
# Amazon-Web-Services

## Exam Questions SCS-C02

AWS Certified Security - Specialty

**NEW QUESTION 1**
- (Exam Topic 1)
A company has multiple IAM accounts that are part of IAM Organizations. The company's Security team wants to ensure that even those Administrators with full access to the company's IAM accounts are unable to access the company's Amazon S3 buckets
How should this be accomplished?

A. UseSCPs
B. Add a permissions boundary to deny access to Amazon S3 and attach it to all roles
C. Use an S3 bucket policy
D. Create a VPC endpoint for Amazon S3 and deny statements for access to Amazon S3

**Answer:** A

**NEW QUESTION 2**
- (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 3**
- (Exam Topic 1)
A Developer reported that IAM CloudTrail was disabled on their account. A Security Engineer investigated the account and discovered the event was undetected by the current security solution. The Security Engineer must recommend a solution that will detect future changes to the CloudTrail configuration and send alerts when changes occur.
What should the Security Engineer do to meet these requirements?

A. Use IAM Resource Access Manager (IAM RAM) to monitor the IAM CloudTrail configuratio
B. Send notifications using Amazon SNS.
C. Create an Amazon CloudWatch Events rule to monitor Amazon GuardDuty finding
D. Send email notifications using Amazon SNS.
E. Update security contact details in IAM account settings for IAM Support to send alerts when suspicious activity is detected.
F. Use Amazon Inspector to automatically detect security issue
G. Send alerts using Amazon SNS.

**Answer:** B

**NEW QUESTION 4**
- (Exam Topic 1)
A company has recently recovered from a security incident that required the restoration of Amazon EC2 instances from snapshots.
After performing a gap analysis of its disaster recovery procedures and backup strategies, the company is concerned that, next time, it will not be able to recover the EC2 instances if the IAM account was compromised and Amazon EBS snapshots were deleted.
All EBS snapshots are encrypted using an IAM KMS CMK. Which solution would solve this problem?

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

**Answer:** A

**NEW QUESTION 5**
- (Exam Topic 1)
A company has implemented centralized logging and monitoring of IAM CloudTrail logs from all Regions in an Amazon S3 bucket. The log Hies are encrypted using IAM KMS. A Security Engineer is attempting to review the log files using a third-party tool hosted on an Amazon EC2 instance The Security Engineer is unable to access the logs in the S3 bucket and receives an access denied error message
What should the Security Engineer do to fix this issue?

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

**Answer:** C

**NEW QUESTION 6**
- (Exam Topic 1)
A security engineer is designing a solution that will provide end-to-end encryption between clients and Docker containers running In Amazon Elastic Container Service (Amazon ECS). This solution will also handle volatile traffic patterns
Which solution would have the MOST scalability and LOWEST latency?

A. Configure a Network Load Balancer to terminate the TLS traffic and then re-encrypt the traffic to the containers
B. Configure an Application Load Balancer to terminate the TLS traffic and then re-encrypt the traffic to the containers
C. Configure a Network Load Balancer with a TCP listener to pass through TLS traffic to the containers
D. Configure Amazon Route 53 to use multivalue answer routing to send traffic to the containers

**Answer:** A

**NEW QUESTION 7**
- (Exam Topic 1)
Unapproved changes were previously made to a company's Amazon S3 bucket. A security engineer configured IAM Config to record configuration changes made to the company's S3 buckets. The engineer discovers there are S3 configuration changes being made, but no Amazon SNS notifications are being sent. The engineer has already checked the configuration of the SNS topic and has confirmed the configuration is valid.
Which combination of steps should the security engineer take to resolve the issue? (Select TWO.)

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

**Answer:** BE

**NEW QUESTION 8**
- (Exam Topic 1)
A company requires that SSH commands used to access its IAM instance be traceable to the user who executed each command.
How should a Security Engineer accomplish this?

A. Allow inbound access on port 22 at the security group attached to the instance Use IAM Systems Manager Session Manager for shell access to Amazon EC2 instances with the user tag defined Enable Amazon CloudWatch togging tor Systems Manager sessions
B. Use Amazon S3 to securely store one Privacy Enhanced Mail Certificate (PEM file) for each user Allow Amazon EC2 to read from Amazon S3 and import every user that wants to use SSH to access EC2 instances Allow inbound access on port 22 at the security group attached to the instance Install the Amazon CloudWatch agent on the EC2 instance and configure it to ingest audit logs for the instance
C. Deny inbound access on port 22 at the security group attached to the instance Use IAM Systems Manager Session Manager tor shell access to Amazon EC2 instances with the user tag defined Enable Amazon CloudWatch togging for Systems Manager sessions
D. Use Amazon S3 to securely store one Privacy Enhanced Mall Certificate (PEM fie) for each team or group Allow Amazon EC2 to read from Amazon S3 and import every user that wants to use SSH to access EC2 instances Allow inbound access on pod 22 at the security group attached to the instance Install the Amazon CloudWatch agent on the EC2 instance and configure it to ingest audit logs for the instance

**Answer:** C

**NEW QUESTION 9**
- (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 10**
- (Exam Topic 1)
A large government organization is moving to the cloud and has specific encryption requirements. The first workload to move requires that a customer's data be immediately destroyed when the customer makes that request.
Management has asked the security team to provide a solution that will securely store the data, allow only authorized applications to perform encryption and decryption and allow for immediate destruction of the data
Which solution will meet these requirements?

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

**Answer:** A

**NEW QUESTION 10**
- (Exam Topic 1)
A company's on-premises data center forwards DNS logs to a third-party security incident events management (SIEM) solution that alerts on suspicious behavior. The company wants to introduce a similar capability to its IAM accounts that includes automatic remediation. The company expects to double in size within the next few months.
Which solution meets the company's current and future logging requirements?

A. Enable Amazon GuardDuty and IAM Security Hub in all Regions and all account
B. Designate a master security account to receive all alerts from the child account
C. Set up specific rules within Amazon Even;Bridge to trigger an IAM Lambda function for remediation steps.
D. Ingest all IAM CloudTrail logs, VPC Flow Logs, and DNS logs into a single Amazon S3 bucket in a designated security accoun
E. Use the current on-premises SIEM to monitor the logs and send a notification to an Amazon SNS topic to alert the security team of remediation steps.
F. Ingest all IAM CloudTrail logs, VPC Flow Logs, and DNS logs into a single Amazon S3 bucket in a designated security accoun
G. Launch an Amazon EC2 instance and install the current SIEM to monitor the logs and send a notification to an Amazon SNS topic to alert the security team of remediation steps.
H. Enable Amazon GuardDuty and IAM Security Hub in all Regions and all account
I. Designate a master security account to receive all alerts from the child account
J. Create an IAM Organizations SCP that denies access to certain API calls that are on an ignore list.

**Answer:** A

**NEW QUESTION 12**
- (Exam Topic 1)
A Security Engineer is looking for a way to control access to data that is being encrypted under a CMK. The Engineer is also looking to use additional authenticated data (AAD) to prevent tampering with ciphertext.
Which action would provide the required functionality?

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

**Answer:** C

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

**NEW QUESTION 15**
- (Exam Topic 1)
A company is collecting IAM CloudTrail log data from multiple IAM accounts by managing individual trails in each account and forwarding log data to a centralized Amazon S3 bucket residing in a log archive account. After CloudTrail introduced support for IAM Organizations trails, the company decided to further centralize management and automate deployment of the CloudTrail logging capability across all of its IAM accounts.
The company's security engineer created an IAM Organizations trail in the master account, enabled server-side encryption with IAM KMS managed keys (SSE-KMS) for the log files, and specified the same bucket as the storage location. However, the engineer noticed that logs recorded by the new trail were not delivered to the bucket.
Which factors could cause this issue? (Select TWO.)

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

**Answer:** AD

**NEW QUESTION 20**
- (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 24**
- (Exam Topic 1)
A company has decided to migrate sensitive documents from on-premises data centers to Amazon S3. Currently, the hard drives are encrypted to meet a compliance requirement regarding data encryption. The CISO wants to improve security by encrypting each file using a different key instead of a single key. Using a different key would limit the security impact of a single exposed key.
Which of the following requires the LEAST amount of configuration when implementing this approach?

A. Place each file into a different S3 bucke
B. Set the default encryption of each bucket to use a different IAM KMS customer managed key.
C. Put all the files in the same S3 bucke
D. Using S3 events as a trigger, write an IAM Lambda function to encrypt each file as it is added using different IAM KMS data keys.
E. Use the S3 encryption client to encrypt each file individually using S3-generated data keys
F. Place all the files in the same S3 bucke
G. Use server-side encryption with IAM KMS-managed keys (SSE-KMS) to encrypt the data

**Answer:** D

**Explanation:**
References:
https://docs.IAM.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html
Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3) When you use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3), each object is encrypted with a unique key. Server-Side Encryption with Customer Master Keys (CMKs) Stored in IAM Key Management Service (SSE-KMS) is similar to SSE-S3, but with some additional benefits and charges for using this service.
When you use SSE-KMS to protect your data without an S3 Bucket Key, Amazon S3 uses an individual IAM KMS data key for every object. It makes a call to IAM KMS every time a request is made against a
KMS-encrypted object. https://docs.IAM.amazon.com/AmazonS3/latest/dev/bucket-key.html
https://docs.IAM.amazon.com/kms/latest/developerguide/symmetric-asymmetric.html

**NEW QUESTION 29**
- (Exam Topic 1)
A Security Engineer has launched multiple Amazon EC2 instances from a private AMI using an IAM CloudFormation template. The Engineer notices instances terminating right after they are launched.
What could be causing these terminations?

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

**Answer:** B

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

**NEW QUESTION 33**
- (Exam Topic 1)
A security engineer has been tasked with implementing a solution that allows the company's development team to have interactive command line access to Amazon EC2 Linux instances using the IAM Management Console.
Which steps should the security engineer take to satisfy this requirement while maintaining least privilege?

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

**Answer:** A

**NEW QUESTION 37**
- (Exam Topic 1)
A company is developing a new mobile app for social media sharing. The company's development team has decided to use Amazon S3 to store at media files generated by mobile app users The company wants to allow users to control whether their own tiles are public, private, of shared with other users in their social network what should the development team do to implement the type of access control with the LEAST administrative effort?

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

**Answer:** A

**NEW QUESTION 39**
- (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 42**
- (Exam Topic 1)
A company is operating an open-source software platform that is internet facing. The legacy software platform no longer receives security updates. The software platform operates using Amazon route 53 weighted load balancing to send traffic to two Amazon EC2 instances that connect to an Amazon POS cluster a recent report suggests this software platform is vulnerable to SQL injection attacks. with samples of attacks provided. The company's security engineer must secure this system against SQL injection attacks within 24 hours. The secure, engineer's solution involve the least amount of effort and maintain normal operations during implementation.
What should the security engineer do to meet these requirements?

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

**Answer:** A

**NEW QUESTION 43**
- (Exam Topic 1)
Two Amazon EC2 instances in different subnets should be able to connect to each other but cannot. It has been confirmed that other hosts in the same subnets are able to communicate successfully, and that security groups have valid ALLOW rules in place to permit this traffic.
Which of the following troubleshooting steps should be performed?

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

**Answer:** C

**NEW QUESTION 46**
- (Exam Topic 1)
A Security Engineer creates an Amazon S3 bucket policy that denies access to all users. A few days later, the Security Engineer adds an additional statement to the bucket policy to allow read-only access to one other employee Even after updating the policy the employee still receives an access denied message.
What is the likely cause of this access denial?

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

**Answer:** D

**NEW QUESTION 48**
- (Exam Topic 1)
A financial institution has the following security requirements:
- Cloud-based users must be contained in a separate authentication domain.
- Cloud-based users cannot access on-premises systems.

As part of standing up a cloud environment, the financial institution is creating a number of Amazon managed databases and Amazon EC2 instances. An Active Directory service exists on-premises that has all the administrator accounts, and these must be able to access the databases and instances.
How would the organization manage its resources in the MOST secure manner? (Choose two.)

A. Configure an IAM Managed Microsoft AD to manage the cloud resources.
B. Configure an additional on-premises Active Directory service to manage the cloud resources.
C. Establish a one-way trust relationship from the existing Active Directory to the new Active Directory service.
D. Establish a one-way trust relationship from the new Active Directory to the existing Active Directoryservice.
E. Establish a two-way trust between the new and existing Active Directory services.

**Answer:** AD

**Explanation:**
Deploy a new forest/domain on IAM with one-way trust. If you are planning on leveraging credentials from an on-premises AD on IAM member servers, you must establish at least a one-way trust to the Active Directory running on IAM. In this model, the IAM domain becomes the resource domain where computer objects are located and on-premises domain becomes the account domain. Ref: https://d1.IAMstatic.com/whitepapers/adds-on-IAM.pdf
https://docs.IAM.amazon.com/directoryservice/latest/admin-guide/directory_microsoft_ad.html

**NEW QUESTION 49**
- (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 50**
- (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 53**
- (Exam Topic 2)
During a recent security audit, it was discovered that multiple teams in a large organization have placed restricted data in multiple Amazon S3 buckets, and the data may have been exposed. The auditor has requested that the organization identify all possible objects that contain personally identifiable information (PII) and then determine whether this information has been accessed.
What solution will allow the Security team to complete this request?

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

**Answer:** B

**NEW QUESTION 58**
- (Exam Topic 2)
A Security Administrator is restricting the capabilities of company root user accounts. The company uses IAM Organizations and has enabled it for all feature sets, including consolidated billing. The top-level account is used for billing and administrative purposes, not for operational IAM resource purposes.
How can the Administrator restrict usage of member root user accounts across the organization?

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

**Answer:** C

**Explanation:**
Applying a "Control Policy" in your organization. A policy applied to: 1) root applies to all accounts in the organization 2) OU applies to all accounts in the OU and to any child OUs 3) account applies to one account only Note- this requires that Acquirements: -all features are enabled for the organization in IAM Organizations

-Only service control policy (SCP) are supported
https://docs.IAM.amazon.com/organizations/latest/userguide/orgs_manage_policies.html

**NEW QUESTION 60**
- (Exam Topic 2)
A Security Engineer is working with a Product team building a web application on IAM. The application uses Amazon S3 to host the static content, Amazon API Gateway to provide RESTful services; and Amazon DynamoDB as the backend data store. The users already exist in a directory that is exposed through a SAML identity provider.
Which combination of the following actions should the Engineer take to enable users to be authenticated into the web application and call APIs? (Choose three.)

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

**Answer:** BDE

**NEW QUESTION 65**
- (Exam Topic 2)
A company plans to move most of its IT infrastructure to IAM. They want to leverage their existing on-premises Active Directory as an identity provider for IAM.
Which combination of steps should a Security Engineer take to federate the company's on-premises Active Directory with IAM? (Choose two.)

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

**Answer:** AD

**Explanation:**
https://IAM.amazon.com/blogs/security/how-to-establish-federated-access-to-your-IAM-resources-by-using-acti

**NEW QUESTION 67**
- (Exam Topic 2)
Which of the following are valid event sources that are associated with web access control lists that trigger IAM WAF rules? (Choose two.)

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

**Answer:** BC

**Explanation:**

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

**NEW QUESTION 70**
- (Exam Topic 2)
Some highly sensitive analytics workloads are to be moved to Amazon EC2 hosts. Threat modeling has found that a risk exists where a subnet could be maliciously or accidentally exposed to the internet.
Which of the following mitigations should be recommended?

A. Use IAM Config to detect whether an Internet Gateway is added and use an IAM Lambda function to provide auto-remediation.
B. Within the Amazon VPC configuration, mark the VPC as private and disable Elastic IP addresses.
C. Use IPv6 addressing exclusively on the EC2 hosts, as this prevents the hosts from being accessed from the internet.
D. Move the workload to a Dedicated Host, as this provides additional network security controls andmonitorin

**Answer:** A

**Explanation:**
By default, Private instance has a private IP address, but no public IP address. These instances can
communicate with each other, but can't access the Internet. You can enable Internet access for an instance launched into a nondefault subnet by attaching an Internet gateway to its VPC (if its VPC is not a default VPC) and associating an Elastic IP address with the instance. Alternatively, to allow an instance in your VPC to initiate outbound connections to the Internet but prevent unsolicited inbound connections from the Internet, you can use a network address translation (NAT) instance. NAT maps multiple private IP addresses to a single public IP address. A NAT instance has an Elastic IP address and is connected to the Internet through an Internet gateway.You can connect an instance in a private subnet to the Internet through the NAT instance, which routes traffic from the instance to the Internet gateway, and routes any responses to the instance.

**NEW QUESTION 73**
- (Exam Topic 2)
The Accounting department at Example Corp. has made a decision to hire a third-party firm, AnyCompany, to monitor Example Corp.'s IAM account to help optimize costs.

The Security Engineer for Example Corp. has been tasked with providing AnyCompany with access to the required Example Corp. IAM resources. The Engineer has created an IAM role and granted permission to AnyCompany's IAM account to assume this role.
When customers contact AnyCompany, they provide their role ARN for validation. The Engineer is concerned that one of AnyCompany's other customers might deduce Example Corp.'s role ARN and potentially compromise the company's account.
What steps should the Engineer perform to prevent this outcome?

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

**Answer:** B

**NEW QUESTION 78**
- (Exam Topic 2)
The Information Technology department has stopped using Classic Load Balancers and switched to Application Load Balancers to save costs. After the switch, some users on older devices are no longer able to connect to the website.
What is causing this situation?

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

**Answer:** D

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

**NEW QUESTION 79**
- (Exam Topic 2)
A Security Engineer must add additional protection to a legacy web application by adding the following HTTP security headers:
-Content Security-Policy
-X-Frame-Options
-X-XSS-Protection
The Engineer does not have access to the source code of the legacy web application. Which of the following approaches would meet this requirement?

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

**Answer:** B

**NEW QUESTION 84**
- (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 87**
- (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 90**
- (Exam Topic 2)
A company has five IAM accounts and wants to use IAM CloudTrail to log API calls. The log files must be stored in an Amazon S3 bucket that resides in a new account specifically built for centralized services with a unique top-level prefix for each trail. The configuration must also enable detection of any modification to the logs.
Which of the following steps will implement these requirements? (Choose three.)

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

**Answer:** ACE

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

**NEW QUESTION 95**
- (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 96**
- (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 100**
- (Exam Topic 2)
A Development team has asked for help configuring the IAM roles and policies in a new IAM account. The team using the account expects to have hundreds of master keys and therefore does not want to manage access control for customer master keys (CMKs).
Which of the following will allow the team to manage IAM KMS permissions in IAM without the complexity of editing individual key policies?

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

**Answer:** B

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

**NEW QUESTION 105**
- (Exam Topic 2)
Your company has defined privileged users for their IAM Account. These users are administrators for key resources defined in the company. There is now a mandate to enhance the security authentication for these users. How can this be accomplished?
Please select:

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

**Answer:** A

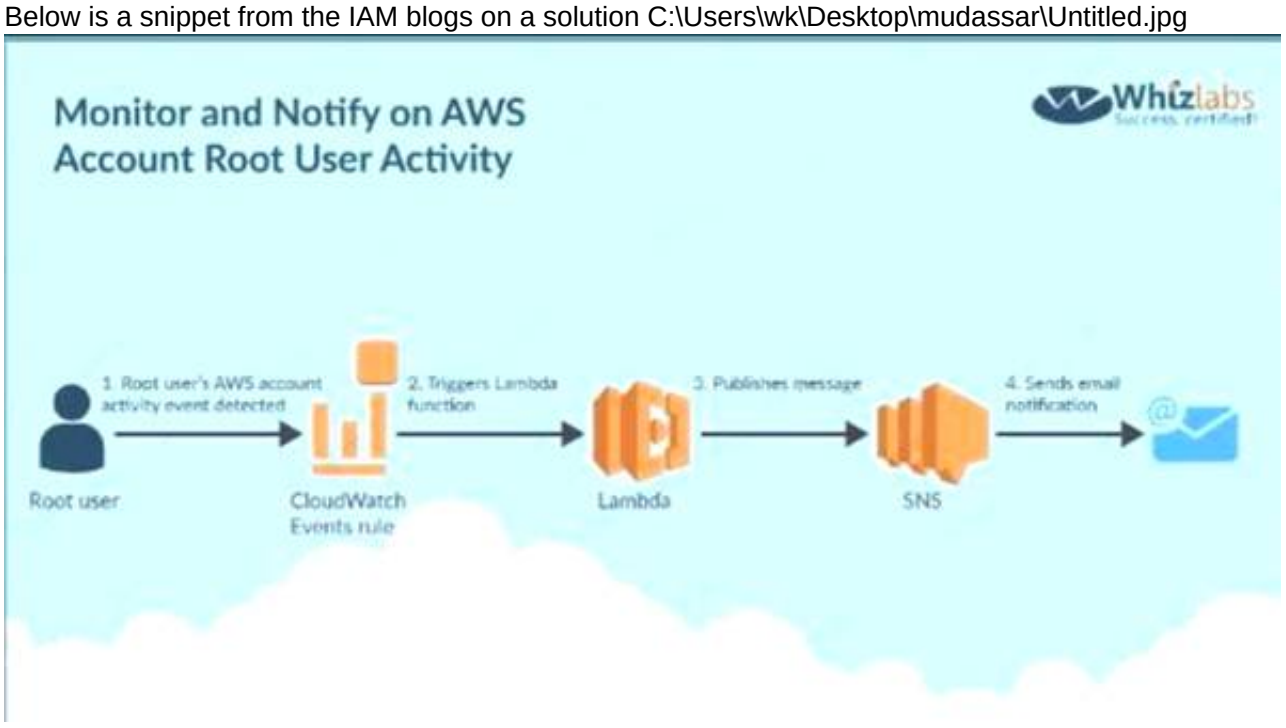
**Explanation:**
The IAM Documentation mentions the following as a best practices for IAM users. For extra security, enable multi-factor authentication (MFA) for privileged IAM users (users who are allowed access to sensitive resources or APIs). With MFA, users have a device that generates unique authentication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

**NEW QUESTION 106**
- (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 108**
- (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 111**
- (Exam Topic 2)
IAM CloudTrail is being used to monitor API calls in an organization. An audit revealed that CloudTrail is failing to deliver events to Amazon S3 as expected.
What initial actions should be taken to allow delivery of CloudTrail events to S3? (Select two.)

A. Verify that the S3 bucket policy allow CloudTrail to write objects.
B. Verify that the IAM role used by CloudTrail has access to write to Amazon CloudWatch Logs.
C. Remove any lifecycle policies on the S3 bucket that are archiving objects to Amazon Glacier.
D. Verify that the S3 bucket defined in CloudTrail exists.
E. Verify that the log file prefix defined in CloudTrail exists in the S3 bucket.

**Answer:** BD

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

**NEW QUESTION 113**
- (Exam Topic 2)
Compliance requirements state that all communications between company on-premises hosts and EC2 instances be encrypted in transit. Hosts use custom proprietary protocols for their communication, and EC2 instances need to be fronted by a load balancer for increased availability.
Which of the following solutions will meet these requirements?

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

**Answer:** B

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

**NEW QUESTION 117**
- (Exam Topic 2)
A distributed web application is installed across several EC2 instances in public subnets residing in two Availability Zones. Apache logs show several intermittent brute-force attacks from hundreds of IP addresses at the layer 7 level over the past six months.
What would be the BEST way to reduce the potential impact of these attacks in the future?

A. Use custom route tables to prevent malicious traffic from routing to the instances.
B. Update security groups to deny traffic from the originating source IP addresses.
C. Use network ACLs.
D. Install intrusion prevention software (IPS) on each instance.

**Answer:** D

**Explanation:**
https://docs.IAM.amazon.com/vpc/latest/userguide/amazon-vpc-limits.html NACL has limit 20 (can increase to maximum 40 rule), and more rule will make more low-latency

**NEW QUESTION 122**
- (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 124**
- (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 127**
- (Exam Topic 2)
A company plans to move most of its IT infrastructure to IAM. The company wants to leverage its existing on-premises Active Directory as an identity provider for IAM.
Which steps should be taken to authenticate to IAM services using the company's on-premises Active Directory? (Choose three).

A. Create IAM roles with permissions corresponding to each Active Directory group.
B. Create IAM groups with permissions corresponding to each Active Directory group.
C. Create a SAML provider with IAM.
D. Create a SAML provider with Amazon Cloud Directory.
E. Configure IAM as a trusted relying party for the Active Directory
F. Configure IAM as a trusted relying party for Amazon Cloud Directory.

**Answer:** ACE

**Explanation:**
https://IAM.amazon.com/blogs/security/IAM-federated-authentication-with-active-directory-federation-services

**NEW QUESTION 129**
- (Exam Topic 2)
While analyzing a company's security solution, a Security Engineer wants to secure the IAM account root user.
What should the Security Engineer do to provide the highest level of security for the account?

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

**Answer:** D

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

**NEW QUESTION 133**
- (Exam Topic 2)
A company is hosting a website that must be accessible to users for HTTPS traffic. Also port 22 should be open for administrative purposes. The administrator's workstation has a static IP address of 203.0.113.1/32. Which of the following security group configurations are the MOST secure but still functional to support these requirements? Choose 2 answers from the options given below
Please select:

A. Port 443 coming from 0.0.0.0/0
B. Port 443 coming from 10.0.0.0/16
C. Port 22 coming from 0.0.0.0/0
D. Port 22 coming from 203.0.113.1/32

**Answer:** AD

**Explanation:**
Since HTTPS traffic is required for all users on the Internet, Port 443 should be open on all IP addresses. For port 22, the traffic should be restricted to an internal subnet.
Option B is invalid, because this only allow traffic from a particular CIDR block and not from the internet Option C is invalid because allowing port 22 from the internet is a security risk
For more information on IAM Security Groups, please visit the following UR
https://docs.IAM.amazon.com/IAMEC2/latest/UserGuide/usins-network-secunty.htmll
The correct answers are: Port 443 coming from 0.0.0.0/0, Port 22 coming from 203.0.113.1 /32 Submit your Feedback/Queries to our Experts

**NEW QUESTION 134**
- (Exam Topic 2)
A company has a customer master key (CMK) with imported key materials. Company policy requires that all encryption keys must be rotated every year.
What can be done to implement the above policy?

A. Enable automatic key rotation annually for the CMK.
B. Use IAM Command Line Interface to create an IAM Lambda function to rotate the existing CMK annually.
C. Import new key material to the existing CMK and manually rotate the CMK.
D. Create a new CMK, import new key material to it, and point the key alias to the new CMK.

**Answer:** D

**Explanation:**
https://docs.IAM.amazon.com/en_pv/kms/latest/developerguide/rotate-keys.html#rotate-keys-manually "You might prefer to rotate keys manually so you can control the rotation frequency. It's also a good solution
for CMKs that are not eligible for automatic key rotation, such as asymmetric CMKs, CMKs in custom key stores and CMKs with imported key material. Because the new CMK is a different resource from the current CMK, it has a different key ID and ARN. When you change CMKs, you need to update references to the CMK ID or ARN in your applications. Aliases, which associate a friendly name with a CMK, make this process easier. Use an alias to refer to a CMK in your applications. Then, when you want to change the CMK that the application uses, change the target CMK of the alias. To update the target CMK of an alias, use UpdateAlias operation in the IAM KMS API. "

**NEW QUESTION 135**
- (Exam Topic 2)
Amazon CloudWatch Logs agent is successfully delivering logs to the CloudWatch Logs service. However, logs stop being delivered after the associated log stream has been active for a specific number of hours.
What steps are necessary to identify the cause of this phenomenon? (Choose two.)

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

**Answer:** AB

**Explanation:**
https://acloud.guru/forums/IAM-certified-security-specialty/discussion/-Lm5A3w6_NybQPhh6tRP/Cloudwatch

**NEW QUESTION 137**
- (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 139**
- (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 144**
- (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 146**
- (Exam Topic 3)
Your company has a set of EC2 Instances defined in IAM. They need to ensure that all traffic packets are monitored and inspected for any security threats. How can this be achieved? Choose 2 answers from the options given below
Please select:

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

**Answer:** AB

**Explanation:**
If you want to inspect the packets themselves, then you need to use custom based software A diagram representation of this is given in the IAM Security best practices
Option C is invalid because VPC Flow logs cannot conduct packet inspection. For more information on IAM Security best practices, please refer to below URL:
The correct answers are: Use a host based intrusion detection system. Use a third party firewall installed on a central EC2
Submit your Feedback/Queries to our Experts

**NEW QUESTION 149**
- (Exam Topic 3)
A company is planning on extending their on-premise IAM Infrastructure to the IAM Cloud. They need to have a solution that would give core benefits of traffic encryption and ensure latency is kept to a minimum. Which of the following would help fulfil this requirement? Choose 2 answers from the options given below
Please select:

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

**Answer:** AD

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

**NEW QUESTION 154**
- (Exam Topic 3)
Your company has the following setup in IAM
* a. A set of EC2 Instances hosting a web application
* b. An application load balancer placed in front of the EC2 Instances
There seems to be a set of malicious requests coming from a set of IP addresses. Which of the following can be used to protect against these requests?
Please select:

A. Use Security Groups to block the IP addresses
B. Use VPC Flow Logs to block the IP addresses
C. Use IAM inspector to block the IP addresses
D. Use IAM WAF to block the IP addresses

**Answer:** D

**Explanation:**
Your answer is incorrect Answer -D
The IAM Documentation mentions the following on IAM WAF which can be used to protect Application Load Balancers and Cloud front
A web access control list (web ACL) gives you fine-grained control over the web requests that your Amazon CloudFront distributions or Application Load Balancers respond to. You can allow or block the following types of requests:
Originate from an IP address or a range of IP addresses Originate from a specific country or countries
Contain a specified string or match a regular expression (regex) pattern in a particular part of requests Exceed a specified length
Appear to contain malicious SQL code (known as SQL injection) Appear to contain malicious scripts (known as cross-site scripting)
Option A is invalid because by default Security Groups have the Deny policy
Options B and C are invalid because these services cannot be used to block IP addresses For information on IAM WAF, please visit the below URL:
https://docs.IAM.amazon.com/waf/latest/developerguide/web-acl.html
The correct answer is: Use IAM WAF to block the IP addresses Submit your Feedback/Queries to our Experts

**NEW QUESTION 155**
- (Exam Topic 3)
What is the result of the following bucket policy?

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

Choose the correct Answer Please select:

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 159**
- (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 162**
- (Exam Topic 3)
Your company has created a set of keys using the IAM KMS service. They need to ensure that each key is only used for certain services. For example , they want one key to be used only for the S3 service. How can this be achieved?
Please select:

A. Create an IAM policy that allows the key to be accessed by only the S3 service.
B. Create a bucket policy that allows the key to be accessed by only the S3 service.
C. Use the kms:ViaService condition in the Key policy
D. Define an IAM user, allocate the key and then assign the permissions to the required service

**Answer:** C

**Explanation:**
Option A and B are invalid because mapping keys to services cannot be done via either the IAM or bucket policy
Option D is invalid because keys for IAM users cannot be assigned to services This is mentioned in the IAM Documentation
The kms:ViaService condition key limits use of a customer-managed CMK to requests from particular IAM services. (IAM managed CMKs in your account, such as IAM/s3, are always restricted to the IAM service that created them.)
For example, you can use kms:V1aService to allow a user to use a customer managed CMK only for requests that Amazon S3 makes on their behalf. Or you can use it to deny the user permission to a CMK when a request on their behalf comes from IAM Lambda.
For more information on key policy's for KMS please visit the following URL: https://docs.IAM.amazon.com/kms/latest/developereuide/policy-conditions.html
The correct answer is: Use the kms:ViaServtce condition in the Key policy Submit your Feedback/Queries to our Experts

**NEW QUESTION 165**
- (Exam Topic 3)
A company hosts data in S3. There is a requirement to control access to the S3 buckets. Which are the 2 ways in which this can be achieved?
Please select:

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

**Answer:** AC

**Explanation:**
The IAM Documentation mentions the following
Amazon S3 offers access policy options broadly categorized as resource-based policies and user policies. Access policies you attach to your resources (buckets and objects) are referred to as resource-based policies. For example, bucket policies and access control lists (ACLs) are resource-based policies. You can also attach access policies to users in your account. These are called user policies. You may choose to use resource-based policies, user policies, or some combination of these to manage permissions to your Amazon S3 resources.

Option B and D are invalid because these cannot be used to control access to S3 buckets For more information on S3 access control, please refer to the below Link: https://docs.IAM.amazon.com/AmazonS3/latest/dev/s3-access-control.htmll
The correct answers are: Use Bucket policies. Use IAM user policies Submit your Feedback/Queries to our Experts

**NEW QUESTION 166**
- (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 170**
- (Exam Topic 3)
A company hosts data in S3. There is now a mandate that going forward all data in the S3 bucket needs to encrypt at rest. How can this be achieved?
Please select:

A. Use IAM Access keys to encrypt the data
B. Use SSL certificates to encrypt the data
C. Enable server side encryption on the S3 bucket
D. Enable MFA on the S3 bucket

**Answer:** C

**Explanation:**
The IAM Documentation mentions the following
Server-side encryption is about data encryption at rest—that is, Amazon S3 encrypts your data at the object level as it writes it to disks in its data centers and decrypts it for you when you access it. As long as you authenticate your request and you have access permissions, there is no difference in the way you access encrypted or unencrypted objects.
Options A and B are invalid because neither Access Keys nor SSL certificates can be used to encrypt data. Option D is invalid because MFA is just used as an extra level of security for S3 buckets
For more information on S3 server side encryption, please refer to the below Link: https://docs.IAM.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html
Submit your Feedback/Queries to our Experts

**NEW QUESTION 171**
- (Exam Topic 3)
One of the EC2 Instances in your company has been compromised. What steps would you take to ensure that you could apply digital forensics on the Instance. Select 2 answers from the options given below
Please select:

A. Remove the role applied to the Ec2 Instance
B. Create a separate forensic instance
C. Ensure that the security groups only allow communication to this forensic instance
D. Terminate the instance

**Answer:** BC

**Explanation:**
Option A is invalid because removing the role will not help completely in such a situation
Option D is invalid because terminating the instance means that you cannot conduct forensic analysis on the instance
One way to isolate an affected EC2 instance for investigation is to place it in a Security Group that only the forensic investigators can access. Close all ports except to receive inbound SSH or RDP traffic from one single IP address from which the investigators can safely examine the instance.
For more information on security scenarios for your EC2 Instance, please refer to below URL: https://d1.IAMstatic.com/Marketplace/scenarios/security/SEC 11 TSB Final.pd1
The correct answers are: Create a separate forensic instance. Ensure that the security groups only allow communication to this forensic instance
Submit your Feedback/Queries to our Experts

**NEW QUESTION 174**
- (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 179**
- (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 181**
- (Exam Topic 3)
A company stores critical data in an S3 bucket. There is a requirement to ensure that an extra level of security is added to the S3 bucket. In addition , it should be ensured that objects are available in a secondary region if the primary one goes down. Which of the following can help fulfil these requirements? Choose 2 answers from the options given below
Please select:

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

**Answer:** AC

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


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

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

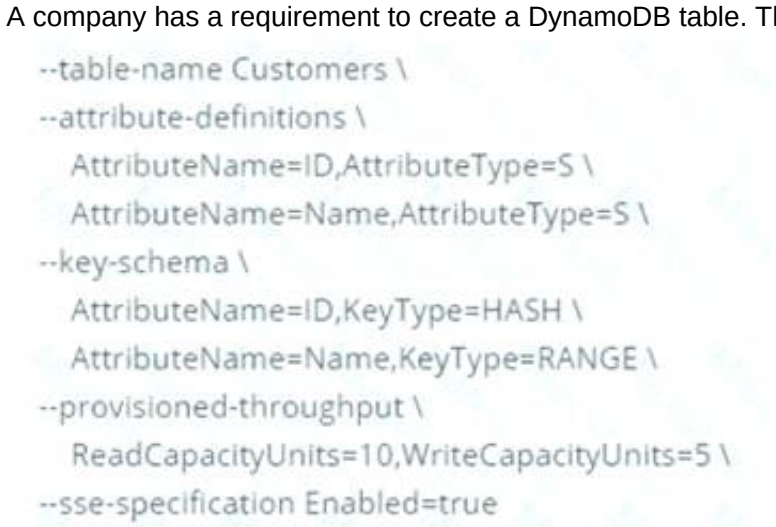
**NEW QUESTION 182**
- (Exam Topic 3)
A company hosts critical data in an S3 bucket. Even though they have assigned the appropriate permissions to the bucket, they are still worried about data deletion. What measures can be taken to restrict the risk of data deletion on the bucket. Choose 2 answers from the options given below
Please select:

A. Enable versioning on the S3 bucket
B. Enable data at rest for the objects in the bucket
C. Enable MFA Delete in the bucket policy
D. Enable data in transit for the objects in the bucket

**Answer:** AC

**Explanation:**
One of the IAM Security blogs mentions the followinj
Versioning keeps multiple versions of an object in the same bucket. When you enable it on a bucket Amazon S3 automatically adds a unique version ID to every object stored in the bucket. At that point, a simple DELETE action does not permanently delete an object version; it merely associates a delete marker with the object. If you want to permanently delete an object version, you must specify its version ID in your DELETE request.
You can add another layer of protection by enabling MFA Delete on a versioned bucket. Once you do so, you must provide your IAM accounts access keys and a valid code from the account's MFA device in order to permanently delete an object version or suspend or reactivate versioning on the bucket.
Option B is invalid because enabling encryption does not guarantee risk of data deletion. Option D is invalid because this option does not guarantee risk of data deletion.
For more information on IAM S3 versioning and MFA please refer to the below URL: https://IAM.amazon.com/blogs/security/securing-access-to-IAM-using-mfa-part-3/
The correct answers are: Enable versioning on the S3 bucket Enable MFA Delete in the bucket policy Submit your Feedback/Queries to our Experts

**NEW QUESTION 185**
- (Exam Topic 3)
A company has a requirement to create a DynamoDB table. The company's software architect has provided the following CLI command for the DynamoDB table




Which of the following has been taken of from a security perspective from the above command? Please select:

A. Since the ID is hashed, it ensures security of the underlying table.
B. The above command ensures data encryption at rest for the Customer table

C. The above command ensures data encryption in transit for the Customer table
D. The right throughput has been specified from a security perspective

**Answer:** B

**Explanation:**
The above command with the "-sse-specification Enabled=true" parameter ensures that the data for the DynamoDB table is encrypted at rest.
Options A,C and D are all invalid because this command is specifically used to ensure data encryption at rest For more information on DynamoDB encryption, please visit the URL: https://docs.IAM.amazon.com/amazondynamodb/latest/developerguide/encryption.tutorial.html
The correct answer is: The above command ensures data encryption at rest for the Customer table

**NEW QUESTION 189**
- (Exam Topic 3)
Every application in a company's portfolio has a separate IAM account for development and production. The security team wants to prevent the root user and all IAM users in the production accounts from accessing a specific set of unneeded services. How can they control this functionality?
Please select:

A. Create a Service Control Policy that denies access to the service
B. Assemble all production accounts in an organizational uni
C. Apply the policy to that organizational unit.
D. Create a Service Control Policy that denies access to the service
E. Apply the policy to the root account.
F. Create an IAM policy that denies access to the service
G. Associate the policy with an IAM group and enlist all users and the root users in this group.
H. Create an IAM policy that denies access to the service
I. Create a Config Rule that checks that all users have the policy m assigne
J. Trigger a Lambda function that adds the policy when found missing.

**Answer:** A

**Explanation:**
As an administrator of the master account of an organization, you can restrict which IAM services and individual API actions the users and roles in each member account can access. This restriction even overrides the administrators of member accounts in the organization. When IAM Organizations blocks access to a service or API action for a member account a user or role in that account can't access any prohibited service or API action, even if an administrator of a member account explicitly grants such permissions in an IAM policy. Organization permissions overrule account permissions.
Option B is invalid because service policies cannot be assigned to the root account at the account level. Option C and D are invalid because IAM policies alone at the account level would not be able to suffice the
requirement
For more information, please visit the below URL id=docs_orgs_console https://docs.IAM.amazon.com/IAM/latest/UserGi manage attach-policy.html
The correct answer is: Create a Service Control Policy that denies access to the services. Assemble all production accounts in an organizational unit. Apply the policy to that organizational unit
Submit your Feedback/Queries to our Experts

**NEW QUESTION 190**
- (Exam Topic 3)
You are designing a connectivity solution between on-premises infrastructure and Amazon VPC. Your server's on-premises will be communicating with your VPC instances. You will be establishing IPSec tunnels over the internet. Yo will be using VPN gateways and terminating the IPsec tunnels on IAM-supported customer gateways. Which of the following objectives would you achieve by implementing an IPSec tunnel as outlined above? Choose 4 answers form the options below
Please select:

A. End-to-end protection of data in transit
B. End-to-end Identity authentication
C. Data encryption across the internet
D. Protection of data in transit over the Internet
E. Peer identity authentication between VPN gateway and customer gateway
F. Data integrity protection across the Internet

**Answer:** CDEF

**Explanation:**
IPSec is a widely adopted protocol that can be used to provide end to end protection for data

**NEW QUESTION 192**
- (Exam Topic 3)
Your company is planning on IAM on hosting its IAM resources. There is a company policy which mandates that all security keys are completely managed within the company itself. Which of the following is the correct measure of following this policy?
Please select:

A. Using the IAM KMS service for creation of the keys and the company managing the key lifecycle thereafter.
B. Generating the key pairs for the EC2 Instances using puttygen
C. Use the EC2 Key pairs that come with IAM
D. Use S3 server-side encryption

**Answer:** B

**Explanation:**
y ensuring that you generate the key pairs for EC2 Instances, you will have complete control of the access keys.
Options A,C and D are invalid because all of these processes means that IAM has ownership of the keys. And the question specifically mentions that you need ownership of the keys
For information on security for Compute Resources, please visit the below URL: https://d1.IAMstatic.com/whitepapers/Security/Security Compute Services

Whitepaper.pdfl
The correct answer is: Generating the key pairs for the EC2 Instances using puttygen Submit your Feedback/Queries to our Experts

**NEW QUESTION 194**
- (Exam Topic 3)
A web application runs in a VPC on EC2 instances behind an ELB Application Load Balancer. The application stores data in an RDS MySQL DB instance. A Linux bastion host is used to apply schema updates to the database - administrators connect to the host via SSH from a corporate workstation. The following security groups are applied to the infrastructure
* sgLB - associated with the ELB
* sgWeb - associated with the EC2 instances.
* sgDB - associated with the database
* sgBastion - associated with the bastion host Which security group configuration will allow the application to be secure and functional?
Please select:

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

**Answer:** D

**Explanation:**
The Load Balancer should accept traffic on ow port 80 and 443 traffic from 0.0.0.0/0 The backend EC2 Instances should accept traffic from the Load Balancer
The database should allow traffic from the Web server
And the Bastion host should only allow traffic from a specific corporate IP address range Option A is incorrect because the Web group should only allow traffic from the Load balancer For more information on IAM Security Groups, please refer to below URL: https://docs.IAM.amazon.com/IAMEC2/latest/UserGuide/usins-network-security.htmll
The correct answer is: sgLB :allow port 80 and 443 traffic from 0.0.0.0/0 sgWeb :allow port 80 and 443 traffic from sgLB
sgDB :allow port 3306 traffic from sgWeb and sgBastion sgBastion: allow port 22 traffic from the corporate IP address range Submit your Feedback/Queries to our Experts

**NEW QUESTION 198**
- (Exam Topic 3)
You are creating a Lambda function which will be triggered by a Cloudwatch Event. The data from these events needs to be stored in a DynamoDB table. How should the Lambda function be given access to the DynamoDB table?
Please select:

A. Put the IAM Access keys in the Lambda function since the Lambda function by default is secure
B. Use an IAM role which has permissions to the DynamoDB table and attach it to the Lambda function.
C. Use the IAM Access keys which has access to DynamoDB and then place it in an S3 bucket.
D. Create a VPC endpoint for the DynamoDB tabl
E. Access the VPC endpoint from the Lambda function.

**Answer:** B

**Explanation:**
IAM Lambda functions uses roles to interact with other IAM services. So use an IAM role which has permissions to the DynamoDB table and attach it to the Lambda function.
Options A and C are all invalid because you should never use IAM keys for access. Option D is invalid because the VPC endpoint is used for VPCs
For more information on Lambda function Permission model, please visit the URL https://docs.IAM.amazon.com/lambda/latest/dg/intro-permission-model.html
The correct answer is: Use an IAM role which has permissions to the DynamoDB table and attach it to the Lambda function. Submit your Feedback/Queries to our Experts

**NEW QUESTION 199**
- (Exam Topic 3)
A Devops team is currently looking at the security aspect of their CI/CD pipeline. They are making use of IAM resource? for their infrastructure. They want to ensure that the EC2 Instances don't have any high security vulnerabilities. They want to ensure a complete DevSecOps process. How can this be achieved?
Please select:

A. Use IAM Config to check the state of the EC2 instance for any sort of security issues.
B. Use IAM Inspector API's in the pipeline for the EC2 Instances
C. Use IAM Trusted Advisor API's in the pipeline for the EC2 Instances
D. Use IAM Security Groups to ensure no vulnerabilities are present

**Answer:** B

**Explanation:**
Amazon Inspector offers a programmatic way to find security defects or misconfigurations in your operating systems and applications. Because you can use API calls to access both the processing of assessments and the results of your assessments, integration of the findings into workflow and notification systems is simple.
DevOps teams can integrate Amazon Inspector into their CI/CD pipelines and use it to identify any pre-existing issues or when new issues are introduced.
Option A.C and D are all incorrect since these services cannot check for Security Vulnerabilities. These can only be checked by the IAM Inspector service.
For more information on IAM Security best practices, please refer to below URL: https://d1.IAMstatic.com/whitepapers/Security/IAM Security Best Practices.pdl
The correct answer is: Use IAM Inspector API's in the pipeline for the EC2 Instances Submit your Feedback/Queries to our Experts

**NEW QUESTION 203**
- (Exam Topic 3)
In your LAMP application, you have some developers that say they would like access to your logs. However, since you are using an IAM Auto Scaling group, your instances are constantly being re-created. What would you do to make sure that these developers can access these log files? Choose the correct answer from the options below
Please select:

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

**Answer:** D

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

**NEW QUESTION 204**
- (Exam Topic 3)
A large organization is planning on IAM to host their resources. They have a number of autonomous departments that wish to use IAM. What could be the strategy to adopt for managing the accounts.
Please select:

A. Use multiple VPCs in the account each VPC for each department
B. Use multiple IAM groups, each group for each department
C. Use multiple IAM roles, each group for each department
D. Use multiple IAM accounts, each account for each department

**Answer:** D

**Explanation:**
A recommendation for this is given in the IAM Security best practices Option A is incorrect since this would be applicable for resources in a VPC Options B and C are incorrect since operationally it would be difficult to manage For more information on IAM Security best practices please refer to the below URL
https://d1.IAMstatic.com/whitepapers/Security/IAM Security Best Practices.pdl
The correct answer is: Use multiple IAM accounts, each account for each department Submit your Feedback/Queries to our Experts

**NEW QUESTION 206**
- (Exam Topic 3)
A windows machine in one VPC needs to join the AD domain in another VPC. VPC Peering has been established. But the domain join is not working. What is the other step that needs to be followed to ensure that the AD domain join can work as intended
Please select:

A. Change the VPC peering connection to a VPN connection
B. Change the VPC peering connection to a Direct Connect connection
C. Ensure the security groups for the AD hosted subnet has the right rule for relevant subnets
D. Ensure that the AD is placed in a public subnet

**Answer:** C

**Explanation:**
In addition to VPC peering and setting the right route tables, the security groups for the AD EC2 instance needs to ensure the right rules are put in place for allowing incoming traffic.
Option A and B is invalid because changing the connection type will not help. This is a problem with the Security Groups.
Option D is invalid since the AD should not be placed in a public subnet
For more information on allowing ingress traffic for AD, please visit the following url
|https://docs.IAM.amazon.com/quickstart/latest/active-directory-ds/ingress.html|
The correct answer is: Ensure the security groups for the AD hosted subnet has the right rule for relevant subnets Submit your Feedback/Queries to our Experts

**NEW QUESTION 209**
- (Exam Topic 3)
A company had developed an incident response plan 18 months ago. Regular implementations of the response plan are carried out. No changes have been made to the response plan have been made since its creation. Which of the following is a right statement with regards to the plan?
Please select:

A. It places too much emphasis on already implemented security controls.
B. The response plan is not implemented on a regular basis
C. The response plan does not cater to new services
D. The response plan is complete in its entirety

**Answer:** C

**Explanation:**
So definitely the case here is that the incident response plan is not catering to newly created services. IAM keeps on changing and adding new services and hence the response plan must cater to these new services.
Option A and B are invalid because we don't know this for a fact.

Option D is invalid because we know that the response plan is not complete, because it does not cater to new features of IAM
For more information on incident response plan please visit the following URL: https://IAM.amazon.com/blogs/publicsector/buildins-a-cloud-specific-incident-response-plan;
The correct answer is: The response plan does not cater to new services Submit your Feedback/Queries to our Experts

**NEW QUESTION 210**
- (Exam Topic 3)
Your company is planning on using IAM EC2 and ELB for deployment for their web applications. The security policy mandates that all traffic should be encrypted. Which of the following options will ensure that this requirement is met. Choose 2 answers from the options below.
Please select:

A. Ensure the load balancer listens on port 80
B. Ensure the load balancer listens on port 443
C. Ensure the HTTPS listener sends requests to the instances on port 443
D. Ensure the HTTPS listener sends requests to the instances on port 80

**Answer:** BC

**Explanation:**
The IAM Documentation mentions the following
You can create a load balancer that listens on both the HTTP (80) and HTTPS (443) ports. If you specify that the HTTPS listener sends requests to the instances on port 80, the load balancer terminates the requests and communication from the load balancer to the instances is not encrypted, if the HTTPS listener sends requests to the instances on port 443, communication from the load balancer to the instances is encrypted.
Option A is invalid because there is a need for secure traffic, so port 80 should not be used Option D is invalid because for the HTTPS listener you need to use port 443
For more information on HTTPS with ELB, please refer to the below Link: https://docs.IAM.amazon.com/elasticloadbalancing/latest/classic/elb-create-https-ssl-load-balancer.htmll
The correct answers are: Ensure the load balancer listens on port 443, Ensure the HTTPS listener sends requests to the instances on port 443
Submit your Feedback/Queries to our Experts

**NEW QUESTION 214**
- (Exam Topic 3)
A company wishes to enable Single Sign On (SSO) so its employees can login to the management console using their corporate directory identity. Which steps below are required as part of the process? Select 2 answers from the options given below.
Please select:

A. Create a Direct Connect connection between on-premise network and IA
B. Use an AD connector for connecting IAM with on-premise active directory.
C. Create IAM policies that can be mapped to group memberships in the corporate directory.
D. Create a Lambda function to assign IAM roles to the temporary security tokens provided to the users.
E. Create IAM users that can be mapped to the employees' corporate identities
F. Create an IAM role that establishes a trust relationship between IAM and the corporate directory identity provider (IdP)

**Answer:** AE

**Explanation:**
Create a Direct Connect connection so that corporate users can access the IAM account
Option B is incorrect because IAM policies are not directly mapped to group memberships in the corporate directory. It is IAM roles which are mapped.
Option C is incorrect because Lambda functions is an incorrect option to assign roles.
Option D is incorrect because IAM users are not directly mapped to employees' corporate identities. For more information on Direct Connect, please refer to below URL:
' https://IAM.amazon.com/directconnect/
From the IAM Documentation, for federated access, you also need to ensure the right policy permissions are in place
Configure permissions in IAM for your federated users
The next step is to create an IAM role that establishes a trust relationship between IAM and your organization's IdP that identifies your IdP as a principal (trusted entity) for purposes of federation. The role also defines what users authenticated your organization's IdP are allowed to do in IAM. You can use the IAM console to create this role. When you create the trust policy that indicates who can assume the role, you specify the SAML provider that you created earlier in IAM along with one or more SAML attributes that a user must match to be allowed to assume the role. For example, you can specify that only users whose SAML eduPersonOrgDN value is ExampleOrg are allowed to sign in. The role wizard automatically adds a condition to test the saml:aud attribute to make sure that the role is assumed only for sign-in to the IAM Management Console. The trust policy for the role might look like this:
C:\Users\wk\Desktop\mudassar\Untitled.jpg

```
{
 "Version": "2012-10-17",
 "Statement": {{
  "Effect": "Allow",
  "Principal": {"Federated": "arn:aws:iam::ACCOUNT-ID-WITHOUT-HYPHENS:saml-provider/ExampleOrgSSOProvider"},
  "Action": "sts:AssumeRoleWithSAML",
  "Condition": {"StringEquals": {
   "saml:edupersonorgdn": "ExampleOrg",
   "saml:aud": "https://signin.aws.amazon.com/saml"
  }}
 }}
}
```

For more information on SAML federation, please refer to below URL: https://docs.IAM.amazon.com/IAM/latest/UserGuide/id_roles_providers_enabli Note:
What directories can I use with IAM SSO?

You can connect IAM SSO to Microsoft Active Directory, running either on-premises or in the IAM Cloud. IAM SSO supports IAM Directory Service for Microsoft Active Directory, also known as IAM Managed Microsoft AD, and AD Connector. IAM SSO does not support Simple AD. See IAM Directory Service Getting Started to learn more.
To connect to your on-premises directory with AD Connector, you need the following: VPC
Set up a VPC with the following:
• At least two subnets. Each of the subnets must be in a different Availability Zone.
• The VPC must be connected to your on-premises network through a virtual private network (VPN) connection or IAM Direct Connect.
• The VPC must have default hardware tenancy.
• https://IAM.amazon.com/single-sign-on/
• https://IAM.amazon.com/single-sign-on/faqs/
• https://IAM.amazon.com/bloj using-corporate-credentials/
• https://docs.IAM.amazon.com/directoryservice/latest/admin
The correct answers are: Create a Direct Connect connection between on-premise network and IAM. Use an AD connector connecting IAM with on-premise active directory.. Create an IAM role that establishes a trust relationship between IAM and corporate directory identity provider (IdP)
Submit your Feedback/Queries to our Experts

**NEW QUESTION 218**
- (Exam Topic 3)
You have several S3 buckets defined in your IAM account. You need to give access to external IAM accounts to these S3 buckets. Which of the following can allow you to define the permissions for the external accounts? Choose 2 answers from the options given below
Please select:

A. IAM policies
B. Buckets ACL's
C. IAM users
D. Bucket policies

**Answer:** BD

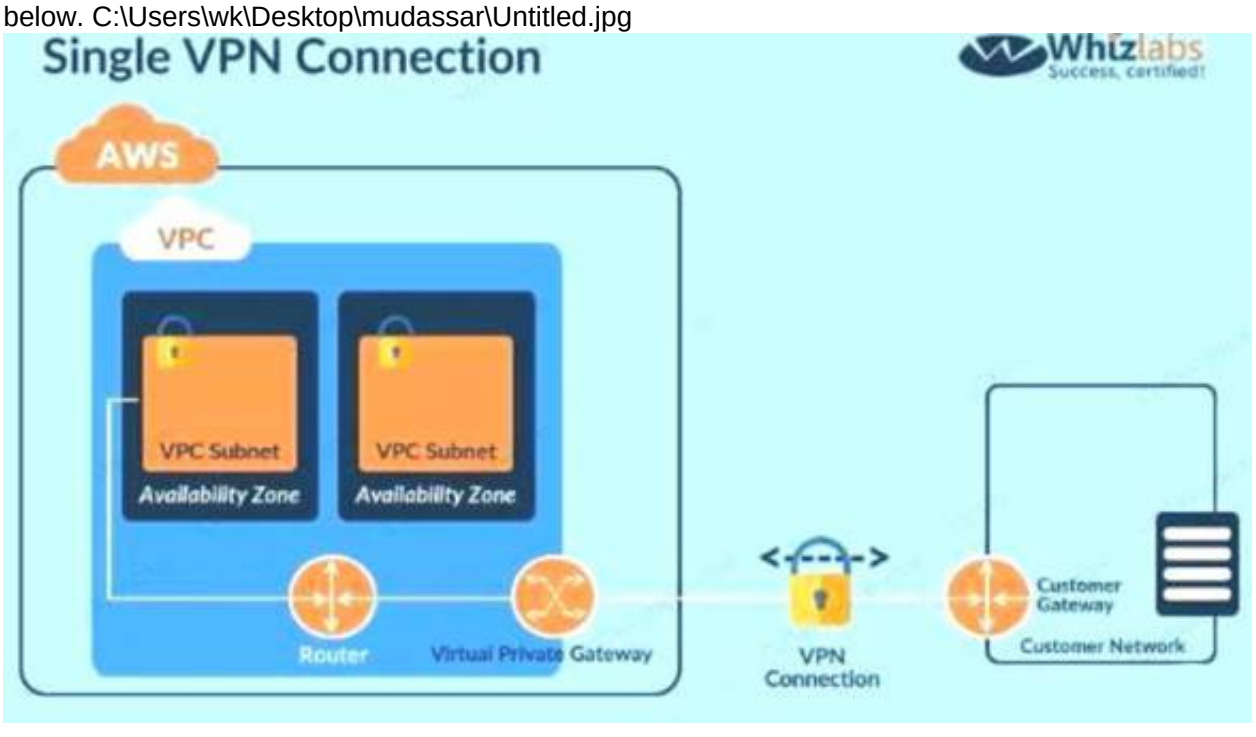
**Explanation:**
The IAM Security whitepaper gives the type of access control and to what level the control can be given Options A and C are incorrect since for external access to buckets, you need to use either Bucket policies or Bucket ACL's or more information on Security for storage services role please refer to the below URL: https://d1.IAMstatic.com/whitepapers/Security/Security Storage Services Whitepaper.pdf The correct answers are: Buckets ACL's, Bucket policies
Submit your Feedback/Queries to our Experts

**NEW QUESTION 220**
- (Exam Topic 3)
You have been given a new brief from your supervisor for a client who needs a web application set up on IAM. The a most important requirement is that MySQL must be used as the database, and this database must not be hosted in t« public cloud, but rather at the client's data center due to security risks. Which of the following solutions would be the ^ best to assure that the client's requirements are met? Choose the correct answer from the options below
Please select:

A. Build the application server on a public subnet and the database at the client's data cente
B. Connect them with a VPN connection which uses IPsec.
C. Use the public subnet for the application server and use RDS with a storage gateway to access and synchronize the data securely from the local data center.
D. Build the application server on a public subnet and the database on a private subnet with a NAT instance between them.
E. Build the application server on a public subnet and build the database in a private subnet with a secure ssh connection to the private subnet from the client's data center.

**Answer:** A

**Explanation:**
Since the database should not be hosted on the cloud all other options are invalid. The best option is to create a VPN connection for securing traffic as shown below. C:\Users\wk\Desktop\mudassar\Untitled.jpg




Option B is invalid because this is the incorrect use of the Storage gateway Option C is invalid since this is the incorrect use of the NAT instance Option D is invalid since this is an incorrect configuration For more information on VPN connections, please visit the below URL
http://docs.IAM.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.htmll
The correct answer is: Build the application server on a public subnet and the database at the client's data center. Connect them with a VPN connection which uses IPsec
Submit your Feedback/Queries to our Experts

**NEW QUESTION 225**
- (Exam Topic 3)
Your company has an external web site. This web site needs to access the objects in an S3 bucket. Which of the following would allow the web site to access the objects in the most secure manner?
Please select:

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

**Answer:** B

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

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

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

**NEW QUESTION 227**
- (Exam Topic 3)
A company is deploying a new web application on IAM. Based on their other web applications, they anticipate being the target of frequent DDoS attacks. Which steps can the company use to protect their application?
Select 2 answers from the options given below. Please select:

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

**Answer:** BD

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

**NEW QUESTION 232**
- (Exam Topic 3)
Your company hosts a large section of EC2 instances in IAM. There are strict security rules governing the EC2 Instances. During a potential security breach , you need to ensure quick investigation of the underlying EC2 Instance. Which of the following service can help you quickly provision a test environment to look into the breached instance.
Please select:

A. IAM Cloudwatch
B. IAM Cloudformation
C. IAM Cloudtrail
D. IAM Config

**Answer:** B

**Explanation:**
The IAM Security best practises mentions the following
Unique to IAM, security practitioners can use CloudFormation to quickly create a new, trusted environment in which to conduct deeper investigation. The CloudFormation template can pre-configure instances in an isolated environment that contains all the necessary tools forensic teams need to determine the cause of the incident This cuts down on the time it takes to gather necessary tools, isolates systems under examination, and ensures that the team is operating in a clean room.
Option A is incorrect since this is a logging service and cannot be used to provision a test environment Option C is incorrect since this is an API logging service and cannot be used to provision a test environment Option D is incorrect since this is a configuration service and cannot be used to provision a test environment
For more information on IAM Security best practises, please refer to below URL: https://d1.IAMstatic.com/whitepapers/architecture/IAM-Security-Pillar.pd1
The correct answer is: IAM Cloudformation Submit your Feedback/Queries to our Experts

**NEW QUESTION 236**
- (Exam Topic 3)
You have an EBS volume attached to an EC2 Instance which uses KMS for Encryption. Someone has now gone ahead and deleted the Customer Key which was used for the EBS encryption. What should be done to ensure the data can be decrypted.
Please select:

A. Create a new Customer Key using KMS and attach it to the existing volume
B. You cannot decrypt the data that was encrypted under the CMK, and the data is not recoverable.
C. Request IAM Support to recover the key
D. Use IAM Config to recover the key

**Answer:** B

**Explanation:**
Deleting a customer master key (CMK) in IAM Key Management Service (IAM KMS) is destructive and potentially dangerous. It deletes the key material and all metadata associated with the CMK, and is irreversible. After a CMK is deleted you can no longer decrypt the data that was encrypted under that CMK, which means that data becomes unrecoverable. You should delete a CMK only when you are sure that you don't need to use it anymore. If you are not sure, consider disabling the CMK instead of deleting it. You can re-enable a disabled CMK if you need to use it again later, but you cannot recover a deleted CMK.
https://docs.IAM.amazon.com/kms/latest/developerguide/deleting-keys.html
A is incorrect because Creating a new CMK and attaching it to the exiting volume will not allow the data to be decrypted, you cannot attach customer master keys after the volume is encrypted
Option C and D are invalid because once the key has been deleted, you cannot recover it For more information on EBS Encryption with KMS, please visit the following URL:
https://docs.IAM.amazon.com/kms/latest/developerguide/services-ebs.html
The correct answer is: You cannot decrypt the data that was encrypted under the CMK, and the data is not recoverable. Submit your Feedback/Queries to our Experts

**NEW QUESTION 240**
.....

# 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