Amazon-Web-Services

Exam Questions SCS-C02

AWS Certified Security - Specialty

NEW QUESTION 1
- (Exam Topic 1)
A Developer is building a serverless application that uses Amazon API Gateway as the front end. The application will not be publicly accessible. Other legacy applications running on Amazon EC2 will make calls to the application A Security Engineer Has been asked to review the security controls for authentication and authorization of the application
Which combination of actions would provide the MOST secure solution? (Select TWO)

A. Configure an IAM policy that allows the least permissive actions to communicate with the API Gateway Attach the policy to the role used by the legacy EC2 instances
B. Enable IAM WAF for API Gateway Configure rules to explicitly allow connections from the legacy EC2 instances
C. Create a VPC endpoint for API Gateway Attach an IAM resource policy that allows the role of the legacy EC2 instances to call specific APIs
D. Create a usage plan Generate a set of API keys for each application that needs to call the API.
E. Configure cross-origin resource sharing (CORS) in each API Share the CORS information with the applications that call the API.

Answer: AE

NEW QUESTION 2
- (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 IAM 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 IAM 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 IAM Systems Manager Agent on the instances Configure an automation document to copy the application log files to IAM 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 3
- (Exam Topic 1)
Which of the following are valid configurations for using SSL certificates with Amazon CloudFront? (Select THREE)

A. Default IAM Certificate Manager certificate
B. Custom SSL certificate stored in IAM KMS
C. Default CloudFront certificate
D. Custom SSL certificate stored in IAM Certificate Manager
E. Default SSL certificate stored in IAM Secrets Manager
F. Custom SSL certificate stored in IAM IAM

Answer: ACD

NEW QUESTION 4
- (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:
• IAM IAM federated with on-premises Active Directory
• Amazon Cognito user pools to accessing an IAM 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 IAM IAM with a minimum password length condition.
D. Update the password length policy in the Amazon Cognito configuration.
E. Create an SCP with IAM Organizations that enforces a minimum password length for IAM IAM and Amazon Cognito.

Answer: AD

NEW QUESTION 5
- (Exam Topic 1)
The Security Engineer is managing a traditional three-tier web application that is running on Amazon EC2 instances. The application has become the target of increasing numbers of malicious attacks from the Internet.
What steps should the Security Engineer take to check for known vulnerabilities and limit the attack surface? (Choose two.)

A. Use IAM Certificate Manager to encrypt all traffic between the client and application servers.
B. Review the application security groups to ensure that only the necessary ports are open.
C. Use Elastic Load Balancing to offload Secure Sockets Layer encryption.
D. Use Amazon Inspector to periodically scan the backend instances.
E. Use IAM Key Management Services to encrypt all the traffic between the client and application servers.

Answer: BD

NEW QUESTION 6
- (Exam Topic 1)
A Web Administrator for the website example.com has created an Amazon CloudFront distribution for dev.example.com, with a requirement to configure HTTPS using a custom TLS certificate imported to IAM Certificate Manager.
Which combination of steps is required to ensure availability of the certificate in the CloudFront console? (Choose two.)

A. Call UploadServerCertificate with /cloudfront/dev/ in the path parameter.
B. Import the certificate with a 4,096-bit RSA public key.
C. Ensure that the certificate, private key, and certificate chain are PKCS #12-encoded.
D. Import the certificate in the us-east-1 (
E. Virginia) Region.
F. Ensure that the certificate, private key, and certificate chain are PEM-encoded.

Answer: DE

NEW QUESTION 7
- (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 IAM account was compromised and Amazon EBS snapshots were deleted.
All EBS snapshots are encrypted using an IAM 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 IAM Systems Manager to distribute a configuration that performs local backups of all attached disks to Amazon S3.
D. Create a new IAM account with limited privilege
E. Allow the new account to access the IAM KMS key used to encrypt the EBS snapshots, and copy the encrypted snapshots to the new account on a recuning basis
F. Use IAM Backup to copy EBS snapshots to Amazon S3.

Answer: A

NEW QUESTION 8
- (Exam Topic 1)
A company uses a third-party identity provider and SAML-based SSO for its IAM accounts After the third-party identity provider renewed an expired signing certificate users saw the following message when trying to log in:

```
Error: Response Signature Invalid (Service: AWSSecurityTokenService; Status Code: 400; Error Code: InvalidIdentityToken)
```

A security engineer needs to provide a solution that corrects the error and minimizes operational overhead Which solution meets these requirements?

A. Upload the third-party signing certificate's new private key to the IAM identity provider entity defined in IAM identity and Access Management (IAM) by using the IAM Management Console
B. Sign the identity provider's metadata file with the new public key Upload the signature to the IAM identity provider entity defined in IAM Identity and Access Management (IAM) by using the IAM CLI.
C. Download the updated SAML metadata tile from the identity service provider Update the file in the IAM identity provider entity defined in IAM Identity and Access Management (IAM) by using the IAM CLI
D. Configure the IAM identity provider entity defined in IAM Identity and Access Management (IAM) to synchronously fetch the new public key by using the IAM Management Console.

Answer: C

NEW QUESTION 9
- (Exam Topic 1)
A company has implemented centralized logging and monitoring of IAM CloudTrail logs from all Regions in an Amazon S3 bucket. The log Hies are encrypted using IAM 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 10
- (Exam Topic 1)
A website currently runs on Amazon EC2 with mostly static content on the site. Recently, the site was subjected to a DDoS 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 IAM 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 IAM 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)
Unapproved changes were previously made to a company's Amazon S3 bucket. A security engineer configured IAM Config to record configuration changes made to the company's S3 buckets. The engineer discovers there are S3 configuration changes being made, but no Amazon SNS notifications are being sent. The engineer has already checked the configuration of the SNS topic and has confirmed the configuration is valid.
Which combination of steps should the security engineer take to resolve the issue? (Select TWO.)

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

Answer: BE

NEW QUESTION 11
- (Exam Topic 1)
A company wants to encrypt the private network between its orvpremises environment and IAM. The company also wants a consistent network experience for its employees.
What should the company do to meet these requirements?

A. Establish an IAM Direct Connect connection with IAM and set up a Direct Connect gatewa
B. In the Direct Connect gateway configuration, enable IPsec and BGP, and then leverage native IAM network encryption between Availability Zones and Regions,
C. Establish an IAM Direct Connect connection with IAM 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 IAM virtual private cloud over the internet
G. Establish an IAM Direct Connect connection with IAM 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: D

NEW QUESTION 14
- (Exam Topic 1)
A global company must mitigate and respond to DDoS attacks at Layers 3, 4 and 7 All of the company's IAM applications are serverless with static content hosted on Amazon S3 using Amazon CloudFront and Amazon Route 53
Which solution will meet these requirements?

A. Use IAM WAF with an upgrade to the IAM Business support plan
B. Use IAM Certificate Manager with an Application Load Balancer configured with an origin access identity
C. Use IAM Shield Advanced
D. Use IAM WAF to protect IAM Lambda functions encrypted with IAM KMS and a NACL restricting all Ingress traffic

Answer: C

NEW QUESTION 16
- (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 IAM 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 18
- (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 IAM 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: C

Explanation:
https://IAM.amazon.com/blogs/security/how-to-protect-the-integrity-of-your-encrypted-data-by-using-IAM-key One of the most important and critical concepts in IAM Key Management Service (KMS) for advanced and secure data usage is EncryptionContext. Using EncryptionContext properly can help significantly improve the security of your applications. EncryptionContext is a key-value map (both strings) that is provided to KMS with each encryption and decryption request. EncryptionContext provides three benefits: Additional authenticated data (AAD), Audit trail, Authorization context

NEW QUESTION 22
- (Exam Topic 1)
A company is collecting IAM CloudTrail log data from multiple IAM 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 IAM Organizations trails, the company decided to further centralize management and automate deployment of the CloudTrail logging capability across all of its IAM accounts.
The company's security engineer created an IAM Organizations trail in the master account, enabled server-side encryption with IAM KMS managed keys (SSE-KMS) for the log files, and specified the same bucket as the storage location. However, the engineer noticed that logs recorded by the new trail were not delivered to the bucket.
Which factors could cause this issue? (Select TWO.)

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

Answer: AD

NEW QUESTION 24
- (Exam Topic 1)
An organization policy states that all encryption keys must be automatically rotated every 12 months. Which IAM Key Management Service (KMS) key type should be used to meet this requirement?

A. IAM managed Customer Master Key (CMK)
B. Customer managed CMK with IAM generated key material
C. Customer managed CMK with imported key material
D. IAM managed data key

Answer: B

NEW QUESTION 28
- (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: C

Explanation:
https://docs.IAM.amazon.com/IAMcloudtrail/latest/userguide/create-s3-bucket-policy-for-cloudtrail.html#cloud

NEW QUESTION 29
- (Exam Topic 1)
An company is using IAM 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 34
- (Exam Topic 1)
A company Is trying to replace its on-premises bastion hosts used to access on-premises Linux servers with IAM Systems Manager Session Manager. A security engineer has installed the Systems Manager Agent on all servers. The security engineer verifies that the agent is running on all the servers, but Session Manager cannot connect to them. 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.)

A. Open inbound port 22 to 0 0.0.0/0 on all Linux servers.
B. Enable the advanced-instances tier in Systems Manager.
C. Create a managed-instance activation for the on-premises servers.
D. Reconfigure the Systems Manager Agent with the activation code and ID.
E. Assign an IAM role to all of the on-premises servers.
F. Initiate an inventory collection with Systems Manager on the on-premises servers

Answer: CEF

NEW QUESTION 39
- (Exam Topic 1)
Users report intermittent availability of a web application hosted on IAM. 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 IAM 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 IAM WAF rules to protect the web applications from malicious traffic.
E. Use the default Amazon VPC for externakfacing systems to allow IAM to actively block malicious network traffic affecting Amazon EC2 instances.

Answer: BD

NEW QUESTION 41
- (Exam Topic 1)
A company has multiple production IAM accounts. Each account has IAM CloudTrail configured to log to a single Amazon S3 bucket in a central account. Two of the production accounts have trails that are not logging anything to the S3 bucket.
Which steps should be taken to troubleshoot the issue? (Choose three.)

A. Verify that the log file prefix is set to the name of the S3 bucket where the logs should go.
B. Verify that the S3 bucket policy allows access for CloudTrail from the production IAM account IDs.
C. Create a new CloudTrail configuration in the account, and configure it to log to the account's S3 bucket.
D. Confirm in the CloudTrail Console that each trail is active and healthy.
E. Open the global CloudTrail configuration in the master account, and verify that the storage location is set to the correct S3 bucket.
F. Confirm in the CloudTrail Console that the S3 bucket name is set correctly.

Answer: BDF

NEW QUESTION 43
- (Exam Topic 1)
A Security Engineer accidentally deleted the imported key material in an IAM KMS CMK. What should the Security Engineer do to restore the deleted key material?

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

Answer: C

NEW QUESTION 48
- (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 IAM Key Management Service (IAM KMS) CM
B. Encrypt the data at rest.
C. Use IAM 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 IAM Encryption SD
G. Use client-side encryption and sign the table items.

Answer: A

NEW QUESTION 51
- (Exam Topic 1)
A Security Engineer has launched multiple Amazon EC2 instances from a private AMI using an IAM CloudFormation template. The Engineer notices instances terminating right after they are launched.
What could be causing these terminations?

A. The IAM user launching those instances is missing ec2:Runinstances permission.
B. The AMI used as encrypted and the IAM does not have the required IAM KMS permissions.
C. The instance profile used with the EC2 instances in unable to query instance metadata.
D. IAM currently does not have sufficient capacity in the Region.

Answer: B

Explanation:
https://docs.IAM.amazon.com/IAMEC2/latest/UserGuide/troubleshooting-launch.html

NEW QUESTION 55
- (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 60
- (Exam Topic 1)
A company's Director of information Security wants a daily email report from IAM that contains recommendations for each company account to meet IAM Security best practices.
Which solution would meet these requirements?

A. in every IAM account, configure IAM Lambda to query me IAM Support API tor IAM Trusted Advisor security checks Send the results from Lambda to an Amazon SNS topic to send reports.
B. Configure Amazon GuardDuty in a master account and invite all other accounts to be managed by the master account Use GuardDuty's integration with Amazon SNS to report on findings
C. Use Amazon Athena and Amazon QuickSight to build reports off of IAM CloudTrail Create a daily Amazon CloudWatch trigger to run the report dally and email It using Amazon SNS
D. Use IAM Artifact's prebuilt reports and subscriptions Subscribe the Director of Information Security to the reports by adding the Director as the security alternate contact tor each account

Answer: A

NEW QUESTION 64
- (Exam Topic 1)
A security engineer has been tasked with implementing a solution that allows the company's development team to have interactive command line access to Amazon EC2 Linux instances using the IAM Management Console.
Which steps should the security engineer take to satisfy this requirement while maintaining least privilege?

A. Enable IAM Systems Manager in the IAM Management Console and configure for access to EC2 instances using the default AmazonEC2RoleforSSM rol
B. Install the Systems Manager Agent on all EC2 Linux instances that need interactive acces
C. Configure IAM user policies to allow development team access to the Systems Manager Session Manager and attach to the team's IAM users.
D. Enable console SSH access in the EC2 consol
E. Configure IAM user policies to allow development team access to the IAM Systems Manager Session Manager and attach to the development team's IAM users.
F. Enable IAM Systems Manager in the IAM Management Console and configure to access EC2 instances using the default AmazonEC2RoleforSSM rol
G. Install the Systems Manager Agent on all EC2 Linux instances that need interactive acces
H. Configure a security group that allows SSH port 22 from all published IP addresse
I. Configure IAM user policies to allow development team access to the IAM Systems Manager Session Manager and attach to the team's IAM users.
J. Enable IAM Systems Manager in the IAM Management Console and configure to access EC2 instances using the default AmazonEC2RoleforSSM role Install the Systems Manager Agent on all EC2 Linux instances that need interactive acces
K. Configure IAM policies to allow development team access to the EC2 console and attach to the teams IAM users.

Answer: A

NEW QUESTION 65
- (Exam Topic 1)
A company's web application is hosted on Amazon EC2 instances running behind an Application Load Balancer (ALB) in an Auto Scaling group. An IAM WAF web ACL is associated with the ALB. IAM CloudTrail is enabled, and stores logs in Amazon S3 and Amazon CloudWatch Logs.
The operations team has observed some EC2 instances reboot at random. After rebooting, all access logs on the instances have been deleted. During an investigation, the operations team found that each reboot happened just after a PHP error occurred on the new-user-creation.php file. The operations team needs to view log information to determine if the company is being attacked.
Which set of actions will identify the suspect attacker's IP address for future occurrences?

A. Configure VPC Flow Logs on the subnet where the ALB is located, and stream the data CloudWatch.Search for the new-user-creation.php occurrences in CloudWatch.
B. Configure the CloudWatch agent on the ALB Configure the agent to send application logs to CloudWatch Update the instance role to allow CloudWatch Logs acces
C. Export the logs to CloudWatch Search for the new-user-creation.php occurrences in CloudWatch.
D. Configure the ALB to export access logs to an Amazon Elasticsearch Service cluster, and use the service to search for the new-user-creation.php occurrences.
E. Configure the web ACL to send logs to Amazon Kinesis Data Firehose, which delivers the logs to an S3 bucket Use Amazon Athena to query the logs and find the new-user-creation php occurrences.

Answer: D

Explanation:
You send logs from your web ACL to an Amazon Kinesis Data Firehose with a configured storage destination. After you enable logging, IAM WAF delivers logs to your storage destination through the HTTPS endpoint of Kinesis Data Firehose. https://docs.IAM.amazon.com/waf/latest/developerguide/logging.html

NEW QUESTION 66
- (Exam Topic 1)
A company's information security team want to do near-real-time anomaly detection on Amazon EC2 performance and usage statistics. Log aggregation is the responsibility of a security engineer. To do the study, the Engineer needs gather logs from all of the company's IAM accounts in a single place.
How should the Security Engineer go about doing this?

A. Log in to each account four times a day and filter the IAM CloudTrail log data, then copy and paste the logs in to the Amazon S3 bucket in the destination account.
B. Set up Amazon CloudWatch to stream data to an Amazon S3 bucket in each source accoun
C. Set up bucket replication for each source account into a centralized bucket owned by the Security Engineer.
D. Set up an IAM Config aggregator to collect IAM configuration data from multiple sources.
E. Set up Amazon CloudWatch cross-account log data sharing with subscriptions in each accoun
F. Send the logs to Amazon Kinesis Data Firehose in the Security Engineer's account.

Answer: D

Explanation:
Read the prerequisites in the question carefully. The solution must support "near real time" analysis of the log data. Cloudwatch doesn't stream logs to S3; it supports exporting them to S3 with an up to 12 hour expected delay:
https://docs.IAM.amazon.com/AmazonCloudWatch/latest/logs/S3Export.html
"Log data can take up to 12 hours to become available for export. For near real-time analysis of log data, see Analyzing log data with CloudWatch Logs Insights or Real-time processing of log data with subscriptions instead."
https://docs.IAM.amazon.com/AmazonCloudWatch/latest/logs/Subscriptions.html
"You can use subscriptions to get access to a real-time feed of log events from CloudWatch Logs and have it delivered to other services such as an Amazon Kinesis stream, an Amazon Kinesis Data Firehose stream, or IAM Lambda for custom processing, analysis, or loading to other systems. When log events are sent to the receiving service, they are Base64 encoded and compressed with the gzip format."
https://docs.IAM.amazon.com/AmazonCloudWatch/latest/logs/CrossAccountSubscriptions.html

NEW QUESTION 70
- (Exam Topic 1)
A company has hundreds of IAM accounts, and a centralized Amazon S3 bucket used to collect IAM 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 IAM 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 IAM 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 74
- (Exam Topic 1)
A company is developing a new mobile app for social media sharing. The company's development team has decided to use Amazon S3 to store at media files generated by mobile app users The company wants to allow users to control whether their own tiles are public, private, of shared with other users in their social network what should the development team do to implement the type of access control with the LEAST administrative effort?

A. Use individual ACLs on each S3 object.
B. Use IAM groups tor sharing files between application social network users
C. Store each user's files in a separate S3 bucket and apery a bucket policy based on the user's sharing settings
D. Generate presigned UPLs for each file access

Answer: A

NEW QUESTION 77
- (Exam Topic 1)
A recent security audit identified that a company's application team injects database credentials into the environment variables of an IAM 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 IAM Secrets Manager secret and specify the key/value pairs to be stored in this secret
C. Modify the application to pull credentials from the IAM 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 IAM Fargate instance, create a script to read the secret value from IAM Secret Manager, and inject the environment variable
G. Ask the application team to redeploy the application.

Answer: BEF

NEW QUESTION 82
- (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 IAM WAF
C. Use IAM Shield to limit the originating traffic hit rate.
D. Implement the GeoLocation feature in Amazon Route 53.

Answer: C

NEW QUESTION 83
- (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 IAM Encryption SDK and set the maximum age to 10 days and the minimum number of messages encrypted to 3" 16. Use IAM Key Management Service (IAM KMS) to generate the master key and data key Use data key caching with the Encryption SDk during the encryption process.
B. Use IAM Key Management Service (IAM KMS) to generate an IAM managed CM
C. Then use Amazon S3 client-side encryption configured to automatically rotate with every object
D. Use IAM 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 85
- (Exam Topic 1)
A company has an encrypted Amazon S3 bucket. An Application Developer has an IAM policy that allows access to the S3 bucket, but the Application Developer is unable to access objects within the bucket.
What is a possible cause of the issue?

A. The S3 ACL for the S3 bucket fails to explicitly grant access to the Application Developer
B. The IAM KMS key for the S3 bucket fails to list the Application Developer as an administrator
C. The S3 bucket policy fails to explicitly grant access to the Application Developer
D. The S3 bucket policy explicitly denies access to the Application Developer

Answer: C

NEW QUESTION 89
- (Exam Topic 1)
A company is using IAM Organizations to manage multiple IAM 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 IAM 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 90
- (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 loT 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 IAM WAF to block requests with a string match condition for the user agent of the loT devic
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 IAM WAF to block requests with a string match condition for the user agent of the loT devic
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 IAM WAF to block requests with a string match condition for the user agent of the loT devic
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 IAM Shield Advanced to enable DDoS protectio
J. Apply an IAM WAF ACL to the AL
K. andconfigure a listener rule on the ALB to block loT devices based on the user agent.

Answer: D

NEW QUESTION 94
- (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 IAM 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: A

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

NEW QUESTION 96
- (Exam Topic 1)
A company is operating an open-source software platform that is internet facing. The legacy software platform no longer receives security updates. The software platform operates using Amazon route 53 weighted load balancing to send traffic to two Amazon EC2 instances that connect to an Amazon POS cluster a recent report suggests this software platform is vulnerable to SQL injection attacks. with samples of attacks provided. The company's security engineer must secure this system against SQL injection attacks within 24 hours. The secure, engineer's solution involve the least amount of effort and maintain normal operations during implementation.
What should the security engineer do to meet these requirements?

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

Answer: A

NEW QUESTION 97
- (Exam Topic 1)
An employee accidentally exposed an IAM 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 IAM CloudTrail for activity.
B. Analyze Amazon CloudWatch Logs for activity.
C. Download and analyze the IAM Use report from IAM Trusted Advisor.
D. Analyze the resource inventory in IAM Config for IAM user activity.
E. Download and analyze a credential report from IAM.

Answer: AD

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

NEW QUESTION 98
- (Exam Topic 1)
An IAM account administrator created an IAM group and applied the following managed policy to require that each individual user authenticate using multi-factor authentication:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:*",
            "Resource": "*"
        },
        {
            "Sid": "BlockAnyAccessUnlessSignedInWithMFA",
            "Effect": "Deny",
            "Action": "ec2:*",
            "Resource": "*",
            "Condition": {
                "BoolIfExists": {
                    "aws:MultiFactorAuthPresent": false
                }
            }
        }
    ]
}
```

After implementing the policy, the administrator receives reports that users are unable to perform Amazon EC2 commands using the IAM CLI. What should the administrator do to resolve this problem while still enforcing multi-factor authentication?

A. Change the value of IAM MultiFactorAuthPresent to true.
B. Instruct users to run the IAM sts get-session-token CLI command and pass the multi-factor authentication —serial-number and —token-code parameter
C. Use these resulting values to make API/CLI calls
D. Implement federated API/CLI access using SAML 2.0, then configure the identity provider to enforce multi-factor authentication.
E. Create a role and enforce multi-factor authentication in the role trust policy Instruct users to run the sts assume-role CLI command and pass --serial-number and —token-code parameters Store the resulting values in environment variable
F. Add sts:AssumeRole to NotAction in the policy.

Answer: B

NEW QUESTION 99
- (Exam Topic 1)
A developer is creating an IAM Lambda function that requires environment variables to store connection information and logging settings. The developer is required to use an IAM KMS Customer Master Key (CMK> supplied by the information security department in order to adhere to company standards for securing Lambda environment variables.
Which of the following are required for this configuration to work? (Select TWO.)

A. The developer must configure Lambda access to the VPC using the --vpc-config parameter.
B. The Lambda function execution role must have the kms:Decrypt- permission added in the IAM IAM policy.
C. The KMS key policy must allow permissions for the developer to use the KMS key.
D. The IAM IAM policy assigned to the developer must have the kmseGcnerate-DataKcy permission added.
E. The Lambda execution role must have the kms:Encrypt permission added in the IAM IAM policy.

Answer: BC

NEW QUESTION 101
- (Exam Topic 1)
Two Amazon EC2 instances in different subnets should be able to connect to each other but cannot. It has been confirmed that other hosts in the same subnets are able to communicate successfully, and that security groups have valid ALLOW rules in place to permit this traffic.
Which of the following troubleshooting steps should be performed?

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

Answer: C

NEW QUESTION 103
- (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 107
- (Exam Topic 1)
A company plans to use custom AMIs to launch Amazon EC2 instances across multiple IAM 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 IAM 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 polic
C. 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
D. Configure EC2 Auto Scaling groups within each applicable account to use the created IAM role to launch EC2 instances.
E. Create a customer-managed CMK in the centralized accoun
F. Allow other applicable accounts to use that key for cryptographical operations by applying proper cross-account permissions in the key polic
G. Create an IAM role in all applicable accounts and configure its access policy with permissions to create grants for the centrally managed CM
H. 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.
I. Create a customer-managed CMK or an IAM managed CMK in the centralized accoun
J. Allow other applicable accounts to use that key for cryptographical operations by applying proper cross-account permissions in the key polic
K. 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.
L. Create a customer-managed CMK or an IAM managed CMK in the centralized accoun
M. Allow other applicable accounts to use that key for cryptographical operations by applying proper cross-account permissions in the key polic
N. Modify the access policy for the EC2 Auto Scaling roles to perform cryptographical operations against the centrally managed CMK.

Answer: B

NEW QUESTION 112
- (Exam Topic 1)
A company has a compliance requirement to rotate its encryption keys on an annual basis. A Security Engineer needs a process to rotate the KMS Customer Master Keys (CMKs) that were created using imported key material.
How can the Engineer perform the key rotation process MOST efficiently?

A. Create a new CMK, and redirect the existing Key Alias to the new CMK
B. Select the option to auto-rotate the key
C. Upload new key material into the existing CMK.
D. Create a new CMK, and change the application to point to the new CMK

Answer: A

NEW QUESTION 114
- (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.IAM.amazon.com/IAMEC2/latest/UserGuide/security-group-rules-reference.html#sg-rules-other-in

NEW QUESTION 118
- (Exam Topic 2)
Your IT Security department has mandated that all data on EBS volumes created for underlying EC2 Instances need to be encrypted. Which of the following can help achieve this?
Please select:

A. IAM KMS API
B. IAM Certificate Manager
C. API Gateway with STS
D. IAM Access Key

Answer: A

Explanation:
The IAM Documentation mentions the following on IAM KMS
IAM Key Management Service (IAM KMS) is a managed service that makes it easy for you to create and control the encryption keys used to encrypt your data. IAM KMS is integrated with other IAM services including Amazon Elastic Block Store (Amazon EBS), Amazon Simple Storage Service (Amazon S3), Amazon Redshift Amazon Elastic Transcoder, Amazon WorkMail, Amazon Relational Database Service (Amazon RDS), and others to make it simple to encrypt your data with encryption keys that you manage
Option B is incorrect - The IAM Certificate manager can be used to generate SSL certificates that can be used to encrypt traffic transit, but not at rest
Option C is incorrect is again used for issuing tokens when using API gateway for traffic in transit. Option D is used for secure access to EC2 Instances
For more information on IAM KMS, please visit the following URL: https://docs.IAM.amazon.com/kms/latest/developereuide/overview.htmll The correct answer is: IAM KMS API
Submit your Feedback/Queries to our Experts

NEW QUESTION 121
- (Exam Topic 2)
A company wants to control access to its IAM resources by using identities and groups that are defined in its existing Microsoft Active Directory.
What must the company create in its IAM account to map permissions for IAM services to Active Directory user attributes?

A. IAM IAM groups
B. IAM IAM users
C. IAM IAM roles
D. IAM IAM access keys

Answer: C

Explanation:
Prerequisites to establish Federation Services in IAM - You have a working AD directory and AD FS server. - You have created an identity provider (IdP) in your IAM account using your XML file from your AD FS server. Remember the name of your IdP because you will use it later in this solution. -You have created the appropriate IAM roles in your IAM account, which will be used for federated access.
https://IAM.amazon.com/blogs/security/how-to-establish-federated-access-to-your-IAM-resources-by-using-acti

NEW QUESTION 124
- (Exam Topic 2)
Your company has an EC2 Instance that is hosted in an IAM 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.IAM.amazon.com/AmazonCloudWatch/latest/logs/Workinj
For more information on Access to Cloudwatch logs, please visit the following URL:
* https://docs.IAM.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 126
- (Exam Topic 2)
During a recent security audit, it was discovered that multiple teams in a large organization have placed restricted data in multiple Amazon S3 buckets, and the data may have been exposed. The auditor has requested that the organization identify all possible objects that contain personally identifiable information (PII) and then determine whether this information has been accessed.
What solution will allow the Security team to complete this request?

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

Answer: B

NEW QUESTION 130
- (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 IAM.
C. Release the volumes back to IA
D. IAM 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 IAM.
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 IAM.

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.IAMstatic.com/whitepapers/IAM-security-whitepaper.pdf

NEW QUESTION 135
- (Exam Topic 2)
The Security Engineer has discovered that a new application that deals with highly sensitive data is storing Amazon S3 objects with the following key pattern, which itself contains highly sensitive data.
Pattern: "randomID_datestamp_PII.csv" Example:
"1234567_12302017_000-00-0000 csv"
The bucket where these objects are being stored is using server-side encryption (SSE). Which solution is the most secure and cost-effective option to protect the sensitive data?

A. Remove the sensitive data from the object name, and store the sensitive data using S3 user-defined metadata.
B. Add an S3 bucket policy that denies the action s3:GetObject
C. Use a random and unique S3 object key, and create an S3 metadata index in Amazon DynamoDB using client-side encrypted attributes.
D. Store all sensitive objects in Binary Large Objects (BLOBS) in an encrypted Amazon RDS instance.

Answer: C

Explanation:
https://docs.IAM.amazon.com/AmazonS3/latest/dev/UsingMetadata.html https://IAM.amazon.com/blogs/database/best-practices-for-securing-sensitive-data-in-IAM-data-stores/

NEW QUESTION 136
- (Exam Topic 2)
The Security Engineer for a mobile game has to implement a method to authenticate users so that they can save their progress. Because most of the users are part of the same OpenID-Connect compatible social media website, the Security Engineer would like to use that as the identity provider.
Which solution is the SIMPLEST way to allow the authentication of users using their social media identities?

A. Amazon Cognito
B. AssumeRoleWithWebIdentity API
C. Amazon Cloud Directory
D. Active Directory (AD) Connector

Answer: A

NEW QUESTION 139
- (Exam Topic 2)
A Security Administrator is restricting the capabilities of company root user accounts. The company uses IAM Organizations and has enabled it for all feature sets, including consolidated billing. The top-level account is used for billing and administrative purposes, not for operational IAM resource purposes.
How can the Administrator restrict usage of member root user accounts across the organization?

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

Answer: C

Explanation:
Applying a "Control Policy" in your organization. A policy applied to: 1) root applies to all accounts in the organization 2) OU applies to all accounts in the OU and to any child OUs 3) account applies to one account only Note- this requires that Acquirements: -all features are enabled for the organization in IAM Organizations -Only service control policy (SCP) are supported
https://docs.IAM.amazon.com/organizations/latest/userguide/orgs_manage_policies.html

NEW QUESTION 142
- (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, IAM 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 IAM Key Management Service (IAM KMS). Create an IAM role with access to IAM 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 IAM 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 IAM 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 IAM 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 143
- (Exam Topic 2)
Which of the following is the most efficient way to automate the encryption of IAM CloudTrail logs using a Customer Master Key (CMK) in IAM 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 IAM API calls generate encrypted CloudTrail log entries using the TLS certificate from the encrypted API call.

Answer: C

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

NEW QUESTION 145
- (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.IAM.amazon.com/vpc/latest/userguide/vpc-network-acls.html

NEW QUESTION 149
- (Exam Topic 2)
Which of the following are valid event sources that are associated with web access control lists that trigger IAM WAF rules? (Choose two.)

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

Answer: BC

Explanation:

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

NEW QUESTION 152
- (Exam Topic 2)
A company wants to have a secure way of generating, storing and managing cryptographic exclusive access for the keys. Which of the following can be used for this purpose?
Please select:

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

Answer: D

Explanation:
The IAM Documentation mentions the following
The IAM CloudHSM service helps you meet corporate, contractual and regulatory compliance requirements for data security by using dedicated Hardware Security Module (HSM) instances within the IAM cloud. IAM and IAM Marketplace partners offer a variety of solutions for protecting sensitive data within the IAM platform, but for some applications and data subject to contractual or regulatory mandates for managing cryptographic keys, additional protection may be necessary. CloudHSM complements existing data protection solutions and allows you to protect your encryption keys within HSMs that are desigr and validated to government

standards for secure key management. CloudHSM allows you to securely generate, store and manage cryptographic keys used for data encryption in a way that keys are accessible only by you.
Option A.B and Care invalid because in all of these cases, the management of the key will be with IAM. Here the question specifically mentions that you want to have exclusive access over the keys. This can be achieved with Cloud HSM
For more information on CloudHSM, please visit the following URL: https://IAM.amazon.com/cloudhsm/faq:
The correct answer is: Use Cloud HSM Submit your Feedback/Queries to our Experts

NEW QUESTION 156
- (Exam Topic 2)
Which option for the use of the IAM Key Management Service (KMS) supports key management best practices that focus on minimizing the potential scope of data exposed by a possible future key compromise?

A. Use KMS automatic key rotation to replace the master key, and use this new master key for future encryption operations without re-encrypting previously encrypted data.
B. Generate a new Customer Master Key (CMK), re-encrypt all existing data with the new CMK, and use it for all future encryption operations.
C. Change the CMK alias every 90 days, and update key-calling applications with the new key alias.
D. Change the CMK permissions to ensure that individuals who can provision keys are not the same individuals who can use the keys.

Answer: A

Explanation:
"automatic key rotation has no effect on the data that the CMK protects. It does not rotate the data keys that the CMK generated or re-encrypt any data protected by the CMK, and it will not mitigate the effect of a compromised data key. You might decide to create a new CMK and use it in place of the original CMK. This has the same effect as rotating the key material in an existing CMK, so it's often thought of as manually rotating the key."
https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html
https://docs.IAM.amazon.com/kms/latest/developerguide/rotate-keys.html#rotate-keys-manually for IAM standards

NEW QUESTION 158
- (Exam Topic 2)
The Accounting department at Example Corp. has made a decision to hire a third-party firm, AnyCompany, to monitor Example Corp.'s IAM account to help optimize costs.
The Security Engineer for Example Corp. has been tasked with providing AnyCompany with access to the required Example Corp. IAM resources. The Engineer has created an IAM role and granted permission to AnyCompany's IAM account to assume this role.
When customers contact AnyCompany, they provide their role ARN for validation. The Engineer is concerned that one of AnyCompany's other customers might deduce Example Corp.'s role ARN and potentially compromise the company's account.
What steps should the Engineer perform to prevent this outcome?

A. Create an IAM user and generate a set of long-term credential
B. Provide the credentials to AnyCompany.Monitor access in IAM access advisor and plan to rotate credentials on a recurring basis.
C. Request an external ID from AnyCompany and add a condition with sts:Externald to the role's trust policy.
D. Require two-factor authentication by adding a condition to the role's trust policy with IAM:MultiFactorAuthPresent.
E. Request an IP range from AnyCompany and add a condition with IAM:SourceIp to the role's trust policy.

Answer: B

NEW QUESTION 163
- (Exam Topic 2)
A company has contracted with a third party to audit several IAM accounts. To enable the audit, cross-account IAM roles have been created in each account targeted for audit. The Auditor is having trouble accessing some of the accounts.
Which of the following may be causing this problem? (Choose three.)

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

Answer: ACF

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

NEW QUESTION 165
- (Exam Topic 2)
A Security Engineer is building a Java application that is running on Amazon EC2. The application communicates with an Amazon RDS instance and authenticates with a user name and password.
Which combination of steps can the Engineer take to protect the credentials and minimize downtime when the credentials are rotated? (Choose two.)

A. Have a Database Administrator encrypt the credentials and store the ciphertext in Amazon S3. Grant permission to the instance role associated with the EC2 instance to read the object and decrypt the ciphertext.
B. Configure a scheduled job that updates the credential in IAM Systems Manager Parameter Store and notifies the Engineer that the application needs to be restarted.

C. Configure automatic rotation of credentials in IAM Secrets Manager.
D. Store the credential in an encrypted string parameter in IAM Systems Manager Parameter Stor
E. Grant permission to the instance role associated with the EC2 instance to access the parameter and the IAM KMS key that is used to encrypt it.
F. Configure the Java application to catch a connection failure and make a call to IAM Secrets Manager to retrieve updated credentials when the password is rotate
G. Grant permission to the instance role associated with the EC2 instance to access Secrets Manager.

Answer: CE

NEW QUESTION 166
- (Exam Topic 2)
A Security Engineer must add additional protection to a legacy web application by adding the following HTTP security headers:
-Content Security-Policy
-X-Frame-Options
-X-XSS-Protection
The Engineer does not have access to the source code of the legacy web application. Which of the following approaches would meet this requirement?

A. Configure an Amazon Route 53 routing policy to send all web traffic that does not include the required headers to a black hole.
B. Implement an IAM Lambda@Edge origin response function that inserts the required headers.
C. Migrate the legacy application to an Amazon S3 static website and front it with an Amazon CloudFront distribution.
D. Construct an IAM WAF rule to replace existing HTTP headers with the required security headers by using regular expressions.

Answer: B

NEW QUESTION 170
- (Exam Topic 2)
A company uses IAM Organization to manage 50 IAM accounts. The finance staff members log in as IAM IAM users in the FinanceDept IAM account. The staff members need to read the consolidated billing information in the MasterPayer IAM account. They should not be able to view any other resources in the MasterPayer IAM account. IAM access to billing has been enabled in the MasterPayer account.
Which of the following approaches grants the finance staff the permissions they require without granting any unnecessary permissions?

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

Answer: D

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

NEW QUESTION 175
- (Exam Topic 2)
During a security event, it is discovered that some Amazon EC2 instances have not been sending Amazon CloudWatch logs.
Which steps can the Security Engineer take to troubleshoot this issue? (Select two.)

A. Connect to the EC2 instances that are not sending the appropriate logs and verify that the CloudWatch Logs agent is running.
B. Log in to the IAM account and select CloudWatch Log
C. Check for any monitored EC2 instances that are in the “Alerting” state and restart them using the EC2 console.
D. Verify that the EC2 instances have a route to the public IAM API endpoints.
E. Connect to the EC2 instances that are not sending log
F. Use the command prompt to verify that the right permissions have been set for the Amazon SNS topic.
G. Verify that the network access control lists and security groups of the EC2 instances have the access to send logs over SNMP.

Answer: AC

Explanation:
https://docs.IAM.amazon.com/AmazonCloudWatch/latest/monitoring/cloudwatch-and-interface-VPC.html

NEW QUESTION 178
- (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 IAM 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 IAM 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 IAM 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 IAM 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 IAM account per region. https://docs.IAM.amazon.com/guardduty/latest/ug/guardduty_upload_lists.html

NEW QUESTION 181
- (Exam Topic 2)
Your company has mandated that all calls to the IAM 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 IAM Documentation states the following
IAM KMS is integrated with CloudTrail, a service that captures API calls made by or on behalf of IAM KMS in your IAM account and delivers the log files to an Amazon S3 bucket that you specify. CloudTrail captures
API calls from the IAM KMS console or from the IAM 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.IAM.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 185
- (Exam Topic 2)
A corporate cloud security policy states that communications between the company's VPC and KMS must travel entirely within the IAM network and not use public service endpoints.
Which combination of the following actions MOST satisfies this requirement? (Choose two.)

A. Add the IAM:sourceVpce condition to the IAM KMS key policy referencing the company's VPC endpoint ID.
B. Remove the VPC internet gateway from the VPC and add a virtual private gateway to the VPC to prevent direct, public internet connectivity.
C. Create a VPC endpoint for IAM KMS with private DNS enabled.
D. Use the KMS Import Key feature to securely transfer the IAM KMS key over a VPN.
E. Add the following condition to the IAM KMS key policy: "IAM:SourceIp": "10.0.0.0/16".

Answer: AC

Explanation:

An IAM policy can deny access to KMS except through your VPC endpoint with the following condition statement:
"Condition": { "StringNotEquals": {
"IAM:sourceVpce": "vpce-0295a3caf8414c94a"
}
}
If you select the Enable Private DNS Name option, the standard IAM KMS DNS hostname (https://kms.<region>.amazonIAM.com) resolves to your VPC endpoint.

NEW QUESTION 187
- (Exam Topic 2)
Due to new compliance requirements, a Security Engineer must enable encryption with customer-provided keys on corporate data that is stored in DynamoDB.
The company wants to retain full control of the encryption keys.
Which DynamoDB feature should the Engineer use to achieve compliance'?

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

Answer: D

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

NEW QUESTION 191
- (Exam Topic 2)
A Security Engineer is trying to determine whether the encryption keys used in an IAM service are in compliance with certain regulatory standards.
Which of the following actions should the Engineer perform to get further guidance?

A. Read the IAM Customer Agreement.
B. Use IAM Artifact to access IAM compliance reports.
C. Post the question on the IAM Discussion Forums.

D. Run IAM Config and evaluate the configuration outputs.

Answer: B

Explanation:
https://IAM.amazon.com/artifact/
Third-party auditors assess the security and compliance of IAM Key Management Service as part of multiple IAM compliance programs. These include SOC, PCI, FedRAMP, HIPPA, and others. The compliance document is found in IAM Artifact.

NEW QUESTION 196
- (Exam Topic 2)
A threat assessment has identified a risk whereby an internal employee could exfiltrate sensitive data from production host running inside IAM (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 IAM 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 addressesassociated 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 200
- (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 IAM Documentation mentions the following
You can connect directly to IAM 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 IAM KMS is conducted entirely within the IAM 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 IAM.
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.IAM.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 203
- (Exam Topic 2)
You are deivising a policy to allow users to have the ability to access objects in a bucket called appbucket. You define the below custom bucket policy

```
{ "ID": "Policy1502987489630",
"Version": "2012-10-17",
"Statement": [
{
"Sid": "Stmt1502987487640",
"Action": [
"s3:GetObject",
"s3:GetObjectVersion"
],
"Effect": "Allow",
"Resource": "arn:aws:s3:::appbucket",
"Principal": "*"
}
]
}
```

But when you try to apply the policy you get the error "Action does not apply to any resource(s) in statement." What should be done to rectify the error
Please select:

A. Change the IAM permissions by applying PutBucketPolicy permissions.

B. Verify that the policy has the same name as the bucket nam
C. If no
D. make it the same.
E. Change the Resource section to "arn:IAM:s3:::appbucket/*'.
F. Create the bucket "appbucket" and then apply the policy.

Answer: C

Explanation:
When you define access to objects in a bucket you need to ensure that you specify to which objects in the bucket access needs to be given to. In this case, the * can be used to assign the permission to all objects in the bucket
Option A is invalid because the right permissions are already provided as per the question requirement Option B is invalid because it is not necessary that the policy has the same name as the bucket
Option D is invalid because this should be the default flow for applying the policy For more information on bucket policies please visit the below URL: https://docs.IAM.amazon.com/AmazonS3/latest/dev/example-bucket-policies.htmll
The correct answer is: Change the Resource section to "arn:IAM:s3:::appbucket/" Submit your Feedback/Queries to our Experts

NEW QUESTION 205
- (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. IAM CloudHSM
C. Amazon DynamoDB with server-side encryption
D. IAM Systems Manager Parameter Store

Answer: B

NEW QUESTION 208
- (Exam Topic 2)
A company has five IAM accounts and wants to use IAM 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 IAM 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 IAM 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 IAM Key Management Service

Answer: ACE

Explanation:
https://docs.IAM.amazon.com/IAMcloudtrail/latest/userguide/best-practices-security.html
If you have created an organization in IAM Organizations, you can create a trail that will log all events for all IAM 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 IAM Organizations, see Organizations Terminology and Concepts. Note Reference: https://docs.IAM.amazon.com/IAMcloudtrail/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 209
- (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 IAM 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 IAM Support to recover the S3 encrypted data.
D. Make a request to IAM Support to restore the deleted CMK, and use it to recover the data.

Answer: A

Explanation:
https://docs.IAM.amazon.com/kms/latest/developerguide/deleting-keys.html#deleting-keys-how-it-works

NEW QUESTION 210

- (Exam Topic 2)
A security alert has been raised for an Amazon EC2 instance in a customer account that is exhibiting strange behavior. The Security Engineer must first isolate the EC2 instance and then use tools for further investigation.
What should the Security Engineer use to isolate and research this event? (Choose three.)

A. IAM CloudTrail
B. Amazon Athena
C. IAM Key Management Service (IAM KMS)
D. VPC Flow Logs
E. IAM Firewall Manager
F. Security groups

Answer: ADF

Explanation:
https://github.com/IAMlabs/aws-well-architected-labs/blob/master/Security/300_Incident_Response_with_IAM

NEW QUESTION 211
- (Exam Topic 2)
A water utility company uses a number of Amazon EC2 instances to manage updates to a fleet of 2,000 Internet of Things (IoT) field devices that monitor water quality. These devices each have unique access credentials.
An operational safety policy requires that access to specific credentials is independently auditable. What is the MOST cost-effective way to manage the storage of credentials?

A. Use IAM Systems Manager to store the credentials as Secure Strings Parameter
B. Secure by using an IAM KMS key.
C. Use IAM Key Management System to store a master key, which is used to encrypt the credential
D. The encrypted credentials are stored in an Amazon RDS instance.
E. Use IAM Secrets Manager to store the credentials.
F. Store the credentials in a JSON file on Amazon S3 with server-side encryption.

Answer: A

Explanation:
https://docs.IAM.amazon.com/systems-manager/latest/userguide/parameter-store-advanced-parameters.html

NEW QUESTION 212
- (Exam Topic 2)
An Amazon EC2 instance is part of an EC2 Auto Scaling group that is behind an Application Load Balancer (ALB). It is suspected that the EC2 instance has been compromised.
Which steps should be taken to investigate the suspected compromise? (Choose three.)

A. Detach the elastic network interface from the EC2 instance.
B. Initiate an Amazon Elastic Block Store volume snapshot of all volumes on the EC2 instance.
C. Disable any Amazon Route 53 health checks associated with the EC2 instance.
D. De-register the EC2 instance from the ALB and detach it from the Auto Scaling group.
E. Attach a security group that has restrictive ingress and egress rules to the EC2 instance.
F. Add a rule to an IAM WAF to block access to the EC2 instance.

Answer: BDE

Explanation:
https://d1.IAMstatic.com/whitepapers/IAM_security_incident_response.pdf

NEW QUESTION 217
- (Exam Topic 2)
An organization is moving non-business-critical applications to IAM while maintaining a mission-critical application in an on-premises data center. An on-premises application must share limited confidential information with the applications in IAM. The internet performance is unpredictable.
Which configuration will ensure continued connectivity between sites MOST securely?

A. VPN and a cached storage gateway
B. IAM Snowball Edge
C. VPN Gateway over IAM Direct Connect
D. IAM Direct Connect

Answer: C

Explanation:
https://docs.IAM.amazon.com/whitepapers/latest/IAM-vpc-connectivity-options/IAM-direct-connect-plus-vpn-n

NEW QUESTION 221
- (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. IAM Access keys
D. IAM SDK keys

Answer: B

Explanation:
The IAM 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 IAM 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 IAM Security credentials, please visit the below URL: https://docs.IAM.amazon.com/eeneral/latest/er/IAM-sec-cred-types.html
The correct answer is: Key pairs
Submit your Feedback/Queries to our Experts

NEW QUESTION 224
- (Exam Topic 2)
An Amazon S3 bucket is encrypted using an IAM KMS CMK. An IAM user is unable to download objects from the S3 bucket using the IAM Management Console; however, other users can download objects from the S3 bucket.
Which policies should the Security Engineer review and modify to resolve this issue? (Select three.)

A. The CMK policy
B. The VPC endpoint policy
C. The S3 bucket policy
D. The S3 ACL
E. The IAM policy

Answer: ACE

Explanation:
https://IAM.amazon.com/premiumsupport/knowledge-center/decrypt-kms-encrypted-objects-s3/

NEW QUESTION 228
- (Exam Topic 2)
An application has a requirement to be resilient across not only Availability Zones within the application's primary region but also be available within another region altogether.
Which of the following supports this requirement for IAM resources that are encrypted by IAM KMS?

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

Answer: C

NEW QUESTION 231
- (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 IAM 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 IAM principals from their own IAM 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 IAM accounts by using IAM roles to manage key acces
H. Programmatically update the IAM trust policy to manage cross-account vendor access.

Answer: A

NEW QUESTION 234
- (Exam Topic 2)
The Security Engineer is managing a web application that processes highly sensitive personal information. The application runs on Amazon EC2. The application has strict compliance requirements, which instruct that all incoming traffic to the application is protected from common web exploits and that all outgoing traffic from the EC2 instances is restricted to specific whitelisted URLs.
Which architecture should the Security Engineer use to meet these requirements?

A. Use IAM Shield to scan inbound traffic for web exploit
B. Use VPC Flow Logs and IAM Lambda to restrict egress traffic to specific whitelisted URLs.
C. Use IAM Shield to scan inbound traffic for web exploit
D. Use a third-party IAM Marketplace solution to restrict egress traffic to specific whitelisted URLs.
E. Use IAM WAF to scan inbound traffic for web exploit
F. Use VPC Flow Logs and IAM Lambda to restrict egress traffic to specific whitelisted URLs.
G. Use IAM WAF to scan inbound traffic for web exploit
H. Use a third-party IAM Marketplace solution to restrict egress traffic to specific whitelisted URLs.

Answer: D

Explanation:
IAM Shield is mainly for DDos Attacks.IAM WAF is mainly for some other types of attacks like Injection and XSS etcIn this scenario, It seems it is WAF functionality that is needed.VPC logs do show the source and destination IP and Port , they never show any URL .. because URL are level 7 while VPC are concerned about lover network levels.
https://docs.IAM.amazon.com/vpc/latest/userguide/flow-logs.html

NEW QUESTION 238
- (Exam Topic 2)
A Security Engineer has created an Amazon CloudWatch event that invokes an IAM Lambda function daily. The Lambda function runs an Amazon Athena query that checks IAM CloudTrail logs in Amazon S3 to detect whether any IAM user accounts or credentials have been created in the past 30 days. The results of the Athena query are created in the same S3 bucket. The Engineer runs a test execution of the Lambda function via the IAM Console, and the function runs successfully.
After several minutes, the Engineer finds that his Athena query has failed with the error message: “Insufficient Permissions”. The IAM permissions of the Security Engineer and the Lambda function are shown below:
Security Engineer

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:*",
                "iam:*",
                "lambda:*",
                "athena:Get*",
                "athena:List*",
                "cloudwatch:*"
            ],
            "Resource": "*"
        }
    ]
}
```

Lambda function execution role

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "athena:*",
                "cloudwatch:*"
            ],
            "Resource": "*"
        }
    ]
}
```

What is causing the error?

A. The Lambda function does not have permissions to start the Athena query execution.
B. The Security Engineer does not have permissions to start the Athena query execution.
C. The Athena service does not support invocation through Lambda.
D. The Lambda function does not have permissions to access the CloudTrail S3 bucket.

Answer: D

NEW QUESTION 242
- (Exam Topic 2)
A company’s database developer has just migrated an Amazon RDS database credential to be stored and managed by IAM Secrets Manager. The developer has also enabled rotation of the credential within the Secrets Manager console and set the rotation to change every 30 days.
After a short period of time, a number of existing applications have failed with authentication errors. What is the MOST likely cause of the authentication errors?

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

Answer: B

Explanation:
https://docs.IAM.amazon.com/secretsmanager/latest/userguide/enable-rotation-rds.html

NEW QUESTION 246
- (Exam Topic 2)
An application makes calls to IAM services using the IAM SDK. The application runs on Amazon EC2 instances with an associated IAM role. When the application attempts to access an object within an Amazon S3 bucket; the Administrator receives the following error message: HTTP 403: Access Denied.
Which combination of steps should the Administrator take to troubleshoot this issue? (Select three.)

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

Answer: BCE

NEW QUESTION 247
- (Exam Topic 2)
A Systems Administrator has written the following Amazon S3 bucket policy designed to allow access to an S3 bucket for only an authorized IAM IAM user from the IP address range 10.10.10.0/24:

```
{
  "Version": "2012-10-17",
  "Id": "S3Policy1",
  "Statement": [
  {
   "Sid": ["OfficeAllowIP"],
   "Effect": ["Allow"],
   "Principal": ["*"],
   "Action": ["s3:*"],
   "Resource": ["arn:aws:s3:::Bucket"],
   "Condition": {
     "IpAddress": [
        {"aws: SourceIp": "10.10.10.0/24"}
      ]
     }
   }]
}
```

When trying to download an object from the S3 bucket from 10.10.10.40, the IAM user receives an access denied message.
What does the Administrator need to change to grant access to the user?

A. Change the "Resource" from "arn: IAM:s3:::Bucket" to "arn:IAM:s3:::Bucket/*".
B. Change the "Principal" from "*" to {IAM:"arn:IAM:iam: : account-number: user/username"}
C. Change the "Version" from "2012-10-17" to the last revised date of the policy
D. Change the "Action" from ["s3:*"] to ["s3:GetObject", "s3:ListBucket"]

Answer: A

NEW QUESTION 250
- (Exam Topic 2)
A security team is responsible for reviewing IAM 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 IAM regions.
What is the SIMPLEST way to meet these requirements?

A. Enable IAM Trusted Advisor security checks in the IAM Console, and report all security incidents for all regions.
B. Enable IAM CloudTrail by creating individual trails for each region, and specify a single Amazon S3 bucket to receive log files for later analysis.
C. Enable IAM 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 IAM services across all regions, and aggregate them to a single Amazon S3 bucket for later analysis.

Answer: C

Explanation:
https://docs.IAM.amazon.com/IAMcloudtrail/latest/userguide/creating-trail-organization.html

NEW QUESTION 251
- (Exam Topic 2)
An application has been built with Amazon EC2 instances that retrieve messages from Amazon SQS. Recently, IAM changes were made and the instances can no longer retrieve messages.
What actions should be taken to troubleshoot the issue while maintaining least privilege. (Select two.)

A. Configure and assign an MFA device to the role used by the instances.
B. Verify that the SQS resource policy does not explicitly deny access to the role used by the instances.
C. Verify that the access key attached to the role used by the instances is active.

D. Attach the AmazonSQSFullAccess managed policy to the role used by the instances.
E. Verify that the role attached to the instances contains policies that allow access to the queue.

Answer: BE

NEW QUESTION 255
- (Exam Topic 2)
Which of the following is not a best practice for carrying out a security audit? Please select:

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

Answer: A

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

NEW QUESTION 258
- (Exam Topic 2)
While analyzing a company's security solution, a Security Engineer wants to secure the IAM 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 IAM accoun
B. Delete the password for the IAM account root user.
C. Create a new IAM user that has administrator permissions in the IAM accoun
D. Modify the permissions for the existing IAM users.
E. Replace the access key for the IAM account root use
F. Delete the password for the IAM account root user.
G. Create a new IAM user that has administrator permissions in the IAM accoun
H. Enable multi-factor authentication for the IAM 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 261
- (Exam Topic 2)
A company has complex connectivity rules governing ingress, egress, and communications between Amazon EC2 instances. The rules are so complex that they cannot be implemented within the limits of the maximum number of security groups and network access control lists (network ACLs).
What mechanism will allow the company to implement all required network rules without incurring additional cost?

A. Configure IAM WAF rules to implement the required rules.
B. Use the operating system built-in, host-based firewall to implement the required rules.
C. Use a NAT gateway to control ingress and egress according to the requirements.
D. Launch an EC2-based firewall product from the IAM Marketplace, and implement the required rules in that product.

Answer: B

NEW QUESTION 262
- (Exam Topic 2)
A company will store sensitive documents in three Amazon S3 buckets based on a data classification scheme of “Sensitive,” “Confidential,” and “Restricted.”
The security solution must meet all of the following
requirements:
- Each object must be encrypted using a unique key.
- Items that are stored in the “Restricted” bucket require two-factor authentication for decryption.
- IAM KMS must automatically rotate encryption keys annually.

Which of the following meets these requirements?

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

G. S3 can then create DEK grants to uniquely encrypt each object within the S3 bucket.
H. Create a CMK with unique imported key material for each data classification type, and rotate them annuall
I. For the “Restricted” key material, define the MFA policy in the key polic
J. Use S3 SSE-KMS to encrypt the objects.

Answer: A

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

NEW QUESTION 265
- (Exam Topic 2)
You have a vendor that needs access to an IAM resource. You create an IAM user account. You want to restrict access to the resource using a policy for just that user over a brief period. Which of the following would be an ideal policy to use?
Please select:

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

Answer: B

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

NEW QUESTION 267
- (Exam Topic 3)
Your company has a set of EBS volumes defined in IAM. The security mandate is that all EBS volumes are encrypted. What can be done to notify the IT admin staff if there are any unencrypted volumes in the account.
Please select:

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

Answer: B

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

NEW QUESTION 271
- (Exam Topic 3)
Your company makes use of S3 buckets for storing data. There is a company policy that all services should have logging enabled. How can you ensure that logging is always enabled for created S3 buckets in the IAM Account?
Please select:

A. Use IAM Inspector to inspect all S3 buckets and enable logging for those where it is not enabled
B. Use IAM Config Rules to check whether logging is enabled for buckets
C. Use IAM Cloudwatch metrics to check whether logging is enabled for buckets
D. Use IAM Cloudwatch logs to check whether logging is enabled for buckets

Answer: B

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

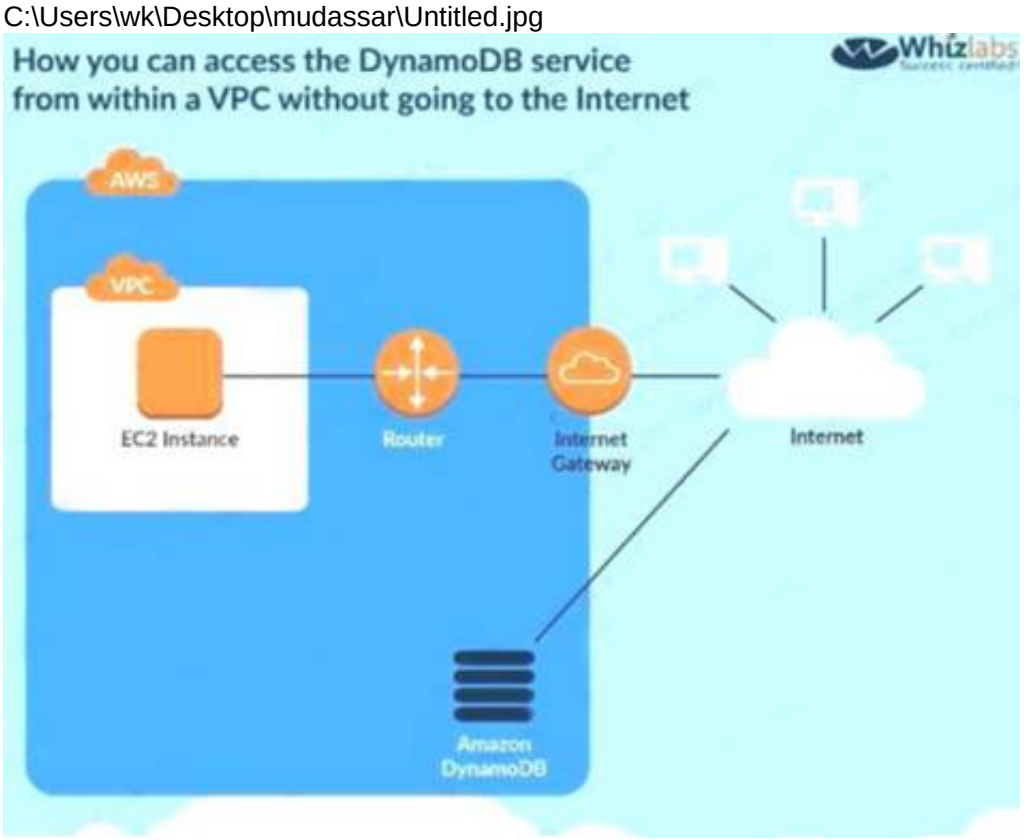
Option C and D are invalid because Cloudwatch cannot be used to check for logging enablement for buckets. For more information on Config Rules please see the below Link:
> https://docs.IAM.amazon.com/config/latest/developerguide/evaluate-config-rules.html
The correct answer is: Use IAM Config Rules to check whether logging is enabled for buckets Submit your Feedback/Queries to our Experts

NEW QUESTION 275
- (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 IAM 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 IAM 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 277
- (Exam Topic 3)
You need to have a requirement to store objects in an S3 bucket with a key that is automatically managed and rotated. Which of the following can be used for this purpose?
Please select:

A. IAM KMS
B. IAM S3 Server side encryption
C. IAM Customer Keys
D. IAM Cloud HSM

Answer: B

Explanation:
The IAM Documentation mentions the following
Server-side encryption protects data at rest. Server-side encryption with Amazon S3-managed encryption keys (SSE-S3) uses strong multi-factor encryption. Amazon S3 encrypts each object with a unique key. As an additional safeguard, it encrypts the key itself with a master key that it rotates regularly. Amazon S3 server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption
Standard (AES-256), to encrypt your data.
All other options are invalid since here you need to ensure the keys are manually rotated since you manage the entire key set Using IAM S3 Server side encryption, IAM will manage the rotation of keys automatically.
For more information on Server side encryption, please visit the following URL:
https://docs.IAM.amazon.com/AmazonS3/latest/dev/UsineServerSideEncryption.htmll
The correct answer is: IAM S3 Server side encryption Submit your Feedback/Queries to our Experts

NEW QUESTION 279
- (Exam Topic 3)
What is the result of the following bucket policy?

```
{
"Statement": [
{
"Sid": "Sid1",
"Action": "s3:*",
"Effect": "Allow",
"Resource": "arn:aws:s3:::mybucket/*.",
"Principal": {
{"AWS": ["arn:aws:iam::111111111:user/mark"]}
}
},
{
"Sid": "Sid2",
"Action": "s3:*",
"Effect": "Deny",
"Resource": "arn:aws:s3:::mybucket/*",
"Principal": {
"AWS": [
"*"
]
}
}
]
}
```

Choose the correct Answer Please select:

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

Answer: C

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

NEW QUESTION 281
- (Exam Topic 3)
You have a set of Keys defined using the IAM KMS service. You want to stop using a couple of keys , but are not sure of which services are currently using the keys. Which of the following would be a safe option to stop using the keys from further usage.
Please select:

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

Answer: B

Explanation:
Option A is invalid because once you schedule the deletion and waiting period ends, you cannot come back from the deletion process.
Option C and D are invalid because these will not check to see if the keys are being used or not The IAM Documentation mentions the following
Deleting a customer master key (CMK) in IAM Key Management Service (IAM KMS) is destructive and potentially dangerous. It deletes the key material and all metadata associated with the CMK, and is irreversible. After a CMK is deleted you can no longer decrypt the data that was encrypted under that CMK, which means that data becomes unrecoverable. You should delete a CMK only when you are sure that you don't need to use it anymore. If you are not sure, consider disabling the CMK instead of deleting it. You can re-enable a disabled CMK if you need to use it again later, but you cannot recover a deleted CMK.
For more information on deleting keys from KMS, please visit the below URL: https://docs.IAM.amazon.com/kms/latest/developereuide/deleting-keys.html
The correct answer is: Disable the keys Submit your Feedback/Queries to our Experts

NEW QUESTION 282
- (Exam Topic 3)
A company is using a Redshift cluster to store their data warehouse. There is a requirement from the Internal IT Security team to ensure that data gets encrypted for the Redshift database. How can this be achieved?
Please select:

A. Encrypt the EBS volumes of the underlying EC2 Instances
B. Use IAM KMS Customer Default master key
C. Use SSL/TLS for encrypting the data
D. Use S3 Encryption

Answer: B

Explanation:
The IAM Documentation mentions the following
Amazon Redshift uses a hierarchy of encryption keys to encrypt the database. You can use either IAM Key Management Servic (IAM KMS) or a hardware security module (HSM) to manage the top-level encryption keys in this hierarchy. The process that Amazon Redshift uses for encryption differs depending on how you manage keys.
Option A is invalid because its the cluster that needs to be encrypted
Option C is invalid because this encrypts objects in transit and not objects at rest Option D is invalid because this is used only for objects in S3 buckets
For more information on Redshift encryption, please visit the following URL: https://docs.IAM.amazon.com/redshift/latest/memt/workine-with-db-encryption.htmll
The correct answer is: Use IAM KMS Customer Default master key Submit your Feedback/Queries to our Experts

NEW QUESTION 287
.....

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-C02 Practice Exam Features:

* SCS-C02 Questions and Answers Updated Frequently

* SCS-C02 Practice Questions Verified by Expert Senior Certified Staff

* SCS-C02 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SCS-C02 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year