

## Exam Questions SCS-C02

AWS Certified Security - Specialty

<https://www.2passeasy.com/dumps/SCS-C02/>



#### NEW QUESTION 1

- (Exam Topic 1)

An application is currently secured using network access control lists and security groups. Web servers are located in public subnets behind an Application Load Balancer (ALB); application servers are located in private subnets.

How can edge security be enhanced to safeguard the Amazon EC2 instances against attack? (Choose two.)

- A. Configure the application's EC2 instances to use NAT gateways for all inbound traffic.
- B. Move the web servers to private subnets without public IP addresses.
- C. Configure IAM WAF to provide DDoS attack protection for the ALB.
- D. Require all inbound network traffic to route through a bastion host in the private subnet.
- E. Require all inbound and outbound network traffic to route through an IAM Direct Connect connection.

**Answer:** BC

#### NEW QUESTION 2

- (Exam Topic 1)

A Security Engineer has several thousand Amazon EC2 instances split across production and development environments. Each instance is tagged with its environment. The Engineer needs to analyze and patch all the development EC2 instances to ensure they are not currently exposed to any common vulnerabilities or exposures (CVEs)

Which combination of steps is the MOST efficient way for the Engineer to meet these requirements? (Select TWO.)

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

**Answer:** CD

#### NEW QUESTION 3

- (Exam Topic 1)

A Developer reported that IAM CloudTrail was disabled on their account. A Security Engineer investigated the account and discovered the event was undetected by the current security solution. The Security Engineer must recommend a solution that will detect future changes to the CloudTrail configuration and send alerts when changes occur.

What should the Security Engineer do to meet these requirements?

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

**Answer:** B

#### NEW QUESTION 4

- (Exam Topic 1)

A company has 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 5

- (Exam Topic 1)

A Security Engineer discovered a vulnerability in an application running on Amazon ECS. The vulnerability allowed attackers to install malicious code. Analysis of the code shows it exfiltrates data on port 5353 in batches at random time intervals.

While the code of the containers is being patched, how can Engineers quickly identify all compromised hosts and stop the egress of data on port 5353?

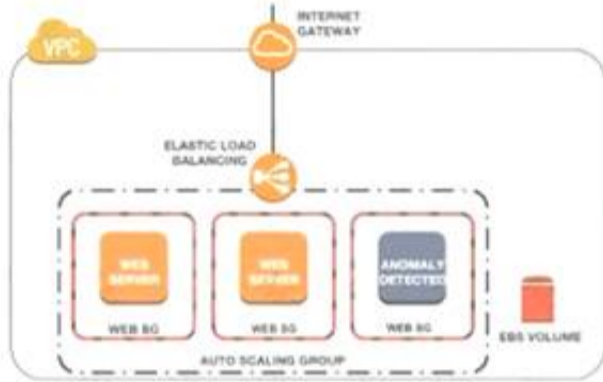
- A. Enable IAM Shield Advanced and IAM WA
- B. Configure an IAM WAF custom filter for egress traffic on port 5353
- C. Enable Amazon Inspector on Amazon ECS and configure a custom assessment to evaluate containers that have port 5353 open
- D. Update the NACLs to block port 5353 outbound.
- E. Create an Amazon CloudWatch custom metric on the VPC Flow Logs identifying egress traffic on port 5353. Update the NACLs to block port 5353 outbound.
- F. Use Amazon Athena to query IAM CloudTrail logs in Amazon S3 and look for any traffic on port 5353. Update the security groups to block port 5353 outbound.

**Answer: C**

#### NEW QUESTION 6

- (Exam Topic 1)

A Security Engineer noticed an anomaly within a company EC2 instance as shown in the image. The Engineer must now investigate what is causing the anomaly. What are the MOST effective steps to take to ensure that the instance is not further manipulated while allowing the Engineer to understand what happened?



- A. Remove the instance from the Auto Scaling group Place the instance within an isolation security group, detach the EBS volume launch an EC2 instance with a forensic toolkit and attach the EBS volume to investigate
- B. Remove the instance from the Auto Scaling group and the Elastic Load Balancer Place the instance within an isolation security group, launch an EC2 instance with a forensic toolkit, and allow the forensic toolkit image to connect to the suspicious Instance to perform the Investigation.
- C. Remove the instance from the Auto Scaling group Place the Instance within an isolation security group, launch an EC2 Instance with a forensic toolkit and use the forensic toolkit image to deploy an ENI as a network span port to inspect all traffic coming from the suspicious instance.
- D. Remove the instance from the Auto Scaling group and the Elastic Load Balancer Place the instance within an isolation security group, make a copy of the EBS volume from a new snapshot, launch an EC2 Instance with a forensic toolkit and attach the copy of the EBS volume to investigate.

**Answer: B**

#### NEW QUESTION 7

- (Exam Topic 1)

A company is configuring three Amazon EC2 instances with each instance in a separate Availability Zone. The EC2 instances will be used as transparent proxies for outbound internet traffic for ports 80 and 443 so the proxies can block traffic to certain internet destinations as required by the company's security policies. A Security Engineer completed the following:

- Set up the proxy software on the EC2 instances.
- Modified the route tables on the private subnets to use the proxy EC2 instances as the default route.
- Created a security group rule opening inbound port 80 and 443 TCP protocols on the proxy EC2 instance security group.

However, the proxy EC2 instances are not successfully forwarding traffic to the internet.

What should the Security Engineer do to make the proxy EC2 instances route traffic to the internet?

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

**Answer: B**

#### NEW QUESTION 8

- (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 bucket
- 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 recurring basis
- F. Use IAM Backup to copy EBS snapshots to Amazon S3.

**Answer: A**

#### NEW QUESTION 9

- (Exam Topic 1)

A company has implemented centralized logging and monitoring of IAM CloudTrail logs from all Regions in an Amazon S3 bucket. The log files 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 to decrypt objects using the KMS CMK and gives access to the S3 bucket and objects.
- D. Check that the role the EC2 instance profile uses grants permission to decrypt objects using the KMS CMK.

**Answer: C**

#### NEW QUESTION 10

- (Exam Topic 1)

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

- A. Configure the S3 bucket ACLs to allow IAM Config to record changes to the buckets.
- B. Configure policies attached to S3 buckets to allow IAM Config to record changes to the buckets.
- C. Attach the AmazonS3ReadOnlyAccess managed policy to the IAM user.
- D. Verify the security engineer's IAM user has an attached policy that allows all IAM Config actions.
- E. Assign the IAMConfigRole managed policy to the IAM Config role.

**Answer: BE**

#### NEW QUESTION 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 logging for 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 for shell access to Amazon EC2 instances with the user tag defined. Enable Amazon CloudWatch logging for Systems Manager sessions.
- D. Use Amazon S3 to securely store one Privacy Enhanced Mail Certificate (PEM file) 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 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.

**Answer: C**

#### NEW QUESTION 15

- (Exam Topic 1)

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

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

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 19

- (Exam Topic 1)

A security engineer needs to ensure their company's uses of IAM meet 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's security team has defined a set of IAM Config rules that must be enforced globally in all IAM accounts the company owns. What should be done to provide a consolidated compliance overview for the security team?

- A. Use IAM Organizations to limit IAM Config rules to the appropriate Regions, and then consolidate the Amazon CloudWatch dashboard into one IAM account.
- B. Use IAM Config aggregation to consolidate the views into one IAM account, and provide role access to the security team.
- C. Consolidate IAM Config rule results with an IAM Lambda function and push data to Amazon SQ
- D. Use Amazon SNS to consolidate and alert when some metrics are triggered.
- E. Use Amazon GuardDuty to load data results from the IAM Config rules compliance status, aggregate GuardDuty findings of all IAM accounts into one IAM account, and provide role access to the security team.

**Answer:** B

#### NEW QUESTION 24

- (Exam Topic 1)

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

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

**Answer:** B

#### NEW QUESTION 28

- (Exam Topic 1)

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

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

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 30

- (Exam Topic 1)

An company is using IAM Secrets Manager to store secrets that are encrypted using a CMK and are stored in the security account 111122223333. One of the company's production accounts. 444455556666, must to retrieve the secret values from the security account 111122223333. A security engineer needs to apply a policy to the secret in the security account based on least privilege access so the production account can retrieve the secret value only.  
Which policy should the security engineer apply?

- A. 

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "secretsmanager:*",
      "Principal": {"AWS": "444455556666"},
      "Resource": "*"
    }
  ]
}
```
- B. 

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "secretsmanager:*",
      "Principal": {"AWS": "111122223333"},
      "Resource": "*"
    }
  ]
}
```

C. {  
 "Version": "2012-10-17",  
 "Statement": [  
 {  
 "Effect": "Allow",  
 "Action": "secretsmanager:GetSecretValue",  
 "Principal": {"AWS": "111122223333"},  
 "Resource": "\*" }  
 ]  
 }

D. {  
 "Version": "2012-10-17",  
 "Statement": [  
 {  
 "Effect": "Allow",  
 "Action": "secretsmanager:GetSecretValue",  
 "Principal": {"AWS": "444455556666"},  
 "Resource": "\*" }  
 ]  
 }

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

Answer: A

#### NEW QUESTION 34

- (Exam Topic 1)

To meet regulatory requirements, a Security Engineer needs to implement an IAM policy that restricts the use of IAM services to the us-east-1 Region. What policy should the Engineer implement?

A

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestedRegion": "us-east-1"
        }
      }
    }
  ]
}
```

B

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "ec2:Region": "us-east-1"
        }
      }
    }
  ]
}
```

C

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": "us-east-1"
        }
      }
    }
  ]
}
```

D

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "NotAction": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestedRegion": "us-east-1"
        }
      }
    }
  ]
}
```

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

**Answer: B**

### NEW QUESTION 39

- (Exam Topic 1)

A company's Developers plan to migrate their on-premises applications to Amazon EC2 instances running Amazon Linux AMIs. The applications are accessed by a group of partner companies. The Security Engineer needs to implement the following host-based security measures for these instances:

- Block traffic from documented known bad IP addresses
- Detect known software vulnerabilities and CIS Benchmarks compliance. Which solution addresses these requirements?

- A. Launch the EC2 instances with an IAM role attached
- B. Include a user data script that uses the IAM CLI to retrieve the list of bad IP addresses from IAM Secrets Manager and uploads it as a threat list in Amazon GuardDuty. Use Amazon Inspector to scan the instances for known software vulnerabilities and CIS Benchmarks compliance.
- C. Launch the EC2 instances with an IAM role attached. Include a user data script that uses the IAM CLI to create NACLs blocking ingress traffic from the known bad IP addresses in the EC2 instance's subnets. Use IAM Systems Manager to scan the instances for known software vulnerabilities, and IAM Trusted Advisor to check instances for CIS Benchmarks compliance.
- D. Launch the EC2 instances with an IAM role attached. Include a user data script that uses the IAM CLI to create and attach security groups that only allow an allow-listed source IP address range inbound.
- E. Use Amazon Inspector to scan the instances for known software vulnerabilities, and IAM Trusted Advisor to check instances for CIS Benchmarks compliance.
- F. Launch the EC2 instances with an IAM role attached. Include a user data script that creates a cron job to periodically retrieve the list of bad IP addresses from Amazon S3, and configures iptables on the instances blocking the list of bad IP addresses. Use Amazon Inspector to scan the instances for known software vulnerabilities and CIS Benchmarks compliance.

**Answer: D**

### NEW QUESTION 41

- (Exam Topic 1)

A company uses SAML federation with IAM Identity and Access Management (IAM) to provide internal users with SSO for their IAM accounts. The company's identity provider certificate was rotated as part of its normal lifecycle. Shortly after, users started receiving the following error when attempting to log in:

"Error: Response Signature Invalid (Service: IAMSecurityTokenService; Status Code: 400; Error Code: InvalidIdentityToken)"

A security engineer needs to address the immediate issue and ensure that it will not occur again. Which combination of steps should the security engineer take to accomplish this? (Select TWO.)

- A. Download a new copy of the SAML metadata file from the identity provider. Create a new IAM identity provider entity.

- B. Upload the new metadata file to the new IAM identity provider entity.
- C. During the next certificate rotation period and before the current certificate expires, add a new certificate as the secondary to the identity provide
- D. Generate a new metadata file and upload it to the IAM identity provider entit
- E. Perform automated or manual rotation of the certificate when required.
- F. Download a new copy of the SAML metadata file from the identity provider Upload the new metadata to the IAM identity provider entity configured for the SAML integration in question.
- G. During the next certificate rotation period and before the current certificate expires, add a new certificateas the secondary to the identity provide
- H. Generate a new copy of the metadata file and create a new IAM identity provider entit
- I. Upload the metadata file to the new IAM identity provider entit
- J. Perform automated or manual rotation of the certificate when required.
- K. Download a new copy of the SAML metadata file from the identity provider Create a new IAM identity provider entit
- L. Upload the new metadata file to the new IAM identity provider entit
- M. Update the identity provider configurations to pass a new IAM identity provider entity name in the SAML assertion.

**Answer:** AD

#### NEW QUESTION 44

- (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 46

- (Exam Topic 1)

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

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

**Answer:** D

#### Explanation:

Read the prerequisites in the question carefully. The solution must support "near real time" analysis of the log data. Cloudwatch doesn't stream logs to S3; it supports exporting them to S3 with an up to 12 hour expected delay:

<https://docs.IAM.amazon.com/AmazonCloudWatch/latest/logs/S3Export.html>

"Log data can take up to 12 hours to become available for export. For near real-time analysis of log data, see Analyzing log data with CloudWatch Logs Insights or Real-time processing of log data with subscriptions instead."

<https://docs.IAM.amazon.com/AmazonCloudWatch/latest/logs/Subscriptions.html>

"You can use subscriptions to get access to a real-time feed of log events from CloudWatch Logs and have it delivered to other services such as an Amazon Kinesis stream, an Amazon Kinesis Data Firehose stream, or IAM Lambda for custom processing, analysis, or loading to other systems. When log events are sent to the receiving service, they are Base64 encoded and compressed with the gzip format."

<https://docs.IAM.amazon.com/AmazonCloudWatch/latest/logs/CrossAccountSubscriptions.html>

#### NEW QUESTION 50

- (Exam Topic 1)

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

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

Answer: A

### NEW QUESTION 53

- (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, or 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 for sharing files between application social network users.
- C. Store each user's files in a separate S3 bucket and apply a bucket policy based on the user's sharing settings.
- D. Generate presigned UPLs for each file access.

Answer: A

### NEW QUESTION 54

- (Exam Topic 1)

A recent security audit identified that a company's application team injects database credentials into the environment variables of an IAM Fargate task. The company's security policy mandates that all sensitive data be encrypted at rest and in transit.

When combination of actions should the security team take to make the application compliant within the security policy? (Select THREE)

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

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

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

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

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

Answer: BEF

### NEW QUESTION 57

- (Exam Topic 1)

A company is using IAM Organizations to manage multiple IAM member accounts. All of these accounts have Amazon GuardDuty enabled in all Regions. The company's IAM Security Operations Center has a centralized security account for logging and monitoring. One of the member accounts has received an excessively high bill. A security engineer discovers that a compromised Amazon EC2 instance is being used to mine crypto currency. The Security Operations Center did not receive a GuardDuty finding in the central security account.

but there was a GuardDuty finding in the account containing the compromised EC2 instance. The security engineer needs to ensure a GuardDuty finding is available in the security account.

What should the security engineer do to resolve this issue?

- A. Set up an Amazon CloudWatch Event rule to forward all GuardDuty findings to the security account. Use an IAM Lambda function as a target to raise findings.
- B. Set up an Amazon CloudWatch Events rule to forward all GuardDuty findings to the security account. Use an IAM Lambda function as a target to raise findings in IAM Security Hub.
- C. Check that GuardDuty in the security account is able to assume a role in the compromised account using the GuardDuty fast findings permission. Schedule an Amazon CloudWatch Events rule and an IAM Lambda function to periodically check for GuardDuty findings.
- D. Use the IAM GuardDuty get-members IAM CLI command in the security account to see if the account is listed. Send an invitation from GuardDuty in the security account to GuardDuty in the compromised account. Accept the invitation to forward all future GuardDuty findings.

Answer: D

### NEW QUESTION 61

- (Exam Topic 1)

A Security Engineer manages IAM Organizations for a company. The Engineer would like to restrict IAM usage to allow Amazon S3 only in one of the organizational units (OUs). The Engineer adds the following SCP to the OU:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowS3",
      "Effect": "Allow",
      "Action": "s3:*",
      "Resource": "*"
    }
  ]
}
```

The next day, API calls to IAM appear in IAM CloudTrail logs in an account under that OU. How should the Security Engineer resolve this issue?

- A. Move the account to a new OU and deny IAM:\* permissions.
- B. Add a Deny policy for all non-S3 services at the account level.
- C. Change the policy to: {"Version": "2012-10-17", "Statement": [{"Sid": "AllowS3", "Effect": "Allow", "Action": "s3:\*", "Resource": "/\*/\*"}]}
- D. Detach the default FullIAMAccess SCP

**Answer: D**

**Explanation:**

[https://docs.IAM.amazonaws.com/organizations/latest/APIReference/API\\_DetachPolicy.html](https://docs.IAM.amazonaws.com/organizations/latest/APIReference/API_DetachPolicy.html)

Every root, OU, and account must have at least one SCP attached. If you want to replace the default FullIAMAccess policy with an SCP that limits the permissions that can be delegated, you must attach the replacement SCP before you can remove the default SCP. This is the authorization strategy of an "allow list". If you instead attach a second SCP and leave the FullIAMAccess SCP still attached, and specify "Effect": "Deny" in the second SCP to override the "Effect": "Allow" in the FullIAMAccess policy (or any other attached SCP), you're using the authorization strategy of a "deny list".

**NEW QUESTION 64**

- (Exam Topic 1)

A company has several production IAM accounts and a central security IAM account. The security account is used for centralized monitoring and has IAM privileges to all resources in every corporate account. All of the company's Amazon S3 buckets are tagged with a value denoting the data classification of their contents.

A Security Engineer is deploying a monitoring solution in the security account that will enforce bucket policy compliance. The system must monitor S3 buckets in all production accounts and confirm that any policy change is in accordance with the bucket's data classification. If any change is out of compliance; the Security team must be notified quickly.

Which combination of actions would build the required solution? (Choose three.)

- A. Configure Amazon CloudWatch Events in the production accounts to send all S3 events to the security account event bus.
- B. Enable Amazon GuardDuty in the security account
- C. and join the production accounts as members.
- D. Configure an Amazon CloudWatch Events rule in the security account to detect S3 bucket creation or modification events.
- E. Enable IAM Trusted Advisor and activate email notifications for an email address assigned to the security contact.
- F. Invoke an IAM Lambda function in the security account to analyze S3 bucket settings in response to S3 events, and send non-compliance notifications to the Security team.
- G. Configure event notifications on S3 buckets for PUT; POST, and DELETE events.

**Answer: DEF**

**NEW QUESTION 66**

- (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 account principals to use the CMK by modifying its policy.
- C. Create an Amazon EC2 instance
- D. Attach the encrypted and suspicious EBS volume
- E. Copy data from the suspicious volume to an unencrypted volume
- F. Snapshot the unencrypted volume
- G. Copy the EBS snapshot to the new decrypted snapshot
- H. Restore a volume from the suspicious EBS snapshot
- I. Create an unencrypted EBS volume of the same size.
- J. Share the target EBS snapshot with the forensics account.

**Answer: ABF**

**NEW QUESTION 70**

- (Exam Topic 1)

An IAM account administrator created an IAM group and applied the following managed policy to require that each individual user authenticate using multi-factor authentication:

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

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

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

**Answer: B**

#### NEW QUESTION 74

- (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 77

- (Exam Topic 1)

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

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

**Answer: C**

#### NEW QUESTION 82

- (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 83

- (Exam Topic 1)

A Security Engineer launches two Amazon EC2 instances in the same Amazon VPC but in separate Availability Zones. Each instance has a public IP address and

is able to connect to external hosts on the internet. The two instances are able to communicate with each other by using their private IP addresses, but they are not able to communicate with each other when using their public IP addresses. Which action should the Security Engineer take to allow communication over the public IP addresses?

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

**Answer:** D

**Explanation:**

<https://docs.IAM.amazon.com/IAM/EC2/latest/UserGuide/security-group-rules-reference.html#sg-rules-other-in>

**NEW QUESTION 84**

- (Exam Topic 2)

A company wants to control access to its IAM resources by using identities and groups that are defined in its existing Microsoft Active Directory. What must the company create in its IAM account to map permissions for IAM services to Active Directory user attributes?

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

**Answer:** C

**Explanation:**

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

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

**NEW QUESTION 88**

- (Exam Topic 2)

An application running on EC2 instances must use a username and password to access a database. The developer has stored those secrets in the SSM Parameter Store with type SecureString using the default KMS CMK. Which combination of configuration steps will allow the application to access the secrets via the API? Select 2 answers from the options below  
Please select:

- A. Add the EC2 instance role as a trusted service to the SSM service role.
- B. Add permission to use the KMS key to decrypt to the SSM service role.
- C. Add permission to read the SSM parameter to the EC2 instance rol
- D. .
- E. Add permission to use the KMS key to decrypt to the EC2 instance role
- F. Add the SSM service role as a trusted service to the EC2 instance role.

**Answer:** CD

**Explanation:**

The below example policy from the IAM Documentation is required to be given to the EC2 Instance in order to read a secure string from IAM KMS. Permissions need to be given to the Get Parameter API and the KMS API call to decrypt the secret.

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

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:GetParameter"
      ],
      "Resource": "arn:aws:ssm:us-west-2:111122223333:parameter/ReadableParameters/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    }
  ]
}
```

Option A is invalid because roles can be attached to EC2 and not EC2 roles to SSM Option B is invalid because the KMS key does not need to decrypt the SSM

service role.

Option E is invalid because this configuration is valid For more information on the parameter store, please visit the below URL:

<https://docs.IAM.amazon.com/kms/latest/developerguide/services-parameter-store.html>

The correct answers are: Add permission to read the SSM parameter to the EC2 instance role., Add permission to use the KMS key to decrypt to the EC2 instance role

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 89

- (Exam Topic 2)

During a recent internal investigation, it was discovered that all API logging was disabled in a production account, and the root user had created new API keys that appear to have been used several times.

What could have been done to detect and automatically remediate the incident?

- A. Using Amazon Inspector, review all of the API calls and configure the inspector agent to leverage SNS topics to notify security of the change to IAM CloudTrail, and revoke the new API keys for the root user.
- B. Using IAM Config, create a config rule that detects when IAM CloudTrail is disabled, as well as any calls to the root user create-api-ke
- C. Then use a Lambda function to re-enable CloudTrail logs and deactivate the root API keys.
- D. Using Amazon CloudWatch, create a CloudWatch event that detects IAM CloudTrail deactivation and a separate Amazon Trusted Advisor check to automatically detect the creation of root API key
- E. Then use a Lambda function to enable IAM CloudTrail and deactivate the root API keys.
- F. Using Amazon CloudTrail, create a new CloudTrail event that detects the deactivation of CloudTrail logs, and a separate CloudTrail event that detects the creation of root API key
- G. Then use a Lambda function to enable CloudTrail and deactivate the root API keys.

**Answer: B**

#### Explanation:

<https://docs.IAM.amazon.com/config/latest/developerguide/cloudtrail-enabled.html> <https://docs.IAM.amazon.com/config/latest/developerguide/iam-root-access-key-check.html>

#### NEW QUESTION 90

- (Exam Topic 2)

During a recent security audit, it was discovered that multiple teams in a large organization have placed restricted data in multiple Amazon S3 buckets, and the data may have been exposed. The auditor has requested that the organization identify all possible objects that contain personally identifiable information (PII) and then determine whether this information has been accessed.

What solution will allow the Security team to complete this request?

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

**Answer: B**

#### NEW QUESTION 93

- (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/ShareObjectPreSignedURL.html>

The correct answer is: Use Pre-signed URL's Submit your Feedback/Queries to our Experts

#### NEW QUESTION 96

- (Exam Topic 2)

You have an instance setup in a test environment in IAM. You installed the required application and the promoted the server to a production environment. Your IT Security team has advised that there maybe traffic flowing in from an unknown IP address to port 22. How can this be mitigated immediately?

Please select:

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

D. Change the Instance type for the instance

**Answer:** B

**Explanation:**

In the test environment the security groups might have been opened to all IP addresses for testing purpose. Always to ensure to remove this rule once all testing is completed.

Option A, C and D are all invalid because this would affect the application running on the server. The easiest way is just to remove the rule for access on port 22.

For more information on authorizing access to an instance, please visit the below URL: <https://docs.IAM.amazon.com/IAMEC2/latest/UserGuide/authorizing-access-to-an-instance.html>

The correct answer is: Remove the rule for incoming traffic on port 22 for the Security Group Submit your Feedback/Queries to our Experts

**NEW QUESTION 101**

- (Exam Topic 2)

You want to get a list of vulnerabilities for an EC2 Instance as per the guidelines set by the Center of Internet Security. How can you go about doing this?

Please select:

A. Enable IAM Guard Duty for the Instance

B. Use IAM Trusted Advisor

C. Use IAM inspector

D. Use IAM Macie

**Answer:** C

**Explanation:**

The IAM Inspector service can inspect EC2 Instances based on specific Rules. One of the rules packages is based on the guidelines set by the Center of Internet Security

Center for Internet security (CIS) Benchmarks

The CIS Security Benchmarks program provides well-defined, un-biased and consensus-based industry best practices to help organizations assess and improve their security. Amazon Web Services is a CIS Security Benchmarks Member company and the list of Amazon Inspector certifications can be viewed here.

Option A is invalid because this can be used to protect an instance but not give the list of vulnerabilities Options B and D are invalid because these services cannot

give a list of vulnerabilities For more information

on the guidelines, please visit the below URL:

\* [https://docs.IAM.amazon.com/inspector/latest/userguide/inspector\\_cis.html](https://docs.IAM.amazon.com/inspector/latest/userguide/inspector_cis.html) The correct answer is: Use IAM Inspector

Submit your Feedback/Queries to our Experts

**NEW QUESTION 102**

- (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 mechanism

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 volume

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 104**

- (Exam Topic 2)

The Security Engineer has discovered that a new application that deals with highly sensitive data is storing Amazon S3 objects with the following key pattern, which itself contains highly sensitive data.

Pattern: "randomID\_datestamp\_PII.csv" Example:

"1234567\_12302017\_000-00-0000.csv"

The bucket where these objects are being stored is using server-side encryption (SSE). Which solution is the most secure and cost-effective option to protect the sensitive data?

A. Remove the sensitive data from the object name, and store the sensitive data using S3 user-defined metadata.

B. Add an S3 bucket policy that denies the action s3:GetObject

C. Use a random and unique S3 object key, and create an S3 metadata index in Amazon DynamoDB using client-side encrypted attributes.

D. Store all sensitive objects in Binary Large Objects (BLOBS) in an encrypted Amazon RDS instance.

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 108

- (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 Manager Patch Manager to generate the report of out of compliance instances/ server
- C. Use Systems Manager Patch Manager to install the missing patches.
- D. Use Systems Manager Patch Manager to generate the report of out of compliance instances/ servers. Redeploy all out of 1 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 Manager Patch Manager to install the missing patches.

**Answer: B**

#### Explanation:

Use the Systems Manager Patch Manager 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 Manager Patch Manager to generate the report of out of compliance instances/ servers. Use Systems Manager Patch Manager to install the missing patches.

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 109

- (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 policy
- B. Add the role to an EC2 instance profile
- 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 policy
- G. Add the role to an EC2 instance profile
- H. Attach the instance profile to the EC2 instances and the Lambda function.
- I. Store the database credentials in IAM Secrets Manager
- J. Create an IAM role with access to Secrets Manager by using the EC2 and Lambda service principals in the role's trust policy
- K. Add the role to an EC2 instance profile
- L. Attach the instance profile to the EC2 instances and the Lambda function.
- M. Store the database credentials in IAM Secrets Manager
- N. Create an IAM role with access to Secrets Manager by using the EC2 and Lambda service principals in the role's trust policy
- O. Add the role to an EC2 instance profile
- P. Attach the instance profile to the EC2 instance
- Q. Set up Lambda to use the new role for execution.

**Answer: D**

#### NEW QUESTION 110

- (Exam Topic 2)

Which of the following is the most efficient way to automate the encryption of IAM CloudTrail logs using a Customer Master Key (CMK) in IAM KMS?

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

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 111

- (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 115

- (Exam Topic 2)

A company is using CloudTrail to log all IAM API activity for all regions in all of its accounts. The CISO has asked that additional steps be taken to protect the integrity of the log files.

What combination of steps will protect the log files from intentional or unintentional alteration? Choose 2 answers from the options given below  
 Please select:

- A. Create an S3 bucket in a dedicated log account and grant the other accounts write only access
- B. Deliver all log files from every account to this S3 bucket.
- C. Write a Lambda function that queries the Trusted Advisor Cloud Trail check
- D. Run the function every 10 minutes.
- E. Enable CloudTrail log file integrity validation
- F. Use Systems Manager Configuration Compliance to continually monitor the access policies of S3 buckets containing Cloud Trail logs.
- G. Create a Security Group that blocks all traffic except calls from the CloudTrail service
- H. Associate the security group with) all the Cloud Trail destination S3 buckets.

**Answer:** AC

#### Explanation:

The IAM Documentation mentions the following

To determine whether a log file was modified, deleted, or unchanged after CloudTrail delivered it you can use CloudTrail log file integrity validation. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.

Option B is invalid because there is no such thing as Trusted Advisor Cloud Trail checks Option D is invalid because Systems Manager cannot be used for this purpose.

Option E is invalid because Security Groups cannot be used to block calls from other services For more information on Cloudtrail log file validation, please visit the below URL:

<https://docs.IAM.amazon.com/IAMcloudtrail/latest/userguide/cloudtrail-log-file-validation-intro.html> For more information on delivering Cloudtrail logs from multiple accounts, please visit the below URL:

<https://docs.IAM.amazon.com/IAMcloudtrail/latest/userguide/cloudtrail-receive-logs-from-multiple-accounts.html>

The correct answers are: Create an S3 bucket in a dedicated log account and grant the other accounts write only access. Deliver all log files from every account to this S3 bucket, Enable Cloud Trail log file integrity validation

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 116

- (Exam Topic 2)

A company has multiple VPCs in their account that are peered, as shown in the diagram. A Security Engineer wants to perform penetration tests of the Amazon EC2 instances in all three VPCs.

How can this be accomplished? (Choose two.)



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

**Answer:** BD

**Explanation:**

<https://IAM.amazon.com/security/penetration-testing/>

**NEW QUESTION 117**

- (Exam Topic 2)

A company's security policy requires that VPC Flow Logs are enabled on all VPCs. A Security Engineer is looking to automate the process of auditing the VPC resources for compliance.

What combination of actions should the Engineer take? (Choose two.)

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

**Answer:** AE

**Explanation:**

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

**NEW QUESTION 122**

- (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 123**

- (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 126**

- (Exam Topic 2)

A Lambda function reads metadata from an S3 object and stores the metadata in a DynamoDB table. The function is triggered whenever an object is stored within the S3 bucket.

How should the Lambda function be given access to the DynamoDB table? Please select:

- A. Create a VPC endpoint for DynamoDB within a VP
- B. Configure the Lambda function to access resources in the VPC.
- C. Create a resource policy that grants the Lambda function permissions to write to the DynamoDB table. Attach the policy to the DynamoDB table.
- D. Create an IAM user with permissions to write to the DynamoDB table
- E. Store an access key for that user in the Lambda environment variables.
- F. Create an IAM service role with permissions to write to the DynamoDB table
- G. Associate that role with the Lambda function.

**Answer:** D

**Explanation:**

The ideal way is to create an IAM role which has the required permissions and then associate it with the Lambda function

The IAM Documentation additionally mentions the following

Each Lambda function has an IAM role (execution role) associated with it. You specify the IAM role when you create your Lambda function. Permissions you grant to this role determine what IAM Lambda can do when it assumes the role. There are two types of permissions that you grant to the IAM role:

If your Lambda function code accesses other IAM resources, such as to read an object from an S3 bucket or write logs to CloudWatch Logs, you need to grant permissions for relevant Amazon S3 and CloudWatch actions to the role.

If the event source is stream-based (Amazon Kinesis Data Streams and DynamoDB streams), IAM Lambda polls these streams on your behalf. IAM Lambda needs permissions to poll the stream and read new records on the stream so you need to grant the relevant permissions to this role.

Option A is invalid because the VPC endpoint allows access instances in a private subnet to access DynamoDB

Option B is invalid because resources policies are present for resources such as S3 and KMS, but not IAM Lambda  
 Option C is invalid because IAM Roles should be used and not IAM Users  
 For more information on the Lambda permission model, please visit the below URL: <https://docs.IAM.amazon.com/lambda/latest/dg/intro-permission-model.html>  
 The correct answer is: Create an IAM service role with permissions to write to the DynamoDB table. Associate that role with the Lambda function.  
 Submit your Feedback/Queries to our Exp

#### NEW QUESTION 129

- (Exam Topic 2)

You have enabled Cloudtrail logs for your company's IAM account. In addition, the IT Security department has mentioned that the logs need to be encrypted. How can this be achieved?

Please select:

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

**Answer: B**

#### Explanation:

The IAM Documentation mentions the following.

By default CloudTrail event log files are encrypted using Amazon S3 server-side encryption (SSE). You can also choose to encryption your log files with an IAM Key Management Service (IAM KMS) key. You can store your log files in your bucket for as long as you want. You can also define Amazon S3 lifecycle rules to archive or delete log files automatically. If you want notifications about lo file delivery and validation, you can set up Amazon SNS notifications.

Option A.C and D are not valid since logs will already be encrypted

For more information on how Cloudtrail works, please visit the following URL: <https://docs.IAM.amazon.com/IAMcloudtrail/latest/useruide/how-cloudtrail-works.html>

The correct answer is: There is no need to do anything since the logs will already be encrypted

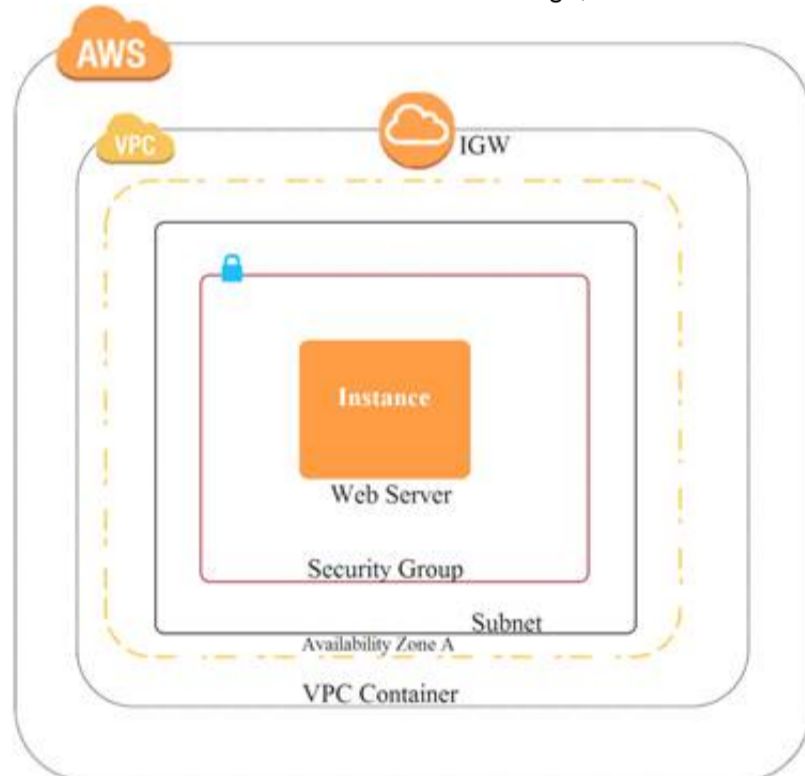
Submit your Feedback/Queries to our Experts

#### NEW QUESTION 133

- (Exam Topic 2)

A company recently experienced a DDoS attack that prevented its web server from serving content. The website is static and hosts only HTML, CSS, and PDF files that users download.

Based on the architecture shown in the image, what is the BEST way to protect the site against future attacks while minimizing the ongoing operational overhead?



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

**Answer: D**

#### Explanation:

<https://docs.IAM.amazon.com/AmazonS3/latest/dev/WebsiteHosting.html>

#### NEW QUESTION 136

- (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 139**

- (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 140**

- (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.amazonaws.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 144**

- (Exam Topic 2)

A company uses user data scripts that contain sensitive information to bootstrap Amazon EC2 instances. A Security Engineer discovers that this sensitive information is viewable by people who should not have access to it.

What is the MOST secure way to protect the sensitive information used to bootstrap the instances?

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

**Answer:** B

**NEW QUESTION 148**

- (Exam Topic 2)

A Security Architect is evaluating managed solutions for storage of encryption keys. The requirements are:

- Storage is accessible by using only VPCs.
- Service has tamper-evident controls.
- Access logging is enabled.
- Storage has high availability.

Which of the following services meets these requirements?

- A. Amazon S3 with default encryption
- B. IAM CloudHSM
- C. Amazon DynamoDB with server-side encryption
- D. IAM Systems Manager Parameter Store

**Answer:** B

**NEW QUESTION 152**

- (Exam Topic 2)

A company has five IAM accounts and wants to use IAM CloudTrail to log API calls. The log files must be stored in an Amazon S3 bucket that resides in a new account specifically built for centralized services with a unique top-level prefix for each trail. The configuration must also enable detection of any modification to the logs.

Which of the following steps will implement these requirements? (Choose three.)

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

**Answer:** ACE

**Explanation:**

<https://docs.IAM.amazon.com/IAMcloudtrail/latest/userguide/best-practices-security.html>

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

**NEW QUESTION 157**

- (Exam Topic 2)

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 158**

- (Exam Topic 2)

A water utility company uses a number of Amazon EC2 instances to manage updates to a fleet of 2,000 Internet of Things (IoT) field devices that monitor water quality. These devices each have unique access credentials.

An operational safety policy requires that access to specific credentials is independently auditable. What is the MOST cost-effective way to manage the storage of credentials?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 161**

- (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 162**

- (Exam Topic 2)

Your company has defined a number of EC2 Instances over a period of 6 months. They want to know if any of the security groups allow unrestricted access to a resource. What is the best option to accomplish this requirement?

Please select:

- A. Use IAM Inspector to inspect all the security Groups
- B. Use the IAM Trusted Advisor to see which security groups have compromised access.
- C. Use IAM Config to see which security groups have compromised access.
- D. Use the IAM CLI to query the security groups and then filter for the rules which have unrestricted access

**Answer:** B

**Explanation:**

The IAM Trusted Advisor can check security groups for rules that allow unrestricted access to a resource. Unrestricted access increases opportunities for malicious activity (hacking, denial-of-service attacks, loss of data).

If you go to IAM Trusted Advisor, you can see the details C:\Users\wk\Desktop\mudassar\Untitled.jpg



Option A is invalid because IAM Inspector is used to detect security vulnerabilities in instances and not for security groups.

Option C is invalid because this can be used to detect changes in security groups but not show you security groups that have compromised access.

Option D is partially valid but would just be a maintenance overhead

For more information on the IAM Trusted Advisor, please visit the below URL: <https://IAM.amazon.com/premiumsupport/trustedadvisor/best-practices>;

The correct answer is: Use the IAM Trusted Advisor to see which security groups have compromised access. Submit your Feedback/Queries to our Experts

**NEW QUESTION 163**

- (Exam Topic 2)

An Amazon EC2 instance is part of an EC2 Auto Scaling group that is behind an Application Load Balancer (ALB). It is suspected that the EC2 instance has been compromised.

Which steps should be taken to investigate the suspected compromise? (Choose three.)

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

**Answer:** BDE

**Explanation:**

[https://d1.IAMstatic.com/whitepapers/IAM\\_security\\_incident\\_response.pdf](https://d1.IAMstatic.com/whitepapers/IAM_security_incident_response.pdf)

**NEW QUESTION 164**

- (Exam Topic 2)

An organization is moving non-business-critical applications to IAM while maintaining a mission-critical application in an on-premises data center. An on-premises application must share limited confidential information with the applications in IAM. The internet performance is unpredictable.

Which configuration will ensure continued connectivity between sites MOST securely?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 169**

- (Exam Topic 2)

Which of the following is used as a secure way to log into an EC2 Linux Instance? Please select:

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

**Answer:** B

**Explanation:**

The IAM Documentation mentions the following

Key pairs consist of a public key and a private key. You use the private key to create a digital signature, and then IAM uses the corresponding public key to

validate the signature. Key pairs are used only for Amazon EC2 and Amazon CloudFront.

Option A.C and D are all wrong because these are not used to log into EC2 Linux Instances For more information on IAM Security credentials, please visit the below URL: <https://docs.IAM.amazon.com/eeneral/latest/er/IAM-sec-cred-types.html>

The correct answer is: Key pairs

Submit your Feedback/Queries to our Experts

## NEW QUESTION 170

- (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 174

- (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:

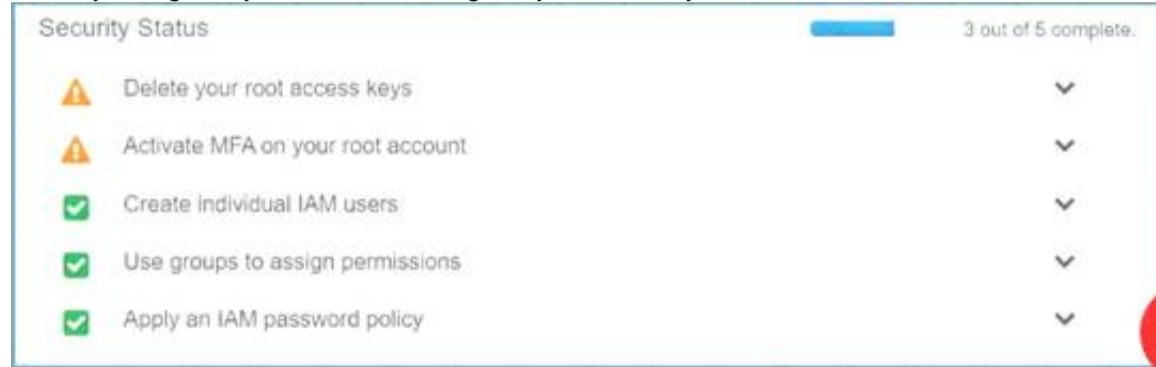
- A. Delete the IAM keys for the root account
- B. Create IAM Groups
- C. Create IAM Roles
- D. Restrict access using IAM policies

**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



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 175

- (Exam Topic 2)

A Security Engineer received an IAM Abuse Notice listing EC2 instance IDs that are reportedly abusing other hosts. Which action should the Engineer take based on this situation? (Choose three.)

- A. Use IAM Artifact to capture an exact image of the state of each instance.
- B. Create EBS Snapshots of each of the volumes attached to the compromised instances.
- C. Capture a memory dump.
- D. Log in to each instance with administrative credentials to restart the instance.
- E. Revoke all network ingress and egress except for to/from a forensics workstation.
- F. Run Auto Recovery for Amazon EC2.

**Answer:** BEF

#### NEW QUESTION 178

- (Exam Topic 2)

A company wants to have an Intrusion detection system available for their VPC in IAM. They want to have complete control over the system. Which of the following would be ideal to implement?

Please select:

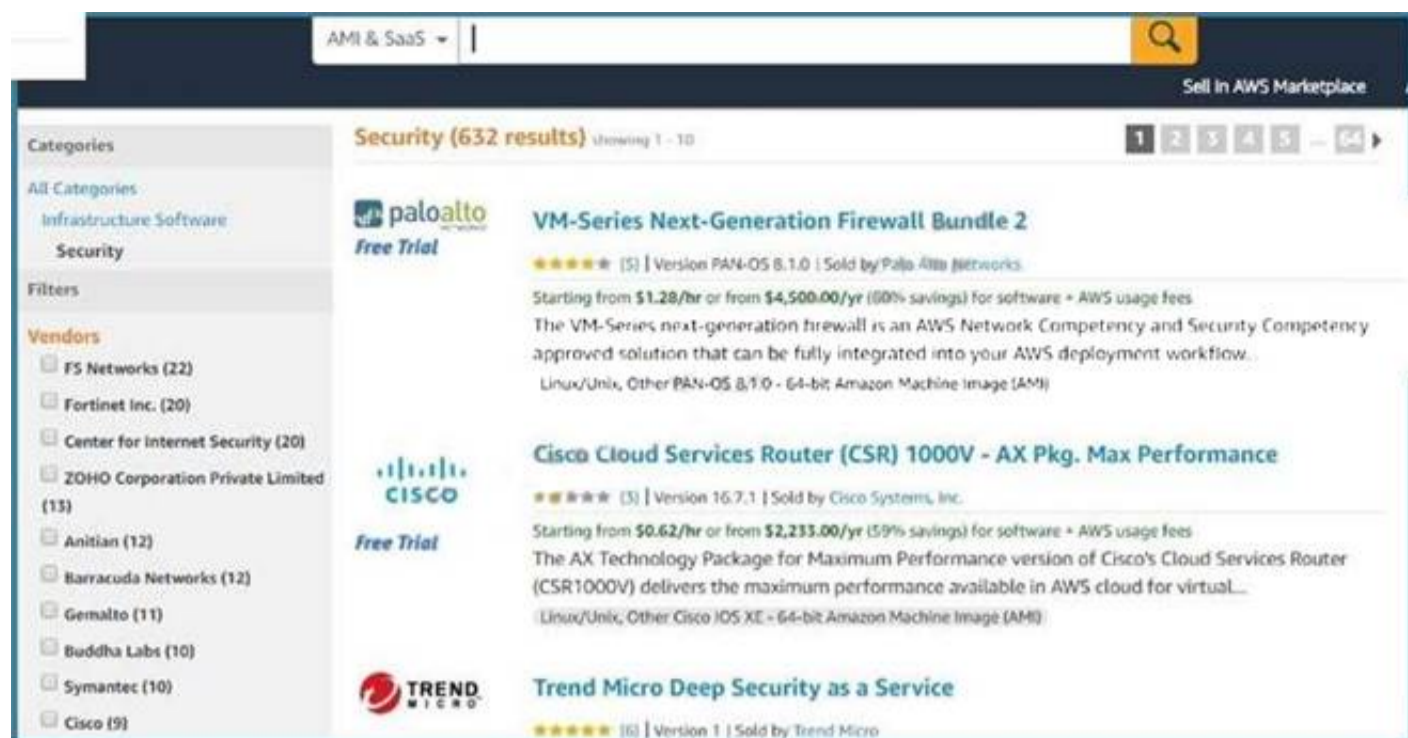
- A. Use IAM WAF to catch all intrusions occurring on the systems in the VPC
- B. Use a custom solution available in the IAM Marketplace
- C. Use VPC Flow logs to detect the issues and flag them accordingly.
- D. Use IAM Cloudwatch to monitor all traffic

**Answer:** B

#### Explanation:

Sometimes companies want to have custom solutions in place for monitoring Intrusions to their systems. In such a case, you can use the IAM Marketplace for looking at custom solutions.

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



Option A, C and D are all invalid because they cannot be used to conduct intrusion detection or prevention. For more information on using custom security solutions please visit the below URL [https://d1.IAMstatic.com/Marketplace/security/IAMMP\\_Security\\_Solution%20Overview.pdf](https://d1.IAMstatic.com/Marketplace/security/IAMMP_Security_Solution%20Overview.pdf)

For more information on using custom security solutions please visit the below URL: [https://d1.IAMstatic.com/Marketplace/security/IAMMP\\_Security\\_Solution%20Overview.pdf](https://d1.IAMstatic.com/Marketplace/security/IAMMP_Security_Solution%20Overview.pdf)

The correct answer is: Use a custom solution available in the IAM Marketplace Submit your Feedback/Queries to our Experts

### NEW QUESTION 182

- (Exam Topic 2)

A Security Engineer is working with the development team to design a supply chain application that stores sensitive inventory data in an Amazon S3 bucket. The application will use an IAM KMS customer master key (CMK) to encrypt the data on Amazon S3. The inventory data on Amazon S3 will be shared with vendors. All vendors will use IAM principals from their own IAM accounts to access the data on Amazon S3. The vendor list may change weekly, and the solution must support cross-account access.

What is the MOST efficient way to manage access control for the KMS CMK?

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

**Answer: A**

### NEW QUESTION 184

- (Exam Topic 2)

When you enable automatic key rotation for an existing CMK key where the backing key is managed by IAM, after how long is the key rotated?

Please select:

- A. After 30 days
- B. After 128 days
- C. After 365 days
- D. After 3 years

**Answer: D**

### Explanation:

The IAM Documentation states the following

- IAM managed CM Ks: You cannot manage key rotation for IAM managed CMKs. IAM KMS automatically rotates IAM managed keys every three years (1095 days).

Note: IAM-managed CMKs are rotated every 3yrs, Customer-Managed CMKs are rotated every 365-days from when rotation is enabled.

Option A, B, C are invalid because the settings for automatic key rotation is not changeable. For more information on key rotation please visit the below URL

<https://docs.IAM.amazon.com/kms/latest/developerguide/rotate-keys.html>

IAM managed CMKs are CMKs in your account that are created, managed, and used on your behalf by an IAM service that is integrated with IAM KMS. This CMK is unique to your IAM account and region. Only the service that created the IAM managed CMK can use it

You can login to your IAM dashboard. Click on "Encryption Keys"

You will find the list based on the services you are using as follows:

- IAM/elasticfilesystem 1 IAM/lightail
- IAM/s3
- IAM/rds and many more Detailed Guide: KMS

You can recognize IAM managed CMKs because their aliases have the format IAM/service-name, such as IAM/redshift. Typically, a service creates its IAM managed CMK in your account when you set up the service or the first time you use the CMK

The IAM services that integrate with IAM KMS can use it in many different ways. Some services create IAM managed CMKs in your account. Other services require that you specify a customer managed CMK that you have created. And, others support both types of CMKs to allow you the ease of an IAM managed CMK or the control of a customer-managed CMK

Rotation period for CMKs is as follows:

- IAM managed CMKs: 1095 days
- Customer managed CMKs: 365 days

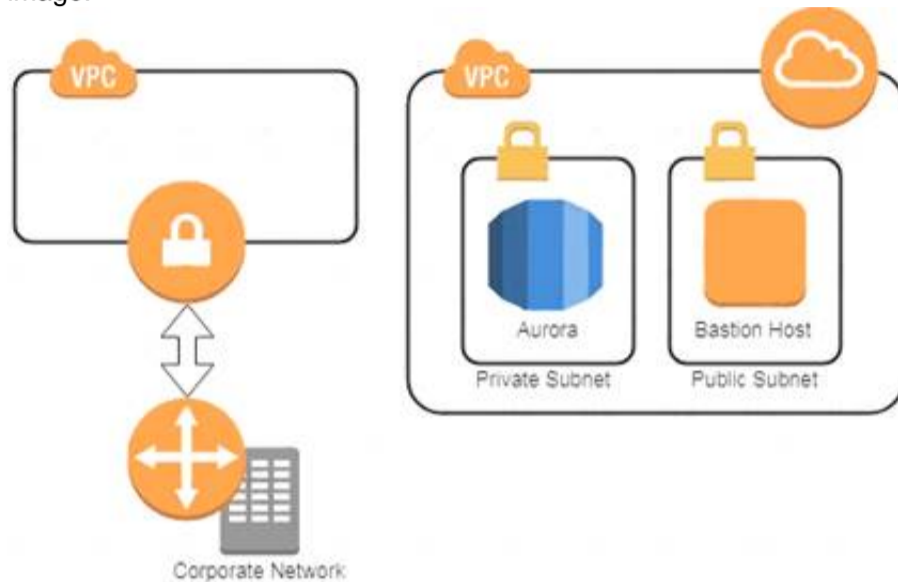
Since question mentions about "CMK where backing keys is managed by IAM", its Amazon(IAM) managed and its rotation period turns out to be 1095 days(every 3 years)

For more details, please check below IAM Docs: <https://docs.IAM.amazon.com/kms/latest/developerguide/concepts.html> The correct answer is: After 3 years  
 Submit your Feedback/Queries to our Experts

#### NEW QUESTION 188

- (Exam Topic 2)

A company has two IAM accounts, each containing one VPC. The first VPC has a VPN connection with its corporate network. The second VPC, without a VPN, hosts an Amazon Aurora database cluster in private subnets. Developers manage the Aurora database from a bastion host in a public subnet as shown in the image.



A security review has flagged this architecture as vulnerable, and a Security Engineer has been asked to make this design more secure. The company has a short deadline and a second VPN connection to the Aurora account is not possible.

How can a Security Engineer securely set up the bastion host?

- A. Move the bastion host to the VPC with VPN connectivity
- B. Create a VPC peering relationship between the bastion host VPC and Aurora VPC.
- C. Create a SSH port forwarding tunnel on the Developer's workstation to the bastion host to ensure that only authorized SSH clients can access the bastion host.
- D. Move the bastion host to the VPC with VPN connectivity
- E. Create a cross-account trust relationship between the bastion VPC and Aurora VPC, and update the Aurora security group for the relationship.
- F. Create an IAM Direct Connect connection between the corporate network and the Aurora account, and adjust the Aurora security group for this connection.

**Answer:** A

#### NEW QUESTION 190

- (Exam Topic 2)

Compliance requirements state that all communications between company on-premises hosts and EC2 instances be encrypted in transit. Hosts use custom proprietary protocols for their communication, and EC2 instances need to be fronted by a load balancer for increased availability.

Which of the following solutions will meet these requirements?

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

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 193

- (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 198

- (Exam Topic 2)

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

Please select:

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

**Answer:** C

**Explanation:**

Option A is invalid because the normal IAM Shield Service will not help in immediate action against a DDos attack. This can be done via the IAM Shield Advanced Service

Option B is invalid because this is a logging service for VPCs traffic flow but cannot specifically protect against DDos attacks.

Option D is invalid because this is a logging service for IAM Services but cannot specifically protect against DDos attacks.

The IAM Documentation mentions the following

IAM Shield Advanced provides enhanced protections for your applications running on Amazon EC2, Elastic Load Balancing (ELB), Amazon CloudFront and Route 53 against larger and more sophisticated attacks. IAM Shield Advanced is available to IAM Business Support and IAM Enterprise Support customers. IAM Shield Advanced protection provides always-on, flow-based monitoring of network traffic and active application monitoring to provide near real-time notifications of DDoS attacks. IAM Shield Advanced also gives customers highly flexible controls over attack mitigations to take actions instantly. Customers can also engage the DDoS Response Team (DRT) 24x7 to manage and mitigate their application layer DDoS attacks.

For more information on IAM Shield, please visit the below URL: <https://IAM.amazon.com/shield/faqs>;

The correct answer is: Consider using the IAM Shield Advanced Service Submit your Feedback/Queries to our Experts

**NEW QUESTION 202**

- (Exam Topic 2)

A Systems Administrator has written the following Amazon S3 bucket policy designed to allow access to an S3 bucket for only an authorized IAM IAM user from the IP address range 10.10.10.0/24:

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

When trying to download an object from the S3 bucket from 10.10.10.40, the IAM user receives an access denied message.

What does the Administrator need to change to grant access to the user?

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

**Answer:** A

**NEW QUESTION 207**

- (Exam Topic 2)

Which approach will generate automated security alerts should too many unauthorized IAM API requests be identified?

- A. Create an Amazon CloudWatch metric filter that looks for API call error codes and then implement an alarm based on that metric's rate.
- B. Configure IAM CloudTrail to stream event data to Amazon Kinesis
- C. Configure an IAM Lambda function on the stream to alarm when the threshold has been exceeded.
- D. Run an Amazon Athena SQL query against CloudTrail log file
- E. Use Amazon QuickSight to create an operational dashboard.
- F. Use the Amazon Personal Health Dashboard to monitor the account's use of IAM services, and raise an alert if service error rates increase.

**Answer:** A

**Explanation:**

<https://docs.IAM.amazon.com/IAMcloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail.html#cloudwatc> Open the CloudWatch console at

<https://console.IAM.amazon.com/cloudwatch/>. In the navigation pane,

choose Logs. In the list of log groups, select the check box next to the log group that you created for CloudTrail log events. Choose Create Metric Filter. On the Define Logs Metric Filter screen, choose Filter Pattern and then type the following: { (\$errorCode = "UnauthorizedOperation") || (\$errorCode = "AccessDenied")} Choose Assign Metric. For Filter Name, type AuthorizationFailures. For Metric Namespace, type CloudTrailMetrics. For Metric Name, type

AuthorizationFailureCount.

#### NEW QUESTION 209

- (Exam Topic 2)

An organization is using IAM CloudTrail, Amazon CloudWatch Logs, and Amazon CloudWatch to send alerts when new access keys are created. However, the alerts are no longer appearing in the Security Operations mail box.

Which of the following actions would resolve this issue?

- A. In CloudTrail, verify that the trail logging bucket has a log prefix configured.
- B. In Amazon SNS, determine whether the "Account spend limit" has been reached for this alert.
- C. In SNS, ensure that the subscription used by these alerts has not been deleted.
- D. In CloudWatch, verify that the alarm threshold "consecutive periods" value is equal to, or greater than 1.

**Answer:** C

#### NEW QUESTION 213

- (Exam Topic 2)

A security team is responsible for reviewing IAM API call activity in the cloud environment for security violations. These events must be recorded and retained in a centralized location for both current and future IAM regions.

What is the SIMPLEST way to meet these requirements?

- A. Enable IAM Trusted Advisor security checks in the IAM Console, and report all security incidents for all regions.
- B. Enable IAM CloudTrail by creating individual trails for each region, and specify a single Amazon S3 bucket to receive log files for later analysis.
- C. Enable IAM CloudTrail by creating a new trail and applying the trail to all region
- D. Specify a single Amazon S3 bucket as the storage location.
- E. Enable Amazon CloudWatch logging for all IAM services across all regions, and aggregate them to a single Amazon S3 bucket for later analysis.

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 217

- (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 218

- (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 account
- B. Delete the password for the IAM account root user.
- C. Create a new IAM user that has administrator permissions in the IAM account
- 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 account
- 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 220

- (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 224

- (Exam Topic 2)

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

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

**Answer:** AD

#### Explanation:

Since HTTPS traffic is required for all users on the Internet, Port 443 should be open on all IP addresses. For port 22, the traffic should be restricted to an internal subnet.

Option B is invalid, because this only allow traffic from a particular CIDR block and not from the internet Option C is invalid because allowing port 22 from the internet is a security risk

For more information on IAM Security Groups, please visit the following UR

<https://docs.IAM.amazon.com/IAMEC2/latest/UserGuide/usins-network-security.html>

The correct answers are: Port 443 coming from 0.0.0.0/0, Port 22 coming from 203.0.113.1 /32 Submit your Feedback/Queries to our Experts

#### NEW QUESTION 225

- (Exam Topic 2)

An application uses Amazon Cognito to manage end users' permissions when directly accessing IAM resources, including Amazon DynamoDB. A new feature request reads as follows:

Provide a mechanism to mark customers as suspended pending investigation or suspended permanently. Customers should still be able to log in when suspended, but should not be able to make changes.

The priorities are to reduce complexity and avoid potential for future security issues. Which approach will meet these requirements and priorities?

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

**Answer:** D

#### Explanation:

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

#### NEW QUESTION 229

- (Exam Topic 2)

A Systems Engineer is troubleshooting the connectivity of a test environment that includes a virtual security appliance deployed inline. In addition to using the virtual security appliance, the Development team wants to use security groups and network ACLs to accomplish various security requirements in the environment. What configuration is necessary to allow the virtual security appliance to route the traffic?

- A. Disable network ACLs.
- B. Configure the security appliance's elastic network interface for promiscuous mode.
- C. Disable the Network Source/Destination check on the security appliance's elastic network interface
- D. Place the security appliance in the public subnet with the internet gateway

**Answer:** C

#### Explanation:

Each EC2 instance performs source/destination checks by default. This means that the instance must be the source or destination of any traffic it sends or receives. In this case virtual security appliance instance must be able to send and receive traffic when the source or destination is not itself. Therefore, you must disable source/destination checks on the NAT instance."

#### NEW QUESTION 230

- (Exam Topic 2)

A Security Engineer must design a system that can detect whether a file on an Amazon EC2 host has been modified. The system must then alert the Security Engineer of the modification.

What is the MOST efficient way to meet these requirements?

- A. Install antivirus software and ensure that signatures are up-to-dat
- B. Configure Amazon CloudWatch alarms to send alerts for security events.
- C. Install host-based IDS software to check for file integrit
- D. Export the logs to Amazon CloudWatch Logs for monitoring and alerting.
- E. Export system log files to Amazon S3. Parse the log files using an IAM Lambda function that will send alerts of any unauthorized system login attempts through Amazon SNS.
- F. Use Amazon CloudWatch Logs to detect file system change
- G. If a change is detected, automatically terminate and recreate the instance from the most recent AM
- H. Use Amazon SNS to send notification of the event.

**Answer:** B

#### NEW QUESTION 232

- (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 it'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 entity, 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 Policies 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 235

- (Exam Topic 3)

Your company has mandated that all data in IAM be encrypted at rest. How can you achieve this for EBS volumes? Choose 2 answers from the options given below

Please select:

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

**Answer:** AB

#### Explanation:

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

Option C is incorrect.

IAM Systems Manager is a management service that helps you automatically collect software inventory, apply OS patches, create system images, and configure Windows and Linux operating systems.

Option D is incorrect

You cannot choose to encrypt a non-encrypted boot volume on instance launch. To have encrypted boot volumes during launch, your custom AMI must have its boot volume encrypted before launch.

For more information on the Security Best Practices, please visit the following URL: [com/whit](https://aws.amazon.com/whit) Security Practices.

The correct answers are: Use Windows BitLocker for EBS volumes on Windows instances. Use TrueEncrypt for EBS volumes on Linux instances

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 236

- (Exam Topic 3)

When managing permissions for the API gateway, what can be used to ensure that the right level of permissions are given to developers, IT admins and users?

These permissions should be easily managed.

Please select:

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

**Answer:** B

#### Explanation:

The IAM Documentation mentions the following

You control access to Amazon API Gateway with IAM permissions by controlling access to the following two API Gateway component processes:

\* To create, deploy, and manage an API in API Gateway, you must grant the API developer permissions to perform the required actions supported by the API management component of API Gateway.

\* To call a deployed API or to refresh the API caching, you must grant the API caller permissions to perform required IAM actions supported by the API execution component of API Gateway.

Option A, C and D are invalid because these cannot be used to control access to IAM services. This needs to be done via policies. For more information on permissions with the API gateway, please visit the following URL:

<https://docs.IAM.amazon.com/apigateway/latest/developerguide/permissions.html>

The correct answer is: Use IAM Policies to create different policies for the different types of users. Submit your Feedback/Queries to our Experts

#### NEW QUESTION 237

- (Exam Topic 3)

There is a set of EC2 Instances in a private subnet. The application hosted on these EC2 Instances needs to access a DynamoDB table. It needs to be ensured that

traffic does not flow out to the internet. How can this be achieved?  
 Please select:

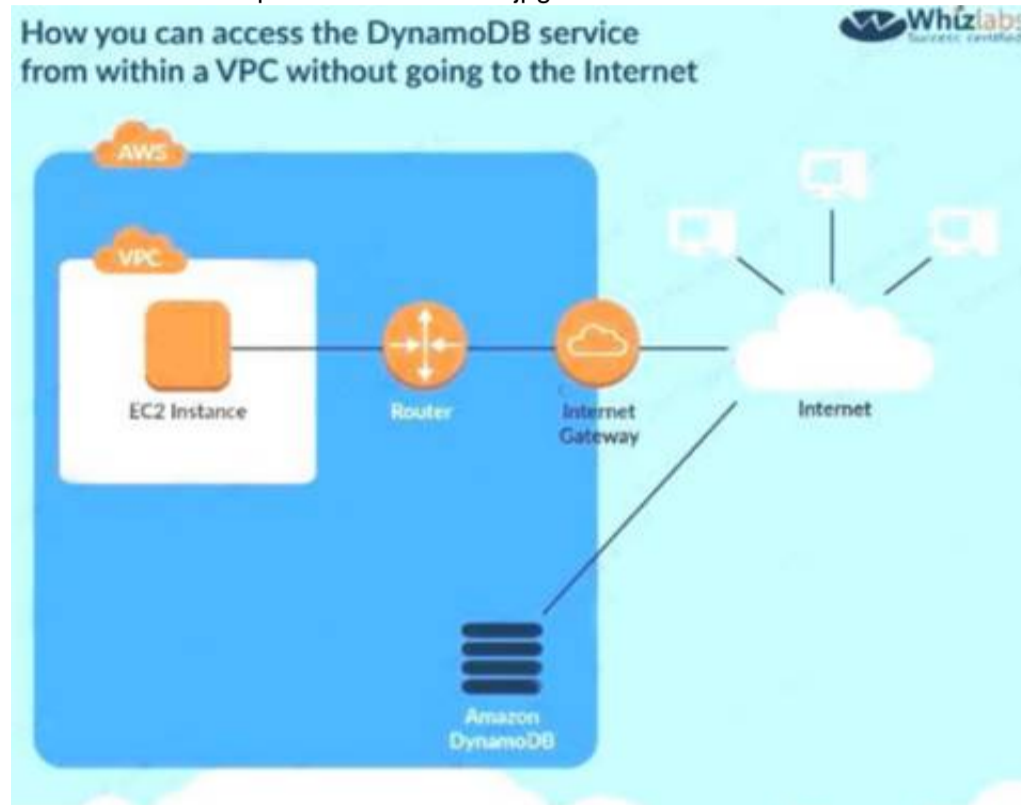
- A. Use a VPC endpoint to the DynamoDB table
- B. Use a VPN connection from the VPC
- C. Use a VPC gateway from the VPC
- D. Use a VPC Peering connection to the DynamoDB table

**Answer:** A

**Explanation:**

The following diagram from the IAM Documentation shows how you can access the DynamoDB service from within a V without going to the Internet This can be done with the help of a VPC endpoint

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



Option B is invalid because this is used for connection between an on-premise solution and IAM Option C is invalid because there is no such option

Option D is invalid because this is used to connect 2 VPCs

For more information on VPC endpointsfor DynamoDB, please visit the URL:

The correct answer is: Use a VPC endpoint to the DynamoDB table Submit your Feedback/Queries to our Experts

**NEW QUESTION 238**

- (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 241**

- (Exam Topic 3)

A company is using a Redshift cluster to store their data warehouse. There is a requirement from the Internal IT Security team to ensure that data gets encrypted for the Redshift database. How can this be achieved?

Please select:

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

**Answer:** B

**Explanation:**

The IAM Documentation mentions the following

Amazon Redshift uses a hierarchy of encryption keys to encrypt the database. You can use either IAM Key Management Service (IAM KMS) or a hardware security module (HSM) to manage the top-level encryption keys in this hierarchy. The process that Amazon Redshift uses for encryption differs depending on how you manage keys.

Option A is invalid because it's the cluster that needs to be encrypted

Option C is invalid because this encrypts objects in transit and not objects at rest Option D is invalid because this is used only for objects in S3 buckets

For more information on Redshift encryption, please visit the following URL: <https://docs.IAM.amazon.com/redshift/latest/mgmt/work-with-db-encryption.html>

The correct answer is: Use IAM KMS Customer Default master key Submit your Feedback/Queries to our Experts

#### NEW QUESTION 242

- (Exam Topic 3)

Which of the following is the correct sequence of how KMS manages the keys when used along with the Redshift cluster service

Please select:

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

**Answer:** A

#### Explanation:

This is mentioned in the IAM Documentation

Amazon Redshift uses a four-tier, key-based architecture for encryption. The architecture consists of data encryption keys, a database key, a cluster key, and a master key.

Data encryption keys encrypt data blocks in the cluster. Each data block is assigned a randomly-generated AES-256 key. These keys are encrypted by using the database key for the cluster.

The database key encrypts data encryption keys in the cluster. The database key is a randomly-generated AES-256 key. It is stored on disk in a separate network from the Amazon Redshift cluster and passed to the cluster across a secure channel.

The cluster key encrypts the database key for the Amazon Redshift cluster.

Option B is incorrect because the master key encrypts the cluster key and not the database key

Option C is incorrect because the master key encrypts the cluster key and not the data encryption keys Option D is incorrect because the master key encrypts the cluster key only

For more information on how keys are used in Redshift, please visit the following URL: <https://docs.IAM.amazon.com/kms/latest/developerguide/services-redshift.html>

The correct answer is: The master key encrypts the cluster key. The cluster key encrypts the database key. The database key encrypts the data encryption keys. Submit your Feedback/Queries to our Experts

#### NEW QUESTION 247

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SCS-C02 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SCS-C02 Product From:

<https://www.2passeasy.com/dumps/SCS-C02/>

## Money Back Guarantee

### SCS-C02 Practice Exam Features:

- \* SCS-C02 Questions and Answers Updated Frequently
- \* SCS-C02 Practice Questions Verified by Expert Senior Certified Staff
- \* SCS-C02 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* SCS-C02 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year