# Amazon-Web-Services

## Exam Questions SCS-C02

AWS Certified Security - Specialty

**NEW QUESTION 1**
- (Exam Topic 1)
Which of the following are valid configurations for using SSL certificates with Amazon CloudFront? (Select THREE )

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

**Answer:** ACD

**NEW QUESTION 2**
- (Exam Topic 1)
A company has a website with an Amazon CloudFront HTTPS distribution, an Application Load Balancer (ALB) with multiple web instances for dynamic website content, and an Amazon S3 bucket for static website content. The company's security engineer recently updated the website security requirements:
• HTTPS needs to be enforced for all data in transit with specific ciphers.
• The CloudFront distribution needs to be accessible from the internet only. Which solution will meet these requirements?

A. Set up an S3 bucket policy with the IAMsecuretransport key Configure the CloudFront origin access identity (OAI) with the S3 bucket Configure CloudFront to use specific cipher
B. Enforce the ALB with an HTTPS listener only and select the appropriate security policy for the ciphers Link the ALB with IAM WAF to allow access from the CloudFront IP ranges.
C. Set up an S3 bucket policy with the IAM:securetransport ke
D. Configure the CloudFront origin access identity (OAI) with the S3 bucke
E. Enforce the ALB with an HTTPS listener only and select the appropriate security policy for the ciphers.
F. Modify the CloudFront distribution to use IAM WA
G. Force HTTPS on the S3 bucket with specific ciphers in the bucket polic
H. Configure an HTTPS listener only for the AL
I. Set up a security group to limit access to the ALB from the CloudFront IP ranges
J. Modify the CloudFront distribution to use the ALB as the origi
K. Enforce an HTTPS listener on the AL
L. Create a path-based routing rule on the ALB with proxies that connect lo Amazon S3. Create a bucket policy to allow access from these proxies only.

**Answer:** A

**Explanation:**
https://IAM.amazon.com/blogs/security/automatically-update-IAM-waf-ip-sets-with-IAM-ip-ranges/ to update CF ip range.

**NEW QUESTION 3**
- (Exam Topic 1)
The Security Engineer is managing a traditional three-tier web application that is running on Amazon EC2 instances. The application has become the target of increasing numbers of malicious attacks from the Internet.
What steps should the Security Engineer take to check for known vulnerabilities and limit the attack surface? (Choose two.)

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

**Answer:** BD

**NEW QUESTION 4**
- (Exam Topic 1)
A Web Administrator for the website example.com has created an Amazon CloudFront distribution for dev.example.com, with a requirement to configure HTTPS using a custom TLS certificate imported to IAM Certificate Manager.
Which combination of steps is required to ensure availability of the certificate in the CloudFront console? (Choose two.)

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

**Answer:** DE

**NEW QUESTION 5**
- (Exam Topic 1)
A security engineer is designing an incident response plan to address the risk of a compromised Amazon EC2 instance. The plan must recommend a solution to meet the following requirements:
• A trusted forensic environment must be provisioned
• Automated response processes must be orchestrated
Which IAM services should be included in the plan? {Select TWO)

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

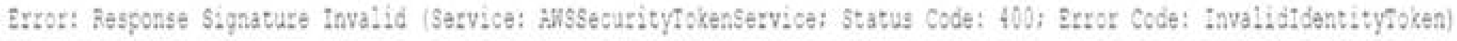
**Answer:** AE

**NEW QUESTION 6**
- (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 7**
- (Exam Topic 1)
A company uses a third-party identity provider and SAML-based SSO for its IAM accounts After the third-party identity provider renewed an expired signing certificate users saw the following message when trying to log in:



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

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

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

**Answer:** C

**NEW QUESTION 8**
- (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 9**
- (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 10**
- (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 10**
- (Exam Topic 1)
A company recently performed an annual security assessment of its IAM environment. The assessment showed that audit logs are not available beyond 90 days and that unauthorized changes to IAM policies are made without detection.
How should a security engineer resolve these issues?

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

**Answer:** D

**Explanation:**
https://docs.IAM.amazon.com/IAMcloudtrail/latest/userguide/best-practices-security.html
"For an ongoing record of events in your IAM account, you must create a trail. Although CloudTrail provides 90 days of event history information for management events in the CloudTrail console without creating a trail, it is not a permanent record, and it does not provide information about all possible types of events. For an ongoing record, and for a record that contains all the event types you specify, you must create a trail, which delivers log files to an Amazon S3 bucket that you specify."
https://IAM.amazon.com/blogs/security/how-to-record-and-govern-your-iam-resource-configurations-using-IAM

**NEW QUESTION 15**
- (Exam Topic 1)
A company wants to encrypt the private network between its orvpremises environment and IAM. The company also wants a consistent network experience for its employees.
What should the company do to meet these requirements?

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

**Answer:** D

**NEW QUESTION 20**
- (Exam Topic 1)
A security engineer need to ensure their company’s uses of IAM meets IAM security best practices. As part of this, the IAM account root user must not be used for daily work. The root user must be monitored for use, and the Security team must be alerted as quickly as possible if the root user is used.
Which solution meets these requirements?

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

**Answer:** A

**NEW QUESTION 21**
- (Exam Topic 1)
A company uses multiple IAM accounts managed with IAM Organizations Security engineers have created a standard set of security groups for all these accounts. The security policy requires that these security groups be used for all applications and delegates modification authority to the security team only.
A recent security audit found that the security groups are inconsistency implemented across accounts and that unauthorized changes have been made to the security groups. A security engineer needs to recommend a solution to improve consistency and to prevent unauthorized changes in the individual accounts in the future.
Which solution should the security engineer recommend?

A. Use IAM Resource Access Manager to create shared resources for each requited security group and apply an IAM policy that permits read-only access to the security groups only.
B. Create an IAM CloudFormation template that creates the required security groups Execute the template as part of configuring new accounts Enable Amazon

Simple Notification Service (Amazon SNS) notifications when changes occur
C. Use IAM Firewall Manager to create a security group policy, enable the policy feature to identify and revert local changes, and enable automatic remediation
D. Use IAM Control Tower to edit the account factory template to enable the snare security groups option Apply an SCP to the OU or individual accounts that prohibits security group modifications from local account users

**Answer:** B

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

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

**Answer:** B

**NEW QUESTION 28**
- (Exam Topic 1)
A company is designing the securely architecture (or a global latency-sensitive web application it plans to deploy to IAM. A Security Engineer needs to configure a highly available and secure two-tier architecture. The security design must include controls to prevent common attacks such as DDoS, cross-site scripting, and SQL injection.
Which solution meets these requirements?

A. Create an Application Load Balancer (ALB) that uses public subnets across multiple Availability Zones within a single Regio
B. Point the ALB to an Auto Scaling group with Amazon EC2 instances in private subnets across multiple Availability Zones within the same Regio
C. Create an AmazonCloudFront distribution that uses the ALB as its origi
D. Create appropriate IAM WAF ACLs and enable them on the CloudFront distribution.
E. Create an Application Load Balancer (ALB) that uses private subnets across multiple Availability Zones within a single Regio
F. Point the ALB to an Auto Scaling group with Amazon EC2 instances in private subnets across multiple Availability Zones within the same Regio
G. Create an Amazon CloudFront distribution that uses the ALB as its origi
H. Create appropriate IAM WAF ACLs and enable them on the CloudFront distribution.
I. Create an Application Load Balancer (ALB) that uses public subnets across multiple Availability Zones within a single Regio
J. Point the ALB to an Auto Scaling group with Amazon EC2 instances in private subnets across multiple Availability Zones within the same Regio
K. Create appropriate IAM WAF ACLs and enable them on the ALB.
L. Create an Application Load Balancer (ALB) that uses private subnets across multiple Availability Zones within a single Regio
M. Point the ALB to an Auto Scaling group with Amazon EC2 instances in private subnets across multiple Availability Zones within the same Regio
N. Create appropriate IAM WAF ACLs and enable them on the ALB.

**Answer:** A

**NEW QUESTION 31**
- (Exam Topic 1)
A Security Engineer for a large company is managing a data processing application used by 1,500 subsidiary companies. The parent and subsidiary companies all use IAM. The application uses TCP port 443 and runs on Amazon EC2 behind a Network Load Balancer (NLB). For compliance reasons, the application should only be accessible to the subsidiaries and should not be available on the public internet. To meet the compliance requirements for restricted access, the Engineer has received the public and private CIDR block ranges for each subsidiary
What solution should the Engineer use to implement the appropriate access restrictions for the application?

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

**Answer:** D

**NEW QUESTION 36**
- (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 40**
- (Exam Topic 1)
A Security Engineer is setting up an IAM CloudTrail trail for all regions in an IAM account. For added security, the logs are stored using server-side encryption with IAM KMS-managed keys (SSE-KMS) and have log integrity validation enabled.
While testing the solution, the Security Engineer discovers that the digest files are readable, but the log files are not. What is the MOST likely cause?

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

**Answer:** B

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

**NEW QUESTION 44**
- (Exam Topic 1)
A Security Engineer has discovered that, although encryption was enabled on the Amazon S3 bucket example bucket, anyone who has access to the bucket has the ability to retrieve the files. The Engineer wants to limit access to each IAM user can access an assigned folder only.
What should the Security Engineer do to achieve this?

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

**Answer:** B

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

**NEW QUESTION 49**
- (Exam Topic 1)
Authorized Administrators are unable to connect to an Amazon EC2 Linux bastion host using SSH over the internet. The connection either fails to respond or generates the following error message:
Network error: Connection timed out.
What could be responsible for the connection failure? (Select THREE )

A. The NAT gateway in the subnet where the EC2 instance is deployed has been misconfigured
B. The internet gateway of the VPC has been reconfigured
C. The security group denies outbound traffic on ephemeral ports
D. The route table is missing a route to the internet gateway
E. The NACL denies outbound traffic on ephemeral ports
F. The host-based firewall is denying SSH traffic

**Answer:** BDF

**NEW QUESTION 53**
- (Exam Topic 1)
A Security Administrator at a university is configuring a fleet of Amazon EC2 instances. The EC2 instances are shared among students, and non-root SSH access is allowed. The Administrator is concerned about students attacking other IAM account resources by using the EC2 instance metadata service.
What can the Administrator do to protect against this potential attack?

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

**Answer:** A

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

metadata-options.html

**NEW QUESTION 57**
- (Exam Topic 1)
A company's web application is hosted on Amazon EC2 instances running behind an Application Load Balancer (ALB) in an Auto Scaling group. An IAM WAF web ACL is associated with the ALB. IAM CloudTrail is enabled, and stores logs in Amazon S3 and Amazon CloudWatch Logs.
The operations team has observed some EC2 instances reboot at random. After rebooting, all access logs on the instances have been deleted. During an investigation, the operations team found that each reboot happened just after a PHP error occurred on the new-user-creation.php file. The operations team needs to view log information to determine if the company is being attacked.
Which set of actions will identify the suspect attacker's IP address for future occurrences?

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

**Answer:** D

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

**NEW QUESTION 62**
- (Exam Topic 1)
A company has hundreds of IAM accounts, and a centralized Amazon S3 bucket used to collect IAM CloudTrail for all of these accounts. A security engineer wants to create a solution that will enable the company to run ad hoc queues against its CloudTrail logs dating back 3 years from when the trails were first enabled in the company's IAM account.
How should the company accomplish this with the least amount of administrative overhead?

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

**Answer:** D

**NEW QUESTION 65**
- (Exam Topic 1)
A company has several workloads running on IAM. Employees are required to authenticate using on-premises ADFS and SSO to access the IAM Management Console. Developers migrated an existing legacy web application to an Amazon EC2 instance. Employees need to access this application from anywhere on the internet, but currently, there is no authentication system built into the application.
How should the Security Engineer implement employee-only access to this system without changing the application?

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

**Answer:** A

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

**NEW QUESTION 69**
- (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 71**

- (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 76**
- (Exam Topic 1)
A security engineer must use IAM Key Management Service (IAM KMS) to design a key management solution for a set of Amazon Elastic Block Store (Amazon EBS) volumes that contain sensitive data. The solution needs to ensure that the key material automatically expires in 90 days.
Which solution meets these criteria?

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

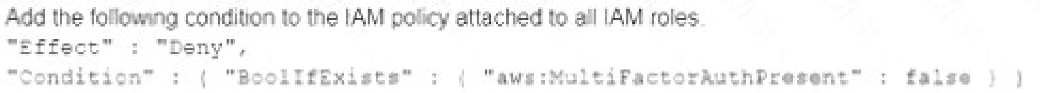
**Answer:** B

**NEW QUESTION 81**
- (Exam Topic 1)
A company wants to encrypt data locally while meeting regulatory requirements related to key exhaustion. The encryption key can be no more than 10 days old or encrypt more than 2" 16 objects Any encryption key must be generated on a FlPS-validated hardware security module (HSM). The company is cost-conscious, as plans to upload an average of 100 objects to Amazon S3 each second for sustained operations across 5 data producers
When approach MOST efficiently meets the company's needs?

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

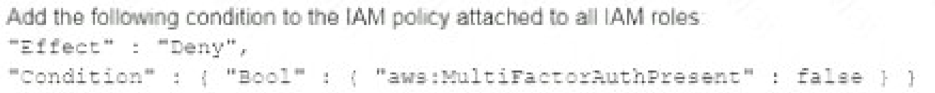
**Answer:** A

**NEW QUESTION 82**
- (Exam Topic 1)
A company has an IAM account and allows a third-party contractor who uses another IAM account, to assume certain IAM roles. The company wants to ensure that IAM roles can be assumed by the contractor only if the contractor has multi-factor authentication enabled on their IAM user accounts
What should the company do to accomplish this?
A)



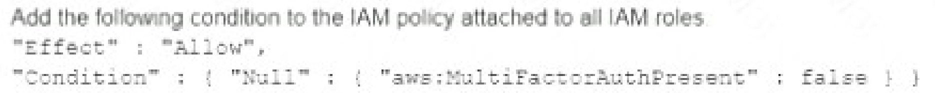
Add the following condition to the IAM policy attached to all IAM roles.
```
"Effect" : "Deny",
"Condition" : { "BoolIfExists" : { "aws:MultiFactorAuthPresent" : false } }
```

B)



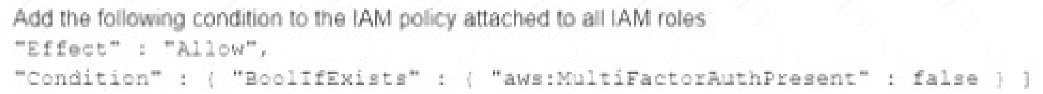
Add the following condition to the IAM policy attached to all IAM roles:
```
"Effect" : "Deny",
"Condition" : { "Bool" : { "aws:MultiFactorAuthPresent" : false } }
```

C)



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

D)



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

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

**Answer:** A

**NEW QUESTION 87**
- (Exam Topic 1)
A company needs its Amazon Elastic Block Store (Amazon EBS) volumes to be encrypted at all times. During a security incident. EBS snapshots of suspicious instances are shared to a forensics account for analysis A security engineer attempting to share a suspicious EBS snapshot to the forensics account receives the

following error
"Unable to share snapshot: An error occurred (OperationNotPermitted) when calling the ModifySnapshotAttribute operation: Encrypted snapshots with EBS default key cannot be shared.
Which combination of steps should the security engineer take in the incident account to complete the sharing operation? (Select THREE )

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

**Answer:** ABF

**NEW QUESTION 88**
- (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 89**
- (Exam Topic 1)
An employee accidentally exposed an IAM access key and secret access key during a public presentation. The company Security Engineer immediately disabled the key.
How can the Engineer assess the impact of the key exposure and ensure that the credentials were not misused? (Choose two.)

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

**Answer:** AD

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

**NEW QUESTION 94**
- (Exam Topic 1)
A company has decided to use encryption in its IAM account to secure the objects in Amazon S3 using server-side encryption. Object sizes range from 16.000 B to 5 MB. The requirements are as follows:
• The key material must be generated and stored in a certified Federal Information Processing Standard (FIPS) 140-2 Level 3 machine.
• The key material must be available in multiple Regions. Which option meets these requirements?

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

**Answer:** D

**NEW QUESTION 95**
- (Exam Topic 1)
A security engineer has noticed that VPC Flow Logs are getting a lot REJECT traffic originating from a single Amazon EC2 instance in an Auto Scaling group. The security engineer is concerned that this EC2 instance may be compromised.
What immediate action should the security engineer take? What immediate action should the security engineer take?

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

**Answer:** B

**NEW QUESTION 98**
- (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 102**
- (Exam Topic 2)
A company plans to migrate a sensitive dataset to Amazon S3. A Security Engineer must ensure that the data is encrypted at rest. The encryption solution must enable the company to generate its own keys without needing to manage key storage or the encryption process.
What should the Security Engineer use to accomplish this?

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

**Answer:** B

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

**NEW QUESTION 106**
- (Exam Topic 2)
You have a web site that is sitting behind IAM Cloudfront. You need to protect the web site against threats such as SQL injection and Cross site scripting attacks. Which of the following service can help in such a scenario Please select:

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

**Answer:** B

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

**NEW QUESTION 108**
- (Exam Topic 2)
You have an S3 bucket hosted in IAM. This is used to host promotional videos uploaded by yourself. You need to provide access to users for a limited duration of time. How can this be achieved?
Please select:

A. Use versioning and enable a timestamp for each version
B. Use Pre-signed URL's
C. Use IAM Roles with a timestamp to limit the access
D. Use IAM policies with a timestamp to limit the access

**Answer:** B

**Explanation:**
The IAM Documentation mentions the following

All objects by default are private. Only the object owner has permission to access these objects. However, the object owner can optionally share objects with others by creating a pre-signed URL using their own security credentials, to grant time-limited permission to download the objects.
Option A is invalid because this can be used to prevent accidental deletion of objects Option C is invalid because timestamps are not possible for Roles
Option D is invalid because policies is not the right way to limit access based on time For more information on pre-signed URL's, please visit the URL:
https://docs.IAM.ama2on.com/AmazonS3/latest/dev/ShareObiectPreSisnedURL.html
The correct answer is: Use Pre-signed URL's Submit your Feedback/Queries to our Experts

**NEW QUESTION 109**
- (Exam Topic 2)
Example.com hosts its internal document repository on Amazon EC2 instances. The application runs on EC2 instances and previously stored the documents on encrypted Amazon EBS volumes. To optimize the application for scale, example.com has moved the files to Amazon S3. The security team has mandated that all the files are securely deleted from the EBS volume, and it must certify that the data is unreadable before releasing the underlying disks.
Which of the following methods will ensure that the data is unreadable by anyone else?

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

**Answer:** D

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

**NEW QUESTION 113**
- (Exam Topic 2)
A security team must present a daily briefing to the CISO that includes a report of which of the company's thousands of EC2 instances and on-premises servers are missing the latest security patches. All instances/servers must be brought into compliance within 24 hours so they do not show up on the next day's report.
How can the security team fulfill these requirements?
Please select:

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

**Answer:** B

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

**NEW QUESTION 114**
- (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 119**
- (Exam Topic 2)
An organization wants to deploy a three-tier web application whereby the application servers run on Amazon EC2 instances. These EC2 instances need access to credentials that they will use to authenticate their SQL connections to an Amazon RDS DB instance. Also, IAM Lambda functions must issue queries to the RDS database by using the same database credentials.
The credentials must be stored so that the EC2 instances and the Lambda functions can access them. No other access is allowed. The access logs must record when the credentials were accessed and by whom.
What should the Security Engineer do to meet these requirements?

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

**Answer:** D

**NEW QUESTION 120**
- (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 125**
- (Exam Topic 2)
A company hosts a popular web application that connects to an Amazon RDS MySQL DB instance running in a private VPC subnet that was created with default ACL settings. The IT Security department has a suspicion that a DDos attack is coming from a suspecting IP. How can you protect the subnets from this attack?
Please select:

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

**Answer:** C

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

**NEW QUESTION 128**
- (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 132**
- (Exam Topic 2)
What are the MOST secure ways to protect the IAM account root user of a recently opened IAM account? (Choose two.)

A. Use the IAM account root user access keys instead of the IAM Management Console
B. Enable multi-factor authentication for the IAM IAM users with the AdministratorAccess managed policy attached to them
C. Enable multi-factor authentication for the IAM account root user
D. Use IAM KMS to encrypt all IAM account root user and IAM IAM access keys and set automatic rotation to 30 days
E. Do not create access keys for the IAM account root user; instead, create IAM IAM users

**Answer:** CE

**NEW QUESTION 135**
- (Exam Topic 2)
Which option for the use of the IAM Key Management Service (KMS) supports key management best practices that focus on minimizing the potential scope of data exposed by a possible future key compromise?

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

**Answer:** A

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

**NEW QUESTION 138**
- (Exam Topic 2)
A Security Administrator is performing a log analysis as a result of a suspected IAM account compromise. The Administrator wants to analyze suspicious IAM CloudTrail log files but is overwhelmed by the volume of audit logs being generated.
What approach enables the Administrator to search through the logs MOST efficiently?

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

**Answer:** C

**NEW QUESTION 141**
- (Exam Topic 2)
An organization wants to be alerted when an unauthorized Amazon EC2 instance in its VPC performs a network port scan against other instances in the VPC. When the Security team performs its own internal tests in a separate account by using pre-approved third-party scanners from the IAM Marketplace, the Security team also then receives multiple Amazon GuardDuty events from Amazon CloudWatch alerting on its test activities.
How can the Security team suppress alerts about authorized security tests while still receiving alerts about the unauthorized activity?

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

**Answer:** B

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

**NEW QUESTION 143**
- (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 147**
- (Exam Topic 2)
Due to new compliance requirements, a Security Engineer must enable encryption with customer-provided keys on corporate data that is stored in DynamoDB.
The company wants to retain full control of the encryption keys.
Which DynamoDB feature should the Engineer use to achieve compliance'?

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

**Answer:** D

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

**NEW QUESTION 148**
- (Exam Topic 2)
A Security Engineer is trying to determine whether the encryption keys used in an IAM service are in compliance with certain regulatory standards.
Which of the following actions should the Engineer perform to get further guidance?

A. Read the IAM Customer Agreement.
B. Use IAM Artifact to access IAM compliance reports.
C. Post the question on the IAM Discussion Forums.
D. Run IAM Config and evaluate the configuration outputs.

**Answer:** B

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

**NEW QUESTION 150**
- (Exam Topic 2)
A threat assessment has identified a risk whereby an internal employee could exfiltrate sensitive data from production host running inside IAM (Account 1). The threat was documented as follows:
Threat description: A malicious actor could upload sensitive data from Server X by configuring credentials for an IAM account (Account 2) they control and uploading data to an Amazon S3 bucket within their control.
Server X has outbound internet access configured via a proxy server. Legitimate access to S3 is required so that the application can upload encrypted files to an S3 bucket. Server X is currently using an IAM instance role. The proxy server is not able to inspect any of the server communication due to TLS encryption.
Which of the following options will mitigate the threat? (Choose two.)

A. Bypass the proxy and use an S3 VPC endpoint with a policy that whitelists only certain S3 buckets within Account 1.
B. Block outbound access to public S3 endpoints on the proxy server.
C. Configure Network ACLs on Server X to deny access to S3 endpoints.
D. Modify the S3 bucket policy for the legitimate bucket to allow access only from the public IP addressesassociated with the application server.
E. Remove the IAM instance role from the application server and save API access keys in a trusted and encrypted application config file.

**Answer:** AB

**NEW QUESTION 153**
- (Exam Topic 2)

A company maintains sensitive data in an Amazon S3 bucket that must be protected using an IAM KMS CMK. The company requires that keys be rotated automatically every year. How should the bucket be configured?

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

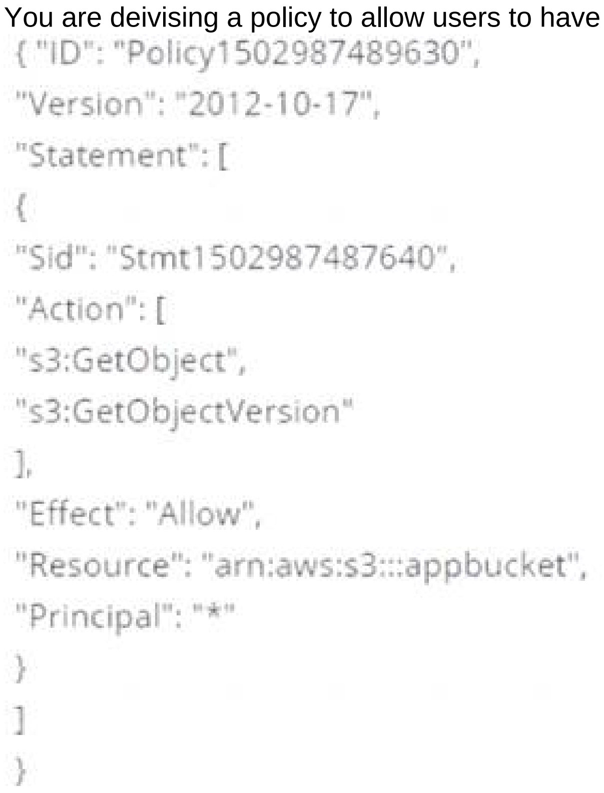
**Answer:** B

**NEW QUESTION 157**
- (Exam Topic 2)
A Security Administrator has a website hosted in Amazon S3. The Administrator has been given the following requirements:
> Users may access the website by using an Amazon CloudFront distribution.
> Users may not access the website directly by using an Amazon S3 URL.
Which configurations will support these requirements? (Choose two.)

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

**Answer:** AC

**NEW QUESTION 160**
- (Exam Topic 2)
You are deivising a policy to allow users to have the ability to access objects in a bucket called appbucket. You define the below custom bucket policy



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

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

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

**Answer:** C

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

**NEW QUESTION 164**
- (Exam Topic 2)
A Systems Engineer has been tasked with configuring outbound mail through Simple Email Service (SES) and requires compliance with current TLS standards.
The mail application should be configured to connect to which of the following endpoints and corresponding ports?

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

**Answer:** C

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

**NEW QUESTION 165**
- (Exam Topic 2)
An IAM Lambda function was misused to alter data, and a Security Engineer must identify who invoked the function and what output was produced. The Engineer cannot find any logs created by the Lambda function in Amazon CloudWatch Logs.
Which of the following explains why the logs are not available?

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

**Answer:** A

**NEW QUESTION 167**
- (Exam Topic 2)
A company runs an application on IAM that needs to be accessed only by employees. Most employees work from the office, but others work remotely or travel.
How can the Security Engineer protect this workload so that only employees can access it?

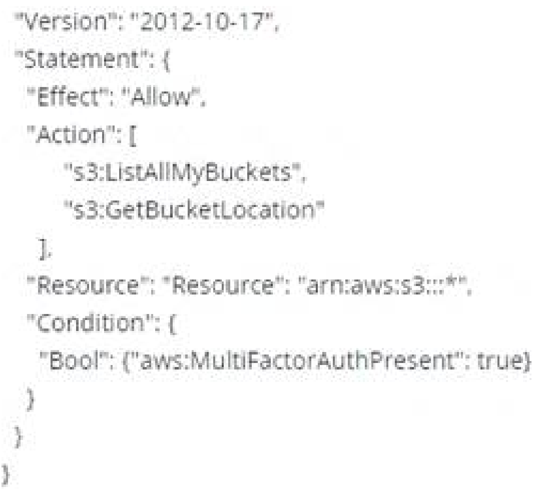
A. Add each employee’s home IP address to the security group for the application so that only those users can access the workload.
B. Create a virtual gateway for VPN connectivity for each employee, and restrict access to the workload from within the VPC.
C. Use a VPN appliance from the IAM Marketplace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

**Answer:** C

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

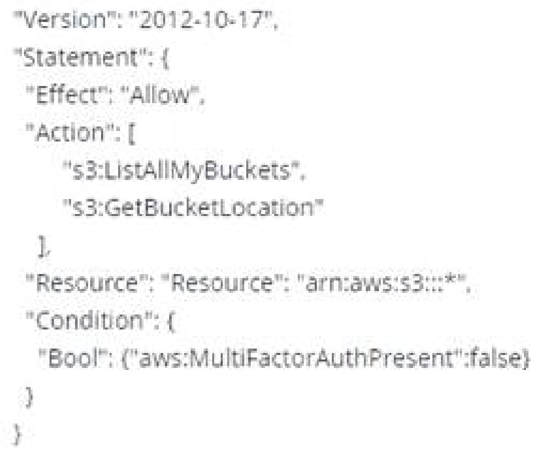
**NEW QUESTION 172**
- (Exam Topic 2)
You are designing a custom IAM policy that would allow uses to list buckets in S3 only if they are MFA authenticated. Which of the following would best match this requirement?

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



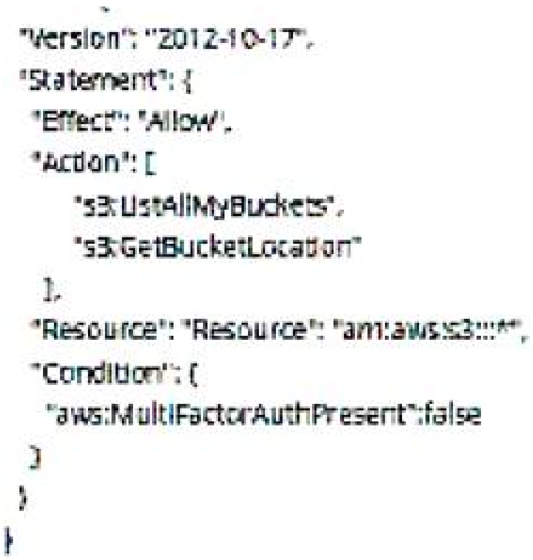
```
"Version": "2012-10-17",
"Statement": {
  "Effect": "Allow",
  "Action": [
      "s3:ListAllMyBuckets",
      "s3:GetBucketLocation"
   ],
  "Resource": "Resource": "arn:aws:s3:::*",
  "Condition": {
   "Bool": {"aws:MultiFactorAuthPresent": true}
  }
 }
}
```

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



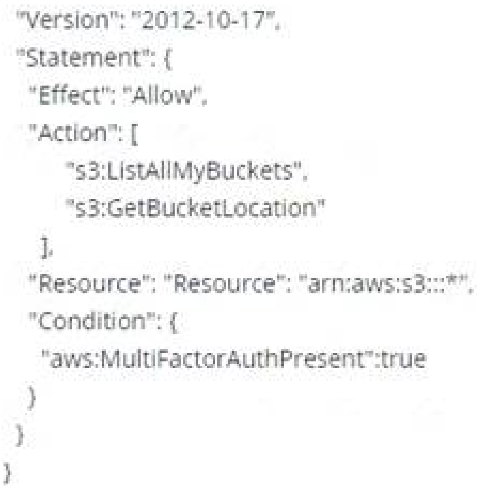
```
"Version": "2012-10-17",
"Statement": {
  "Effect": "Allow",
  "Action": [
      "s3:ListAllMyBuckets",
      "s3:GetBucketLocation"
   ],
  "Resource": "Resource": "arn:aws:s3:::*",
  "Condition": {
   "Bool": {"aws:MultiFactorAuthPresent":false}
  }
 }
```

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



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

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



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

**Answer:** A

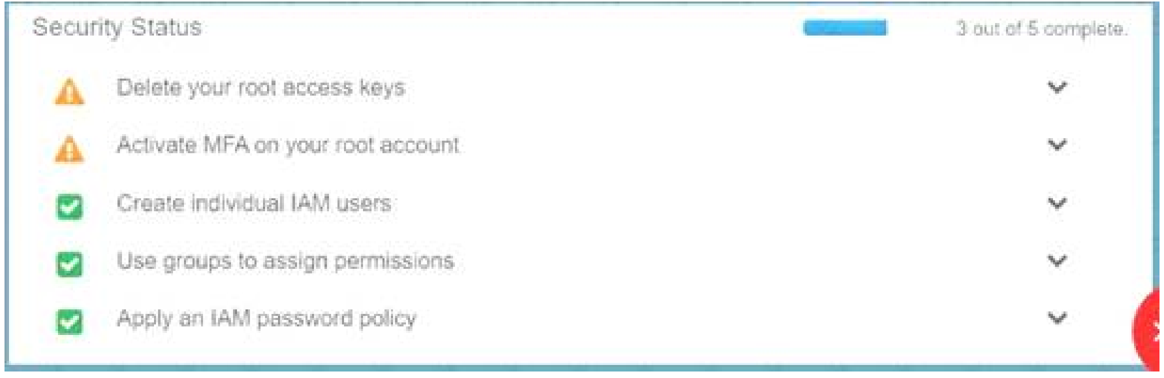
**Explanation:**
The Condition clause can be used to ensure users can only work with resources if they are MFA authenticated. Option B and C are wrong since the IAM:MultiFactorAuthPresent clause should be marked as true. Here you are saying that onl if the user has been MFA activated, that means it is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

**NEW QUESTION 177**
- (Exam Topic 2)
Your development team has started using IAM resources for development purposes. The IAM account has just been created. Your IT Security team is worried about possible leakage of IAM keys. What is the first level of measure that should be taken to protect the IAM account.
Please select:

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

**Answer:** A

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



Security Status — 3 out of 5 complete.

⚠ Delete your root access keys
⚠ Activate MFA on your root account
☑ Create individual IAM users
☑ Use groups to assign permissions
☑ Apply an IAM password policy

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

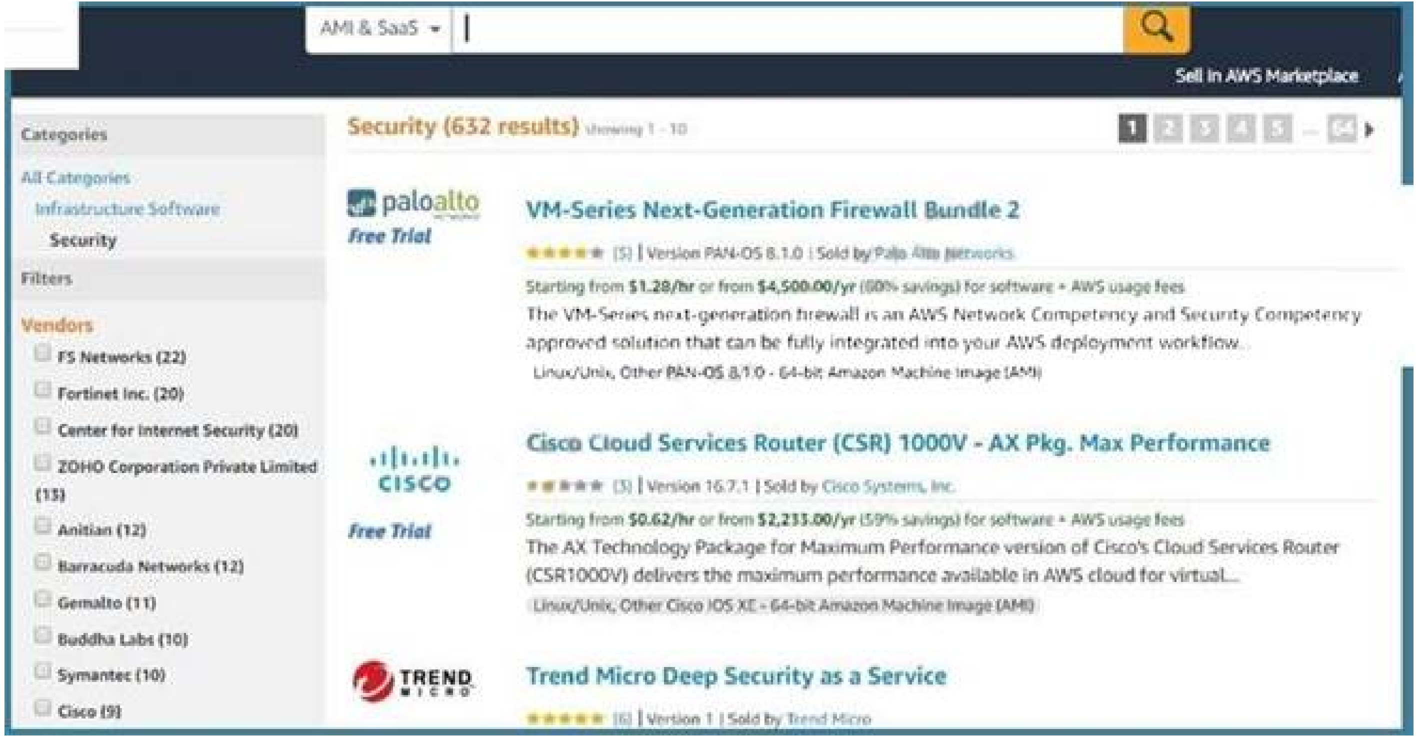
**NEW QUESTION 182**
- (Exam Topic 2)
A company wants to have an Intrusion detection system available for their VPC in IAM. They want to have complete control over the system. Which of the following would be ideal to implement?

Please select:

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

**Answer:** B

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



VM-Series Next-Generation Firewall Bundle 2

★★★★★ (5) | Version PAN-OS 8.1.0 | Sold by Palo Alto Networks

Starting from $1.28/hr or from $4,500.00/yr (60% savings) for software + AWS usage fees
The VM-Series next-generation firewall is an AWS Network Competency and Security Competency approved solution that can be fully integrated into your AWS deployment workflow.
Linux/Unix, Other PAN-OS 8.1.0 - 64-bit Amazon Machine Image (AMI)

Cisco Cloud Services Router (CSR) 1000V - AX Pkg. Max Performance

★★★★★ (3) | Version 16.7.1 | Sold by Cisco Systems, Inc.

Starting from $0.62/hr or from $2,233.00/yr (59% savings) for software + AWS usage fees
The AX Technology Package for Maximum Performance version of Cisco's Cloud Services Router (CSR1000V) delivers the maximum performance available in AWS cloud for virtual...
Linux/Unix, Other Cisco IOS XE - 64-bit Amazon Machine Image (AMI)

Trend Micro Deep Security as a Service

★★★★★ (6) | Version 1 | Sold by Trend Micro

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

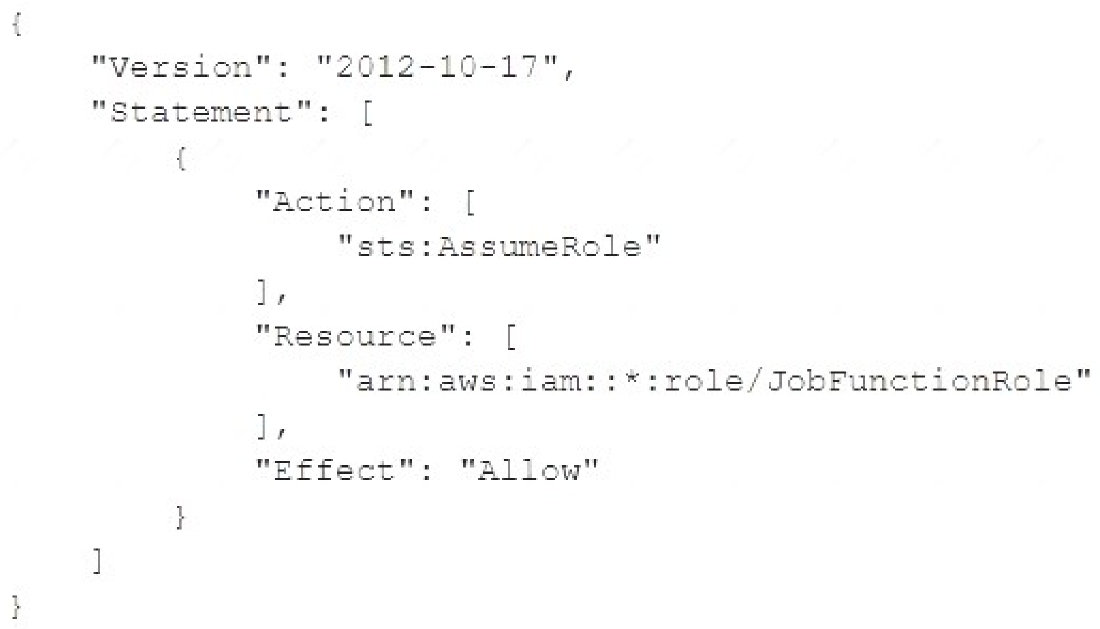
**NEW QUESTION 185**
- (Exam Topic 2)
A Developer who is following IAM best practices for secure code development requires an application to encrypt sensitive data to be stored at rest, locally in the application, using IAM KMS. What is the simplest and MOST secure way to decrypt this data when required?

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

**Answer:** D

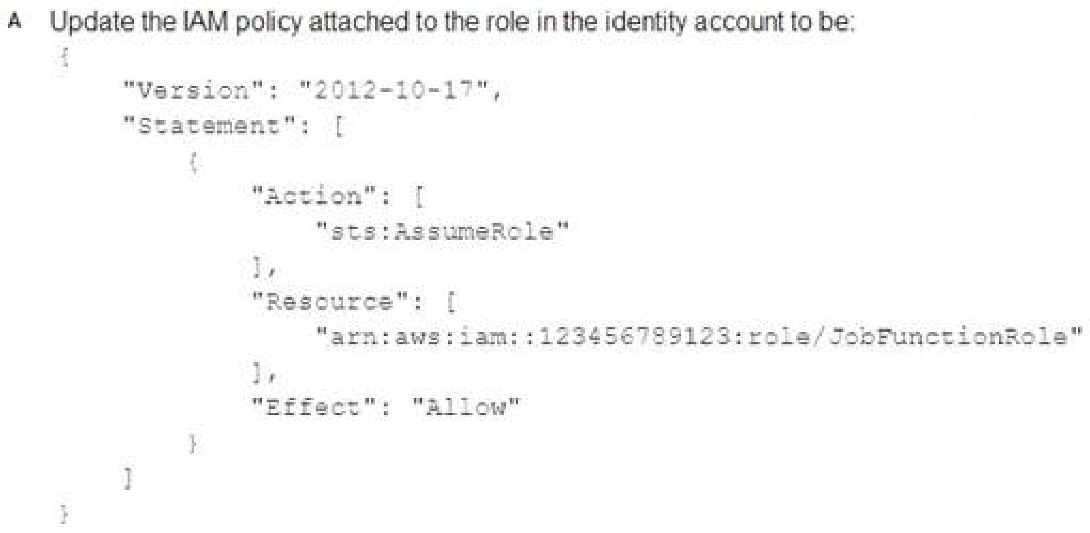
**Explanation:**
We recommend that you use the following pattern to locally encrypt data: call the GenerateDataKey API, use the key returned in the Plaintext response field to locally encrypt data, and then erase the plaintext data key from memory. Store the encrypted data key (contained in the CiphertextBlob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

**NEW QUESTION 187**
- (Exam Topic 2)
A company uses identity federation to authenticate users into an identity account (987654321987) where the users assume an IAM role named IdentityRole. The users then assume an IAM role named JobFunctionRole in the target IAM account (123456789123) to perform their job functions.
A user is unable to assume the IAM role in the target account. The policy attached to the role in the identity account is:



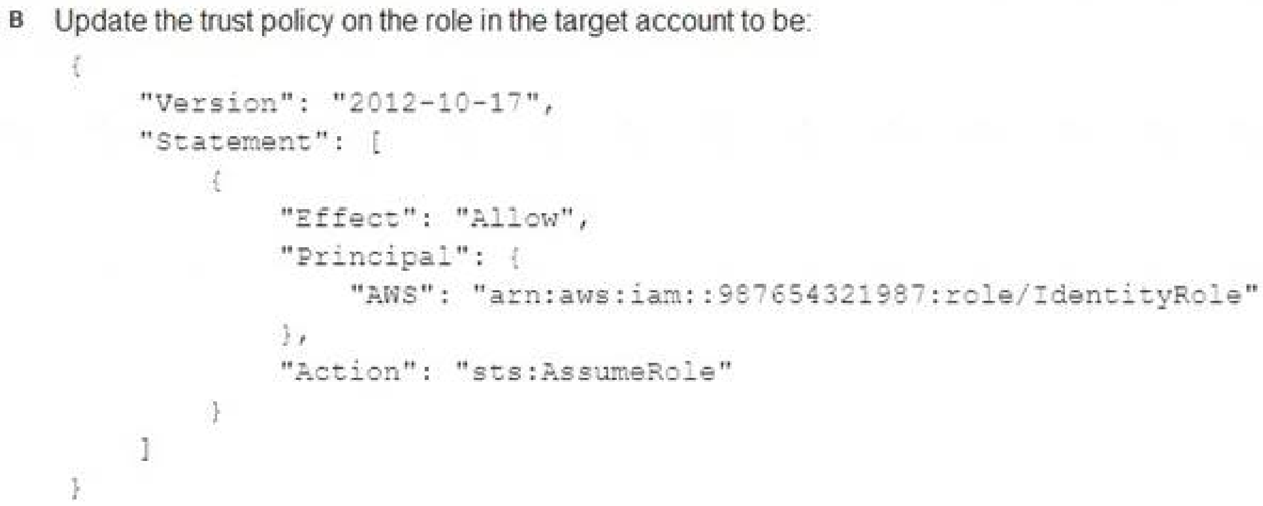
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/JobFunctionRole"
            ],
            "Effect": "Allow"
        }
    ]
}
```

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



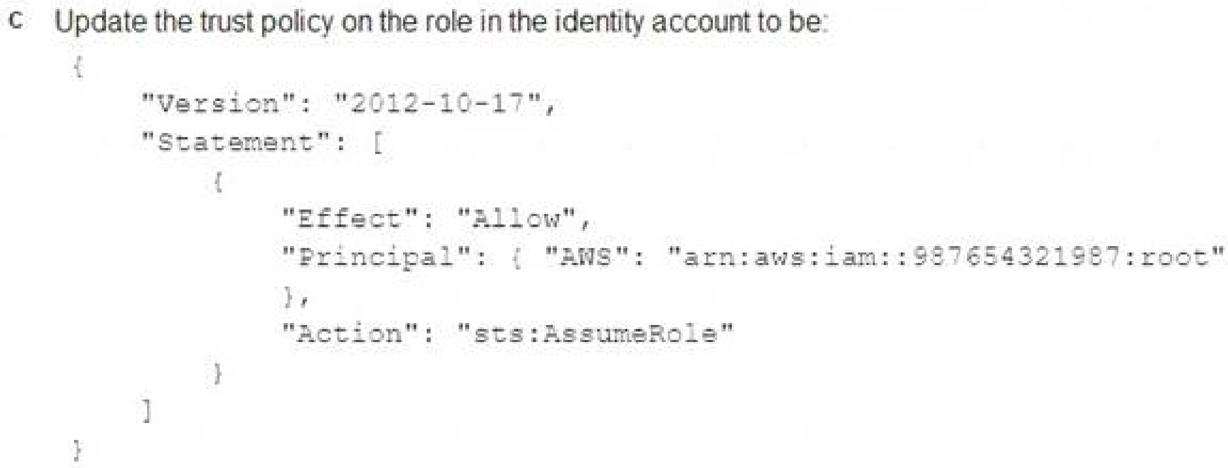
A Update the IAM policy attached to the role in the identity account to be:

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



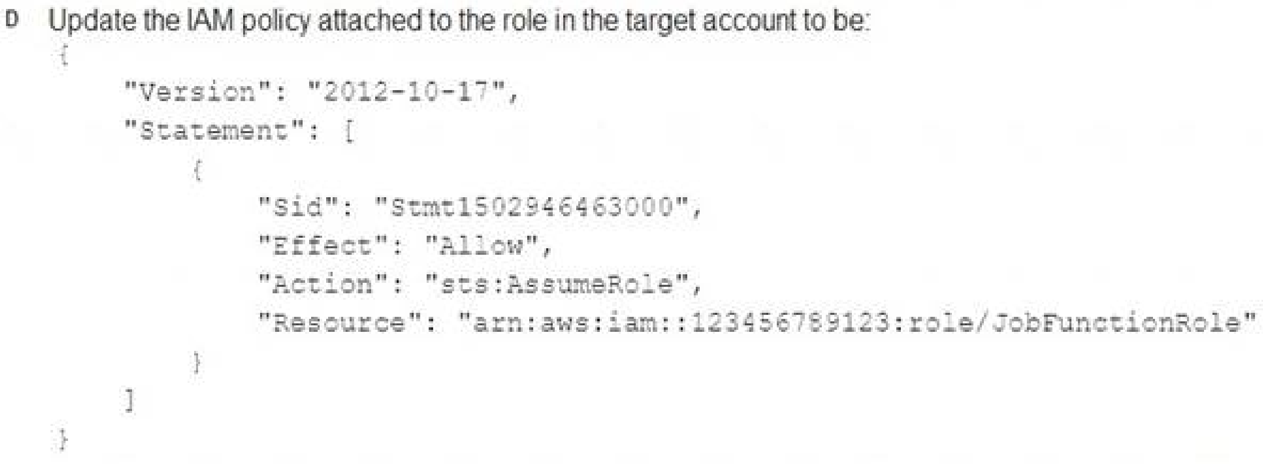
B Update the trust policy on the role in the target account to be:

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



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

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



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

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

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

**Answer:** A

**NEW QUESTION 190**
- (Exam Topic 2)
The Security Engineer is managing a web application that processes highly sensitive personal information. The application runs on Amazon EC2. The application has strict compliance requirements, which instruct that all incoming traffic to the application is protected from common web exploits and that all outgoing traffic from the EC2 instances is restricted to specific whitelisted URLs.
Which architecture should the Security Engineer use to meet these requirements?

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

**Answer:** D

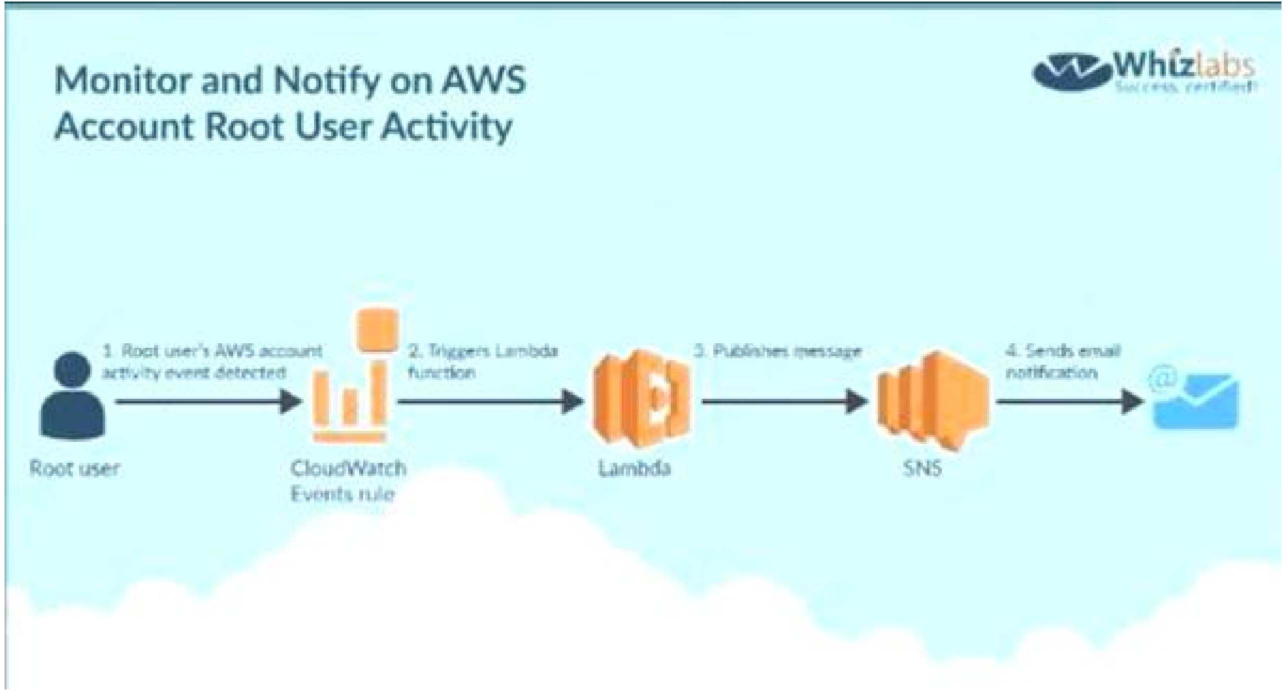
**Explanation:**
IAM Shield is mainly for DDos Attacks.IAM WAF is mainly for some other types of attacks like Injection and XSS etcIn this scenario, It seems it is WAF functionality that is needed.VPC logs do show the source and destination IP and Port , they never show any URL .. because URL are level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

**NEW QUESTION 191**
- (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



Monitor and Notify on AWS Account Root User Activity

Whizlabs
Success certified!
1. Root user's AWS account activity event detected
2. Triggers Lambda function
3. Publishes message
4. Sends email notification
@
Root user
CloudWatch Events rule
Lambda
SNS

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 195**
- (Exam Topic 2)
A company's database developer has just migrated an Amazon RDS database credential to be stored and managed by IAM Secrets Manager. The developer has also enabled rotation of the credential within the Secrets Manager console and set the rotation to change every 30 days.
After a short period of time, a number of existing applications have failed with authentication errors. What is the MOST likely cause of the authentication errors?

A. Migrating the credential to RDS requires that all access come through requests to the Secrets Manager.

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

**Answer:** B

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

**NEW QUESTION 196**
- (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 197**
- (Exam Topic 2)
Your IT Security team has advised to carry out a penetration test on the resources in their company's IAM Account. This is as part of their capability to analyze the security of the Infrastructure. What should be done first in this regard?
Please select:

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

**Answer:** C

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

**NEW QUESTION 202**
- (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 204**
- (Exam Topic 2)
An application makes calls to IAM services using the IAM SDK. The application runs on Amazon EC2 instances with an associated IAM role. When the application attempts to access an object within an Amazon S3 bucket; the Administrator receives the following error message: HTTP 403: Access Denied.
Which combination of steps should the Administrator take to troubleshoot this issue? (Select three.)

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

**Answer:** BCE

**NEW QUESTION 209**
- (Exam Topic 2)
A pharmaceutical company has digitized versions of historical prescriptions stored on premises. The company would like to move these prescriptions to IAM and perform analytics on the data in them. Any operation with this data requires that the data be encrypted in transit and at rest.
Which application flow would meet the data protection requirements on IAM?

A. Digitized files -> Amazon Kinesis Data Analytics
B. Digitized files -> Amazon Kinesis Data Firehose -> Amazon S3 -> Amazon Athena
C. Digitized files -> Amazon Kinesis Data Streams -> Kinesis Client Library consumer -> Amazon S3 -> Athena
D. Digitized files -> Amazon Kinesis Data Firehose -> Amazon Elasticsearch

**Answer:** A

**Explanation:**
(Amazon Kinesis Data Analytics is the easiest way to analyze streaming data, also provide encryption at rest and in-transit)
-https://docs.IAM.amazon.com/kinesisanalytics/latest/dev/data-protection.html

**NEW QUESTION 213**
- (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 214**
- (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 218**
- (Exam Topic 2)
A company has complex connectivity rules governing ingress, egress, and communications between Amazon EC2 instances. The rules are so complex that they cannot be implemented within the limits of the maximum number of security groups and network access control lists (network ACLs).
What mechanism will allow the company to implement all required network rules without incurring additional cost?

A. Configure IAM WAF rules to implement the required rules.

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

**Answer:** B

**NEW QUESTION 222**
- (Exam Topic 2)
You have a vendor that needs access to an IAM resource. You create an IAM user account. You want to restrict access to the resource using a policy for just that user over a brief period. Which of the following would be an ideal policy to use?
Please select:

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

**Answer:** B

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

**NEW QUESTION 226**
- (Exam Topic 2)
You have just received an email from IAM Support stating that your IAM account might have been
compromised. Which of the following steps would you look to carry out immediately. Choose 3 answers from the options below.
Please select:

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

**Answer:** ABD

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

**NEW QUESTION 228**
- (Exam Topic 2)
Your company is planning on hosting an internal network in IAM. They want machines in the VPC to authenticate using private certificates. They want to minimize the work and maintenance in working with certificates. What is the ideal way to fulfil this requirement.
Please select:

A. Consider using Windows Server 2016 Certificate Manager
B. Consider using IAM Certificate Manager
C. Consider using IAM Access keys to generate the certificates
D. Consider using IAM Trusted Advisor for managing the certificates

**Answer:** B

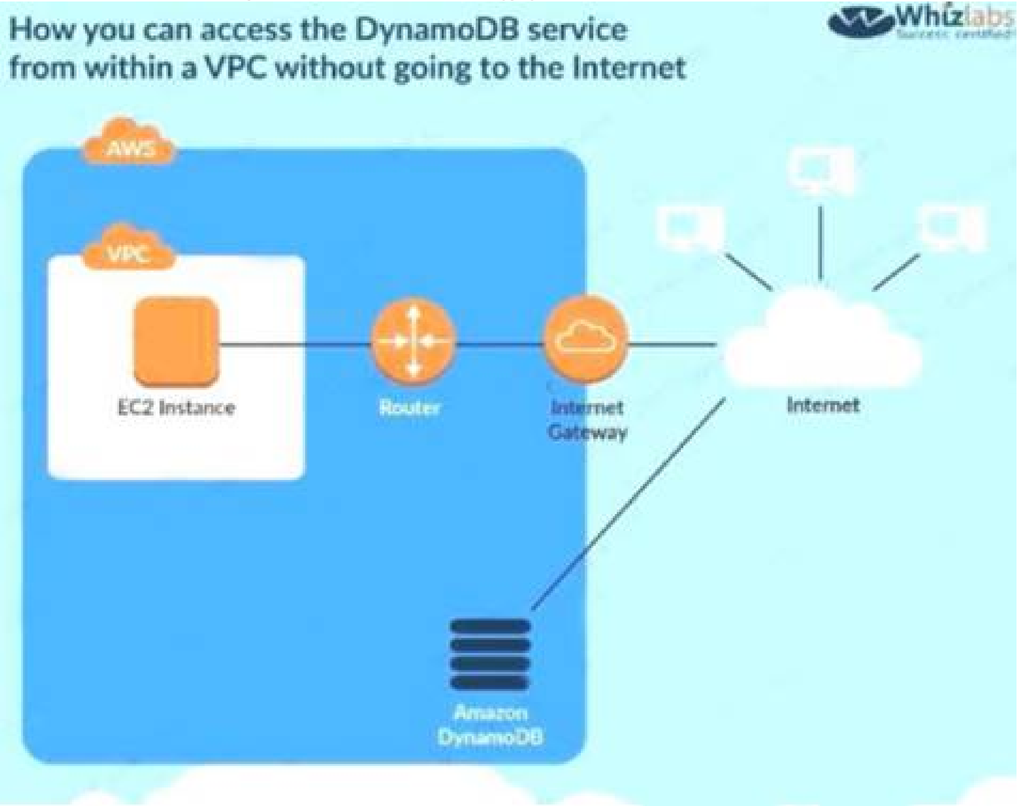
**Explanation:**
The IAM Documentation mentions the following
ACM is tightly linked with IAM Certificate Manager Private Certificate Authority. You can use ACM PCA to create a private certificate authority (CA) and then use ACM to issue private certificates. These are SSL/TLS X.509 certificates that identify users, computers, applications, services, servers, and other devices internally.
Private certificates cannot be publicly trusted
Option A is partially invalid. Windows Server 2016 Certificate Manager can be used but since there is a requirement to "minimize the work and maintenance", IAM Certificate Manager should be used
Option C and D are invalid because these cannot be used for managing certificates. For more information on ACM, please visit the below URL:
https://docs.IAM.amazon.com/acm/latest/userguide/acm-overview.html
The correct answer is: Consider using IAM Certificate Manager Submit your Feedback/Queries to our Experts

**NEW QUESTION 232**
- (Exam Topic 3)
There is a set of Ec2 Instances in a private subnet. The application hosted on these EC2 Instances need to access a DynamoDB table. It needs to be ensured that traffic does not flow out to the internet. How can this be achieved?
Please select:

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

**Answer:** A

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


How you can access the DynamoDB service from within a VPC without going to the Internet
Whizlabs
AWS
VPC
EC2 Instance
Router
Internet Gateway
Internet
Amazon DynamoDB

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

**NEW QUESTION 233**
- (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 234**
- (Exam Topic 3)
An employee keeps terminating EC2 instances on the production environment. You've determined the best way to ensure this doesn't happen is to add an extra layer of defense against terminating the instances. What is the best method to ensure the employee does not terminate the production instances? Choose the 2 correct answers from the options below
Please select:

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

**Answer:** AB

**Explanation:**
Tags enable you to categorize your IAM resources in different ways, for example, by purpose, owner, or environment. This is useful when you have many resources of the same type — you can quickly identify a specific resource based on the tags you've assigned to it. Each tag consists of a key and an optional value, both of which you define
Options C&D are incorrect because it will not ensure that the employee cannot terminate the instance. For more information on tagging answer resources please refer to the below URL:
http://docs.IAM.amazon.com/IAMEC2/latest/UserGuide/Usins_Tags.htmll
The correct answers are: Tag the instance with a production-identifying tag and add resource-level permissions to the employe user with an explicit deny on the terminate API call to instances with the production tag.. Tag the instance with a production-identifying tag and modify the employees group to allow only start stop, and reboot API calls and not the terminate instance
Submit your Feedback/Queries to our Experts

**NEW QUESTION 239**
- (Exam Topic 3)
You have a set of Keys defined using the IAM KMS service. You want to stop using a couple of keys , but are not sure of which services are currently using the keys. Which of the following would be a safe option to stop using the keys from further usage.
Please select:

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

**Answer:** B

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

**NEW QUESTION 243**
- (Exam Topic 3)
Your company has a set of 1000 EC2 Instances defined in an IAM Account. They want to effectively automate several administrative tasks on these instances. Which of the following would be an effective way to achieve this?
Please select:

A. Use the IAM Systems Manager Parameter Store
B. Use the IAM Systems Manager Run Command
C. Use the IAM Inspector
D. Use IAM Config

**Answer:** B

**Explanation:**
The IAM Documentation mentions the following
IAM Systems Manager Run Command lets you remotely and securely manage the configuration of your managed instances. A managed instance is any Amazon EC2 instance or on-premises machine in your hybrid environment that has been configured for Systems Manager. Run Command enables you to automate common administrative tasks and perform ad hoc configuration changes at scale. You can use Run Command from the IAM console, the IAM Command Line Interface, IAM Tools for Windows PowerShell, or the IAM SDKs. Run Command is offered at no additional cost.
Option A is invalid because this service is used to store parameter Option C is invalid because this service is used to scan vulnerabilities in an EC2 Instance.
Option D is invalid because this service is used to check for configuration changes For more information on executing remote commands, please visit the below U
https://docs.IAM.amazon.com/systems-manaEer/latest/usereuide/execute-remote-commands.htmll (
The correct answer is: Use the IAM Systems Manager Run Command Submit your Feedback/Queries to our Experts

**NEW QUESTION 248**
- (Exam Topic 3)
A company has a set of EC2 instances hosted in IAM. These instances have EBS volumes for storing critical information. There is a business continuity requirement and in order to boost the agility of the business and to ensure data durability which of the following options are not required.
Please select:

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

**Answer:** CD

**Explanation:**
Data stored in Amazon EBS volumes is redundantly stored in multiple physical locations as part of normal operation of those services and at no additional charge. However, Amazon EBS replication is stored within the same availability zone, not across multiple zones; therefore, it is highly recommended that you conduct regular snapshots to Amazon S3 for long-term data durability.
You can use Amazon Data Lifecycle Manager (Amazon DLM) to automate the creation, retention, and deletion of snapshots
taken to back up your Amazon EBS volumes.
With lifecycle management, you can be sure that snapshots are cleaned up regularly and keep costs under control.
EBS Lifecycle Policies
A lifecycle policy consists of these core settings:
• Resource type—The IAM resource managed by the policy, in this case, EBS volumes.
• Target tag—The tag that must be associated with an EBS volume for it to be managed by the policy.
• Schedule—Defines how often to create snapshots and the maximum number of snapshots to keep. Snapshot creation starts within an hour of the specified start time. If creating a new snapshot exceeds the maximum number of snapshots to keep for the volume, the oldest snapshot is deleted.
Option C is correct. Each Amazon EBS volume is automatically replicated within its Availability Zone to protect you from component failure, offering high availability and durability. But it does not have an explicit feature like that.
Option D is correct Encryption does not ensure data durability
For information on security for Compute Resources, please visit the below URL https://d1.IAMstatic.com/whitepapers/Security/Security Compute Services Whitepaper.pdl
The correct answers are: Use EBS volume replication. Use EBS volume encryption Submit your Feedback/Queries to our Experts

**NEW QUESTION 252**
- (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

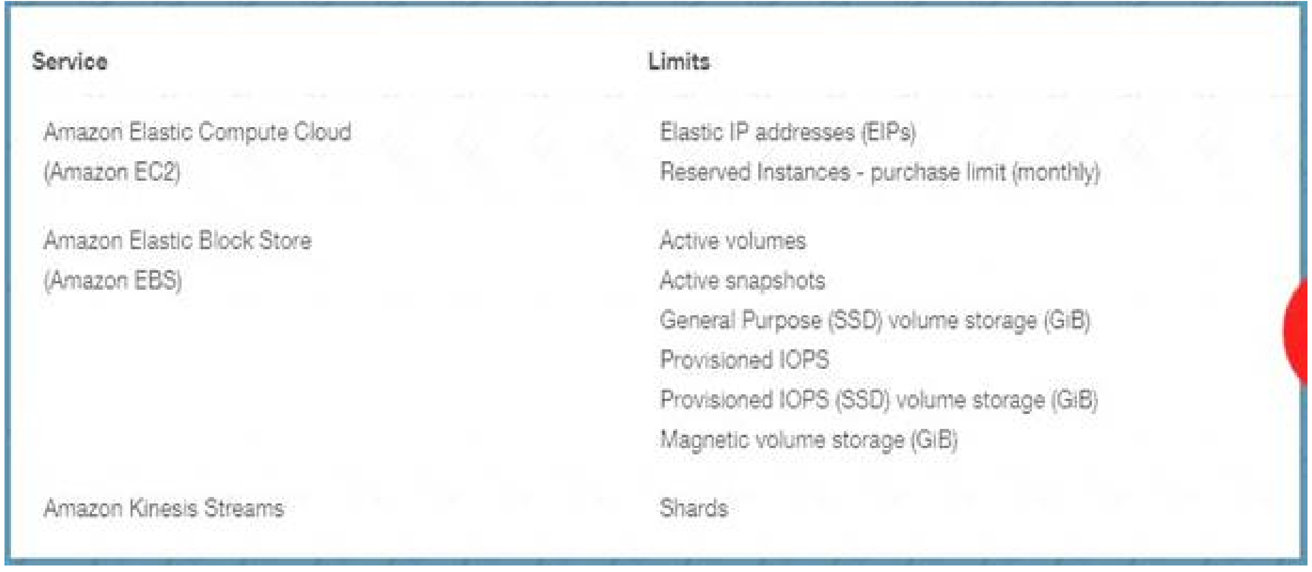
**Explanation:**
The IAM Documentation mentions the following
Server-side encryption is about data encryption at rest—that is, Amazon S3 encrypts your data at the object level as it writes it to disks in its data centers and decrypts it for you when you access it. As long as you authenticate your request 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 255**
- (Exam Topic 3)
You want to ensure that you keep a check on the Active EBS Volumes, Active snapshots and Elastic IP addresses you use so that you don't go beyond the service limit. Which of the below services can help in this regard?
Please select:

A. IAM Cloudwatch
B. IAM EC2
C. IAM Trusted Advisor
D. IAM SNS

**Answer:** C

**Explanation:**
Below is a snapshot of the service limits that the Trusted Advisor can monitor C:\Users\wk\Desktop\mudassar\Untitled.jpg



| Service | Limits |
|---|---|
| Amazon Elastic Compute Cloud<br>(Amazon EC2) | Elastic IP addresses (EIPs)<br>Reserved Instances - purchase limit (monthly) |
| Amazon Elastic Block Store<br>(Amazon EBS) | Active volumes<br>Active snapshots<br>General Purpose (SSD) volume storage (GiB)<br>Provisioned IOPS<br>Provisioned IOPS (SSD) volume storage (GiB)<br>Magnetic volume storage (GiB) |
| Amazon Kinesis Streams | Shards |

Option A is invalid because even though you can monitor resources, it cannot be checked against the service limit.
Option B is invalid because this is the Elastic Compute cloud service Option D is invalid because it can be send notification but not check on service limit For more information on the Trusted Advisor monitoring, please visit the below URL:
https://IAM.amazon.com/premiumsupport/ta-faqs> The correct answer is: IAM Trusted Advisor Submit your Feedback/Queries to our Experts

**NEW QUESTION 256**
- (Exam Topic 3)
An application running on EC2 instances in a VPC must call an external web service via TLS (port 443). The instances run in public subnets.
Which configurations below allow the application to function and minimize the exposure of the instances? Select 2 answers from the options given below
Please select:

A. A network ACL with a rule that allows outgoing traffic on port 443.
B. A network ACL with rules that allow outgoing traffic on port 443 and incoming traffic on ephemeral ports
C. A network ACL with rules that allow outgoing traffic on port 443 and incoming traffic on port 443.
D. A security group with a rule that allows outgoing traffic on port 443
E. A security group with rules that allow outgoing traffic on port 443 and incoming traffic on ephemeral ports.
F. A security group with rules that allow outgoing traffic on port 443 and incoming traffic on port 443.

**Answer:** BD

**Explanation:**
Since here the traffic needs to flow outbound from the Instance to a web service on Port 443, the outbound rules on both the Network and Security Groups need to allow outbound traffic. The Incoming traffic should be allowed on ephermal ports for the Operating System on the Instance to allow a connection to be established on any desired or available port.
Option A is invalid because this rule alone is not enough. You also need to ensure incoming traffic on ephemeral ports
Option C is invalid because need to ensure incoming traffic on ephemeral ports and not only port 443 Option E and F are invalid since here you are allowing additional ports on Security groups which are not
required
For more information on VPC Security Groups, please visit the below URL:
https://docs.IAM.amazon.com/AmazonVPC/latest/UserGuideA/PC_SecurityGroups.htmll
The correct answers are: A network ACL with rules that allow outgoing traffic on port 443 and incoming traffic on ephemeral ports, A security group with a rule that allows outgoing traffic on port 443
Submit your Feedback/Queries to our Experts

**NEW QUESTION 260**
- (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 264**
- (Exam Topic 3)
Your company has been using IAM for the past 2 years. They have separate S3 buckets for logging the various IAM services that have been used. They have hired an external vendor for analyzing their log files. They have their own IAM account. What is the best way to ensure that the partner account can access the log files in the company account for analysis. Choose 2 answers from the options given below
Please select:

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

**Answer:** BD

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

**NEW QUESTION 266**
- (Exam Topic 3)

An application running on EC2 instances in a VPC must access sensitive data in the data center. The access must be encrypted in transit and have consistent low latency. Which hybrid architecture will meet these requirements?
Please select:

A. Expose the data with a public HTTPS endpoint.
B. A VPN between the VPC and the data center over a Direct Connect connection
C. A VPN between the VPC and the data center.
D. A Direct Connect connection between the VPC and data center

**Answer:** B

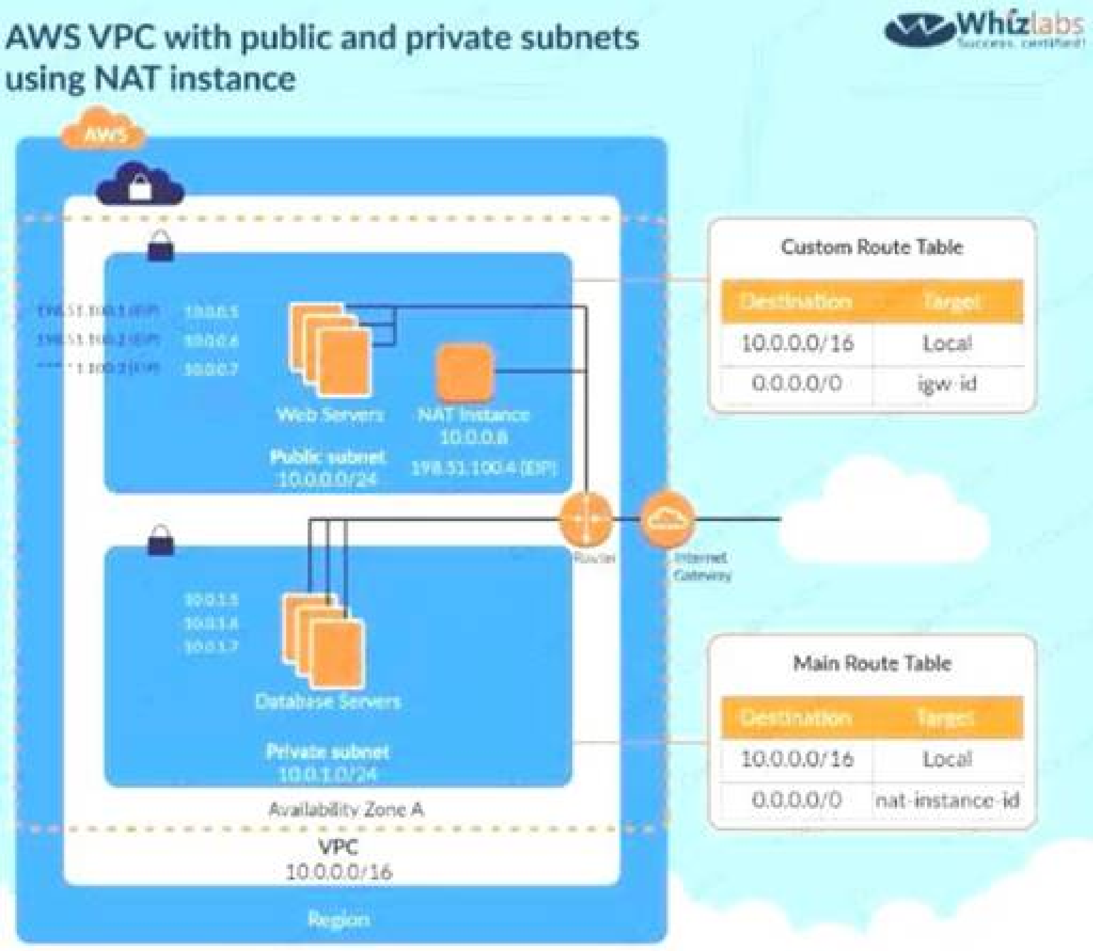
**Explanation:**
Since this is required over a consistency low latency connection, you should use Direct Connect. For encryption, you can make use of a VPN
Option A is invalid because exposing an HTTPS endpoint will not help all traffic to flow between a VPC and the data center.
Option C is invalid because low latency is a key requirement Option D is invalid because only Direct Connect will not suffice
For more information on the connection options please see the below Link: https://IAM.amazon.com/answers/networking/IAM-multiple-vpc-vpn-connection-sharint
The correct answer is: A VPN between the VPC and the data center over a Direct Connect connection Submit your Feedback/Queries to our Experts

**NEW QUESTION 267**
- (Exam Topic 3)
You have an Amazon VPC that has a private subnet and a public subnet in which you have a NAT instance server. You have created a group of EC2 instances that configure themselves at startup by downloading a bootstrapping script from S3 that deploys an application via GIT.
Which one of the following setups would give us the highest level of security? Choose the correct answer from the options given below.
Please select:

A. EC2 instances in our public subnet, no EIPs, route outgoing traffic via the IGW
B. EC2 instances in our public subnet, assigned EIPs, and route outgoing traffic via the NAT
C. EC2 instance in our private subnet, assigned EIPs, and route our outgoing traffic via our IGW
D. EC2 instances in our private subnet, no EIPs, route outgoing traffic via the NAT

**Answer:** D

**Explanation:**
The below diagram shows how the NAT instance works. To make EC2 instances very secure, they need to be in a private sub such as the database server shown below with no EIP and all traffic routed via the NAT.
C:\Users\wk\Desktop\mudassar\Untitled.jpg



Options A and B are invalid because the instances need to be in the private subnet
Option C is invalid because since the instance needs to be in the private subnet, you should not attach an EIP to the instance
For more information on NAT instance, please refer to the below Link: http://docs.IAM.amazon.com/AmazonVPC/latest/UserGuideA/PC lnstance.html!
The correct answer is: EC2 instances in our private subnet no EIPs, route outgoing traffic via the NAT Submit your Feedback/Queries to our Experts

**NEW QUESTION 270**
- (Exam Topic 3)
DDoS attacks that happen at the application layer commonly target web applications with lower volumes of traffic compared to infrastructure attacks. To mitigate these types of attacks, you should probably want to include a WAF (Web Application Firewall) as part of your infrastructure. To inspect all HTTP requests, WAFs sit in-line with your application traffic. Unfortunately, this creates a scenario where WAFs can become a point of failure or bottleneck. To mitigate this problem, you need the ability to run multiple WAFs on demand during traffic spikes. This type of scaling for WAF is done via a "WAF sandwich." Which of the following statements best describes what a "WAF sandwich" is? Choose the correct answer from the options below
Please select:

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

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

**Answer:** D

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

**NEW QUESTION 275**
- (Exam Topic 3)
Your company has just started using IAM and created an IAM account. They are aware of the potential issues when root access is enabled. How can they best safeguard the account when it comes to root access? Choose 2 answers fro the options given below
Please select:

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

**Answer:** BD

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

**NEW QUESTION 278**
- (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 279**
- (Exam Topic 3)
You are building a large-scale confidential documentation web server on IAMand all of the documentation for it will be stored on S3. One of the requirements is that it cannot be publicly accessible from S3 directly, and you will need to use Cloud Front to accomplish this. Which of the methods listed below would satisfy the requirements as outlined? Choose an answer from the options below
Please select:

A. Create an Identity and Access Management (IAM) user for CloudFront and grant access to the objects in your S3 bucket to that IAM User.
B. Create an Origin Access Identity (OAI) for CloudFront and grant access to the objects in your S3 bucket to that OAI.
C. Create individual policies for each bucket the documents are stored in and in that policy grant access to only CloudFront.
D. Create an S3 bucket policy that lists the CloudFront distribution ID as the Principal and the target bucket as the Amazon Resource Name (ARN).

**Answer:** B

**Explanation:**
If you want to use CloudFront signed URLs or signed cookies to provide access to objects in your Amazon S3 bucket you probably also want to prevent users from accessing your Amazon S3 objects using Amazon S3 URLs. If users access your objects directly in Amazon S3, they bypass the controls provided by CloudFront signed URLs or signed cookies, for example, control over the date and time that a user can no longer access your content and control over which IP addresses can be used to access content. In addition, if user's access objects both through CloudFront and directly by using Amazon S3 URLs, CloudFront ace logs are less useful because they're incomplete.
Option A is invalid because you need to create a Origin Access Identity for Cloudfront and not an IAM user
Option C and D are invalid because using policies will not help fulfil the requirement For more information on Origin Access Identity please see the below Link:
http://docs.IAM.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restrictine-access-to-s3
The correct answer is: Create an Origin Access Identity (OAI) for CloudFront and grant access to the objects in your S3 bucket to that OAI.
(

**NEW QUESTION 280**

......

# Relate Links

**100% Pass Your SCS-C02 Exam with Exambible Prep Materials**

https://www.exambible.com/SCS-C02-exam/

# Contact us

**We are proud of our high-quality customer service, which serves you around the clock 24/7.**

**Viste -** https://www.exambible.com/