Amazon-Web-Services

Exam Questions SCS-C02

AWS Certified Security - Specialty

NEW QUESTION 1
- (Exam Topic 1)
A security engineer has created an Amazon Cognito user pool. The engineer needs to manually verify the ID and access token sent by the application for troubleshooting purposes
What is the MOST secure way to accomplish this?

A. Extract the subject (sub), audience (aud), and cognito:username from the ID token payload Manually check the subject and audience for the user name In the user pool
B. Search for the public key with a key ID that matches the key ID In the header of the toke
C. Then use a JSON Web Token (JWT) library to validate the signature of the token and extract values, such as the expiry date
D. Verify that the token is not expire
E. Then use the token_use claim function In Amazon Cognito to validate the key IDs
F. Copy the JSON Web Token (JWT) as a JSON document Obtain the public JSON Web Key (JWK) and convert It to a pem fil
G. Then use the file to validate the original JWT.

Answer: A

NEW QUESTION 2
- (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 3
- (Exam Topic 1)
A company is configuring three Amazon EC2 instances with each instance in a separate Availability Zone. The EC2 instances wilt be used as transparent proxies for outbound internet traffic for ports 80 and 443 so the proxies can block traffic to certain internet destinations as required by the company's security policies. A Security Engineer completed the following:
• Set up the proxy software on the EC2 instances.
• Modified the route tables on the private subnets to use the proxy EC2 instances as the default route.
• Created a security group rule opening inbound port 80 and 443 TCP protocols on the proxy EC2 instance security group.
However, the proxy EC2 instances are not successfully forwarding traffic to the internet.
What should the Security Engineer do to make the proxy EC2 instances route traffic to the internet?

A. Put all the proxy EC2 instances in a cluster placement group.
B. Disable source and destination checks on the proxy EC2 instances.
C. Open all inbound ports on the proxy EC2 instance security group.
D. Change the VPC's DHCP domain-name-server’s options set to the IP addresses of proxy EC2 instances.

Answer: B

NEW QUESTION 4
- (Exam Topic 1)
A security engineer needs to configure monitoring and auditing for IAM Lambda.
Which combination of actions using IAM services should the security engineer take to accomplish this goal? (Select TWO.)

A. Use IAM Config to track configuration changes to Lambda functions, runtime environments, tags, handler names, code sizes, memory allocation, timeout settings, and concurrency settings, along with Lambda IAM execution role, subnet, and security group associations.
B. Use IAM CloudTrail to implement governance, compliance, operational, and risk auditing for Lambda.
C. Use Amazon Inspector to automatically monitor for vulnerabilities and perform governance, compliance, operational, and risk auditing for Lambda.
D. Use IAM Resource Access Manager to track configuration changes to Lambda functions, runtime environments, tags, handler names, code sizes, memory allocation, timeout settings, and concurrency settings, along with Lambda IAM execution role, subnet, and security group associations.
E. Use Amazon Macie to discover, classify, and protect sensitive data being executed inside the Lambda function.

Answer: AB

NEW QUESTION 5
- (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 6
- (Exam Topic 1)
A security engineer is responsible for providing secure access to IAM resources for thousands of developer in a company's corporate identity provider (idp). The developers access a set of IAM services from the corporate premises using IAM credential. Due to the velum of require for provisioning new IAM users, it is taking a long time to grant access permissions. The security engineer receives reports that developer are sharing their IAM credentials with others to avoid provisioning delays. The causes concern about overall security for the security engineer.
Which actions will meet the program requirements that address security?

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

Answer: B

NEW QUESTION 7
- (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 8
- (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 9
- (Exam Topic 1)
A security engineer need to ensure their company's uses of IAM meets IAM security best practices. As part of this, the IAM account root user must not be used for daily work. The root user must be monitored for use, and the Security team must be alerted as quickly as possible if the root user is used.
Which solution meets these requirements?

A. Set up an Amazon CloudWatch Events rule that triggers an Amazon SNS notification.
B. Set up an Amazon CloudWatch Events rule that triggers an Amazon SNS notification logs from S3 and generate notifications using Amazon SNS.
C. Set up a rule in IAM config to trigger root user event
D. Trigger an IAM Lambda function and generate notifications using Amazon SNS.
E. Use Amazon Inspector to monitor the usage of the root user and generate notifications using Amazon SNS

Answer: A

NEW QUESTION 10
- (Exam Topic 1)
A security engineer must develop an encryption tool for a company. The company requires a cryptographic solution that supports the ability to perform cryptographic erasure on all resources protected by the key material in 15 minutes or less
Which IAM Key Management Service (IAM KMS) key solution will allow the security engineer to meet these requirements?

A. Use Imported key material with CMK
B. Use an IAM KMS CMK
C. Use an IAM managed CMK.
D. Use an IAM KMS customer managed CMK

Answer: C

NEW QUESTION 10
- (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 12
- (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 16
- (Exam Topic 1)
A Security Engineer is setting up an IAM CloudTrail trail for all regions in an IAM account. For added security, the logs are stored using server-side encryption with IAM KMS-managed keys (SSE-KMS) and have log integrity validation enabled.
While testing the solution, the Security Engineer discovers that the digest files are readable, but the log files are not. What is the MOST likely cause?

A. The log files fail integrity validation and automatically are marked as unavailable.
B. The KMS key policy does not grant the Security Engineer's IAM user or role permissions to decrypt with it.
C. The bucket is set up to use server-side encryption with Amazon S3-managed keys (SSE-S3) as the default and does not allow SSE-KMS-encrypted files.
D. An IAM policy applicable to the Security Engineer's IAM user or role denies access to the "CloudTrail/" prefix in the Amazon S3 bucket

Answer: B

Explanation:
Enabling server-side encryption encrypts the log files but not the digest files with SSE-KMS. Digest files are encrypted with Amazon S3-managed encryption keys (SSE-S3). https://docs.IAM.amazon.com/IAMcloudtrail/latest/userguide/encrypting-cloudtrail-log-files-with-IAM-kms.htm

NEW QUESTION 19
- (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 23
- (Exam Topic 1)
A Security Engineer has discovered that, although encryption was enabled on the Amazon S3 bucket example bucket, anyone who has access to the bucket has the ability to retrieve the files. The Engineer wants to limit access to each IAM user can access an assigned folder only.
What should the Security Engineer do to achieve this?

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

Answer: B

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

NEW QUESTION 27
- (Exam Topic 1)
A Security Administrator at a university is configuring a fleet of Amazon EC2 instances. The EC2 instances are shared among students, and non-root SSH access is allowed. The Administrator is concerned about students attacking other IAM account resources by using the EC2 instance metadata service.
What can the Administrator do to protect against this potential attack?

A. Disable the EC2 instance metadata service.
B. Log all student SSH interactive session activity.
C. Implement ip tables-based restrictions on the instances.
D. Install the Amazon Inspector agent on the instances.

Answer: A

Explanation:
"To turn off access to instance metadata on an existing instance....." https://docs.IAM.amazon.com/IAMEC2/latest/UserGuide/configuring-instance-metadata-service.html You can disable the service for existing (running or stopped) ec2 instances. https://docs.IAM.amazon.com/cli/latest/reference/ec2/modify-instance-metadata-options.html

NEW QUESTION 30
- (Exam Topic 1)
A company has several workloads running on IAM. Employees are required to authenticate using on-premises ADFS and SSO to access the IAM Management Console. Developers migrated an existing legacy web application to an Amazon EC2 instance. Employees need to access this application from anywhere on the internet, but currently, there is no authentication system built into the application.
How should the Security Engineer implement employee-only access to this system without changing the application?

A. Place the application behind an Application Load Balancer (ALB). Use Amazon Cognito as authentication for the AL
B. Define a SAML-based Amazon Cognito user pool and connect it to ADFS.
C. Implement IAM SSO in the master account and link it to ADFS as an identity provide
D. Define the EC2 instance as a managed resource, then apply an IAM policy on the resource.
E. Define an Amazon Cognito identity pool, then install the connector on the Active Directory serve
F. Use the Amazon Cognito SDK on the application instance to authenticate the employees using their Active Directory user names and passwords.
G. Create an IAM Lambda custom authorizer as the authenticator for a reverse proxy on Amazon EC2.Ensure the security group on Amazon EC2 only allows access from the Lambda function.

Answer: A

Explanation:
https://docs.IAM.amazon.com/elasticloadbalancing/latest/application/listener-authenticate-users.html
- Authenticate users through social IdPs, such as Amazon, Facebook, or Google, through the user pools supported by Amazon Cognito.
- Authenticate users through corporate identities, using SAML, LDAP, or Microsoft AD, through the user pools supported by Amazon Cognito.

NEW QUESTION 33
- (Exam Topic 1)
A company has the software development teams that are creating applications that store sensitive data in Amazon S3 Each team's data must always be separate. The company's security team must design a data encryption strategy for both teams that provides the ability to audit key usage. The solution must also minimize operational overhead
what should me security team recommend?

A. Tell the application teams to use two different S3 buckets with separate IAM Key Management Service (IAM KMS) IAM managed CMKs Limit the key process to allow encryption and decryption of the CMKs to their respective teams onl
B. Force the teams to use encryption context to encrypt and decrypt
C. Tell the application teams to use two different S3 buckets with a single IAM Key Management Service (IAM KMS) IAM managed CMK Limit the key policy to allow encryption and decryption of the CMK onl
D. Do not allow the teams to use encryption context to encrypt and decrypt
E. Tell the application teams to use two different S3 buckets with separate IAM Key Management Service (IAM KMS) customer managed CMKs Limit the key policies to allow encryption and decryption of the CMKs to their respective teams only Force the teams to use encryption context to encrypt and decrypt
F. Tell the application teams to use two different S3 buckets with a single IAM Key Management Service (IAM KMS) customer managed CMK Limit the key policy to allow encryption and decryption of the CMK only Do not allow the teams to use encryption context to encrypt and decrypt

Answer: A

NEW QUESTION 36
- (Exam Topic 1)
A company's Security Officer is concerned about the risk of IAM account root user logins and has assigned a Security Engineer to implement a notification solution for near-real-time alerts upon account root user logins.
How should the Security Engineer meet these requirements?

A. Create a cron job that runs a script lo download the IAM IAM security credentials W
B. parse the file for account root user logins and email the Security team's distribution 1st
C. Run IAM CloudTrail logs through Amazon CloudWatch Events to detect account roo4 user logins and trigger an IAM Lambda function to send an Amazon SNS notification to the Security team's distribution list.
D. Save IAM CloudTrail logs to an Amazon S3 bucket in the Security team's account Process the CloudTrail logs with the Security Engineer's logging solution for account root user logins Send an Amazon SNS notification to the Security team upon encountering the account root user login events
E. Save VPC Plow Logs to an Amazon S3 bucket in the Security team's account and process the VPC Flow Logs with their logging solutions for account root user logins Send an Amazon SNS notification to the Security team upon encountering the account root user login events

Answer: B

NEW QUESTION 38
- (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 40
- (Exam Topic 1)
A company has an IAM account and allows a third-party contractor who uses another IAM account, to assume certain IAM roles. The company wants to ensure that IAM roles can be assumed by the contractor only if the contractor has multi-factor authentication enabled on their IAM user accounts
What should the company do to accomplish this?
A)

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

B)

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

C)

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

D)

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

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

Answer: A

NEW QUESTION 44
- (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 48
- (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 52
- (Exam Topic 1)
A company's security information events management (SIEM) tool receives new IAM CloudTrail logs from an Amazon S3 bucket that is configured to send all object created event notification to an Amazon SNS topic An Amazon SQS queue is subscribed to this SNS topic. The company's SEM tool then ports this SQS queue for new messages using an IAM role and fetches new log events from the S3 bucket based on the SQS messages.
After a recent security review that resulted m restricted permissions, the SEM tool has stopped receiving new CloudTral logs
Which of the following are possible causes of this issue? (Select THREE)

A. The SOS queue does not allow the SQS SendMessage action from the SNS topic
B. The SNS topic does not allow the SNS Publish action from Amazon S3
C. The SNS topic is not delivering raw messages to the SQS queue
D. The S3 bucket policy does not allow CloudTrail to perform the PutObject action
E. The IAM role used by the 5EM tool does not have permission to subscribe to the SNS topic
F. The IAM role used by the SEM tool does not allow the SQS DeleteMessage action.

Answer: ADF

NEW QUESTION 57
- (Exam Topic 1)
A company has decided to use encryption in its IAM account to secure the objects in Amazon S3 using server-side encryption. Object sizes range from 16.000 B to 5 MB. The requirements are as follows:
• The key material must be generated and stored in a certified Federal Information Processing Standard (FIPS) 140-2 Level 3 machine.
• The key material must be available in multiple Regions. Which option meets these requirements?

A. Use an IAM KMS customer managed key and store the key material in IAM with replication across Regions
B. Use an IAM customer managed key, import the key material into IAM KMS using in-house IAM CloudHS
C. and store the key material securely in Amazon S3.
D. Use an IAM KMS custom key store backed by IAM CloudHSM clusters, and copy backups across Regions
E. Use IAM CloudHSM to generate the key material and backup keys across Regions Use the Java Cryptography Extension (JCE) and Public Key Cryptography Standards #11 (PKCS #11) encryption libraries to encrypt and decrypt the data.

Answer: D

NEW QUESTION 59
- (Exam Topic 1)
A Security Engineer is setting up a new IAM account. The Engineer has been asked to continuously monitor the company's IAM account using automated compliance checks based on IAM best practices and Center for Internet Security (CIS) IAM Foundations Benchmarks
How can the Security Engineer accomplish this using IAM services?

A. Enable IAM Config and set it to record all resources in all Regions and global resource
B. Then enable IAM Security Hub and confirm that the CIS IAM Foundations compliance standard is enabled
C. Enable Amazon Inspector and configure it to scan all Regions for the CIS IAM Foundations Benchmark
D. Then enable IAM Security Hub and configure it to ingest theAmazon Inspector findings
E. Enable Amazon Inspector and configure it to scan all Regions for the CIS IAM Foundations Benchmark
F. Then enable IAM Shield in all Regions to protect the account from DDoS attacks.
G. Enable IAM Config and set it to record all resources in all Regions and global resources Then enable Amazon Inspector and configure it to enforce CIS IAM Foundations Benchmarks using IAM Config rules.

Answer: A

Explanation:
https://docs.IAM.amazon.com/securityhub/latest/userguide/securityhub-standards-cis-config-resources.html

NEW QUESTION 60
- (Exam Topic 1)
A security engineer is auditing a production system and discovers several additional IAM roles that are not required and were not previously documented during the last audit 90 days ago. The engineer is trying to find out who created these IAM roles and when they were created. The solution must have the lowest operational overhead.
Which solution will meet this requirement?

A. Import IAM CloudTrail logs from Amazon S3 into an Amazon Elasticsearch Service cluster, and search through the combined logs for CreateRole events.
B. Create a table in Amazon Athena for IAM CloudTrail event
C. Query the table in Amazon Athena for CreateRole events.
D. Use IAM Config to look up the configuration timeline for the additional IAM roles and view the linked IAM CloudTrail event.
E. Download the credentials report from the IAM console to view the details for each IAM entity, including the creation dates.

Answer: A

NEW QUESTION 62
- (Exam Topic 2)
The Security Engineer created a new IAM Key Management Service (IAM KMS) key with the following key policy:

```
{
    "Effect": "Allow",
    "Principal": {"AWS": "arn:aws:iam::111122223333:root"),
    "Action": "kms:*";
    "Resource": "*"
 }
```

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

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

Answer: AC

Explanation:
Giving the IAM account full access to the CMK does this; it enables you to use IAM policies to give IAM users and roles in the account access to the CMK. It does not by itself give any IAM users or roles access to the CMK, but it enables you to use IAM policies to do so.
https://docs.IAM.amazon.com/kms/latest/developerguide/key-policies.html#key-policy-default-allow-root-enabl

NEW QUESTION 64
- (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 68
- (Exam Topic 2)
A company plans to migrate a sensitive dataset to Amazon S3. A Security Engineer must ensure that the data is encrypted at rest. The encryption solution must enable the company to generate its own keys without needing to manage key storage or the encryption process.
What should the Security Engineer use to accomplish this?

A. Server-side encryption with Amazon S3-managed keys (SSE-S3)
B. Server-side encryption with IAM KMS-managed keys (SSE-KMS)
C. Server-side encryption with customer-provided keys (SSE-C)
D. Client-side encryption with an IAM KMS-managed CMK

Answer: B

Explanation:
Reference https://IAM.amazon.com/s3/faqs/

NEW QUESTION 72
- (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 75
- (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 76
- (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 79
- (Exam Topic 2)
A company's security policy requires that VPC Flow Logs are enabled on all VPCs. A Security Engineer is looking to automate the process of auditing the VPC resources for compliance.
What combination of actions should the Engineer take? (Choose two.)

A. Create an IAM Lambda function that determines whether Flow Logs are enabled for a given VPC.
B. Create an IAM Config configuration item for each VPC in the company IAM account.
C. Create an IAM Config managed rule with a resource type of IAM:: Lambda:: Function.
D. Create an Amazon CloudWatch Event rule that triggers on events emitted by IAM Config.
E. Create an IAM Config custom rule, and associate it with an IAM Lambda function that contains the evaluating logic.

Answer: AE

Explanation:
https://medium.com/mudita-misra/how-to-audit-your-aws-resources-for-security-compliance-by-using-custom-I

NEW QUESTION 84
- (Exam Topic 2)
The Information Technology department has stopped using Classic Load Balancers and switched to Application Load Balancers to save costs. After the switch, some users on older devices are no longer able to connect to the website.
What is causing this situation?

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

Answer: D

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

NEW QUESTION 86
- (Exam Topic 2)
A Security Engineer is implementing a solution to allow users to seamlessly encrypt Amazon S3 objects without having to touch the keys directly. The solution must be highly scalable without requiring continual management. Additionally, the organization must be able to immediately delete the encryption keys.
Which solution meets these requirements?

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

Answer: B

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

NEW QUESTION 90
- (Exam Topic 2)
An Amazon EC2 instance is denied access to a newly created IAM KMS CMK used for decrypt actions. The environment has the following configuration:
- The instance is allowed the kms:Decrypt action in its IAM role for all resources
- The IAM KMS CMK status is set to enabled
- The instance can communicate with the KMS API using a configured VPC endpoint What is causing the issue?

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

Answer: D

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

NEW QUESTION 94
- (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 98
- (Exam Topic 2)
You have enabled Cloudtrail logs for your company's IAM account. In addition, the IT Security department has mentioned that the logs need to be encrypted. How can this be achieved?
Please select:

A. Enable SSL certificates for the Cloudtrail logs
B. There is no need to do anything since the logs will already be encrypted
C. Enable Server side encryption for the trail
D. Enable Server side encryption for the destination S3 bucket

Answer: B

Explanation:
The IAM Documentation mentions the following.
By default CloudTrail event log files are encrypted using Amazon S3 server-side encryption (SSE). You can also choose to encryption your log files with an IAM Key Management Service (IAM KMS) key. You can store your log files in your bucket for as long as you want. You can also define Amazon S3 lifecycle rules to archive or delete log files automatically. If you want notifications about lo file delivery and validation, you can set up Amazon SNS notifications.
Option A.C and D are not valid since logs will already be encrypted
For more information on how Cloudtrail works, please visit the following URL: https://docs.IAM.amazon.com/IAMcloudtrail/latest/usereuide/how-cloudtrail-works.htmll
The correct answer is: There is no need to do anything since the logs will already be encrypted
Submit your Feedback/Queries to our Experts

NEW QUESTION 101
- (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 104
- (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 108
- (Exam Topic 2)
Your company has a set of resources defined in the IAM Cloud. Their IT audit department has requested to get a list of resources that have been defined across the account. How can this be achieved in the easiest manner?
Please select:

A. Create a powershell script using the IAM CL
B. Query for all resources with the tag of production.
C. Create a bash shell script with the IAM CL
D. Query for all resources in all region
E. Store the results in an S3 bucket.
F. Use Cloud Trail to get the list of all resources
G. Use IAM Config to get the list of all resources

Answer: D

Explanation:
The most feasible option is to use IAM Config. When you turn on IAM Config, you will get a list of resources defined in your IAM Account.
A sample snapshot of the resources dashboard in IAM Config is shown below C:\Users\wk\Desktop\mudassar\Untitled.jpg

Option A is incorrect because this would give the list of production based resources and now all resources Option B is partially correct But this will just add more maintenance overhead.
Option C is incorrect because this can be used to log API activities but not give an account of all resou For more information on IAM Config, please visit the below URL: https://docs.IAM.amazon.com/config/latest/developereuide/how-does-confie-work.html
The correct answer is: Use IAM Config to get the list of all resources
Submit your Feedback/Queries to our Experts

NEW QUESTION 112
- (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 113
- (Exam Topic 2)
A company uses user data scripts that contain sensitive information to bootstrap Amazon EC2 instances. A Security Engineer discovers that this sensitive information is viewable by people who should not have access to it.
What is the MOST secure way to protect the sensitive information used to bootstrap the instances?

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

Answer: B

NEW QUESTION 114
- (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 119
- (Exam Topic 2)
A Systems Engineer has been tasked with configuring outbound mail through Simple Email Service (SES) and requires compliance with current TLS standards. The mail application should be configured to connect to which of the following endpoints and corresponding ports?

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

Answer: C

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

NEW QUESTION 123
- (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 124
- (Exam Topic 2)
An IAM Lambda function was misused to alter data, and a Security Engineer must identify who invoked the function and what output was produced. The Engineer cannot find any logs created by the Lambda function in Amazon CloudWatch Logs.

Which of the following explains why the logs are not available?

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

Answer: A

NEW QUESTION 129
- (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 131
- (Exam Topic 2)
A company runs an application on IAM that needs to be accessed only by employees. Most employees work from the office, but others work remotely or travel.
How can the Security Engineer protect this workload so that only employees can access it?

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

Answer: C

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

NEW QUESTION 132
- (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 133
- (Exam Topic 2)
You are designing a custom IAM policy that would allow uses to list buckets in S3 only if they are MFA authenticated. Which of the following would best match this requirement?

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

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

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


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


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


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


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


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


Answer: A

Explanation:
The Condition clause can be used to ensure users can only work with resources if they are MFA authenticated. Option B and C are wrong since the IAM:MultiFactorAuthPresent clause should be marked as true. Here you are saying that onl if the user has been MFA activated, that means it is true, then allow access.
Option D is invalid because the "boor clause is missing in the evaluation for the condition clause. Boolean conditions let you construct Condition elements that restrict access based on comparing a key to
"true" or "false."
Here in this scenario the boot attribute in the condition element will return a value True for option A which will ensure that access is allowed on S3 resources.
For more information on an example on such a policy, please visit the following URL:

NEW QUESTION 137
- (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 138
- (Exam Topic 2)
A Developer’s laptop was stolen. The laptop was not encrypted, and it contained the SSH key used to access multiple Amazon EC2 instances. A Security Engineer has verified that the key has not been used, and has blocked port 22 to all EC2 instances while developing a response plan.
How can the Security Engineer further protect currently running instances?

A. Delete the key-pair key from the EC2 console, then create a new key pair.

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

Answer: C

NEW QUESTION 141
- (Exam Topic 2)
A Security Engineer must design a solution that enables the Incident Response team to audit for changes to a user's IAM permissions in the case of a security incident.
How can this be accomplished?

A. Use IAM Config to review the IAM policy assigned to users before and after the incident.
B. Run the GenerateCredentialReport via the IAM CLI, and copy the output to Amazon S3 daily for auditing purposes.
C. Copy IAM CloudFormation templates to S3, and audit for changes from the template.
D. Use Amazon EC2 Systems Manager to deploy images, and review IAM CloudTrail logs for changes.

Answer: A

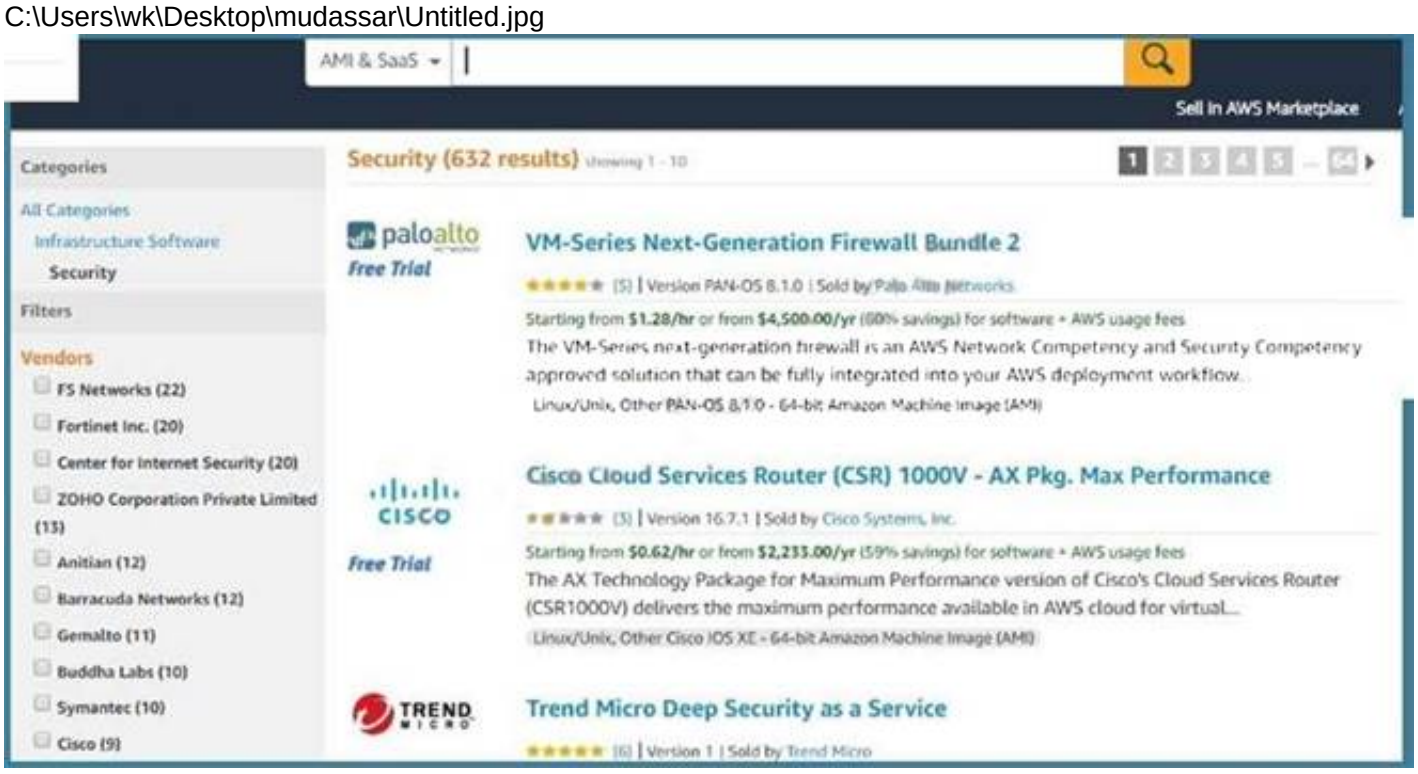
Explanation:
https://IAM.amazon.com/blogs/security/how-to-record-and-govern-your-iam-resource-configurations-using-IAM

NEW QUESTION 142
- (Exam Topic 2)
A company wants to have an Intrusion detection system available for their VPC in IAM. They want to have complete control over the system. Which of the following would be ideal to implement?
Please select:

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

Answer: B

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



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

NEW QUESTION 145
- (Exam Topic 2)
A Developer who is following IAM best practices for secure code development requires an application to encrypt sensitive data to be stored at rest, locally in the application, using IAM KMS. What is the simplest and MOST secure way to decrypt this data when required?

A. Request KMS to provide the stored unencrypted data key and then use the retrieved data key to decrypt the data.
B. Keep the plaintext data key stored in Amazon DynamoDB protected with IAM policie
C. Query DynamoDB to retrieve the data key to decrypt the data
D. Use the Encrypt API to store an encrypted version of the data key with another customer managed key.Decrypt the data key and use it to decrypt the data when required.
E. Store the encrypted data key alongside the encrypted dat
F. Use the Decrypt API to retrieve the data key to decrypt the data when required.

Answer: D

Explanation:
We recommend that you use the following pattern to locally encrypt data: call the GenerateDataKey API, use the key returned in the Plaintext response field to locally encrypt data, and then erase the plaintext data key from memory. Store the encrypted data key (contained in the CiphertextBlob field) alongside of the locally encrypted data. The Decrypt API returns the plaintext key from the encrypted key.
https://docs.IAM.amazon.com/sdkfornet/latest/apidocs/items/MKeyManagementServiceKeyManagementServic

NEW QUESTION 149
- (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

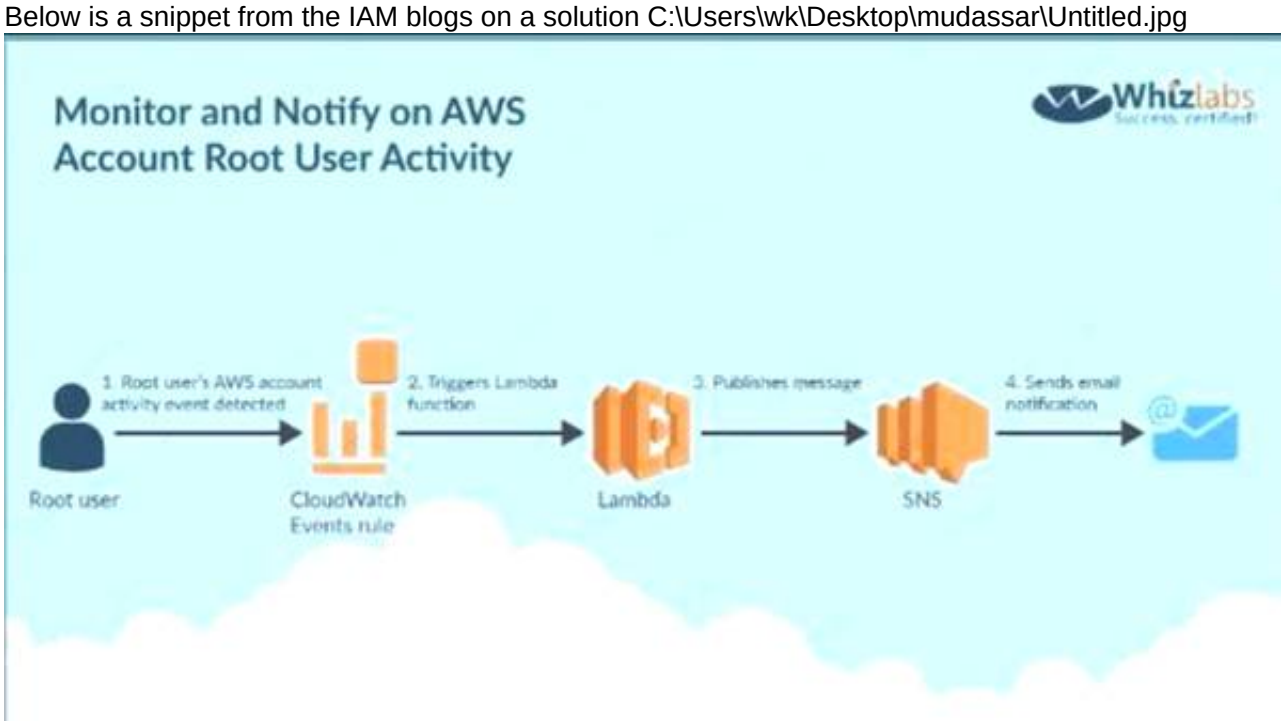
NEW QUESTION 152
- (Exam Topic 2)
Your company has a requirement to monitor all root user activity by notification. How can this best be achieved? Choose 2 answers from the options given below. Each answer forms part of the solution
Please select:

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

Answer: AC

Explanation:

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



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

NEW QUESTION 154
- (Exam Topic 2)
The InfoSec team has mandated that in the future only approved Amazon Machine Images (AMIs) can be used.
How can the InfoSec team ensure compliance with this mandate?

A. Terminate all Amazon EC2 instances and relaunch them with approved AMIs.
B. Patch all running instances by using IAM Systems Manager.
C. Deploy IAM Config rules and check all running instances for compliance.
D. Define a metric filter in Amazon CloudWatch Logs to verify compliance.

Answer: C

Explanation:
https://docs.IAM.amazon.com/config/latest/developerguide/approved-amis-by-id.html

NEW QUESTION 157
- (Exam Topic 2)
You have just recently set up a web and database tier in a VPC and hosted the application. When testing the app , you are not able to reach the home page for the app. You have verified the security groups. What can help you diagnose the issue.
Please select:

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

Answer: B

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

NEW QUESTION 162
- (Exam Topic 2)
Your IT Security team has advised to carry out a penetration test on the resources in their company's IAM Account. This is as part of their capability to analyze the security of the Infrastructure. What should be done first in this regard?
Please select:

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

Answer: C

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

NEW QUESTION 166
- (Exam Topic 2)
You have a 2 tier application hosted in IAM. It consists of a web server and database server (SQL Server) hosted on separate EC2 Instances. You are devising the security groups for these EC2 Instances. The Web tier needs to be accessed by users across the Internet. You have created a web security group(wg-123) and database security group(db-345). Which combination of the following security group rules will allow the application to be secure and functional. Choose 2 answers from the options given below.
Please select:
A. wg-123 -Allow ports 80 and 443 from 0.0.0.0/0
B. db-345 - Allow port 1433 from wg-123
C. wg-123 - Allow port 1433 from wg-123
D. db-345 -Allow ports 1433 from 0.0.0.0/0

Answer: AB

Explanation:
The Web security groups should allow access for ports 80 and 443 for HTTP and HTTPS traffic to all users from the internet.
The database security group should just allow access from the web security group from port 1433. Option C is invalid because this is not a valid configuration
Option D is invalid because database security should not be allowed on the internet For more information on Security Groups please visit the below URL:
https://docs.IAM.amazon.com/IAMEC2/latest/UserGuide/usins-network-security.htmll
The correct answers are: wg-123 - Allow ports 80 and 443 from 0.0.0.0/0, db-345 - Allow port 1433 from wg-123
Submit your Feedback/Queries to our Experts

NEW QUESTION 171
- (Exam Topic 2)
A Security Engineer discovers that developers have been adding rules to security groups that allow SSH and RDP traffic from 0.0.0.0/0 instead of the organization firewall IP.
What is the most efficient way to remediate the risk of this activity?

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

Answer: D

NEW QUESTION 176
- (Exam Topic 2)
A company hosts a critical web application on the IAM Cloud. This is a key revenue generating application for the company. The IT Security team is worried about potential DDos attacks against the web site. The senior management has also specified that immediate action needs to be taken in case of a potential DDos attack. What should be done in this regard?
Please select:

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

Answer: C

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

NEW QUESTION 181
- (Exam Topic 2)
An organization receives an alert that indicates that an EC2 instance behind an ELB Classic Load Balancer has been compromised.
What techniques will limit lateral movement and allow evidence gathering?

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

Answer: B

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

NEW QUESTION 186
- (Exam Topic 2)
A company has a few dozen application servers in private subnets behind an Elastic Load Balancer (ELB) in an IAM Auto Scaling group. The application is accessed from the web over HTTPS. The data must always be encrypted in transit. The Security Engineer is worried about potential key exposure due to vulnerabilities in the application software.
Which approach will meet these requirements while protecting the external certificate during a breach?

A. Use a Network Load Balancer (NLB) to pass through traffic on port 443 from the internet to port 443 on the instances.
B. Purchase an external certificate, and upload it to the IAM Certificate Manager (for use with the ELB) and to the instance
C. Have the ELB decrypt traffic, and route and re-encrypt with the same certificate.
D. Generate an internal self-signed certificate and apply it to the instance
E. Use IAM Certificate Manager to generate a new external certificate for the EL
F. Have the ELB decrypt traffic, and route and re-encrypt with the internal certificate.
G. Upload a new external certificate to the load balance
H. Have the ELB decrypt the traffic and forward it on port 80 to the instances.

Answer: C

NEW QUESTION 188
- (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 189
- (Exam Topic 2)
An application uses Amazon Cognito to manage end users' permissions when directly accessing IAM resources, including Amazon DynamoDB. A new feature request reads as follows:
Provide a mechanism to mark customers as suspended pending investigation or suspended permanently. Customers should still be able to log in when suspended, but should not be able to make changes.
The priorities are to reduce complexity and avoid potential for future security issues. Which approach will meet these requirements and priorities?

A. Create a new database field "suspended_status" and modify the application logic to validate that field when processing requests.
B. Add suspended customers to second Cognito user pool and update the application login flow to check both user pools.
C. Use Amazon Cognito Sync to push out a "suspension_status" parameter and split the IAM policy into normal users and suspended users.
D. Move suspended customers to a second Cognito group and define an appropriate IAM access policy for the group.

Answer: D

Explanation:
https://IAM.amazon.com/blogs/IAM/new-amazon-cognito-groups-and-fine-grained-role-based-access-control-2

NEW QUESTION 191
- (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 194
- (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 198
- (Exam Topic 2)
You have just received an email from IAM Support stating that your IAM account might have been
compromised. Which of the following steps would you look to carry out immediately. Choose 3 answers from the options below.
Please select:

A. Change the root account password.
B. Rotate all IAM access keys
C. Keep all resources running to avoid disruption
D. Change the password for all IAM users.

Answer: ABD

Explanation:
One of the articles from IAM mentions what should be done in such a scenario
If you suspect that your account has been compromised, or if you have received a notification from IAM that the account has been compromised, perform the following tasks:
Change your IAM root account password and the passwords of any IAM users.
Delete or rotate all root and IAM Identity and Access Management (IAM) access keys.
Delete any resources on your account you didn't create, especially running EC2 instances, EC2 spot bids, or IAM users.
Respond to any notifications you received from IAM Support through the IAM Support Center.
Option C is invalid because there could be compromised instances or resources running on your environment. They should be shutdown or stopped immediately.
For more information on the article, please visit the below URL: https://IAM.amazon.com/premiumsupport/knowledee-center/potential-account-compromise>
The correct answers are: Change the root account password. Rotate all IAM access keys. Change the password for all IAM users. Submit your Feedback/Queries to our Experts

NEW QUESTION 200
- (Exam Topic 3)
You company has mandated that all data in IAM be encrypted at rest. How can you achieve this for EBS volumes? Choose 2 answers from the options given below
Please select:

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

Answer: AB

Explanation:
EBS encryption can also be enabled when the volume is created and not for existing volumes. One can use existing tools for OS level encryption.
Option C is incorrect.

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

NEW QUESTION 202
- (Exam Topic 3)
When managing permissions for the API gateway, what can be used to ensure that the right level of permissions are given to developers, IT admins and users? These permissions should be easily managed.
Please select:

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

Answer: B

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

NEW QUESTION 205
- (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 206
- (Exam Topic 3)
An employee keeps terminating EC2 instances on the production environment. You've determined the best way to ensure this doesn't happen is to add an extra layer of defense against terminating the instances. What is the best method to ensure the employee does not terminate the production instances? Choose the 2 correct answers from the options below
Please select:

A. Tag the instance with a production-identifying tag and add resource-level permissions to the employee user with an explicit deny on the terminate API call to instances with the production ta
B. <
C. Tag the instance with a production-identifying tag and modify the employees group to allow only start stop, and reboot API calls and not the terminate instance call.
D. Modify the IAM policy on the user to require MFA before deleting EC2 instances and disable MFA access to the employee
E. Modify the IAM policy on the user to require MFA before deleting EC2 instances

Answer: AB

Explanation:
Tags enable you to categorize your IAM resources in different ways, for example, by purpose, owner, or environment. This is useful when you have many resources of the same type — you can quickly identify a specific resource based on the tags you've assigned to it. Each tag consists of a key and an optional value,

both of which you define
Options C&D are incorrect because it will not ensure that the employee cannot terminate the instance. For more information on tagging answer resources please refer to the below URL:
http://docs.IAM.amazon.com/IAMEC2/latest/UserGuide/Usins_Tags.htmll
The correct answers are: Tag the instance with a production-identifying tag and add resource-level permissions to the employe user with an explicit deny on the terminate API call to instances with the production tag.. Tag the instance with a production-identifying tag and modify the employees group to allow only start stop, and reboot API calls and not the terminate instance
Submit your Feedback/Queries to our Experts

NEW QUESTION 211
- (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 213
- (Exam Topic 3)
Your company is planning on developing an application in IAM. This is a web based application. The application user will use their facebook or google identities for authentication. You want to have the ability to manage user profiles without having to add extra coding to manage this. Which of the below would assist in this.
Please select:

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

Answer: C

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

NEW QUESTION 214
- (Exam Topic 3)
Which of the following is the correct sequence of how KMS manages the keys when used along with the Redshift cluster service
Please select:

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

Answer: A

Explanation:

This is mentioned in the IAM Documentation
Amazon Redshift uses a four-tier, key-based architecture for encryption. The architecture consists of data encryption keys, a database key, a cluster key, and a master key.
Data encryption keys encrypt data blocks in the cluster. Each data block is assigned a randomly-generated AES-256 key. These keys are encrypted by using the database key for the cluster.
The database key encrypts data encryption keys in the cluster. The database key is a randomly-generated AES-256 key. It is stored on disk in a separate network from the Amazon Redshift cluster and passed to the cluster across a secure channel.
The cluster key encrypts the database key for the Amazon Redshift cluster.
Option B is incorrect because the master key encrypts the cluster key and not the database key
Option C is incorrect because the master key encrypts the cluster key and not the data encryption keys Option D is incorrect because the master key encrypts the cluster key only
For more information on how keys are used in Redshift, please visit the following URL: https://docs.IAM.amazon.com/kms/latest/developereuide/services-redshift.html
The correct answer is: The master keys encrypts the cluster key. The cluster key encrypts the database key. The database key encrypts the data encryption keys.
Submit your Feedback/Queries to our Experts

NEW QUESTION 217
- (Exam Topic 3)
You are planning on using the IAM KMS service for managing keys for your application. For which of the following can the KMS CMK keys be used for encrypting? Choose 2 answers from the options given below
Please select:

A. Image Objects
B. Large files
C. Password
D. RSA Keys

Answer: CD

Explanation:
The CMK keys themselves can only be used for encrypting data that is maximum 4KB in size. Hence it can be used for encryptii information such as passwords and RSA keys.
Option A and B are invalid because the actual CMK key can only be used to encrypt small amounts of data and not large amoui of data. You have to generate the data key from the CMK key in order to encrypt high amounts of data
For more information on the concepts for KMS, please visit the following URL: https://docs.IAM.amazon.com/kms/latest/developereuide/concepts.htmll
The correct answers are: Password, RSA Keys Submit your Feedback/Queries to our Experts

NEW QUESTION 219
- (Exam Topic 3)
You need to establish a secure backup and archiving solution for your company, using IAM. Documents should be immediately accessible for three months and available for five years for compliance reasons. Which IAM service fulfills these requirements in the most cost-effective way? Choose the correct Answer
Please select:

A. Upload data to S3 and use lifecycle policies to move the data into Glacier for long-term archiving.
B. Upload the data on EBS, use lifecycle policies to move EBS snapshots into S3 and later into Glacier for long-term archiving.
C. Use Direct Connect to upload data to S3 and use IAM policies to move the data into Glacier for long-term archiving.
D. Use Storage Gateway to store data to S3 and use lifecycle policies to move the data into Redshift for long-term archiving.

Answer: A

Explanation:
amazon Glacier is a secure, durable, and extremely low-cost cloud storage service for data archiving and long-term backup. Customers can reliably store large or small amounts of data for as little as $0,004 per gigabyte per month, a significant savings compared to on-premises solutions.
With Amazon lifecycle policies you can create transition actions in which you define when objects transition to another Amazon S3 storage class. For example, you may choose to transition objects to the STANDARDJA (IA, for infrequent access) storage class 30 days after creation, or archive objects to the GLACIER storage class one year after creation.
Option B is invalid because lifecycle policies are not available for EBS volumes Option C is invalid because IAM policies cannot be used to move data to Glacier
Option D is invalid because lifecycle policies is not used to move data to Redshif For more information on S3 lifecycle policies, please visit the URL: http://docs.IAM.amazon.com/AmazonS3/latest/dev/obiect-lifecycle-mgmt.html
The correct answer is: Upload data to S3 and use lifecycle policies to move the data into Glacier for long-term archiving.
Submit your Feedback/Queries to our Experts

NEW QUESTION 224
- (Exam Topic 3)
A company has a set of EC2 instances hosted in IAM. These instances have EBS volumes for storing critical information. There is a business continuity requirement and in order to boost the agility of the business and to ensure data durability which of the following options are not required.
Please select:

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

Answer: CD

Explanation:
Data stored in Amazon EBS volumes is redundantly stored in multiple physical locations as part of normal operation of those services and at no additional charge. However, Amazon EBS replication is stored within the same availability zone, not across multiple zones; therefore, it is highly recommended that you conduct regular snapshots to Amazon S3 for long-term data durability.
You can use Amazon Data Lifecycle Manager (Amazon DLM) to automate the creation, retention, and deletion of snapshots

taken to back up your Amazon EBS volumes.
With lifecycle management, you can be sure that snapshots are cleaned up regularly and keep costs under control.
EBS Lifecycle Policies
A lifecycle policy consists of these core settings:
• Resource type—The IAM resource managed by the policy, in this case, EBS volumes.
• Target tag—The tag that must be associated with an EBS volume for it to be managed by the policy.
• Schedule—Defines how often to create snapshots and the maximum number of snapshots to keep. Snapshot creation starts within an hour of the specified start time. If creating a new snapshot exceeds the maximum number of snapshots to keep for the volume, the oldest snapshot is deleted.
Option C is correct. Each Amazon EBS volume is automatically replicated within its Availability Zone to protect you from component failure, offering high availability and durability. But it does not have an explicit feature like that.
Option D is correct Encryption does not ensure data durability
For information on security for Compute Resources, please visit the below URL https://d1.IAMstatic.com/whitepapers/Security/Security Compute Services Whitepaper.pdl
The correct answers are: Use EBS volume replication. Use EBS volume encryption Submit your Feedback/Queries to our Experts

NEW QUESTION 226
- (Exam Topic 3)
You have a set of application , database and web servers hosted in IAM. The web servers are placed behind an ELB. There are separate security groups for the application, database and web servers. The network security groups have been defined accordingly. There is an issue with the communication between the application and database servers. In order to troubleshoot the issue between just the application and database server, what is the ideal set of MINIMAL steps you would take?
Please select:

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

Answer: A

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

NEW QUESTION 231
- (Exam Topic 3)
Which of the below services can be integrated with the IAM Web application firewall service. Choose 2 answers from the options given below
Please select:

A. IAM Cloudfront
B. IAM Lambda
C. IAM Application Load Balancer
D. IAM Classic Load Balancer

Answer: AC

Explanation:
The IAM documentation mentions the following on the Application Load Balancer
IAM WAF can be deployed on Amazon CloudFront and the Application Load Balancer (ALB). As part of Amazon CloudFront it car be part of your Content Distribution Network (CDN) protecting your resources and content at the Edge locations and as part of the Application Load Balancer it can protect your origin web servers running behind the ALBs.
Options B and D are invalid because only Cloudfront and the Application Load Balancer services are supported by IAM WAF.
For more information on the web application firewall please refer to the below URL: https://IAM.amazon.com/waf/faq;
The correct answers are: IAM Cloudfront IAM Application Load Balancer Submit your Feedback/Queries to our Experts

NEW QUESTION 232
- (Exam Topic 3)
You need to ensure that the cloudtrail logs which are being delivered in your IAM account is encrypted. How can this be achieved in the easiest way possible?
Please select:

A. Don't do anything since CloudTrail logs are automatically encrypted.
B. Enable S3-SSE for the underlying bucket which receives the log files
C. Enable S3-KMS for the underlying bucket which receives the log files
D. Enable KMS encryption for the logs which are sent to Cloudwatch

Answer: A

Explanation:
The IAM Documentation mentions the following
By default the log files delivered by CloudTrail to your bucket are encrypted by Amazon server-side encryption with Amazon S3-managed encryption keys (SSE-S3)
Option B,C and D are all invalid because by default all logs are encrypted when they sent by Cloudtrail to S3 buckets
For more information on IAM Cloudtrail log encryption, please visit the following URL: https://docs.IAM.amazon.com/IAMcloudtrail/latest/usereuide/encryptine-

cloudtrail-loe-files-with-IAM-kms.htm The correct answer is: Don't do anything since CloudTrail logs are automatically encrypted. Submit your Feedback/Queries to our Experts

NEW QUESTION 237
- (Exam Topic 3)
You are working for a company and been allocated the task for ensuring that there is a federated authentication mechanism setup between IAM and their On-premise Active Directory. Which of the following are important steps that need to be covered in this process? Choose 2 answers from the options given below. Please select:

A. Ensure the right match is in place for On-premise AD Groups and IAM Roles.
B. Ensure the right match is in place for On-premise AD Groups and IAM Groups.
C. Configure IAM as the relying party in Active Directory
D. Configure IAM as the relying party in Active Directory Federation services

Answer: AD

Explanation:
The IAM Documentation mentions some key aspects with regards to the configuration of On-premise AD with IAM
One is the Groups configuration in AD Active Directory Configuration
Determining how you will create and delineate your AD groups and IAM roles in IAM is crucial to how you secure access to your account and manage resources. SAML assertions to the IAM environment and the respective IAM role access will be managed through regular expression (regex) matching between your on-premises AD group name to an IAM IAM role.
One approach for creating the AD groups that uniquely identify the IAM IAM role mapping is by selecting a common group naming convention. For example, your AD groups would start with an identifier, for example, IAM-, as this will distinguish your IAM groups from others within the organization. Next include the 12- digitIAM account number. Finally, add the matching role name within the IAM account. Here is an example:
C:\Users\wk\Desktop\mudassar\Untitled.jpg

And next is the configuration of the relying party which is IAM
ADFS federation occurs with the participation of two parties; the identity or claims provider (in this case the owner of the identity repository - Active Directory) and the relying party, which is another application that wishes to outsource authentication to the identity provider; in this case Amazon Secure Token Service (STS).
The relying party is a federation partner that is represented by a claims provider trust in the federation service.
Option B is invalid because AD groups should not be matched to IAM Groups
Option C is invalid because the relying party should be configured in Active Directory Federation services For more information on the federated access, please visit the following URL:
1
https://IAM.amazon.com/blogs/security/IAM-federated-authentication-with-active-directory-federation-services
The correct answers are: Ensure the right match is in place for On-premise AD Groups and IAM Roles., Configure IAM as the relying party in Active Directory Federation services
Submit your Feedback/Queries to our Experts

NEW QUESTION 242
- (Exam Topic 3)
A company has several Customer Master Keys (CMK), some of which have imported key material. Each CMK must be rotated annually.
What two methods can the security team use to rotate each key? Select 2 answers from the options given below Please select:

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

Answer: AD

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

NEW QUESTION 246
- (Exam Topic 3)
A company has been using the IAM KMS service for managing its keys. They are planning on carrying out housekeeping activities and deleting keys which are no

longer in use. What are the ways that can be incorporated to see which keys are in use? Choose 2 answers from the options given below
Please select:

A. Determine the age of the master key
B. See who is assigned permissions to the master key
C. See Cloudtrail for usage of the key
D. Use IAM cloudwatch events for events generated for the key

Answer: BC

Explanation:
The direct ways that can be used to see how the key is being used is to see the current access permissions and cloudtrail logs
Option A is invalid because seeing how long ago the key was created would not determine the usage of the key
Option D is invalid because Cloudtrail Event is better for seeing for events generated by the key This is also mentioned in the IAM Documentation
Examining CMK Permissions to Determine the Scope of Potential Usage
Determining who or what currently has access to a customer master key (CMK) might help you determine how widely the CM was used and whether it is still needed. To learn how to determine who or what currently has access to a CMK, go to Determining Access to an IAM KMS Customer Master Key.
Examining IAM CloudTrail Logs to Determine Actual Usage
IAM KMS is integrated with IAM CloudTrail, so all IAM KMS API activity is recorded in CloudTrail log files. If you have CloudTrail turned on in the region where your customer master key (CMK) is located, you can examine your CloudTrail log files to view a history of all IAM KMS API activity for a particular CMK, and thus its usage history. You might be able to use a CMK's usage history to help you determine whether or not you still need it
For more information on determining the usage of CMK keys, please visit the following URL:
> https://docs.IAM.amazon.com/kms/latest/developerguide/deleting-keys-determining-usage.html
The correct answers are: See who is assigned permissions to the master key. See Cloudtrail for usage of the key Submit your Feedback/Queries to our Experts

NEW QUESTION 247
- (Exam Topic 3)
You have a set of Customer keys created using the IAM KMS service. These keys have been used for around 6 months. You are now trying to use the new KMS features for the existing set of key's but are not able to do so. What could be the reason for this.
Please select:

A. You have not explicitly given access via the key policy
B. You have not explicitly given access via the IAM policy
C. You have not given access via the IAM roles
D. You have not explicitly given access via IAM users

Answer: A

Explanation:
By default, keys created in KMS are created with the default key policy. When features are added to KMS, you need to explii update the default key policy for these keys.
Option B,C and D are invalid because the key policy is the main entity used to provide access to the keys For more information on upgrading key policies please visit the following URL: https://docs.IAM.ama20n.com/kms/latest/developerguide/key-policy-upgrading.html
(
The correct answer is: You have not explicitly given access via the key policy Submit your Feedback/Queries to our Experts

NEW QUESTION 250
- (Exam Topic 3)
A customer has an instance hosted in the IAM Public Cloud. The VPC and subnet used to host the Instance have been created with the default settings for the Network Access Control Lists. They need to provide an IT Administrator secure access to the underlying instance. How can this be accomplished.
Please select:

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

Answer: C

Explanation:
Options A & B are invalid as default NACL rule will allow all inbound and outbound traffic.
The requirement is that the IT administrator should be able to access this EC2 instance from his workstation. For that we need to enable the Security Group of EC2 instance to allow traffic from the IT administrator's workstation. Hence option C is correct.
Option D is incorrect as we need to enable the Inbound SSH traffic on the EC2 instance Security Group since the traffic originate' , from the IT admin's workstation.
The correct answer is: Ensure that the security group allows Inbound SSH traffic from the IT Administrator's Workstation Submit your Feedback/Queries to our Experts

NEW QUESTION 251
- (Exam Topic 3)
DDoS attacks that happen at the application layer commonly target web applications with lower volumes of traffic compared to infrastructure attacks. To mitigate these types of attacks, you should probably want to include a WAF (Web Application Firewall) as part of your infrastructure. To inspect all HTTP requests, WAFs sit in-line with your application traffic. Unfortunately, this creates a scenario where WAFs can become a point of failure or bottleneck. To mitigate this problem, you need the ability to run multiple WAFs on demand during traffic spikes. This type of scaling for WAF is done via a "WAF sandwich." Which of the following statements best describes what a "WAF sandwich" is? Choose the correct answer from the options below
Please select:

A. The EC2 instance running your WAF software is placed between your private subnets and any NATed connections to the internet.
B. The EC2 instance running your WAF software is placed between your public subnets and your Internet Gateway.
C. The EC2 instance running your WAF software is placed between your public subnets and your private subnets.

D. The EC2 instance running your WAF software is included in an Auto Scaling group and placed in between two Elastic load balancers.

Answer: D

Explanation:
The below diagram shows how a WAF sandwich is created. Its the concept of placing the Ec2 instance which hosts the WAF software in between 2 elastic load balancers.
Option A.B and C are incorrect since the EC2 Instance with the WAF software needs to be placed in an Autoscaling Group For more information on a WAF sandwich please refer to the below Link:
https://www.cloudaxis.eom/2016/11/2l/waf-sandwich/l
The correct answer is: The EC2 instance running your WAF software is included in an Auto Scaling group and placed in between two Elastic load balancers.
Submit your Feedback/Queries to our Experts

NEW QUESTION 255
- (Exam Topic 3)
Your company has just started using IAM and created an IAM account. They are aware of the potential issues when root access is enabled. How can they best safeguard the account when it comes to root access? Choose 2 answers fro the options given below
Please select:

A. Delete the root access account
B. Create an Admin IAM user with the necessary permissions
C. Change the password for the root account.
D. Delete the root access keys

Answer: BD

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

NEW QUESTION 257
- (Exam Topic 3)
Your company looks at the gaming domain and hosts several Ec2 Instances as game servers. The servers each experience user loads in the thousands. There is a concern of DDos attacks on the EC2 Instances which could cause a huge revenue loss to the company. Which of the following can help mitigate this security concern and
also ensure minimum downtime for the servers. Please select:

A. Use VPC Flow logs to monitor the VPC and then implement NACL's to mitigate attacks
B. Use IAM Shield Advanced to protect the EC2 Instances
C. Use IAM Inspector to protect the EC2 Instances
D. Use IAM Trusted Advisor to protect the EC2 Instances

Answer: B

Explanation:
Below is an excerpt from the IAM Documentation on some of the use cases for IAM Shield C:\Users\wk\Desktop\mudassar\Untitled.jpg

Example AWS Shield Advanced Use Cases

You can use Shield Advanced to protect your resources in many types of scenarios. However, in some cases you should use other services or combine other services with Shield Advanced to offer the best protection. Following are examples of how to use Shield Advanced or other AWS services to help protect your resources.

Goal	Suggested services	Related service documentation
Protect a web application and RESTful APIs against a DDoS attack	Shield Advanced protecting an Amazon CloudFront distribution and an Application Load Balancer	Amazon Elastic Load Balancing Documentation, Amazon CloudFront Documentation
Protect a TCP-based application against a DDoS attack	Shield Advanced protecting a Network Load Balancer attached to an Elastic IP address	Amazon Elastic Load Balancing Documentation
Protect a UDP-based game server against a DDoS attack	Shield Advanced protecting an Amazon EC2 instance attached to an Elastic IP address	Amazon Elastic Compute Cloud Documentation

NEW QUESTION 258
- (Exam Topic 3)
An organization has setup multiple IAM users. The organization wants that each IAM user accesses the IAM console only within the organization and not from outside. How can it achieve this?
Please select:

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

Answer: B

Explanation:

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

NEW QUESTION 262
- (Exam Topic 3)
Your organization is preparing for a security assessment of your use of IAM. In preparation for this assessment, which three IAM best practices should you consider implementing?
Please select:

A. Create individual IAM users
B. Configure MFA on the root account and for privileged IAM users
C. Assign IAM users and groups configured with policies granting least privilege access
D. Ensure all users have been assigned and dre frequently rotating a password, access ID/secret key, andX.509 certificate

Answer: ABC

Explanation:
When you go to the security dashboard, the security status will show the best practices for initiating the first level of security.
Option D is invalid because as per the dashboard, this is not part of the security recommendation For more information on best security practices please visit the URL:
https://IAM.amazon.com/whitepapers/IAM-security-best-practices;
The correct answers are: Create individual IAM users, Configure MFA on the root account and for privileged IAM users. Assign IAM users and groups configured with policies granting least privilege access
Submit your Feedback/Queries to our Experts

NEW QUESTION 267
- (Exam Topic 3)
Your company currently has a set of EC2 Instances hosted in a VPC. The IT Security department is suspecting a possible DDos attack on the instances. What can you do to zero in on the IP addresses which are receiving a flurry of requests.
Please select:

A. Use VPC Flow logs to get the IP addresses accessing the EC2 Instances
B. Use IAM Cloud trail to get the IP addresses accessing the EC2 Instances
C. Use IAM Config to get the IP addresses accessing the EC2 Instances
D. Use IAM Trusted Advisor to get the IP addresses accessing the EC2 Instances

Answer: A

Explanation:
With VPC Flow logs you can get the list of IP addresses which are hitting the Instances in your VPC You can then use the information in the logs to see which external IP addresses are sending a flurry of requests which could be the potential threat foi a DDos attack.
Option B is incorrect Cloud Trail records IAM API calls for your account. VPC FLowlogs logs network traffic for VPC, subnets. Network interfaces etc.
As per IAM,
VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC where as IAM CloudTrail, is a service that captures API calls and delivers the log files to an Amazon S3 bucket that you specify.
Option C is invalid this is a config service and will not be able to get the IP addresses
Option D is invalid because this is a recommendation service and will not be able to get the IP addresses For more information on VPC Flow Logs, please visit the following URL: https://docs.IAM.amazon.com/AmazonVPC/latest/UserGuide/flow-logs.html
The correct answer is: Use VPC Flow logs to get the IP addresses accessing the EC2 Instances Submit your Feedback/Queries to our Experts

NEW QUESTION 270
.....

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