exhaustion. The encryption key can be no more than 10 days old or encrypt more than 2" 16 objects Any encryption key must be generated on a FIPS-validated hardware security module (HSM). The company is cost-conscious, as plans to upload an average of 100 objects to Amazon S3 each second for sustained operations across 5 data producers
When approach MOST efficiently meets the company's needs?

A. Use the AWS Encryption SDK and set the maximum age to 10 days and the minimum number of messages encrypted to 3" 16. Use AWS Key Management Service (AWS KMS) to generate the master key and data key Use data key caching with the Encryption SDk during the encryption process.
B. Use AWS Key Management Service (AWS KMS) to generate an AWS managed CM
C. Then use Amazon S3 client-side encryption configured to automatically rotate with every object
D. Use AWS CloudHSM to generate the master key and data key
E. Then use Boto 3 and Python to locally encrypt data before uploading the object Rotate the data key every 10 days or after 2" 16 objects have been Uploaded to Amazon 33
F. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3) and set the master key to automatically rotate.

Answer: A

NEW QUESTION 6
- (Exam Topic 1)
A company has hundreds of AWS accounts, and a centralized Amazon S3 bucket used to collect AWS CloudTrail for all of these accounts. A security engineer wants to create a solution that will enable the company to run ad hoc queues against its CloudTrail logs dating back 3 years from when the trails were first enabled in the company's AWS account.
How should the company accomplish this with the least amount of administrative overhead?

A. Run an Amazon EMP cluster that uses a MapReduce job to be examine the CloudTrail trails.
B. Use the events history/feature of the CloudTrail console to query the CloudTrail trails.
C. Write an AWS Lambda function to query the CloudTrail trails Configure the Lambda function to be executed whenever a new file is created in the CloudTrail S3 bucket.
D. Create an Amazon Athena table that tools at the S3 bucket the CloudTrail trails are being written to Use Athena to run queries against the trails.

Answer: D

NEW QUESTION 7
- (Exam Topic 1)
An application running on Amazon EC2 instances generates log files in a folder on a Linux file system. The instances block access to the console and file transfer utilities, such as Secure Copy Protocol (SCP) and Secure File Transfer Protocol (SFTP). The Application Support team wants to automatically monitor the application log files so the team can set up notifications in the future.
A Security Engineer must design a solution that meets the following requirements:
• Make the log files available through an AWS managed service.
• Allow for automatic monitoring of the logs.
• Provide an Interlace for analyzing logs.
• Minimize effort.
Which approach meets these requirements^

A. Modify the application to use the AWS SD
B. Write the application logs lo an Amazon S3 bucket
C. install the unified Amazon CloudWatch agent on the instances Configure the agent to collect the application log dies on the EC2 tile system and send them to Amazon CloudWatch Logs
D. Install AWS Systems Manager Agent on the instances Configure an automation document to copy the application log files to AWS DeepLens
E. Install Amazon Kinesis Agent on the instances Stream the application log files to Amazon Kinesis Data Firehose and sot the destination to Amazon Elasticsearch Service

Answer: D

NEW QUESTION 8
- (Exam Topic 1)
Users report intermittent availability of a web application hosted on AWS. Monitoring systems report an excess of abnormal network traffic followed by high CPU utilization on the application web tier. Which of the following techniques will improve the availability of the application? (Select TWO.)

A. Deploy AWS WAF to block all unsecured web applications from accessing the internet.
B. Deploy an Intrusion Detection/Prevention System (IDS/IPS) to monitor or block unusual incoming network traffic.
C. Configure security groups to allow outgoing network traffic only from hosts that are protected with up-to-date antivirus software.
D. Create Amazon CloudFront distribution and configure AWS WAF rules to protect the web applications from malicious traffic.
E. Use the default Amazon VPC for externakfacing systems to allow AWS to actively block malicious network traffic affecting Amazon EC2 instances.

Answer: BD

NEW QUESTION 9
- (Exam Topic 1)
A website currently runs on Amazon EC2 with mostly static content on the site. Recently, the site was subjected to a ODoS attack, and a Security Engineer was tasked with redesigning the edge security to help mitigate this risk in the future
What are some ways the Engineer could achieve this? (Select THREE)

A. Use AWS X-Ray to inspect the traffic going 10 the EC2 instances
B. Move the state content to Amazon S3 and font this with an Amazon CloudFront distribution
C. Change the security group configuration to block the source of the attack traffic
D. Use AWS WAF security rules to inspect the inbound traffic
E. Use Amazon inspector assessment templates to inspect the inbound traffic
F. Use Amazon Route 53 to distribute traffic

Answer: BDF

NEW QUESTION 10
- (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 10
- (Exam Topic 1)
A Security Engineer launches two Amazon EC2 instances in the same Amazon VPC but in separate Availability Zones. Each instance has a public IP address and is able to connect to external hosts on the internet. The two instances are able to communicate with each other by using their private IP addresses, but they are not able to communicate with each other when using their public IP addresses.
Which action should the Security Engineer take to allow communication over the public IP addresses?

A. Associate the instances to the same security groups.
B. Add 0.0.0.0/0 to the egress rules of the instance security groups.
C. Add the instance IDs to the ingress rules of the instance security groups.
D. Add the public IP addresses to the ingress rules of the instance security groups.

Answer: D

Explanation:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/security-group-rules-reference.html#sg-rules-other-ins

NEW QUESTION 13
- (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 15
- (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 16
- (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 18
- (Exam Topic 1)
A company needs its Amazon Elastic Block Store (Amazon EBS) volumes to be encrypted at all times. During a security incident. EBS snapshots of suspicious instances are shared to a forensics account for analysis A security engineer attempting to share a suspicious EBS snapshot to the forensics account receives the following error
"Unable to share snapshot: An error occurred (OperationNotPermitted) when calling the ModifySnapshotAttribute operation: Encrypted snapshots with EBS default key cannot be shared.
Which combination of steps should the security engineer take in the incident account to complete the sharing operation? (Select THREE)

A. Create a customer managed CMK Copy the EBS snapshot encrypting the destination snapshot using the new CMK.
B. Allow forensics accounting principals to use the CMK by modifying its policy.
C. Create an Amazon EC2 instanc
D. Attach the encrypted and suspicious EBS volum
E. Copy data from the suspicious volume to an unencrypted volum
F. Snapshot the unencrypted volume
G. Copy the EBS snapshot to the new decrypted snapshot
H. Restore a volume from the suspicious EBS snapsho
I. Create an unencrypted EBS volume of the samesize.
J. Share the target EBS snapshot with the forensics account.

Answer: ABF

NEW QUESTION 22
- (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 26
- (Exam Topic 1)
A company plans to use custom AMIs to launch Amazon EC2 instances across multiple AWS accounts in a single Region to perform security monitoring and analytics tasks. The EC2 instances are launched in EC2 Auto Scaling groups. To increase the security of the solution, a Security Engineer will manage the lifecycle of the custom AMIs in a centralized account and will encrypt them with a centrally managed AWS KMS CMK. The Security Engineer configured the KMS key policy to allow cross-account access. However, the EC2 instances are still not being properly launched by the EC2 Auto Scaling groups.
Which combination of configuration steps should the Security Engineer take to ensure the EC2 Auto Scaling groups have been granted the proper permissions to execute tasks?

A. Create a customer-managed CMK in the centralized accoun
B. Allow other applicable accounts to use that key for cryptographical operations by applying proper cross-account permissions in the key policy.Create an IAM role in all applicable accounts and configure its access policy to allow the use of the centrally managed CMK for cryptographical operation
C. Configure EC2 Auto Scaling groups within each applicable account to use the created IAM role to launch EC2 instances.
D. Create a customer-managed CMK in the centralized accoun
E. Allow other applicable accounts to use that key for cryptographical operations by applying proper cross-account permissions in the key polic
F. Create an IAM role in all applicable accounts and configure its access policy with permissions to create grants for the centrally managed CM
G. Use this IAM role to create a grant for the centrally managed CMK with permissions to perform cryptographical operations and with the EC2 Auto Scalingservice-linked role defined as the grantee principal.
H. Create a customer-managed CMK or an AWS managed CMK in the centralized accoun
I. Allow other applicable accounts to use that key for cryptographical operations by applying proper cross-account permissions in the key polic
J. Use the CMK administrator to create a CMK grant that includes permissions to perform cryptographical operations that define EC2 Auto Scaling service-linked roles from all other accounts as the grantee principal.
K. Create a customer-managed CMK or an AWS managed CMK in the centralized accoun
L. Allow other applicable accounts to use that key for cryptographical operations by applying proper cross-account permissions in the key polic
M. Modify the access policy for the EC2 Auto Scaling roles to perform cryptographical operations against the centrally managed CMK.

Answer: B

NEW QUESTION 27
- (Exam Topic 1)
The Development team receives an error message each time the team members attempt to encrypt or decrypt a Secure String parameter from the SSM Parameter Store by using an AWS KMS customer managed key (CMK).
Which CMK-related issues could be responsible? (Choose two.)

A. The CMK specified in the application does not exist.
B. The CMK specified in the application is currently in use.
C. The CMK specified in the application is using the CMK KeyID instead of CMK Amazon Resource Name.
D. The CMK specified in the application is not enabled.
E. The CMK specified in the application is using an alias.

Answer: AD

Explanation:
https://docs.amazonaws.cn/en_us/kms/latest/developerguide/services-parameter-store.html

NEW QUESTION 31
- (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 36

- (Exam Topic 1)
A security engineer is asked to update an AW3 CoudTrail log file prefix for an existing trail. When attempting to save the change in the CloudTrail console, the security engineer receives the following error message. "There is a problem with the bucket policy''
What will enable the security engineer to saw the change?

A. Create a new trail with the updated log file prefix, and then delete the original nail Update the existing bucket policy in the Amazon S3 console with the new log the prefix, and then update the log file prefix in the CloudTrail console
B. Update the existing bucket policy in the Amazon S3 console to allow the security engineers principal to perform PutBucketPolic
C. and then update the log file prefix in the CloudTrail console
D. Update the existing bucket policy in the Amazon S3 console with the new log file prefix, and then update the log file prefix in the CloudTrail console.
E. Update the existing bucket policy in the Amazon S3 console to allow the security engineers principal to perform GetBucketPolicy, and then update the log file prefix in the CloudTrail console

Answer: B

NEW QUESTION 37
- (Exam Topic 1)
A recent security audit identified that a company's application team injects database credentials into the environment variables of an AWS Fargate task. The company's security policy mandates that all sensitive data be encrypted at rest and in transit.
When combination of actions should the security team take to make the application compliant within the security policy? (Select THREE)

A. Store the credentials securely in a file in an Amazon S3 bucket with restricted access to the application team IAM role Ask the application team to read the credentials from the S3 object instead
B. Create an AWS Secrets Manager secret and specify the key/value pairs to be stored in this secret
C. Modify the application to pull credentials from the AWS Secrets Manager secret instead of the environment variables.
D. Add the following statement to the container instance IAM role policy

```
{
    "Effect": "Allow",
    "Action": [
        "ssm:GetParameters",
        "secretsmanager:GetSecretValue",
        "kms:Decrypt"
    ],
    "Resource": [
        "arn:aws:secretsmanager:<region>:<aws_account_id>:secret:secret_name",
        "arn:aws:kms:<region>:<aws_account_id>:key/key_id"
    ]
}
```

E. Add the following statement to the execution role policy.

```
{
    "Effect": "Allow",
    "Action": [
        "ssm:GetParameters",
        "secretsmanager:GetSecretValue",
        "kms:Decrypt"
    ],
    "Resource": [
        "arn:aws:secretsmanager:<region>:<aws_account_id>:secret:secret_name",
        "arn:aws:kms:<region>:<aws_account_id>:key/key_id"
    ]
}
```

F. Log in to the AWS Fargate instance, create a script to read the secret value from AWS Secret Manager, and inject the environment variable
G. Ask the application team to redeploy the application.

Answer: BEF

NEW QUESTION 39
- (Exam Topic 1)
A Security Engineer for a large company is managing a data processing application used by 1,500 subsidiary companies. The parent and subsidiary companies all use AWS. The application uses TCP port 443 and runs on Amazon EC2 behind a Network Load Balancer (NLB). For compliance reasons, the application should only be accessible to the subsidiaries and should not be available on the public internet. To meet the compliance requirements for restricted access, the Engineer has received the public and private CIDR block ranges for each subsidiary
What solution should the Engineer use to implement the appropriate access restrictions for the application?

A. Create a NACL to allow access on TCP port 443 from the 1;500 subsidiary CIDR block ranges.Associate the NACL to both the NLB and EC2 instances
B. Create an AWS security group to allow access on TCP port 443 from the 1,500 subsidiary CIDR block range
C. Associate the security group to the NL
D. Create a second security group for EC2 instances with access on TCP port 443 from the NLB security group.
E. Create an AWS PrivateLink endpoint service in the parent company account attached to the NL
F. Create an AWS security group for the instances to allow access on TCP port 443 from the AWS PrivateLink endpoin
G. Use AWS PrivateLink interface endpoints in the 1,500 subsidiary AWS accounts to connect to the data processing application.
H. Create an AWS security group to allow access on TCP port 443 from the 1,500 subsidiary CIDR block range
I. Associate the security group with EC2 instances.

Answer: D

NEW QUESTION 44
- (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 graphicaI operations.

Answer: AD

NEW QUESTION 45
- (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 50
- (Exam Topic 1)
A company has recently recovered from a security incident that required the restoration of Amazon EC2 instances from snapshots.
After performing a gap analysis of its disaster recovery procedures and backup strategies, the company is concerned that, next time, it will not be able to recover the EC2 instances if the AWS account was compromised and Amazon EBS snapshots were deleted.
All EBS snapshots are encrypted using an AWS KMS CMK. Which solution would solve this problem?

A. Create a new Amazon S3 bucket Use EBS lifecycle policies to move EBS snapshots to the new S3 bucke
B. Move snapshots to Amazon S3 Glacier using lifecycle policies, and apply Glacier Vault Lock policies to prevent deletion
C. Use AWS Systems Manager to distribute a configuration that performs local backups of all attached disks to Amazon S3.
D. Create a new AWS account with limited privilege
E. Allow the new account to access the AWS KMS key used to encrypt the EBS snapshots, and copy the encrypted snapshots to the new account on a recuning basis
F. Use AWS Backup to copy EBS snapshots to Amazon S3.

Answer: A

NEW QUESTION 51
- (Exam Topic 1)
A Security Engineer has several thousand Amazon EC2 instances split across production and development environments. Each instance is tagged with its environment. The Engineer needs to analyze and patch all the development EC2 instances to ensure they are not currently exposed to any common vulnerabilities or exposures (CVEs)
Which combination of steps is the MOST efficient way for the Engineer to meet these requirements? (Select TWO.)

A. Log on to each EC2 instance, check and export the different software versions installed, and verify this against a list of current CVEs.
B. Install the Amazon Inspector agent on all development instances Build a custom rule package, and configure Inspector to perform a scan using this custom rule on all instances tagged as being in the development environment.
C. Install the Amazon Inspector agent on all development instances Configure Inspector to perform a scan using the CVE rule package on all instances tagged as being in the development environment.
D. Install the Amazon EC2 System Manager agent on all development instances Issue the Run command to EC2 System Manager to update all instances
E. Use AWS Trusted Advisor to check that all EC2 instances have been patched to the most recent versionof operating system and installed software.

Answer: CD

NEW QUESTION 56
- (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 61
- (Exam Topic 1)
An employee accidentally exposed an AWS access key and secret access key during a public presentation. The company Security Engineer immediately disabled the key.
How can the Engineer assess the impact of the key exposure and ensure that the credentials were not misused? (Choose two.)

A. Analyze AWS CloudTrail for activity.
B. Analyze Amazon CloudWatch Logs for activity.
C. Download and analyze the IAM Use report from AWS Trusted Advisor.
D. Analyze the resource inventory in AWS Config for IAM user activity.
E. Download and analyze a credential report from IAM.

Answer: AD

Explanation:
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_getting-report.html

NEW QUESTION 62
- (Exam Topic 1)
A company's application runs on Amazon EC2 and stores data in an Amazon S3 bucket The company wants additional security controls in place to limit the likelihood of accidental exposure of data to external parties
Which combination of actions will meet this requirement? (Select THREE.)

A. Encrypt the data in Amazon S3 using server-side encryption with Amazon S3 managed encryption keys (SSE-S3)
B. Encrypt the data in Amazon S3 using server-side encryption with AWS KMS managed encryption keys (SSE-KMS)
C. Create a new Amazon S3 VPC endpoint and modify the VPC's routing tables to use the new endpoint
D. Use the Amazon S3 Block Public Access feature.
E. Configure the bucket policy to allow access from the application instances only
F. Use a NACL to filter traffic to Amazon S3

Answer: BCE

NEW QUESTION 64
- (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 67
- (Exam Topic 1)
A company has implemented centralized logging and monitoring of AWS CloudTrail logs from all Regions in
an Amazon S3 bucket. The log Hies are encrypted using AWS KMS. A Security Engineer is attempting to review the log files using a third-party tool hosted on an Amazon EC2 instance The Security Engineer is unable to access the logs in the S3 bucket and receives an access denied error message
What should the Security Engineer do to fix this issue?

A. Check that the role the Security Engineer uses grants permission to decrypt objects using the KMS CMK.
B. Check that the role the Security Engineer uses grants permission to decrypt objects using the KMS CMK and gives access to the S3 bucket and objects
C. Check that the role the EC2 instance profile uses grants permission lo decrypt objects using the KMS CMK and gives access to the S3 bucket and objects
D. Check that the role the EC2 instance profile uses grants permission to decrypt objects using the KMS CMK

Answer: C

NEW QUESTION 70
- (Exam Topic 1)
A company is using AWS Organizations to manage multiple AWS accounts. The company has an application that allows users to assume the AppUser IAM role to download files from an Amazon S3 bucket that is encrypted with an AWS KMS CMK However when users try to access the files in the S3 bucket they get an access denied error.
What should a Security Engineer do to troubleshoot this error? (Select THREE)

A. Ensure the KMS policy allows the AppUser role to have permission to decrypt for the CMK
B. Ensure the S3 bucket policy allows the AppUser role to have permission to get objects for the S3 bucket
C. Ensure the CMK was created before the S3 bucket.
D. Ensure the S3 block public access feature is enabled for the S3 bucket.
E. Ensure that automatic key rotation is disabled for the CMK
F. Ensure the SCPs within Organizations allow access to the S3 bucket.

Answer: ABF

NEW QUESTION 75
- (Exam Topic 1)
While securing the connection between a company's VPC and its on-premises data center, a Security Engineer sent a ping command from an on-premises host (IP address 203.0.113.12) to an Amazon EC2 instance (IP address 172.31.16.139). The ping command did not return a response. The flow log in the VPC showed the following:
2 123456789010 eni-1235b8ca 203.0.113.12 172.31.16.139 0 0 1 4 336 1432917027 1432917142 ACCEPT OK
2 123456789010 eni-1235b8ca 172.31.16.139 203.0.113.12 0 0 1 4 336 1432917094 1432917142 REJECT OK
What action should be performed to allow the ping to work?

A. In the security group of the EC2 instance, allow inbound ICMP traffic.
B. In the security group of the EC2 instance, allow outbound ICMP traffic.
C. In the VPC's NACL, allow inbound ICMP traffic.
D. In the VPC's NACL, allow outbound ICMP traffic.

Answer: D

NEW QUESTION 80
- (Exam Topic 1)
A company hosts its public website on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances are in an EC2 Auto Scaling group across multiple Availability Zones. The website is under a DDoS attack by a specific IoT device brand that is visible in the user agent A security engineer needs to mitigate the attack without impacting the availability of the public website.
What should the security engineer do to accomplish this?

A. Configure a web ACL rule for AWS WAF to block requests with a string match condition for the user agent of the IoT device
B. Associate the v/eb ACL with the ALB.
C. Configure an Amazon CloudFront distribution to use the ALB as an origi
D. Configure a web ACL rule for AWS WAF to block requests with a string match condition for the user agent of the IoT device
E. Associate the web ACL with the ALB Change the public DNS entry of the website to point to the CloudFront distribution.
F. Configure an Amazon CloudFront distribution to use a new ALB as an origi
G. Configure a web ACL rule for AWS WAF to block requests with a string match condition for the user agent of the IoT device
H. Change the ALB security group to alow access from CloudFront IP address ranges only Change the public DNS entry of the website to point to the CloudFront distribution.
I. Activate AWS Shield Advanced to enable DDoS protectio
J. Apply an AWS WAF ACL to the AL
K. and configure a listener rule on the ALB to block IoT devices based on the user agent.

Answer: D

NEW QUESTION 83
- (Exam Topic 1)
A Security Engineer creates an Amazon S3 bucket policy that denies access to all users. A few days later, the Security Engineer adds an additional statement to the bucket policy to allow read-only access to one other employee Even after updating the policy the employee still receives an access denied message.
What is the likely cause of this access denial?

A. The ACL in the bucket needs to be updated.
B. The IAM policy does not allow the user to access the bucket
C. It takes a few minutes for a bucket policy to take effect
D. The allow permission is being overridden by the deny.

Answer: D

NEW QUESTION 87
- (Exam Topic 1)
A security engineer has noticed an unusually high amount of traffic coming from a single IP address. This was discovered by analyzing the Application Load Balancer's access logs. How can the security engineer limit the number of requests from a specific IP address without blocking the IP address?

A. Add a rule to the Application Load Balancer to route the traffic originating from the IP address in question and show a static webpage.
B. Implement a rate-based rule with AWS WAF
C. Use AWS Shield to limit the originating traffic hit rate.
D. Implement the GeoLocation feature in Amazon Route 53.

Answer: C

NEW QUESTION 89
- (Exam Topic 1)
A security engineer must use AWS Key Management Service (AWS KMS) to design a key management solution for a set of Amazon Elastic Block Store (Amazon EBS) volumes that contain sensitive data. The solution needs to ensure that the key material automatically expires in 90 days.
Which solution meets these criteria?

A. A customer managed CMK that uses customer provided key material
B. A customer managed CMK that uses AWS provided key material
C. An AWS managed CMK
D. Operating system-native encryption that uses GnuPG

Answer: B

NEW QUESTION 90
- (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 95
- (Exam Topic 1)
A Security Engineer is troubleshooting a connectivity issue between a web server that is writing log files to the logging server in another VPC. The Engineer has confirmed that a peering relationship exists between the two VPCs. VPC flow logs show that requests sent from the web server are accepted by the togging server but the web server never receives a reply
Which of the following actions could fix this issue1?

A. Add an inbound rule to the security group associated with the logging server that allows requests from the web server
B. Add an outbound rule to the security group associated with the web server that allows requests to the logging server.
C. Add a route to the route table associated with the subnet that hosts the logging server that targets the peering connection
D. Add a route to the route table associated with the subnet that hosts the web server that targets the peering connection

Answer: C

NEW QUESTION 96
- (Exam Topic 1)
A Security Engineer has discovered that, although encryption was enabled on the Amazon S3 bucket example bucket, anyone who has access to the bucket has the ability to retrieve the files. The Engineer wants to limit access to each IAM user can access an assigned folder only.
What should the Security Engineer do to achieve this?

A. Use envelope encryption with the AWS-managed CMK aws/s3.
B. Create a customer-managed CMK with a key policy granting "kms:Decrypt" based on the "${aws:username}" variable.
C. Create a customer-managed CMK for each use
D. Add each user as a key user in their corresponding key policy.
E. Change the applicable IAM policy to grant S3 access to "Resource": "arn:aws:s3:::examplebucket/${aws:username}/*"

Answer: B

Explanation:
Reference: https://aws.amazon.com/premiumsupport/knowledge-center/iam-s3-user-specific-folder/

NEW QUESTION 100
- (Exam Topic 1)
A company has a website with an Amazon CloudFront HTTPS distribution, an Application Load Balancer (ALB) with multiple web instances for dynamic website content, and an Amazon S3 bucket for static website content. The company's security engineer recently updated the website security requirements:
• HTTPS needs to be enforced for all data in transit with specific ciphers.
• The CloudFront distribution needs to be accessible from the internet only. Which solution will meet these requirements?

A. Set up an S3 bucket policy with the awssecuretransport key Configure the CloudFront origin access identity (OAI) with the S3 bucket Configure CloudFront to use specific cipher
B. Enforce the ALB with an HTTPS listener only and select the appropriate security policy for the ciphers Link the ALB with AWS WAF to allow access from the CloudFront IP ranges.
C. Set up an S3 bucket policy with the aws:securetransport ke
D. Configure the CloudFront origin access identity (OAI) with the S3 bucke
E. Enforce the ALB with an HTTPS listener only and select the appropriate security policy for the ciphers.
F. Modify the CloudFront distribution to use AWS WA
G. Force HTTPS on the S3 bucket with specific ciphers in the bucket polic
H. Configure an HTTPS listener only for the AL
I. Set up a security group to limit access to the ALB from the CloudFront IP ranges
J. Modify the CloudFront distribution to use the ALB as the origi
K. Enforce an HTTPS listener on the AL
L. Create a path-based routing rule on the ALB with proxies that connect lo Amazon S3. Create a bucket policy to allow access from these proxies only.A company Is trying to replace its on-premises bastion hosts used to access on-premises Linux servers with AWS Systems Manager Session Manage
M. A security engineer has installed the Systems Manager Agent on all server
N. The security engineer verifies that the agent is running on all the servers, but Session Manager cannot connect to the
O. The security engineer needs to perform verification steps before Session Manager will work on the servers.Which combination of steps should the security engineer perform? (Select THREE.)
P. Open inbound port 22 to 0 0.0.0/0 on all Linux servers.
Q. Enable the advanced-instances tier in Systems Manager.
R. Create a managed-instance activation for the on-premises servers.
S. Reconfigure the Systems Manager Agent with the activation code and ID.
T. Assign an IAM role to all of the on-premises servers.
. Initiate an inventory collection with Systems Manager on the on-premises servers

Answer: CEF

NEW QUESTION 101
- (Exam Topic 1)
A company hosts a web-based application that captures and stores sensitive data in an Amazon DynamoDB table. A security audit reveals that the application does not provide end-to-end data protection or the ability to detect unauthorized data changes The software engineering team needs to make changes that will address the audit findings.
Which set of steps should the software engineering team take?

A. Use an AWS Key Management Service (AWS KMS) CM
B. Encrypt the data at rest.
C. Use AWS Certificate Manager (ACM) Private Certificate Authority Encrypt the data in transit.
D. Use a DynamoDB encryption clien
E. Use client-side encryption and sign the table items
F. Use the AWS Encryption SD
G. Use client-side encryption and sign the table items.

Answer: A

NEW QUESTION 103
- (Exam Topic 2)
A company hosts a popular web application that connects to an Amazon RDS MySQL DB instance running in a private VPC subnet that was created with default ACL settings. The IT Security department has a suspicion that a DDos attack is coming from a suspecting IP. How can you protect the subnets from this attack?
Please select:

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

Answer: C

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

NEW QUESTION 108
- (Exam Topic 2)
A Security Engineer who was reviewing AWS Key Management Service (AWS KMS) key policies found this statement in each key policy in the company AWS account.

```
{
    "Sid": "Enable IAM User Permissions",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
    },
    "Action": "kms:*",
    "Resource": "*"
}
```

What does the statement allow?

A. All principals from all AWS accounts to use the key.
B. Only the root user from account 111122223333 to use the key.
C. All principals from account 111122223333 to use the key but only on Amazon S3.
D. Only principals from account 111122223333 that have an IAM policy applied that grants access to this key to use the key.

Answer: D

NEW QUESTION 109
- (Exam Topic 2)
Your development team has started using AWS resources for development purposes. The AWS account has just been created. Your IT Security team is worried about possible leakage of AWS keys. What is the first level of measure that should be taken to protect the AWS account.
Please select:

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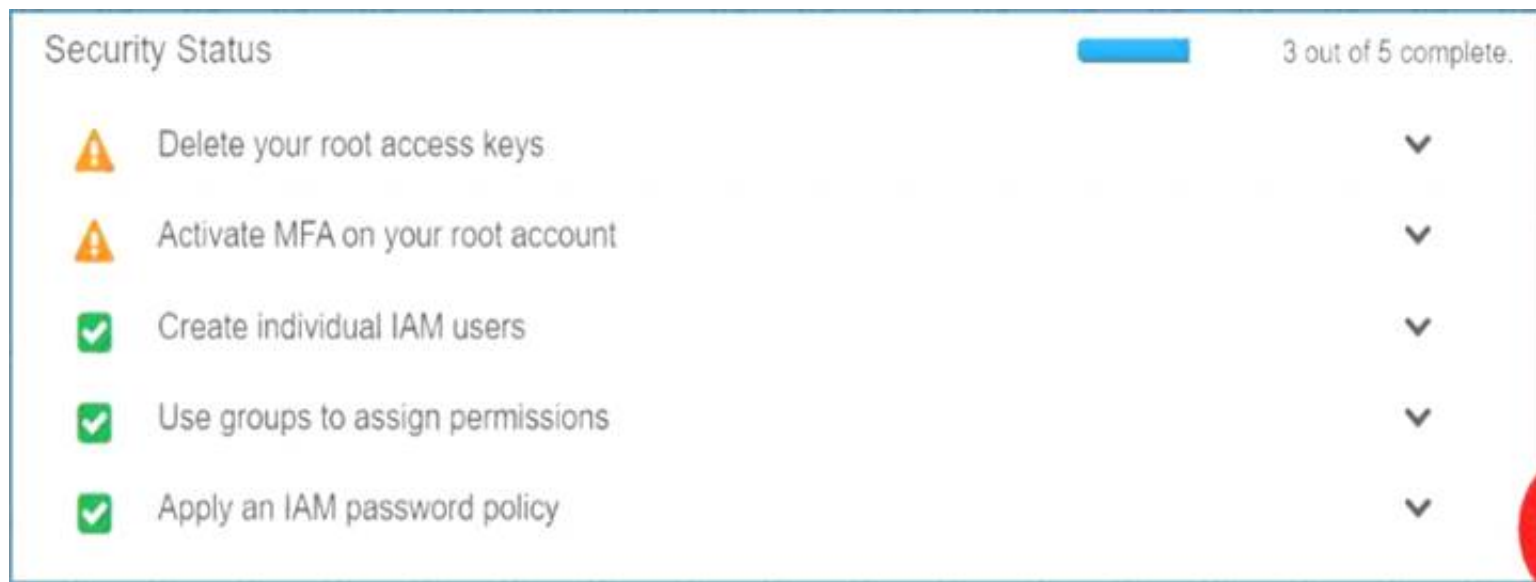C. Create IAM Roles
D. Restrict access using IAM policies

Answer: A

Explanation:
The first level or measure that should be taken is to delete the keys for the IAM root user
When you log into your account and go to your Security Access dashboard, this is the first step that can be seen
C:\Users\wk\Desktop\mudassar\Untitled.jpg

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

NEW QUESTION 111
- (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 112
- (Exam Topic 2)
An organization wants to deploy a three-tier web application whereby the application servers run on Amazon EC2 instances. These EC2 instances need access to credentials that they will use to authenticate their SQL connections to an Amazon RDS DB instance. Also, AWS Lambda functions must issue queries to the RDS database by using the same database credentials.
The credentials must be stored so that the EC2 instances and the Lambda functions can access them. No other access is allowed. The access logs must record when the credentials were accessed and by whom.
What should the Security Engineer do to meet these requirements?

A. Store the database credentials in AWS Key Management Service (AWS KMS). Create an IAM role with access to AWS KMS by using the EC2 and Lambda service principals in the role's trust polic
B. Add the role to an EC2 instance profil
C. Attach the instance profile to the EC2 instance
D. Set up Lambda to use the new role for execution.
E. Store the database credentials in AWS KM
F. Create an IAM role with access to KMS by using the EC2 and Lambda service principals in the role's trust polic
G. Add the role to an EC2 instance profil
H. Attach the instance profile to the EC2 instances and the Lambda function.
I. Store the database credentials in AWS Secrets Manage
J. Create an IAM role with access to Secrets Manager by using the EC2 and Lambda service principals in the role's trust polic
K. Add the role to an EC2 instance profil
L. Attach the instance profile to the EC2 instances and the Lambda function.
M. Store the database credentials in AWS Secrets Manage
N. Create an IAM role with access to Secrets Manager by using the EC2 and Lambda service principals in the role's trust polic
O. Add the role to an EC2 instance profil
P. Attach the instance profile to the EC2 instance
Q. Set up Lambda to use the new role for execution.

Answer: D

NEW QUESTION 114

- (Exam Topic 2)
A company has five AWS accounts and wants to use AWS CloudTrail to log API calls. The log files must be stored in an Amazon S3 bucket that resides in a new account specifically built for centralized services with a unique top-level prefix for each trail. The configuration must also enable detection of any modification to the logs.
Which of the following steps will implement these requirements? (Choose three.)

A. Create a new S3 bucket in a separate AWS account for centralized storage of CloudTrail logs, and enable "Log File Validation" on all trails.
B. Use an existing S3 bucket in one of the accounts, apply a bucket policy to the new centralized S3 bucket that permits the CloudTrail service to use the "s3: PutObject" action and the "s3 GetBucketACL" action, and specify the appropriate resource ARNs for the CloudTrail trails.
C. Apply a bucket policy to the new centralized S3 bucket that permits the CloudTrail service to use the "s3 PutObject" action and the "s3 GelBucketACL" action, and specify the appropriate resource ARNs for the CloudTrail trails.
D. Use unique log file prefixes for trails in each AWS account.
E. Configure CloudTrail in the centralized account to log all accounts to the new centralized S3 bucket.
F. Enable encryption of the log files by using AWS Key Management Service

Answer: ACE

Explanation:
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/best-practices-security.html
If you have created an organization in AWS Organizations, you can create a trail that will log all events for all AWS accounts in that organization. This is sometimes referred to as an organization trail. You can also choose to edit an existing trail in the master account and apply it to an organization, making it an organization trail. Organization trails log events for the master account and all member accounts in the organization. For more information about AWS Organizations, see Organizations Terminology and Concepts. Note Reference: https://docs.aws.amazon.com/awscloudtrail/latest/userguide/creating-trail-organization.html You must be logged in with the master account for the organization in order to create an organization trail. You must also have sufficient permissions for the IAM user or role in the master account in order to successfully create an organization trail. If you do not have sufficient permissions, you will not see the option to apply a trail to an organization.

NEW QUESTION 115
- (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?
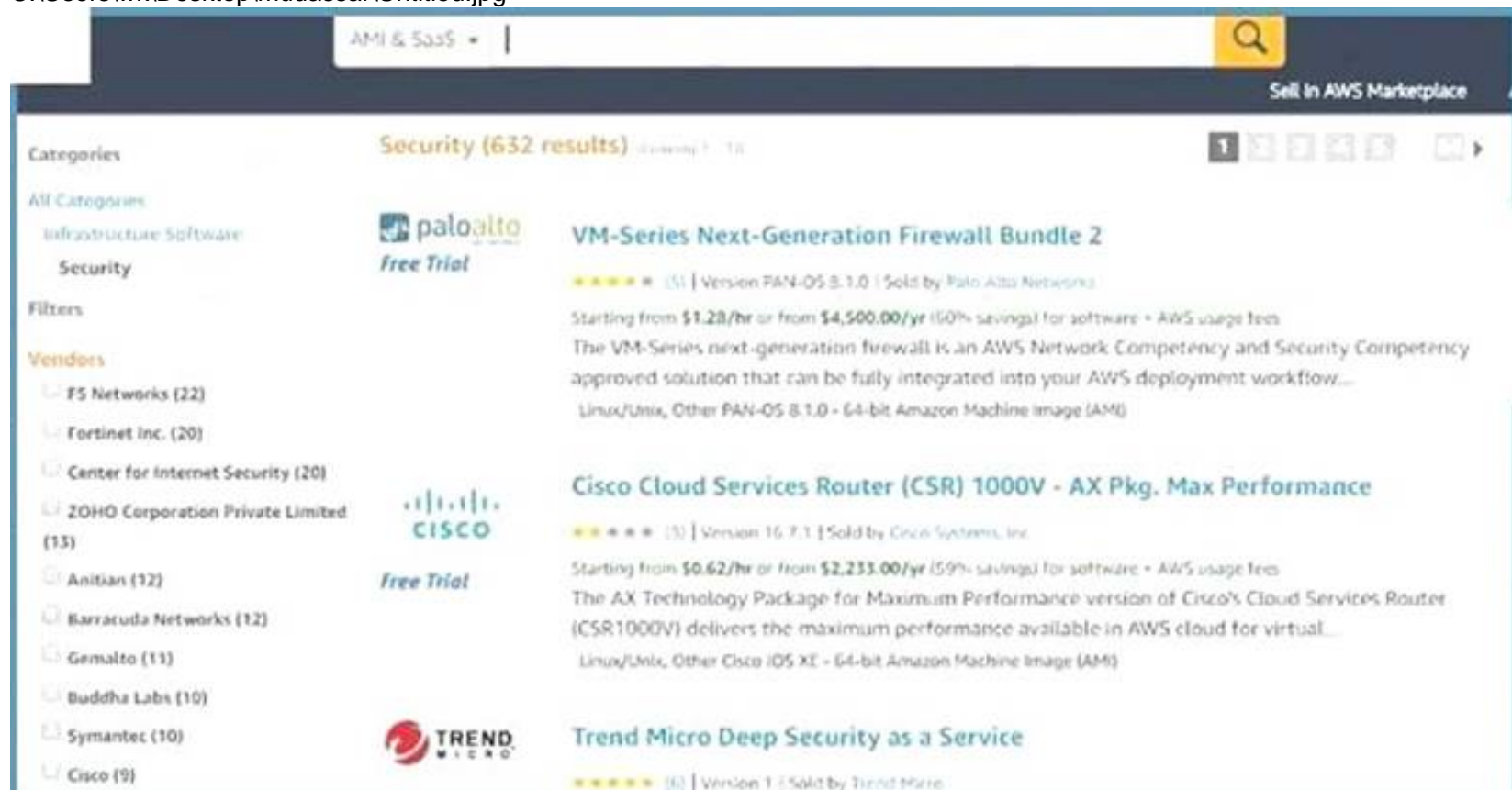Please select:

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%20verview.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 116
- (Exam Topic 2)
An organization is using Amazon CloudWatch Logs with agents deployed on its Linux Amazon EC2 instances. The agent configuration files have been checked and the application log files to be pushed are configured correctly. A review has identified that logging from specific instances is missing.
Which steps should be taken to troubleshoot the issue? (Choose two.)

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

Answer: AB

Explanation:
EC2 run command - can run scripts, install software, collect metrics and log files, manage patches and more. Bringing these two services together - can create CloudWatch Events rules that use EC2 Run Command to perform actions on EC2 instances or on-premises servers.

NEW QUESTION 117
- (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 119
- (Exam Topic 2)
A company has a few dozen application servers in private subnets behind an Elastic Load Balancer (ELB) in an AWS Auto Scaling group. The application is accessed from the web over HTTPS. The data must always be encrypted in transit. The Security Engineer is worried about potential key exposure due to vulnerabilities in the application software.
Which approach will meet these requirements while protecting the external certificate during a breach?

A. Use a Network Load Balancer (NLB) to pass through traffic on port 443 from the internet to port 443 on the instances.
B. Purchase an external certificate, and upload it to the AWS Certificate Manager (for use with the ELB) and to the instance

C. Have the ELB decrypt traffic, and route and re-encrypt with the same certificate.
D. Generate an internal self-signed certificate and apply it to the instance
E. Use AWS Certificate Manager to generate a new external certificate for the EL
F. Have the ELB decrypt traffic, and route and re-encrypt with the internal certificate.
G. Upload a new external certificate to the load balance
H. Have the ELB decrypt the traffic and forward it on port 80 to the instances.

Answer: C

NEW QUESTION 124
- (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 129
- (Exam Topic 2)
A company stores data on an Amazon EBS volume attached to an Amazon EC2 instance. The data is asynchronously replicated to an Amazon S3 bucket. Both the EBS volume and the S3 bucket are encrypted with the same AWS KMS Customer Master Key (CMK). A former employee scheduled a deletion of that CMK before leaving the company.
The company's Developer Operations department learns about this only after the CMK has been deleted. Which steps must be taken to address this situation?

A. Copy the data directly from the EBS encrypted volume before the volume is detached from the EC2 instance.
B. Recover the data from the EBS encrypted volume using an earlier version of the KMS backing key.
C. Make a request to AWS Support to recover the S3 encrypted data.
D. Make a request to AWS Support to restore the deleted CMK, and use it to recover the data.

Answer: C

NEW QUESTION 132
- (Exam Topic 2)
An IAM user with fill EC2 permissions could bot start an Amazon EC2 instance after it was stopped for a maintenance task. Upon starting the instance, the instance state would change to "Pending", but after a few seconds, it would switch back to "Stopped".
An inspection revealed that the instance has attached Amazon EBS volumes that were encrypted by using a Customer Master Key (CMK). When these encrypted volumes were detached, the IAM user was able to start the EC2 instances.
The IAM user policy is as follows:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
            <Action>
            ],
            "Resource": [
                "arn:aws:kms:us-east-1:012345678910:key/ebs-encryption-key"
            ]
            <CONDITION>
        }
    ]
}
```

What additional items need to be added to the IAM user policy? (Choose two.)

A. kms:GenerateDataKey
B. kms:Decrypt
C. kms:CreateGrant
D. "Condition": {"Bool": {"kms:ViaService": "ec2.us-west-2.amazonaws.com"}}
E. "Condition": {"Bool": {"kms:GrantIsForAWSResource": true}}

Answer: CE

Explanation:
The EBS which is AWS resource service is encrypted with CMK and to allow EC2 to decrypt , the IAM user should create a grant (action) and a boolean condition for the AWs resource . This link explains how AWS keys works. https://docs.aws.amazon.com/kms/latest/developerguide/key-policies.html

NEW QUESTION 137

- (Exam Topic 2)
Example.com hosts its internal document repository on Amazon EC2 instances. The application runs on EC2 instances and previously stored the documents on encrypted Amazon EBS volumes. To optimize the application for scale, example.com has moved the files to Amazon S3. The security team has mandated that all the files are securely deleted from the EBS volume, and it must certify that the data is unreadable before releasing the underlying disks.
Which of the following methods will ensure that the data is unreadable by anyone else?

A. Change the volume encryption on the EBS volume to use a different encryption mechanis
B. Then, release the EBS volumes back to AWS.
C. Release the volumes back to AW
D. AWS immediately wipes the disk after it is deprovisioned.
E. Delete the encryption key used to encrypt the EBS volum
F. Then, release the EBS volumes back to AWS.
G. Delete the data by using the operating system delete command
H. Run Quick Format on the drive and then release the EBS volumes back to AWS.

Answer: D

Explanation:
Amazon EBS volumes are presented to you as raw unformatted block devices that have been wiped prior to being made available for use. Wiping occurs immediately before reuse so that you can be assured that the wipe process completed. If you have procedures requiring that all data be wiped via a specific method, such as those detailed in NIST 800-88 ("Guidelines for Media Sanitization"), you have the ability to do so on Amazon EBS. You should conduct a specialized wipe procedure prior to deleting the volume for compliance with your established requirements.
https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

NEW QUESTION 139
- (Exam Topic 2)
While analyzing a company's security solution, a Security Engineer wants to secure the AWS account root user.
What should the Security Engineer do to provide the highest level of security for the account?

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

Answer: D

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

NEW QUESTION 143
- (Exam Topic 2)
A security team must present a daily briefing to the CISO that includes a report of which of the company's thousands of EC2 instances and on-premises servers are missing the latest security patches. All instances/servers must be brought into compliance within 24 hours so they do not show up on the next day's report.
How can the security team fulfill these requirements?
Please select:

A. Use Amazon QuickSight and Cloud Trail to generate the report of out of compliance instances/servers.Redeploy all out of compliance instances/servers using an AMI with the latest patches.
B. Use Systems Manger Patch Manger to generate the report of out of compliance instances/ server
C. Use Systems Manager Patch Manger to install the missing patches.
D. Use Systems Manger Patch Manger to generate the report of out of compliance instances/ servers.Redeploy all out of1 compliance instances/servers using an AMI with the latest patches.
E. Use Trusted Advisor to generate the report of out of compliance instances/server
F. Use Systems Manger Patch Manger to install the missing patches.

Answer: B

Explanation:
Use the Systems Manger Patch Manger to generate the report and also install the missing patches The AWS Documentation mentions the following
AWS Systems Manager Patch Manager automates the process of patching managed instances with
security-related updates. For Linux-based instances, you can also install patches for non-security updates. You can patch fleets of Amazon EC2 instances or your on-premises servers and virtual machines (VMs) by operating system type. This includes supported versions of Windows, Ubuntu Server, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), and Amazon Linux. You can scan instances to see only a report of missing patches, or you can scan and automatically install all missing patches.
Option A is invalid because Amazon QuickSight and Cloud Trail cannot be used to generate the list of servers that don't meet compliance needs.
Option C is wrong because deploying instances via new AMI'S would impact the applications hosted on these servers
Option D is invalid because Amazon Trusted Advisor cannot be used to generate the list of servers that don't meet compliance needs.
For more information on the AWS Patch Manager, please visit the below URL:
https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-patch.html (
The correct answer is: Use Systems Manger Patch Manger to generate the report of out of compliance instances/ servers. Use Systems Manager Patch Manger to install the missing patches.
Submit your Feedback/Queries to our Experts

NEW QUESTION 147

- (Exam Topic 2)
Your company has mandated that all calls to the AWS KMS service be recorded. How can this be achieved? Please select:

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

Answer: B

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

NEW QUESTION 149
- (Exam Topic 2)
The AWS Systems Manager Parameter Store is being used to store database passwords used by an AWS Lambda function. Because this is sensitive data, the parameters are stored as type SecureString and protected by an AWS KMS key that allows access through IAM. When the function executes, this parameter cannot be retrieved as the result of an access denied error.
Which of the following actions will resolve the access denied error?

A. Update the ssm.amazonaws.com principal in the KMS key policy to allow kms: Decrypt.
B. Update the Lambda configuration to launch the function in a VPC.
C. Add a policy to the role that the Lambda function uses, allowing kms: Decrypt for the KMS key.
D. Add lambda.amazonaws.com as a trusted entity on the IAM role that the Lambda function uses.

Answer: C

Explanation:
https://docs.amazonaws.cn/en_us/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Integrating.Authorizing

NEW QUESTION 152
- (Exam Topic 2)
A Developer's laptop was stolen. The laptop was not encrypted, and it contained the SSH key used to access multiple Amazon EC2 instances. A Security Engineer has verified that the key has not been used, and has blocked port 22 to all EC2 instances while developing a response plan.
How can the Security Engineer further protect currently running instances?

A. Delete the key-pair key from the EC2 console, then create a new key pair.
B. Use the modify-instance-attribute API to change the key on any EC2 instance that is using the key.
C. Use the EC2 RunCommand to modify the authorized_keys file on any EC2 instance that is using the key.
D. Update the key pair in any AMI used to launch the EC2 instances, then restart the EC2 instances.

Answer: C

NEW QUESTION 157
- (Exam Topic 2)
A Software Engineer is trying to figure out why network connectivity to an Amazon EC2 instance does not appear to be working correctly. Its security group allows inbound HTTP traffic from 0.0.0.0/0, and the outbound rules have not been modified from the default. A custom network ACL associated with its subnet allows inbound HTTP traffic from 0.0.0.0/0 and has no outbound rules.
What would resolve the connectivity issue?

A. The outbound rules on the security group do not allow the response to be sent to the client on the ephemeral port range.
B. The outbound rules on the security group do not allow the response to be sent to the client on the HTTP port.
C. An outbound rule must be added to the network ACL to allow the response to be sent to the client on the ephemeral port range.
D. An outbound rule must be added to the network ACL to allow the response to be sent to the client on the HTTP port.

Answer: C

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

NEW QUESTION 158
- (Exam Topic 2)
A threat assessment has identified a risk whereby an internal employee could exfiltrate sensitive data from production host running inside AWS (Account 1). The threat was documented as follows:
Threat description: A malicious actor could upload sensitive data from Server X by configuring credentials for an AWS account (Account 2) they control and uploading data to an Amazon S3 bucket within their control.
Server X has outbound internet access configured via a proxy server. Legitimate access to S3 is required so that the application can upload encrypted files to an S3 bucket. Server X is currently using an IAM instance role. The proxy server is not able to inspect any of the server communication due to TLS encryption.
Which of the following options will mitigate the threat? (Choose two.)

A. Bypass the proxy and use an S3 VPC endpoint with a policy that whitelists only certain S3 buckets within Account 1.

B. Block outbound access to public S3 endpoints on the proxy server.
C. Configure Network ACLs on Server X to deny access to S3 endpoints.
D. Modify the S3 bucket policy for the legitimate bucket to allow access only from the public IP addresses associated with the application server.
E. Remove the IAM instance role from the application server and save API access keys in a trusted and encrypted application config file.

Answer: AB

NEW QUESTION 163
- (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 168
- (Exam Topic 2)
Amazon CloudWatch Logs agent is successfully delivering logs to the CloudWatch Logs service. However, logs stop being delivered after the associated log stream has been active for a specific number of hours.
What steps are necessary to identify the cause of this phenomenon? (Choose two.)

A. Ensure that file permissions for monitored files that allow the CloudWatch Logs agent to read the file have not been modified.
B. Verify that the OS Log rotation rules are compatible with the configuration requirements for agent streaming.
C. Configure an Amazon Kinesis producer to first put the logs into Amazon Kinesis Streams.
D. Create a CloudWatch Logs metric to isolate a value that changes at least once during the period before logging stops.
E. Use AWS CloudFormation to dynamically create and maintain the configuration file for the CloudWatch Logs agent.

Answer: AB

Explanation:
https://acloud.guru/forums/aws-certified-security-specialty/discussion/-Lm5A3w6_NybQPhh6tRP/Cloudwatch%

NEW QUESTION 172
- (Exam Topic 2)
A company uses user data scripts that contain sensitive information to bootstrap Amazon EC2 instances. A Security Engineer discovers that this sensitive information is viewable by people who should not have access to it.
What is the MOST secure way to protect the sensitive information used to bootstrap the instances?

A. Store the scripts in the AMI and encrypt the sensitive data using AWS KMS Use the instance role profile to control access to the KMS keys needed to decrypt the data.

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

Answer: B

NEW QUESTION 177
- (Exam Topic 2)
An AWS Lambda function was misused to alter data, and a Security Engineer must identify who invoked the function and what output was produced. The Engineer cannot find any logs created by the Lambda function in Amazon CloudWatch Logs.
Which of the following explains why the logs are not available?

A. The execution role for the Lambda function did not grant permissions to write log data to CloudWatch Logs.
B. The Lambda function was executed by using Amazon API Gateway, so the logs are not stored in CloudWatch Logs.
C. The execution role for the Lambda function did not grant permissions to write to the Amazon S3 bucket where CloudWatch Logs stores the logs.
D. The version of the Lambda function that was executed was not current.

Answer: A

NEW QUESTION 180
- (Exam Topic 2)
A Security Administrator is performing a log analysis as a result of a suspected AWS account compromise. The Administrator wants to analyze suspicious AWS CloudTrail log files but is overwhelmed by the volume of audit logs being generated.
What approach enables the Administrator to search through the logs MOST efficiently?

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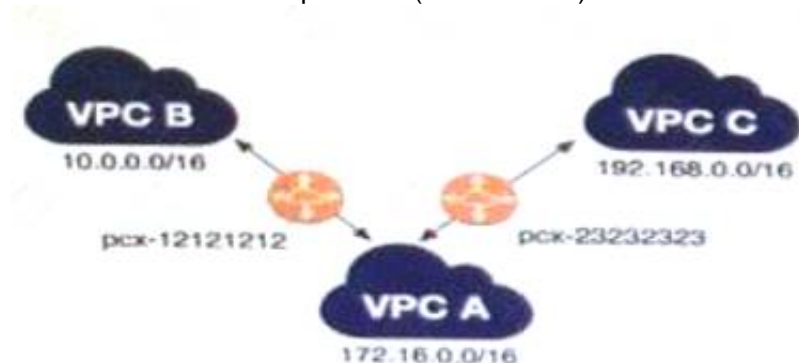
Answer: C

NEW QUESTION 185
- (Exam Topic 2)
A company has multiple VPCs in their account that are peered, as shown in the diagram. A Security Engineer wants to perform penetration tests of the Amazon EC2 instances in all three VPCs.
How can this be accomplished? (Choose two.)

A. Deploy a pre-authorized scanning engine from the AWS Marketplace into VPC B, and use it to scan instances in all three VPC
B. Do not complete the penetration test request form.
C. Deploy a pre-authorized scanning engine from the Marketplace into each VPC, and scan instances in each VPC from the scanning engine in that VP
D. Do not complete the penetration test request form.
E. Create a VPN connection from the data center to VPC
F. Use an on-premises scanning engine to scan the instances in all three VPC
G. Complete the penetration test request form for all three VPCs.
H. Create a VPN connection from the data center to each of the three VPC
I. Use an on-premises scanning engine to scan the instances in each VP
J. Do not complete the penetration test request form.
K. Create a VPN connection from the data center to each of the three VPC
L. Use an on-premises scanning engine to scan the instances in each VP
M. Complete the penetration test request form for all three VPCs.

Answer: BD

Explanation:
https://aws.amazon.com/security/penetration-testing/

NEW QUESTION 186
- (Exam Topic 2)
You are designing a custom IAM policy that would allow uses to list buckets in S3 only if they are MFA authenticated. Which of the following would best match this requirement?

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

```
"Version": "2012-10-17",
"Statement": {
 "Effect": "Allow",
 "Action": [
     "s3:ListAllMyBuckets",
     "s3:GetBucketLocation"
 ],
 "Resource": "Resource": "arn:aws:s3:::*",
 "Condition": {
  "Bool": {"aws:MultiFactorAuthPresent": true}
 }
 }
}
```

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

```
"Version": "2012-10-17",
"Statement": {
 "Effect": "Allow",
 "Action": [
     "s3:ListAllMyBuckets",
     "s3:GetBucketLocation"
 ],
 "Resource": "Resource": "arn:aws:s3:::*",
 "Condition": {
  "Bool": {"aws:MultiFactorAuthPresent":false}
 }
 }
}
```

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

```
"Version": "2012-10-17",
"Statement": {
 "Effect": "Allow",
 "Action": [
     "s3:ListAllMyBuckets",
     "s3:GetBucketLocation"
 ],
 "Resource": "Resource": "arn:aws:s3:::*",
 "Condition": {
   "aws:MultiFactorAuthPresent":false
 }
 }
}
```

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

```
"Version": "2012-10-17",
"Statement": {
 "Effect": "Allow",
 "Action": [
     "s3:ListAllMyBuckets",
     "s3:GetBucketLocation"
 ],
 "Resource": "Resource": "arn:aws:s3:::*",
 "Condition": {
   "aws:MultiFactorAuthPresent":true
 }
 }
}
```

Answer: A

Explanation:
The Condition clause can be used to ensure users can only work with resources if they are MFA authenticated. Option B and C are wrong since the aws:MultiFactorAuthPresent clause should be marked as true. Here you
are saying that onl if the user has been MFA activated, that means it is true, then allow access.
Option D is invalid because the "boor clause is missing in the evaluation for the condition clause. Boolean conditions let you construct Condition elements that restrict access based on comparing a key to
"true" or "false."
Here in this scenario the boot attribute in the condition element will return a value True for option A which

will ensure that access is allowed on S3 resources.
For more information on an example on such a policy, please visit the following URL:

NEW QUESTION 189
- (Exam Topic 2)
An organization has three applications running on AWS, each accessing the same data on Amazon S3. The data on Amazon S3 is server-side encrypted by using an AWS KMS Customer Master Key (CMK).
What is the recommended method to ensure that each application has its own programmatic access control permissions on the KMS CMK?

A. Change the key policy permissions associated with the KMS CMK for each application when it must access the data in Amazon S3.
B. Have each application assume an IAM role that provides permissions to use the AWS Certificate Manager CMK.
C. Have each application use a grant on the KMS CMK to add or remove specific access controls on the KMS CMK.
D. Have each application use an IAM policy in a user context to have specific access permissions on the KMS CMK.

Answer: C

NEW QUESTION 191
- (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 192
- (Exam Topic 2)
A Security Analyst attempted to troubleshoot the monitoring of suspicious security group changes. The Analyst was told that there is an Amazon CloudWatch alarm in place for these AWS CloudTrail log events. The Analyst tested the monitoring setup by making a configuration change to the security group but did not receive any alerts.
Which of the following troubleshooting steps should the Analyst perform?

A. Ensure that CloudTrail and S3 bucket access logging is enabled for the Analyst's AWS accoun
B. Verify that a metric filter was created and then mapped to an alar
C. Check the alarm notification action.
D. Check the CloudWatch dashboards to ensure that there is a metric configured with an appropriate dimension for security group changes.
E. Verify that the Analyst's account is mapped to an IAM policy that includes permissions for cloudwatch: GetMetricStatistics and Cloudwatch: ListMetrics.

Answer: B

Explanation:
MetricFilter:
Type: 'AWS::Logs::MetricFilter' Properties:
LogGroupName: '' FilterPattern: >
{ ($.eventName = AuthorizeSecurityGroupIngress) || ($.eventName = AuthorizeSecurityGroupEgress) || ($.eventName = RevokeSecurityGroupIngress) || ($.eventName = RevokeSecurityGroupEgress)
|| ($.eventName = CreateSecurityGroup) || ($.eventName = DeleteSecurityGroup) }
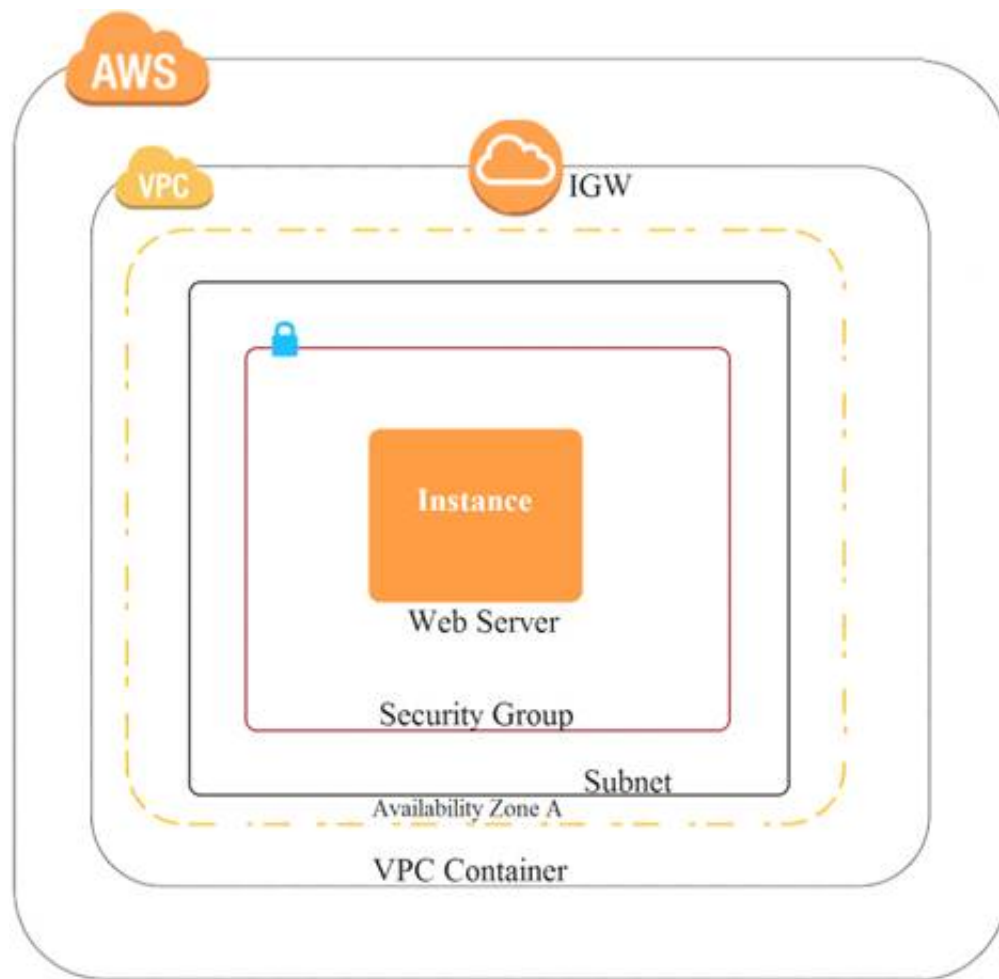MetricTransformations:
- MetricValue: '1'
MetricNamespace: CloudTrailMetrics MetricName: SecurityGroupEventCount

NEW QUESTION 197
- (Exam Topic 2)
A company recently experienced a DDoS attack that prevented its web server from serving content. The website is static and hosts only HTML, CSS, and PDF files that users download.
Based on the architecture shown in the image, what is the BEST way to protect the site against future attacks while minimizing the ongoing operational overhead?

A. Move all the files to an Amazon S3 bucke
B. Have the web server serve the files from the S3 bucket.
C. Launch a second Amazon EC2 instance in a new subne
D. Launch an Application Load Balancer in front of both instances.
E. Launch an Application Load Balancer in front of the EC2 instanc
F. Create an Amazon CloudFront distribution in front of the Application Load Balancer.
G. Move all the files to an Amazon S3 bucke
H. Create a CloudFront distribution in front of the bucket and terminate the web server.

Answer: D

Explanation:
https://docs.aws.amazon.com/AmazonS3/latest/dev/WebsiteHosting.html

NEW QUESTION 200
- (Exam Topic 2)
Your company has defined privileged users for their AWS Account. These users are administrators for key resources defined in the company. There is now a mandate to enhance the security authentication for these users. How can this be accomplished?
Please select:

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

Answer: A

Explanation:
The AWS Documentation mentions the following as a best practices for IAM users. For extra security, enable multi-factor authentication (MFA) for privileged IAM users (users who are allowed access to sensitive resources or APIs). With MFA, users have a device that generates unique authentication code (a one-time password, or OTP). Users must provide both their normal credentials (like their user name and password) and the OTP. The MFA device can either be a special piece of hardware, or it can be a virtual device (for example, it can run in an app on a smartphone).
Option B,C and D are invalid because no such security options are available in AWS For more information on IAM best practices, please visit the below URL https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html The correct answer is: Enable MFA for these user accounts
Submit your Feedback/Queries to our Experts

NEW QUESTION 204
- (Exam Topic 2)
A company plans to move most of its IT infrastructure to AWS. They want to leverage their existing on-premises Active Directory as an identity provider for AWS. Which combination of steps should a Security Engineer take to federate the company's on-premises Active Directory with AWS? (Choose two.)

A. Create IAM roles with permissions corresponding to each Active Directory group.
B. Create IAM groups with permissions corresponding to each Active Directory group.
C. Configure Amazon Cloud Directory to support a SAML provider.
D. Configure Active Directory to add relying party trust between Active Directory and AWS.
E. Configure Amazon Cognito to add relying party trust between Active Directory and AWS.

Answer: AD

Explanation:
https://aws.amazon.com/blogs/security/how-to-establish-federated-access-to-your-aws-resources-by-using-activ

NEW QUESTION 207
- (Exam Topic 2)
You have an instance setup in a test environment in AWS. You installed the required application and the promoted the server to a production environment. Your IT Security team has advised that there maybe traffic flowing in from an unknown IP address to port 22. How can this be mitigated immediately?
Please select:

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

Answer: B

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

NEW QUESTION 212
- (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 216
- (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 221
- (Exam Topic 2)
Your company has a requirement to monitor all root user activity by notification. How can this best be achieved? Choose 2 answers from the options given below. Each answer forms part of the solution
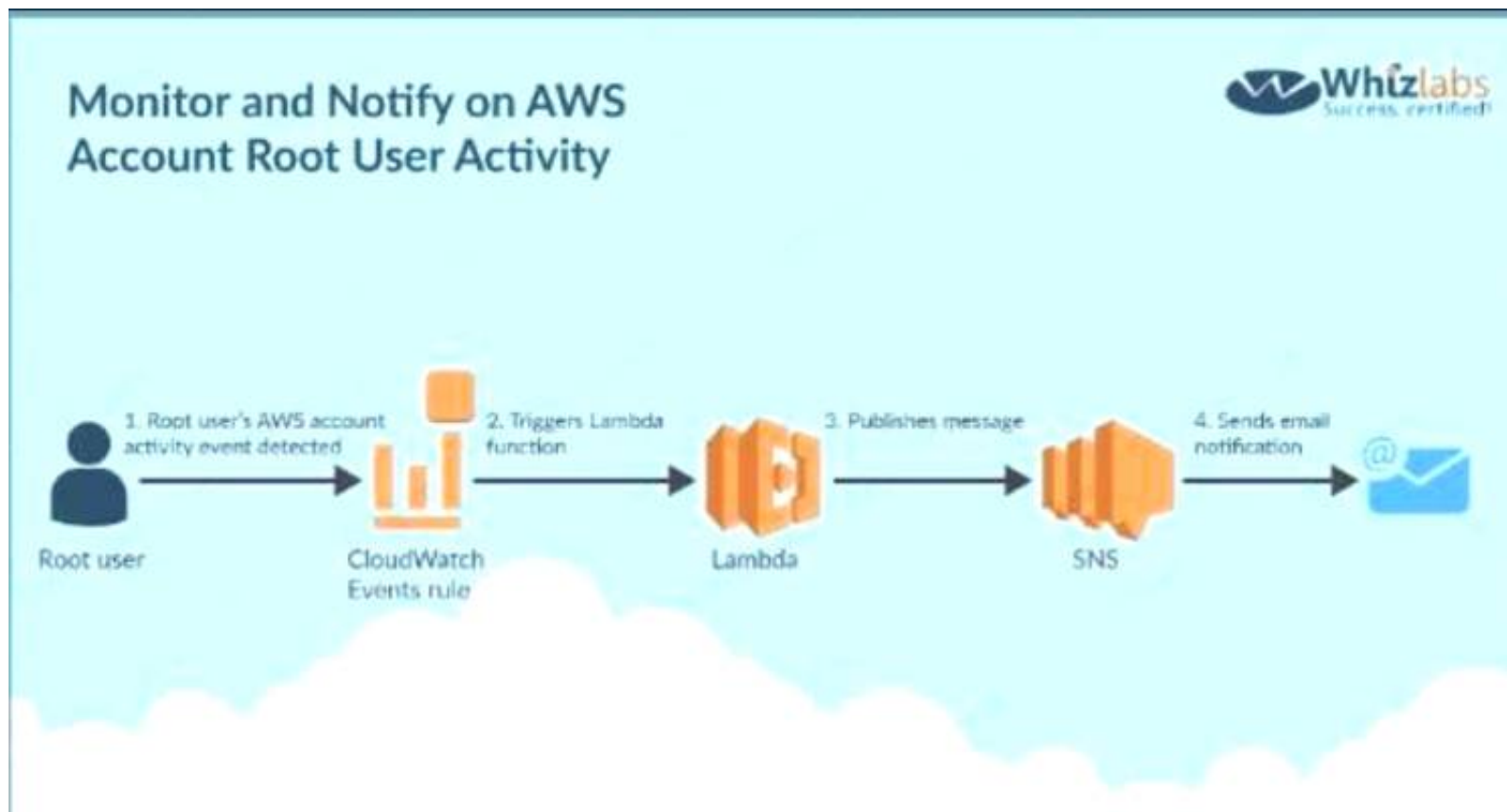Please select:

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

Answer: AC

Explanation:
Below is a snippet from the AWS blogs on a solution C:\Users\wk\Desktop\mudassar\Untitled.jpg

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

NEW QUESTION 224
- (Exam Topic 2)
A Security Engineer has been asked to create an automated process to disable IAM user access keys that are more than three months old.
Which of the following options should the Security Engineer use?

A. In the AWS Console, choose the IAM service and select "Users". Review the "Access Key Age" column.
B. Define an IAM policy that denies access if the key age is more than three months and apply to all users.
C. Write a script that uses the GenerateCredentialReport, GetCredentialReport, and UpdateAccessKey APIs.
D. Create an Amazon CloudWatch alarm to detect aged access keys and use an AWS Lambda function to disable the keys older than 90 days.

Answer: C

Explanation:
https://docs.aws.amazon.com/IAM/latest/APIReference/API_UpdateAccessKey.html
https://docs.aws.amazon.com/IAM/latest/APIReference/API_GenerateCredentialReport.html
https://docs.aws.amazon.com/IAM/latest/APIReference/API_GetCredentialReport.html

NEW QUESTION 228
- (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 233
- (Exam Topic 2)
A company has enabled Amazon GuardDuty in all Regions as part of its security monitoring strategy. In one of the VPCs, the company hosts an Amazon EC2 instance working as an FTP server that is contacted by a high number of clients from multiple locations. This is identified by GuardDuty as a brute force attack due to the high number of connections that happen every hour.
The finding has been flagged as a false positive. However, GuardDuty keeps raising the issue. A Security Engineer has been asked to improve the signal-to-noise ratio. The Engineer needs to ensure that changes do not compromise the visibility of potential anomalous behavior.
How can the Security Engineer address the issue?

A. Disable the FTP rule in GuardDuty in the Region where the FTP server is deployed
B. Add the FTP server to a trusted IP list and deploy it to GuardDuty to stop receiving the notifications
C. Use GuardDuty filters with auto archiving enabled to close the findings
D. Create an AWS Lambda function that closes the finding whenever a new occurrence is reported

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.
References:

NEW QUESTION 237
- (Exam Topic 2)
A Security Engineer is working with a Product team building a web application on AWS. The application uses Amazon S3 to host the static content, Amazon API Gateway to provide RESTful services; and Amazon DynamoDB as the backend data store. The users already exist in a directory that is exposed through a SAML identity provider.
Which combination of the following actions should the Engineer take to enable users to be authenticated into the web application and call APIs? (Choose three.)

A. Create a custom authorization service using AWS Lambda.
B. Configure a SAML identity provider in Amazon Cognito to map attributes to the Amazon Cognito user pool attributes.
C. Configure the SAML identity provider to add the Amazon Cognito user pool as a relying party.
D. Configure an Amazon Cognito identity pool to integrate with social login providers.
E. Update DynamoDB to store the user email addresses and passwords.
F. Update API Gateway to use a COGNITO_USER_POOLS authorizer.

Answer: BDE

NEW QUESTION 241
- (Exam Topic 2)
Your company has an EC2 Instance that is hosted in an AWS VPC. There is a requirement to ensure that logs files from the EC2 Instance are stored accordingly. The access should also be limited for the destination of the log files. How can this be accomplished? Choose 2 answers from the options given below. Each answer forms part of the solution
Please select:

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

Answer: BD

Explanation:
You can create a Log group and send all logs from the EC2 Instance to that group. You can then limit the access to the Log groups via an IAM policy.
Option A is invalid because Cloudtrail is used to record API activity and not for storing log files Option C is invalid because Cloudtrail is the wrong service to be used for this requirement
For more information on Log Groups and Log Streams, please visit the following URL:
* https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/Workinj
For more information on Access to Cloudwatch logs, please visit the following URL:
* https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/auth-and-access-control-cwl.html
The correct answers are: Stream the log files to a separate Cloudwatch Log group. Create an IAM policy that gives the desired level of access to the Cloudwatch Log group
Submit your Feedback/Queries to our Experts

NEW QUESTION 244
- (Exam Topic 2)
Which of the following is the most efficient way to automate the encryption of AWS CloudTrail logs using a Customer Master Key (CMK) in AWS KMS?

A. Use the KMS direct encrypt function on the log data every time a CloudTrail log is generated.
B. Use the default Amazon S3 server-side encryption with S3-managed keys to encrypt and decrypt the CloudTrail logs.
C. Configure CloudTrail to use server-side encryption using KMS-managed keys to encrypt and decrypt CloudTrail logs.
D. Use encrypted API endpoints so that all AWS API calls generate encrypted CloudTrail log entries using the TLS certificate from the encrypted API call.

Answer: C

Explanation:
https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingKMSEncryption.html

NEW QUESTION 248
- (Exam Topic 2)
Compliance requirements state that all communications between company on-premises hosts and EC2 instances be encrypted in transit. Hosts use custom proprietary protocols for their communication, and EC2 instances need to be fronted by a load balancer for increased availability.
Which of the following solutions will meet these requirements?

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

Answer: B

Explanation:
https://aws.amazon.com/blogs/compute/maintaining-transport-layer-security-all-the-way-to-your-container-usin

NEW QUESTION 251
- (Exam Topic 2)

A company has a forensic logging use case whereby several hundred applications running on Docker on EC2 need to send logs to a central location. The Security Engineer must create a logging solution that is able to perform real-time analytics on the log files, grants the ability to replay events, and persists data.
Which AWS Services, together, can satisfy this use case? (Select two.)

A. Amazon Elasticsearch
B. Amazon Kinesis
C. Amazon SQS
D. Amazon CloudWatch
E. Amazon Athena

Answer: AB

Explanation:
https://docs.aws.amazon.com/whitepapers/latest/aws-overview/analytics.html#amazon-athena

NEW QUESTION 253
- (Exam Topic 2)
A Security Administrator is configuring an Amazon S3 bucket and must meet the following security requirements:

> Encryption in transit

> Encryption at rest

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

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

Answer: ACE

NEW QUESTION 255
- (Exam Topic 2)
A Security Engineer discovers that developers have been adding rules to security groups that allow SSH and RDP traffic from 0.0.0.0/0 instead of the organization firewall IP.
What is the most efficient way to remediate the risk of this activity?

A. Delete the internet gateway associated with the VPC.
B. Use network access control lists to block source IP addresses matching 0.0.0.0/0.
C. Use a host-based firewall to prevent access from all but the organization's firewall IP.
D. Use AWS Config rules to detect 0.0.0.0/0 and invoke an AWS Lambda function to update the security group with the organization's firewall IP.

Answer: D

NEW QUESTION 259
- (Exam Topic 2)
A Security Engineer is working with the development team to design a supply chain application that stores sensitive inventory data in an Amazon S3 bucket. The application will use an AWS KMS customer master key (CMK) to encrypt the data on Amazon S3. The inventory data on Amazon S3 will be shared of vendors. All vendors will use AWS principals from their own AWS accounts to access the data on Amazon S3. The vendor list may change weekly, and the solution must support cross-account access.
What is the MOST efficient way to manage access control for the KMS CMK7?

A. Use KMS grants to manage key acces
B. Programmatically create and revoke grants to manage vendor access.
C. Use an IAM role to manage key acces
D. Programmatically update the IAM role policies to manage vendor access.
E. Use KMS key policies to manage key acces
F. Programmatically update the KMS key policies to manage vendor access.
G. Use delegated access across AWS accounts by using IAM roles to manage key access.Programmatically update the IAM trust policy to manage cross-account vendor access.

Answer: A

NEW QUESTION 261
- (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 263
- (Exam Topic 2)
The Security team believes that a former employee may have gained unauthorized access to AWS resources sometime in the past 3 months by using an identified access key.
What approach would enable the Security team to find out what the former employee may have done within AWS?

A. Use the AWS CloudTrail console to search for user activity.
B. Use the Amazon CloudWatch Logs console to filter CloudTrail data by user.
C. Use AWS Config to see what actions were taken by the user.
D. Use Amazon Athena to query CloudTrail logs stored in Amazon S3.

Answer: A

Explanation:
You can use CloudTrail to search event history for the last 90 days. You can use CloudWatch queries to search API history beyond the last 90 days. You can use Athena to query CloudTrail logs over the last 90 days. https://aws.amazon.com/premiumsupport/knowledge-center/view-iam-history/

NEW QUESTION 264
- (Exam Topic 2)
Which of the following minimizes the potential attack surface for applications?

A. Use security groups to provide stateful firewalls for Amazon EC2 instances at the hypervisor level.
B. Use network ACLs to provide stateful firewalls at the VPC level to prevent access to any specific AWS resource.
C. Use AWS Direct Connect for secure trusted connections between EC2 instances within private subnets.
D. Design network security in a single layer within the perimeter network (also known as DMZ, demilitarized zone, and screened subnet) to facilitate quicker responses to threats.

Answer: A

Explanation:
https://aws.amazon.com/answers/networking/vpc-security-capabilities/ Security Group is stateful and hypervisor level.

NEW QUESTION 265
- (Exam Topic 2)
You have an Ec2 Instance in a private subnet which needs to access the KMS service. Which of the following methods can help fulfil this requirement, keeping security in perspective
Please select:

A. Use a VPC endpoint
B. Attach an Internet gateway to the subnet
C. Attach a VPN connection to the VPC
D. Use VPC Peering

Answer: A

Explanation:
The AWS Documentation mentions the following
You can connect directly to AWS KMS through a private endpoint in your VPC instead of connecting over the internet. When you use a VPC endpoint communication between your VPC and AWS KMS is conducted entirely within the AWS network.
Option B is invalid because this could open threats from the internet
Option C is invalid because this is normally used for communication between on-premise environments and AWS.
Option D is invalid because this is normally used for communication between VPCs
For more information on accessing KMS via an endpoint, please visit the following URL https://docs.aws.amazon.com/kms/latest/developerguide/kms-vpc-endpoint.htmll
The correct answer is: Use a VPC endpoint Submit your Feedback/Queries to our Experts

NEW QUESTION 266
- (Exam Topic 2)
A company runs an application on AWS that needs to be accessed only by employees. Most employees work from the office, but others work remotely or travel.
How can the Security Engineer protect this workload so that only employees can access it?

A. Add each employee's home IP address to the security group for the application so that only those users can access the workload.
B. Create a virtual gateway for VPN connectivity for each employee, and restrict access to the workload from within the VPC.
C. Use a VPN appliance from the AWS Marketplace for users to connect to, and restrict workload access to traffic from that appliance.
D. Route all traffic to the workload through AWS WA
E. Add each employee's home IP address into an AWS WAF rule, and block all other traffic.

Answer: C

Explanation:
https://docs.aws.amazon.com/vpn/latest/clientvpn-admin/what-is.html

NEW QUESTION 268

- (Exam Topic 2)
Which of the following is used as a secure way to log into an EC2 Linux Instance? Please select:

A. IAM User name and password
B. Key pairs
C. AWS Access keys
D. AWS SDK keys

Answer: B

Explanation:
The AWS Documentation mentions the following
Key pairs consist of a public key and a private key. You use the private key to create a digital signature, and then AWS uses the corresponding public key to validate the signature. Key pairs are used only for Amazon EC2 and Amazon CloudFront.
Option A.C and D are all wrong because these are not used to log into EC2 Linux Instances For more information on AWS Security credentials, please visit the below URL: https://docs.aws.amazon.com/eeneral/latest/er/aws-sec-cred-types.html
The correct answer is: Key pairs
Submit your Feedback/Queries to our Experts

NEW QUESTION 269
- (Exam Topic 2)
An organization has tens of applications deployed on thousands of Amazon EC2 instances. During testing, the Application team needs information to let them know whether the network access control lists (network ACLs) and security groups are working as expected.
How can the Application team's requirements be met?

A. Turn on VPC Flow Logs, send the logs to Amazon S3, and use Amazon Athena to query the logs.
B. Install an Amazon Inspector agent on each EC2 instance, send the logs to Amazon S3, and use Amazon EMR to query the logs.
C. Create an AWS Config rule for each network ACL and security group configuration, send the logs to Amazon S3, and use Amazon Athena to query the logs.
D. Turn on AWS CloudTrail, send the trails to Amazon S3, and use AWS Lambda to query the trails.

Answer: A

NEW QUESTION 272
- (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 274
- (Exam Topic 2)
A company maintains sensitive data in an Amazon S3 bucket that must be protected using an AWS KMS CMK. The company requires that keys be rotated automatically every year.
How should the bucket be configured?

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

Answer: B

NEW QUESTION 277
- (Exam Topic 2)
A Security Engineer is defining the logging solution for a newly developed product. Systems Administrators and Developers need to have appropriate access to event log files in AWS CloudTrail to support and troubleshoot the product.
Which combination of controls should be used to protect against tampering with and unauthorized access to log files? (Choose two.)

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

Answer: AD

NEW QUESTION 280
- (Exam Topic 3)
A company has an existing AWS account and a set of critical resources hosted in that account. The employee who was in-charge of the root account has left the company. What must be now done to secure the account. Choose 3 answers from the options given below.
Please select:

A. Change the access keys for all IAM users.
B. Delete all custom created IAM policies
C. Delete the access keys for the root account
D. Confirm MFAtoa secure device
E. Change the password for the root account
F. Change the password for all IAM users

Answer: CDE

Explanation:
Now if the root account has a chance to be compromised, then you have to carry out the below steps
* 1. Delete the access keys for the root account
* 2. Confirm MFA to a secure device
* 3. Change the password for the root account
This will ensure the employee who has left has no change to compromise the resources in AWS. Option A is invalid because this would hamper the working of the current IAM users
Option B is invalid because this could hamper the current working of services in your AWS account Option F is invalid because this would hamper the working of the current IAM users
For more information on IAM root user, please visit the following URL: https://docs.aws.amazon.com/IAM/latest/UserGuide/id root-user.html
The correct answers are: Delete the access keys for the root account Confirm MFA to a secure device. Change the password for the root account
Submit Your Feedback/Queries to our Experts

NEW QUESTION 282
- (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 284
- (Exam Topic 3)
You have a set of application , database and web servers hosted in AWS. The web servers are placed behind an ELB. There are separate security groups for the application, database and web servers. The network security groups have been defined accordingly. There is an issue with the communication between the application and database servers. In order to troubleshoot the issue between just the application and database server, what is the ideal set of MINIMAL steps you would take?
Please select:

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

Answer: A

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

NEW QUESTION 286
- (Exam Topic 3)
There is a set of Ec2 Instances in a private subnet. The application hosted on these EC2 Instances need to access a DynamoDB table. It needs to be ensured that traffic does not flow out to the internet. How can this be achieved?
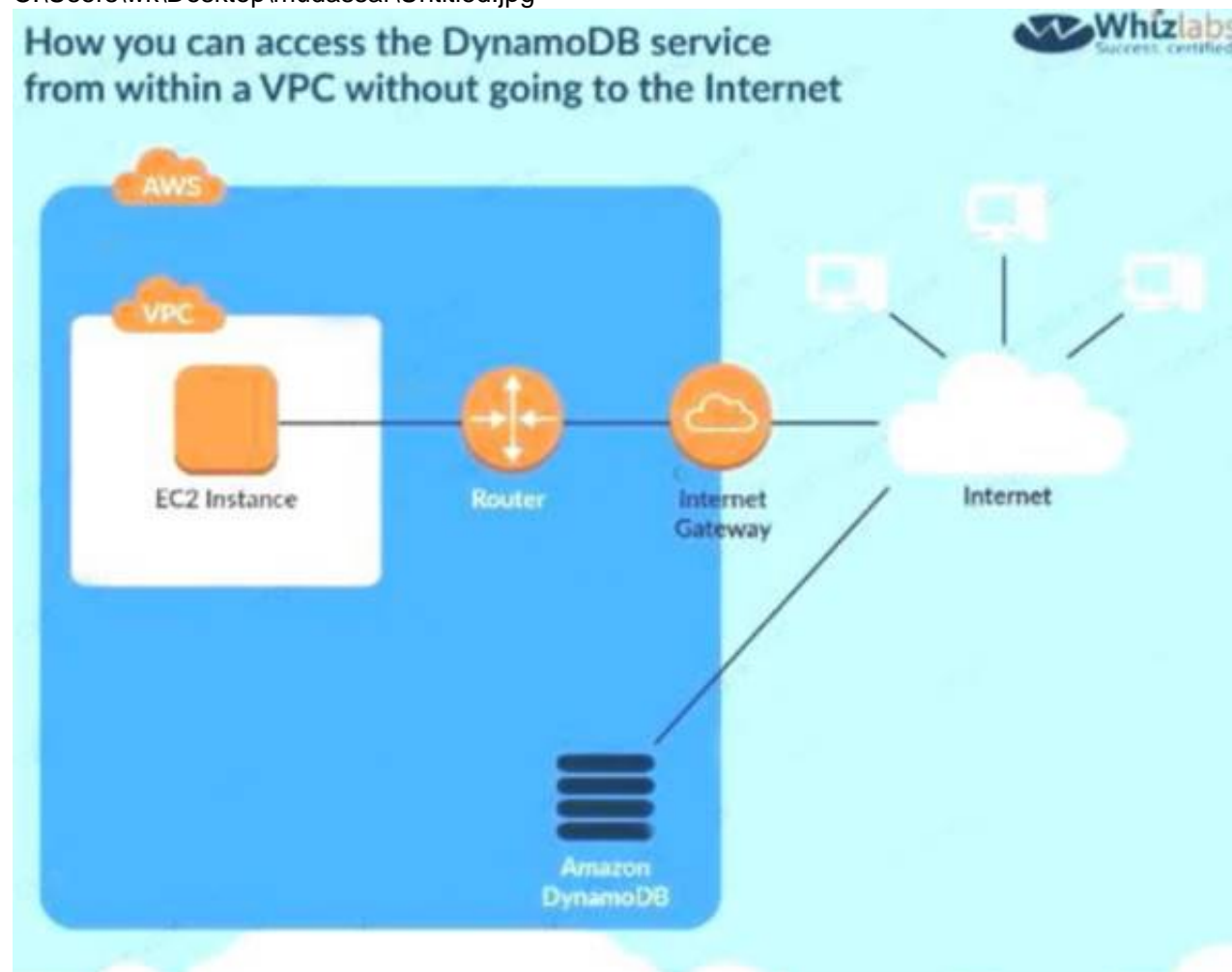Please select:

A. Use a VPC endpoint to the DynamoDB table

B. Use a VPN connection from the VPC
C. Use a VPC gateway from the VPC
D. Use a VPC Peering connection to the DynamoDB table

Answer: A

Explanation:
The following diagram from the AWS Documentation shows how you can access the DynamoDB service from within a V without going to the Internet This can be done with the help of a VPC endpoint
C:\Users\wk\Desktop\mudassar\Untitled.jpg

Option B is invalid because this is used for connection between an on-premise solution and AWS Option C is invalid because there is no such option
Option D is invalid because this is used to connect 2 VPCs
For more information on VPC endpointsfor DynamoDB, please visit the URL:
The correct answer is: Use a VPC endpoint to the DynamoDB table Submit your Feedback/Queries to our Experts

NEW QUESTION 288
- (Exam Topic 3)
Your company has a hybrid environment, with on-premise servers and servers hosted in the AWS cloud. They are planning to use the Systems Manager for patching servers. Which of the following is a pre-requisite for this to work;
Please select:

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

Answer: B

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

NEW QUESTION 290
......

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

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

100% Actual & Verified — Instant Download, Please Click
Order The SCS-C01 Practice Test Here