

# Amazon-Web-Services

## Exam Questions SCS-C02

AWS Certified Security - Specialty



**NEW QUESTION 1**

- (Exam Topic 1)

A Security Engineer has been asked to troubleshoot inbound connectivity to a web server. This single web server is not receiving inbound connections from the internet, whereas all other web servers are functioning properly.

The architecture includes network ACLs, security groups, and a virtual security appliance. In addition, the Development team has implemented Application Load Balancers (ALBs) to distribute the load across all web servers. It is a requirement that traffic between the web servers and the internet flow through the virtual security appliance.

The Security Engineer has verified the following:

- \* 1. The rule set in the Security Groups is correct
- \* 2. The rule set in the network ACLs is correct
- \* 3. The rule set in the virtual appliance is correct

Which of the following are other valid items to troubleshoot in this scenario? (Choose two.)

- A. Verify that the 0.0.0.0/0 route in the route table for the web server subnet points to a NAT gateway.
- B. Verify which Security Group is applied to the particular web server's elastic network interface (ENI).
- C. Verify that the 0.0.0.0/0 route in the route table for the web server subnet points to the virtual security appliance.
- D. Verify the registered targets in the ALB.
- E. Verify that the 0.0.0.0/0 route in the public subnet points to a NAT gateway.

**Answer:** CD

**Explanation:**

<https://docs.IAM.amazon.com/IAMEC2/latest/UserGuide/using-eni.html>

**NEW QUESTION 2**

- (Exam Topic 1)

A company has multiple IAM accounts that are part of IAM Organizations. The company's Security team wants to ensure that even those Administrators with full access to the company's IAM accounts are unable to access the company's Amazon S3 buckets

How should this be accomplished?

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

**Answer:** A

**NEW QUESTION 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 IAM:securetransport 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 city is implementing an election results reporting website that will use Amazon CloudFront. The website runs on a fleet of Amazon EC2 instances behind an Application Load Balancer (ALB) in an Auto Scaling group. Election results are updated hourly and are stored as .pdf files in an Amazon S3 bucket. A Security Engineer needs to ensure that all external access to the website goes through CloudFront.

Which solution meets these requirements?

- A. Create an IAM role that allows CloudFront to access the specific S3 bucket
- B. Modify the S3 bucket policy to allow only the new IAM role to access its content
- C. Create an interface VPC endpoint for CloudFront to securely communicate with the ALB.
- D. Create an IAM role that allows CloudFront to access the specific S3 bucket
- E. Modify the S3 bucket policy to allow only the new IAM role to access its content
- F. Associate the ALB with a security group that allows only incoming traffic from the CloudFront service to communicate with the ALB.
- G. Create an origin access identity (OAI) in CloudFront
- H. Modify the S3 bucket policy to allow only the new OAI to access the bucket content
- I. Create an interface VPC endpoint for CloudFront to securely communicate with the ALB.
- J. Create an origin access identity (OAI) in CloudFront
- K. Modify the S3 bucket policy to allow only the new OAI to access the bucket content
- L. Associate the ALB with a security group that allows only incoming traffic from the CloudFront service to communicate with the ALB.

**Answer: C**

**NEW QUESTION 6**

- (Exam Topic 1)

An external Auditor finds that a company's user passwords have no minimum length. The company is currently using two identity providers:

- IAM IAM federated with on-premises Active Directory
  - Amazon Cognito user pools to accessing an IAM Cloud application developed by the company
- Which combination of actions should the Security Engineer take to solve this issue? (Select TWO.)

- A. Update the password length policy In the on-premises Active Directory configuration.
- B. Update the password length policy In the IAM configuration.
- C. Enforce an IAM policy In Amazon Cognito and IAM IAM with a minimum password length condition.
- D. Update the password length policy in the Amazon Cognito configuration.
- E. Create an SCP with IAM Organizations that enforces a minimum password length for IAM IAM and Amazon Cognito.

**Answer: AD**

**NEW QUESTION 7**

- (Exam Topic 1)

A company is building a data lake on Amazon S3. The data consists of millions of small files containing sensitive information. The security team has the following requirements for the architecture:

- Data must be encrypted in transit.
- Data must be encrypted at rest.
- The bucket must be private, but if the bucket is accidentally made public, the data must remain confidential. Which combination of steps would meet the requirements? (Select THREE.)

- A. Enable AES-256 encryption using server-side encryption with Amazon S3-managed encryption keys (SSE-S3) on the S3 bucket
- B. Enable default encryption with server-side encryption with IAM KMS-managed keys (SSE-KMS) on the S3 bucket.
- C. Add a bucket policy that includes a deny if a PutObject request does not include IAM:SecureTransferOnly.
- D. Add a bucket policy with s3:PutObject to Allow uploads and downloads from the corporate intranet only.
- E. Add a bucket policy that includes a deny if a PutObject request does not include s3:x-amz-server-side-encryption: "IAM: kms".
- F. Enable Amazon Macie to monitor and act on changes to the data lake's S3 bucket.

**Answer: BDF**

**NEW QUESTION 8**

- (Exam Topic 1)

A company had one of its Amazon EC2 key pairs compromised. A Security Engineer must identify which current Linux EC2 instances were deployed and used the compromised key pair.

How can this task be accomplished?

- A. Obtain the list of instances by directly querying Amazon EC2 using: `aws ec2 describe-instances --filters "Name=key-name,Values=KEYNAMEHERE"`.
- B. Obtain the fingerprint for the key pair from the IAM Management Console, then search for the fingerprint in the Amazon Inspector logs.
- C. Obtain the output from the EC2 instance metadata using: `curl http://169.254.169.254/latest/meta-data/public-keys/0/`.
- D. Obtain the fingerprint for the key pair from the IAM Management Console, then search for the fingerprint in Amazon CloudWatch Logs using: `aws logs filter-log-events`.

**Answer: A**

**NEW QUESTION 9**

- (Exam Topic 1)

A company's architecture requires that its three Amazon EC2 instances run behind an Application Load Balancer (ALB). The EC2 instances transmit sensitive data between each other. Developers use SSL certificates to encrypt the traffic between the public users and the ALB. However, the Developers are unsure of how to encrypt the data in transit between the ALB and the EC2 instances and the traffic between the EC2 instances.

Which combination of activities must the company implement to meet its encryption requirements? (Select TWO.)

- A. Configure SSLTLS on the EC2 instances and configure the ALB target group to use HTTPS
- B. Ensure that all resources are in the same VPC so the default encryption provided by the VPC is used to encrypt the traffic between the EC2 instances.
- C. In the AL
- D. select the default encryption to encrypt the traffic between the ALB and the EC2 instances
- E. In the code for the application, include a cryptography library and encrypt the data before sending it between the EC2 instances
- F. Configure IAM Direct Connect to provide an encrypted tunnel between the EC2 instances

**Answer:** BC

#### NEW QUESTION 10

- (Exam Topic 1)

A security engineer is designing an incident response plan to address the risk of a compromised Amazon EC2 instance. The plan must recommend a solution to meet the following requirements:

- A trusted forensic environment must be provisioned
- Automated response processes must be orchestrated

Which IAM services should be included in the plan? (Select TWO)

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

**Answer:** AE

#### NEW QUESTION 10

- (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 11

- (Exam Topic 1)

A security engineer needs to configure monitoring and auditing for IAM Lambda.

Which combination of actions using IAM services should the security engineer take to accomplish this goal? (Select TWO.)

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

**Answer:** AB

#### NEW QUESTION 15

- (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 18

- (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 20

- (Exam Topic 1)

A company recently performed an annual security assessment of its IAM environment. The assessment showed that audit logs are not available beyond 90 days and that unauthorized changes to IAM policies are made without detection.

How should a security engineer resolve these issues?

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

**Answer:** D

#### Explanation:

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

"For an ongoing record of events in your IAM account, you must create a trail. Although CloudTrail provides 90 days of event history information for management events in the CloudTrail console without creating a trail, it is not a permanent record, and it does not provide information about all possible types of events. For an ongoing record, and for a record that contains all the event types you specify, you must create a trail, which delivers log files to an Amazon S3 bucket that you specify."

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

#### NEW QUESTION 24

- (Exam Topic 1)

A company's security engineer is configuring Amazon S3 permissions to ban all current and future public buckets However, the company hosts several websites directly off S3 buckets with public access enabled

The engineer needs to block me pubic S3 buckets without causing any outages on me easting websites The engineer has set up an Amazon CloudFrom distribution (or each website

Which set or steps should the security engineer implement next?

- A. Configure an S3 bucket as the origin an origin access identity (OAI) for the CloudFront distribution Switch the DNS records from websites to point to the CloudFront distribution Enable Nock public access settings at the account level
- B. Configure an S3 bucket as the origin with an origin access identity (OAI) for the CloudFront distribution Switch the ONS records tor the websites to point to the CloudFront disinfection Then, tor each S3 bucket enable block public access settings
- C. Configure an S3 bucket as the origin with an origin access identity (OAI) for the CloudFront distribution Enable block public access settings at the account level
- D. Configure an S3 bucket as the origin for me CloudFront distribution Configure the S3 bucket policy to accept connections from the CloudFront points of presence only Switch the DNS records for the websites to point to the CloudFront distribution Enable block public access settings at me account level

**Answer:** A

#### NEW QUESTION 28

- (Exam Topic 1)

A company has an application hosted in an Amazon EC2 instance and wants the application to access secure strings stored in IAM Systems Manager Parameter Store When the application tries to access the secure string key value, it fails.

Which factors could be the cause of this failure? (Select TWO.)

- A. The EC2 instance role does not have decrypt permissions on the IAM Key Management Sen/ice (IAM KMS) key used to encrypt the secret
- B. The EC2 instance role does not have read permissions to read the parameters In Parameter Store
- C. Parameter Store does not have permission to use IAM Key Management Service (IAM KMS) to decrypt the parameter
- D. The EC2 instance role does not have encrypt permissions on the IAM Key Management Service (IAM KMS) key associated with the secret
- E. The EC2 instance does not have any tags associated.

**Answer:** AB

#### Explanation:

<https://docs.IAM.amazon.com/systems-manager/latest/userguide/sysman-paramstore-access.html>

#### NEW QUESTION 29

- (Exam Topic 1)

A large government organization is moving to the cloud and has specific encryption requirements. The first workload to move requires that a customer's data be immediately destroyed when the customer makes that request.

Management has asked the security team to provide a solution that will securely store the data, allow only authorized applications to perform encryption and decryption and allow for immediate destruction of the data

Which solution will meet these requirements?

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

customer.

**Answer:** A

### NEW QUESTION 33

- (Exam Topic 1)

A global company must mitigate and respond to DDoS attacks at Layers 3, 4 and 7 All of the company's IAM applications are serverless with static content hosted on Amazon S3 using Amazon CloudFront and Amazon Route 53

Which solution will meet these requirements?

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

**Answer:** C

### NEW QUESTION 36

- (Exam Topic 1)

A security engineer must develop an encryption tool for a company. The company requires a cryptographic solution that supports the ability to perform cryptographic erasure on all resources protected by the key material in 15 minutes or less

Which IAM Key Management Service (IAM KMS) key solution will allow the security engineer to meet these requirements?

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

**Answer:** C

### NEW QUESTION 40

- (Exam Topic 1)

A company is collecting IAM CloudTrail log data from multiple IAM accounts by managing individual trails in each account and forwarding log data to a centralized Amazon S3 bucket residing in a log archive account. After CloudTrail introduced support for IAM Organizations trails, the company decided to further centralize management and automate deployment of the CloudTrail logging capability across all of its IAM accounts.

The company's security engineer created an IAM Organizations trail in the master account, enabled server-side encryption with IAM KMS managed keys (SSE-KMS) for the log files, and specified the same bucket as the storage location. However, the engineer noticed that logs recorded by the new trail were not delivered to the bucket.

Which factors could cause this issue? (Select TWO.)

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

**Answer:** AD

### NEW QUESTION 42

- (Exam Topic 1)

A security engineer is asked to update an AW3 CloudTrail 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 trail 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 PutBucketPolicy
- 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 43

- (Exam Topic 1)

Users report intermittent availability of a web application hosted on IAM. Monitoring systems report an excess of abnormal network traffic followed by high CPU utilization on the application web tier. Which of the following techniques will improve the availability of the application? (Select TWO.)

- A. Deploy IAM WAF to block all unsecured web applications from accessing the internet.
- B. Deploy an Intrusion Detection/Prevention System (IDS/IPS) to monitor or block unusual incoming network traffic.
- C. Configure security groups to allow outgoing network traffic only from hosts that are protected with up-to-date antivirus software.
- D. Create Amazon CloudFront distribution and configure IAM WAF rules to protect the web applications from malicious traffic.
- E. Use the default Amazon VPC for external-facing systems to allow IAM to actively block malicious network traffic affecting Amazon EC2 instances.

**Answer:** BD

#### NEW QUESTION 44

- (Exam Topic 1)

A Security Engineer has launched multiple Amazon EC2 instances from a private AMI using an IAM CloudFormation template. The Engineer notices instances terminating right after they are launched.

What could be causing these terminations?

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 49

- (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 52

- (Exam Topic 1)

A security engineer must use IAM Key Management Service (IAM KMS) to design a key management solution for a set of Amazon Elastic Block Store (Amazon EBS) volumes that contain sensitive data. The solution needs to ensure that the key material automatically expires in 90 days.

Which solution meets these criteria?

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

**Answer:** B

#### NEW QUESTION 57

- (Exam Topic 1)

A company uses HTTP Live Streaming (HLS) to stream live video content to paying subscribers by using

Amazon CloudFront. HLS splits the video content into chunks so that the user can request the right chunk based on different conditions Because the video events last for several hours, the total video is made up of thousands of chunks

The origin URL is not disclosed and every user is forced to access the CloudFront URL The company has a web application that authenticates the paying users against an internal repository and a CloudFront key pair that is already issued.

What is the simplest and MOST effective way to protect the content?

- A. Develop the application to use the CloudFront key pair to create signed URLs that users will use to access the content.
- B. Develop the application to use the CloudFront key pair to set the signed cookies that users will use to access the content.
- C. Develop the application to issue a security token that Lambda@Edge will receive to authenticate and authorize access to the content
- D. Keep the CloudFront URL encrypted inside the application, and use IAM KMS to resolve the URL on-the-fly after the user is authenticated.

**Answer:** B

#### NEW QUESTION 61

- (Exam Topic 1)

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

A)

Add the following condition to the IAM policy attached to all IAM roles:

```
"Effect" : "Deny",  
"Condition" : { "BoolIfExists" : { "aws:MultiFactorAuthPresent" : false } }
```

B)

Add the following condition to the IAM policy attached to all IAM roles:

```
"Effect" : "Deny",  
"Condition" : { "Bool" : { "aws:MultiFactorAuthPresent" : false } }
```

C)

Add the following condition to the IAM policy attached to all IAM roles:

```
"Effect" : "Allow",  
"Condition" : { "Null" : { "aws:MultiFactorAuthPresent" : false } }
```

D)

Add the following condition to the IAM policy attached to all IAM roles:

```
"Effect" : "Allow",  
"Condition" : { "BoolIfExists" : { "aws:MultiFactorAuthPresent" : false } }
```

A. Option A

B. Option B

C. Option C

D. Option D

**Answer:** A

#### NEW QUESTION 66

- (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 70

- (Exam Topic 1)

A Solutions Architect is designing a web application that uses Amazon CloudFront, an Elastic Load Balancing Application Load Balancer, and an Auto Scaling group of Amazon EC2 instances. The load balancer and EC2 instances are in the US West (Oregon) region. It has been decided that encryption in transit is necessary by using a customer-branded domain name from the client to CloudFront and from CloudFront to the load balancer.

Assuming that IAM Certificate Manager is used, how many certificates will need to be generated?

A. One in the US West (Oregon) region and one in the US East (Virginia) region.

B. Two in the US West (Oregon) region and none in the US East (Virginia) region.

C. One in the US West (Oregon) region and none in the US East (Virginia) region.

D. Two in the US East (Virginia) region and none in the US West (Oregon) region.

**Answer:** A

#### Explanation:

Why? If you want to require HTTPS between viewers and CloudFront, you must change the IAM Region to US East (N. Virginia) in the IAM Certificate Manager console before you request or import a certificate. If you want to require HTTPS between CloudFront and your origin, and you're using an ELB load balancer as your origin, you can request or import a certificate in any Region.

<https://docs.IAM.amazon.com/AmazonCloudFront/latest/DeveloperGuide/cnames-and-https-requirements.html>

#### NEW QUESTION 71

- (Exam Topic 1)

An employee accidentally exposed an IAM access key and secret access key during a public presentation. The company Security Engineer immediately disabled



the key.

How can the Engineer assess the impact of the key exposure and ensure that the credentials were not misused? (Choose two.)

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

**Answer:** AD

**Explanation:**

[https://docs.IAM.amazon.com/IAM/latest/UserGuide/id\\_credentials\\_getting-report.html](https://docs.IAM.amazon.com/IAM/latest/UserGuide/id_credentials_getting-report.html)

#### NEW QUESTION 74

- (Exam Topic 1)

A developer is creating an IAM Lambda function that requires environment variables to store connection information and logging settings. The developer is required to use an IAM KMS Customer Master Key (CMK) supplied by the information security department in order to adhere to company standards for securing Lambda environment variables.

Which of the following are required for this configuration to work? (Select TWO.)

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

**Answer:** BC

#### NEW QUESTION 79

- (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 CloudHSM
- 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 83

- (Exam Topic 1)

An application developer is using an IAM Lambda function that must use IAM KMS to perform encrypt and decrypt operations for API keys that are less than 2 KB Which key policy would allow the application to do this while granting least privilege?

- A. 

```
{
  "Sid": "AllowUseOfTheKey",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::444455556666:role/EncryptionApp"},
  "Action": [
    "kms:*"
  ],
  "Resource": "*"
}
```
- B. 

```
{
  "Sid": "AllowUseOfTheKey",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::444455556666:role/EncryptionApp"},
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt"
  ],
  "Resource": "*"
}
```
- C. 

```
{
  "Sid": "AllowUseOfTheKey",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::444455556666:role/EncryptionApp"},
  "Action": [
    "kms:DescribeKey",
    "kms:GenerateDataKey*",
    "kms:Encrypt",
    "kms:ReEncrypt*",
    "kms:Decrypt"
  ],
  "Resource": "*"
}
```

D. 

```
{
  "Sid": "AllowUseOfTheKey",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::444455556666:role/EncryptionApp"},
  "Action": [
    "kms:DescribeKey",
    "kms:GenerateDataKey*",
    "kms:Encrypt",
    "kms:ReEncrypt*",
    "kms:Disable*",
    "kms:Decrypt"
  ]
}
```

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

**Answer: C**

#### NEW QUESTION 88

- (Exam Topic 2)

Your IT Security department has mandated that all data on EBS volumes created for underlying EC2 Instances need to be encrypted. Which of the following can help achieve this?

Please select:

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

**Answer: A**

#### Explanation:

The IAM Documentation mentions the following on IAM KMS

IAM Key Management Service (IAM KMS) is a managed service that makes it easy for you to create and control the encryption keys used to encrypt your data.

IAM KMS is integrated with other IAM services including Amazon Elastic Block Store (Amazon EBS), Amazon Simple Storage Service (Amazon S3), Amazon Redshift Amazon Elastic Transcoder, Amazon WorkMail, Amazon Relational Database Service (Amazon RDS), and others to make it simple to encrypt your data with encryption keys that you manage

Option B is incorrect - The IAM Certificate manager can be used to generate SSL certificates that can be used to encrypt traffic transit, but not at rest

Option C is incorrect is again used for issuing tokens when using API gateway for traffic in transit. Option D is used for secure access to EC2 Instances

For more information on IAM KMS, please visit the following URL: <https://docs.IAM.amazon.com/kms/latest/developereuide/overview.html> The correct answer is:

IAM KMS API

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 92

- (Exam Topic 2)

The Security Engineer created a new IAM Key Management Service (IAM KMS) key with the following key policy:

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

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

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

**Answer: AC**

#### Explanation:

Giving the IAM account full access to the CMK does this; it enables you to use IAM policies to give IAM users and roles in the account access to the CMK. It does not by itself give any IAM users or roles access to the CMK, but it enables you to use IAM policies to do so.

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

#### NEW QUESTION 97

- (Exam Topic 2)

Your company has an EC2 Instance that is hosted in an IAM VPC. There is a requirement to ensure that logs files from the EC2 Instance are stored accordingly.

The access should also be limited for the destination of the log files. How can this be accomplished? Choose 2 answers from the options given below. Each answer forms part of the solution

Please select:

- A. Stream the log files to a separate Cloudtrail trail
- B. Stream the log files to a separate Cloudwatch Log group
- C. Create an IAM policy that gives the desired level of access to the Cloudtrail trail

D. Create an IAM policy that gives the desired level of access to the Cloudwatch Log group

**Answer:** BD

**Explanation:**

You can create a Log group and send all logs from the EC2 Instance to that group. You can then limit the access to the Log groups via an IAM policy.

Option A is invalid because Cloudtrail is used to record API activity and not for storing log files Option C is invalid because Cloudtrail is the wrong service to be used for this requirement

For more information on Log Groups and Log Streams, please visit the following URL:

\* <https://docs.IAM.amazon.com/AmazonCloudWatch/latest/logs/Working>

For more information on Access to Cloudwatch logs, please visit the following URL:

\* <https://docs.IAM.amazon.com/AmazonCloudWatch/latest/logs/auth-and-access-control-cwl.html>

The correct answers are: Stream the log files to a separate Cloudwatch Log group. Create an IAM policy that gives the desired level of access to the Cloudwatch Log group

Submit your Feedback/Queries to our Experts

**NEW QUESTION 98**

- (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 function
- 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 classification
- 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 classification
- 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 classification
- H. For identified objects that contain PII, query the S3 bucket logs by using Athena for GET operations.

**Answer:** B

**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 103**

- (Exam Topic 2)

A company has Windows Amazon EC2 instances in a VPC that are joined to on-premises Active Directory servers for domain services. The security team has enabled Amazon GuardDuty on the IAM account to alert on issues with the instances.

During a weekly audit of network traffic, the Security Engineer notices that one of the EC2 instances is attempting to communicate with a known command-and-control server but failing. This alert does not show up in GuardDuty.

Why did GuardDuty fail to alert to this behavior?

- A. GuardDuty did not have the appropriate alerts activated.
- B. GuardDuty does not see these DNS requests.
- C. GuardDuty only monitors active network traffic flow for command-and-control activity.
- D. GuardDuty does not report on command-and-control activity.

**Answer:** B

**Explanation:**

[https://docs.IAM.amazon.com/guardduty/latest/ug/guardduty\\_data-sources.html](https://docs.IAM.amazon.com/guardduty/latest/ug/guardduty_data-sources.html) [https://docs.IAM.amazon.com/guardduty/latest/ug/guardduty\\_backdoor.html](https://docs.IAM.amazon.com/guardduty/latest/ug/guardduty_backdoor.html)

**NEW QUESTION 107**

- (Exam Topic 2)

An organization operates a web application that serves users globally. The application runs on Amazon EC2 instances behind an Application Load Balancer. There is an Amazon CloudFront distribution in front of the load balancer, and the organization uses IAM WAF. The application is currently experiencing a volumetric attack whereby the attacker is exploiting a bug in a popular mobile game.

The application is being flooded with HTTP requests from all over the world with the User-Agent set to the following string: Mozilla/5.0 (compatible; ExampleCorp; ExampleGame/1.22; Mobile/1.0)

What mitigation can be applied to block attacks resulting from this bug while continuing to service legitimate requests?

- A. Create a rule in IAM WAF rules with conditions that block requests based on the presence of ExampleGame/1.22 in the User-Agent header
- B. Create a geographic restriction on the CloudFront distribution to prevent access to the application from most geographic regions
- C. Create a rate-based rule in IAM WAF to limit the total number of requests that the web application services.
- D. Create an IP-based blacklist in IAM WAF to block the IP addresses that are originating from requests that contain ExampleGame/1.22 in the User-Agent header.

**Answer:** A

**Explanation:**

Since all the attack has http header- User-Agent set to string: Mozilla/5.0 (compatible; ExampleCorp;) it would be much more easier to block these attack by simply denying traffic with the header match . HTH ExampleGame/1.22; Mobile/1.0)

**NEW QUESTION 109**

- (Exam Topic 2)

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

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

**Answer:** C

**Explanation:**

Option A and B are invalid because by default the Security Groups already block traffic. You can use NACL's as an additional security layer for the subnet to deny traffic.

Option D is invalid since just changing the Inbound Rules is sufficient The IAM Documentation mentions the following

A network access control list (ACL) is an optional layer of security for your VPC that acts as a firewall for

controlling traffic in and out of one or more subnets. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC.

The correct answer is: Change the Inbound NACL to deny access from the suspecting IP

**NEW QUESTION 110**

- (Exam Topic 2)

An IAM user with full EC2 permissions could not start an Amazon EC2 instance after it was stopped for a maintenance task. Upon starting the instance, the instance state would change to "Pending", but after a few seconds, it would switch back to "Stopped".

An inspection revealed that the instance has attached Amazon EBS volumes that were encrypted by using a Customer Master Key (CMK). When these encrypted volumes were detached, the IAM user was able to start the EC2 instances.

The IAM user policy is as follows:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        <Action>
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:012345678910:key/ebs-encryption-key"
      ]
    }
  ]
}
```

What additional items need to be added to the IAM user policy? (Choose two.)

- A. kms:GenerateDataKey
- B. kms:Decrypt
- C. kms:CreateGrant
- D. "Condition": {"Bool": {"kms:ViaService": "ec2.us-west-2.amazonaws.com"}}
- E. "Condition": {"Bool": {"kms:GrantIsForIAMResource": true}}

**Answer:** CE

**Explanation:**

The EBS which is IAM resource service is encrypted with CMK and to allow EC2 to decrypt , the IAM user should create a grant ( action) and a boolean condition for the IAM resource . This link explains how IAM keys works. <https://docs.IAM.amazon.com/kms/latest/developerguide/key-policies.html>

**NEW QUESTION 113**



- (Exam Topic 2)

What is the function of the following IAM Key Management Service (KMS) key policy attached to a customer master key (CMK)?

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:user/ExampleUser"
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:GenerateDataKey*",
    "kms:CreateGrant",
    "kms:ListGrants"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:ViaService": [
        "workmail.us-west-2.amazonaws.com",
        "ses.us-west-2.amazonaws.com"
      ]
    }
  }
}
```

- A. The Amazon WorkMail and Amazon SES services have delegated KMS encrypt and decrypt permissions to the ExampleUser principal in the 111122223333 account.
- B. The ExampleUser principal can transparently encrypt and decrypt email exchanges specifically between ExampleUser and IAM.
- C. The CMK is to be used for encrypting and decrypting only when the principal is ExampleUser and the request comes from WorkMail or SES in the specified region.
- D. The key policy allows WorkMail or SES to encrypt or decrypt on behalf of the user for any CMK in the account.

**Answer:** C

#### NEW QUESTION 114

- (Exam Topic 2)

A Security Engineer has been asked to create an automated process to disable IAM user access keys that are more than three months old. Which of the following options should the Security Engineer use?

- A. In the IAM Console, choose the IAM service and select "Users". Review the "Access Key Age" column.
- B. Define an IAM policy that denies access if the key age is more than three months and apply to all users.
- C. Write a script that uses the GenerateCredentialReport, GetCredentialReport, and UpdateAccessKey APIs.
- D. Create an Amazon CloudWatch alarm to detect aged access keys and use an IAM Lambda function to disable the keys older than 90 days.

**Answer:** C

#### Explanation:

[https://docs.IAM.amazon.com/IAM/latest/APIReference/API\\_UpdateAccessKey.html](https://docs.IAM.amazon.com/IAM/latest/APIReference/API_UpdateAccessKey.html)

[https://docs.IAM.amazon.com/IAM/latest/APIReference/API\\_GenerateCredentialReport.html](https://docs.IAM.amazon.com/IAM/latest/APIReference/API_GenerateCredentialReport.html)

[https://docs.IAM.amazon.com/IAM/latest/APIReference/API\\_GetCredentialReport.html](https://docs.IAM.amazon.com/IAM/latest/APIReference/API_GetCredentialReport.html)

#### NEW QUESTION 117

- (Exam Topic 2)

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

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

**Answer:** ACF

#### Explanation:

Using IAM to grant access to a Third-Party Account 1) Create a role to provide access to the require resources 1.1) Create a role policy that specifies the IAM Account ID to be accessed, "sts:AssumeRole" as action, and "sts:ExternalID" as condition 1.2) Create a role using the role policy just created 1.3) Assign a resource policy to the role. This will provide permission to access resource ARNs to the auditor 2) Repeat steps 1 and 2 on all IAM accounts 3) The auditor connects to the IAM account IAM Security Token Service (STS). The auditor must provide its ExternalID from step 1.2, the ARN of the role he is trying to assume from step 1.3, sts:ExternalID 4) STS provide the auditor with temporary credentials that provides the role access from step 1

[https://docs.IAM.amazon.com/IAM/latest/UserGuide/id\\_roles\\_create\\_for-user\\_externalid.html](https://docs.IAM.amazon.com/IAM/latest/UserGuide/id_roles_create_for-user_externalid.html)

<https://IAM.amazon.com/blogs/security/how-to-audit-cross-account-roles-using-IAM-cloudtrail-and-amazon-clo>

#### NEW QUESTION 122

- (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 125

- (Exam Topic 2)

An application has been written that publishes custom metrics to Amazon CloudWatch. Recently, IAM changes have been made on the account and the metrics are no longer being reported.

Which of the following is the LEAST permissive solution that will allow the metrics to be delivered?

- A. Add a statement to the IAM policy used by the application to allow logs:putLogEvents and logs:createLogStream
- B. Modify the IAM role used by the application by adding the CloudWatchFullAccess managed policy.
- C. Add a statement to the IAM policy used by the application to allow cloudwatch:putMetricData.
- D. Add a trust relationship to the IAM role used by the application for cloudwatch.amazonaws.com.

**Answer: C**

#### Explanation:

<https://docs.IAM.amazonaws.com/AmazonCloudWatch/latest/monitoring/permissions-reference-cw.html>

#### NEW QUESTION 127

- (Exam Topic 2)

A Security Engineer is building a Java application that is running on Amazon EC2. The application communicates with an Amazon RDS instance and authenticates with a user name and password.

Which combination of steps can the Engineer take to protect the credentials and minimize downtime when the credentials are rotated? (Choose two.)

- A. Have a Database Administrator encrypt the credentials and store the ciphertext in Amazon S3. Grant permission to the instance role associated with the EC2 instance to read the object and decrypt the ciphertext.
- B. Configure a scheduled job that updates the credential in IAM Systems Manager Parameter Store and notifies the Engineer that the application needs to be restarted.
- C. Configure automatic rotation of credentials in IAM Secrets Manager.
- D. Store the credential in an encrypted string parameter in IAM Systems Manager Parameter Store
- E. Grant permission to the instance role associated with the EC2 instance to access the parameter and the IAM KMS key that is used to encrypt it.
- F. Configure the Java application to catch a connection failure and make a call to IAM Secrets Manager to retrieve updated credentials when the password is rotate
- G. Grant permission to the instance role associated with the EC2 instance to access Secrets Manager.

**Answer: CE**

#### NEW QUESTION 129

- (Exam Topic 2)

A company uses IAM Organization to manage 50 IAM accounts. The finance staff members log in as IAM IAM users in the FinanceDept IAM account. The staff members need to read the consolidated billing information in the MasterPayer IAM account. They should not be able to view any other resources in the MasterPayer IAM account. IAM access to billing has been enabled in the MasterPayer account.

Which of the following approaches grants the finance staff the permissions they require without granting any unnecessary permissions?

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

**Answer: D**

#### Explanation:

IAM Region that You Request a Certificate In (for IAM Certificate Manager) If you want to require HTTPS between viewers and CloudFront, you must change the IAM region to US East (N. Virginia) in the IAM Certificate Manager console before you request or import a certificate. If you want to require HTTPS between CloudFront and your origin, and you're using an ELB load balancer as your origin, you can request or import a certificate in any region.

<https://docs.IAM.amazonaws.com/AmazonCloudFront/latest/DeveloperGuide/cnames-and-https-requirements.html>

#### NEW QUESTION 132

- (Exam Topic 2)

An IAM account includes two S3 buckets: bucket1 and bucket2. The bucket2 does not have a policy defined, but bucket1 has the following bucket policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": { "AWS": "arn:aws:iam: : 123456789012: user/alice" },
      "Action": "s3:*",
      "Resource": [ "arn:aws:s3: : :bucket1", "arn:aws:s3: : :bucket1/*" ]
    }
  ]
}
```

In addition, the same account has an IAM User named “alice”, with the following IAM policy.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "s3:*",
    "Resource": [ "arn:aws:s3: : :bucket2", "arn:aws:s3: : :bucket2/*" ]
  }]
}
```

Which buckets can user “alice” access?

- A. Bucket1 only
- B. Bucket2 only
- C. Both bucket1 and bucket2
- D. Neither bucket1 nor bucket2

**Answer:** C

**Explanation:**

Both S3 policies and IAM policies can be used to grant access to buckets. IAM policies specify what actions are allowed or denied on what IAM resources (e.g. allow ec2:TerminateInstance on the EC2 instance with instance\_id=i-8b3620ec). You attach IAM policies to IAM users, groups, or roles, which are then subject to the permissions you’ve defined. In other words, IAM policies define what a principal can do in your IAM environment. S3 bucket policies, on the other hand, are attached only to S3 buckets. S3 bucket policies specify what actions are allowed or denied for which principals on the bucket that the bucket policy is attached to (e.g. allow user Alice to PUT but not DELETE objects in the bucket).

<https://IAM.amazon.com/blogs/security/iam-policies-and-bucket-policies-and-acls-oh-my-controlling-access-to>

**NEW QUESTION 136**

- (Exam Topic 2)

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

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

**Answer:** AC

**Explanation:**

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

**NEW QUESTION 139**

- (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 log 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/userguide/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 140**

- (Exam Topic 2)

An organization wants to be alerted when an unauthorized Amazon EC2 instance in its VPC performs a network port scan against other instances in the VPC.

When the Security team performs its own internal tests in a separate account by using pre-approved third-party scanners from the IAM Marketplace, the Security team also then receives multiple Amazon GuardDuty events from Amazon CloudWatch alerting on its test activities.

How can the Security team suppress alerts about authorized security tests while still receiving alerts about the unauthorized activity?

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 144**

- (Exam Topic 2)

You have an Ec2 Instance in a private subnet which needs to access the KMS service. Which of the following methods can help fulfil this requirement, keeping security in perspective

Please select:

- A. Use a VPC endpoint
- B. Attach an Internet gateway to the subnet
- C. Attach a VPN connection to the VPC
- D. Use VPC Peering

**Answer: A**

**Explanation:**

The IAM Documentation mentions the following

You can connect directly to IAM KMS through a private endpoint in your VPC instead of connecting over the internet. When you use a VPC endpoint communication between your VPC and IAM KMS is conducted entirely within the IAM network.

Option B is invalid because this could open threats from the internet

Option C is invalid because this is normally used for communication between on-premise environments and IAM.

Option D is invalid because this is normally used for communication between VPCs

For more information on accessing KMS via an endpoint, please visit the following URL <https://docs.IAM.amazon.com/kms/latest/developerguide/kms-vpc-endpoint.html>

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

**NEW QUESTION 147**

- (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 149**

- (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 policies
- F. Remove all scripts and clear the logs after execution.

**Answer:** B

#### NEW QUESTION 154

- (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 155

- (Exam Topic 2)

A security alert has been raised for an Amazon EC2 instance in a customer account that is exhibiting strange behavior. The Security Engineer must first isolate the EC2 instance and then use tools for further investigation.

What should the Security Engineer use to isolate and research this event? (Choose three.)

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

**Answer:** ADF

#### Explanation:

[https://github.com/IAMlabs/aws-well-architected-labs/blob/master/Security/300\\_Incident\\_Response\\_with\\_IAM](https://github.com/IAMlabs/aws-well-architected-labs/blob/master/Security/300_Incident_Response_with_IAM)

#### NEW QUESTION 156

- (Exam Topic 2)

An IAM Lambda function was misused to alter data, and a Security Engineer must identify who invoked the function and what output was produced. The Engineer cannot find any logs created by the Lambda function in Amazon CloudWatch Logs.

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

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

**Answer:** A

#### NEW QUESTION 157

- (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 160

- (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 162

- (Exam Topic 2)

A Development team has asked for help configuring the IAM roles and policies in a new IAM account. The team using the account expects to have hundreds of master keys and therefore does not want to manage access control for customer master keys (CMKs).

Which of the following will allow the team to manage IAM KMS permissions in IAM without the complexity of editing individual key policies?

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 167

- (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:

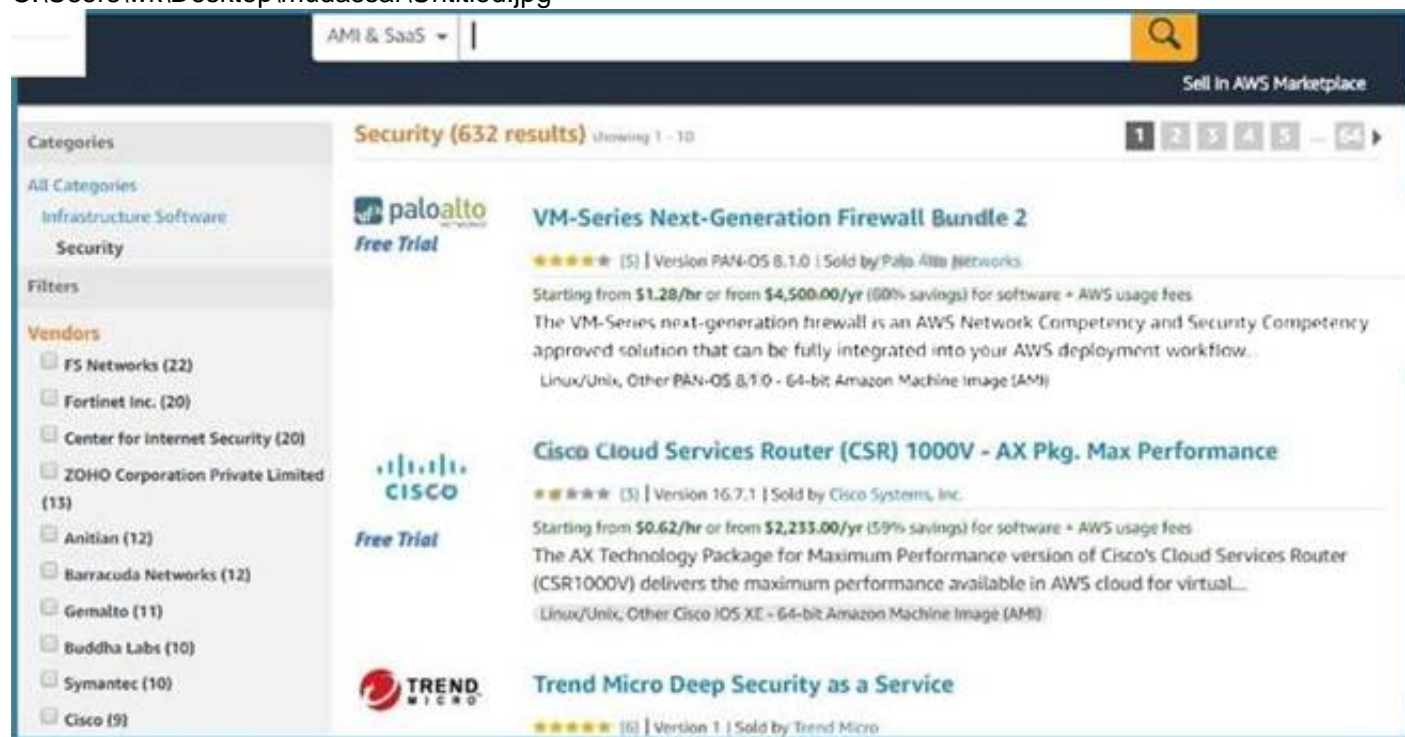
- A. Use IAM WAF to catch all intrusions occurring on the systems in the VPC
- B. Use a custom solution available in the IAM Marketplace
- C. Use VPC Flow logs to detect the issues and flag them accordingly.
- D. Use IAM Cloudwatch to monitor all traffic

**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 168

- (Exam Topic 2)

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

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

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

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

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

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

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

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

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

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

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

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

**Answer:** A

#### NEW QUESTION 173

- (Exam Topic 2)

A Security Administrator is configuring an Amazon S3 bucket and must meet the following security requirements:

- > Encryption in transit
- > Encryption at rest
- > Logging of all object retrievals in IAM CloudTrail

Which of the following meet these security requirements? (Choose three.)

- A. Specify "IAM:SecureTransport": "true" within a condition in the S3 bucket policy.
- B. Enable a security group for the S3 bucket that allows port 443, but not port 80.
- C. Set up default encryption for the S3 bucket.
- D. Enable Amazon CloudWatch Logs for the IAM account.
- E. Enable API logging of data events for all S3 objects.
- F. Enable S3 object versioning for the S3 bucket.

**Answer:** ACE

#### NEW QUESTION 175

- (Exam Topic 2)

The Security Engineer is managing a web application that processes highly sensitive personal information. The application runs on Amazon EC2. The application has strict compliance requirements, which instruct that all incoming traffic to the application is protected from common web exploits and that all outgoing traffic from the EC2 instances is restricted to specific whitelisted URLs.

Which architecture should the Security Engineer use to meet these requirements?

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

**Answer:** D

#### Explanation:

IAM Shield is mainly for DDos Attacks. IAM WAF is mainly for some other types of attacks like Injection and XSS etc. In this scenario, It seems it is WAF functionality that is needed. VPC logs do show the source and destination IP and Port, they never show any URL .. because URL are level 7 while VPC are concerned about lower network levels.

<https://docs.IAM.amazon.com/vpc/latest/userguide/flow-logs.html>

#### NEW QUESTION 177

- (Exam Topic 2)

A Security Engineer discovers that developers have been adding rules to security groups that allow SSH and RDP traffic from 0.0.0.0/0 instead of the organization firewall IP.

What is the most efficient way to remediate the risk of this activity?

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

**Answer:** D

#### NEW QUESTION 181

- (Exam Topic 2)



An organization receives an alert that indicates that an EC2 instance behind an ELB Classic Load Balancer has been compromised. What techniques will limit lateral movement and allow evidence gathering?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 186**

- (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 188**

- (Exam Topic 2)

A company requires that IP packet data be inspected for invalid or malicious content. Which of the following approaches achieve this requirement? (Choose two.)

- A. Configure a proxy solution on Amazon EC2 and route all outbound VPC traffic through i
- B. Perform inspection within proxy software on the EC2 instance.
- C. Configure the host-based agent on each EC2 instance within the VP
- D. Perform inspection within the host-based agent.
- E. Enable VPC Flow Logs for all subnets in the VP
- F. Perform inspection from the Flow Log data within Amazon CloudWatch Logs.
- G. Configure Elastic Load Balancing (ELB) access log
- H. Perform inspection from the log data within the ELB access log files.
- I. Configure the CloudWatch Logs agent on each EC2 instance within the VP
- J. Perform inspection from the log data within CloudWatch Logs.

**Answer:** AB

**Explanation:**

"EC2 Instance IDS/IPS solutions offer key features to help protect your EC2 instances. This includes alerting administrators of malicious activity and policy violations, as well as identifying and taking action against attacks. You can use IAM services and third party IDS/IPS solutions offered in IAM Marketplace to stay one step ahead of potential attackers."

**NEW QUESTION 190**

- (Exam Topic 2)

The IAM Systems Manager Parameter Store is being used to store database passwords used by an IAM Lambda function. Because this is sensitive data, the parameters are stored as type SecureString and protected by an IAM KMS key that allows access through IAM. When the function executes, this parameter cannot be retrieved as the result of an access denied error.

Which of the following actions will resolve the access denied error?

- A. Update the ssm.amazonaws.com principal in the KMS key policy to allow kms: Decrypt.
- B. Update the Lambda configuration to launch the function in a VPC.
- C. Add a policy to the role that the Lambda function uses, allowing kms: Decrypt for the KMS key.
- D. Add lambda.amazonaws.com as a trusted entity on the IAM role that the Lambda function uses.

**Answer:** C

**Explanation:**

[https://docs.amazonaws.cn/en\\_us/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Integrating.Authorizin](https://docs.amazonaws.cn/en_us/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Integrating.Authorizin)

**NEW QUESTION 193**

- (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 196**

- (Exam Topic 2)

A company will store sensitive documents in three Amazon S3 buckets based on a data classification scheme of "Sensitive," "Confidential," and "Restricted." The security solution must meet all of the following requirements:

- Each object must be encrypted using a unique key.
- Items that are stored in the "Restricted" bucket require two-factor authentication for decryption.
- IAM KMS must automatically rotate encryption keys annually.

Which of the following meets these requirements?

- A. Create a Customer Master Key (CMK) for each data classification type, and enable the rotation of it annually
- B. For the "Restricted" CMK, define the MFA policy within the key policy
- C. Use S3 SSE-KMS to encrypt the objects.
- D. Create a CMK grant for each data classification type with EnableKeyRotation and MultiFactorAuthPresent set to true
- E. S3 can then use the grants to encrypt each object with a unique CMK.
- F. Create a CMK for each data classification type, and within the CMK policy, enable rotation of it annually, and define the MFA policy
- G. S3 can then create DEK grants to uniquely encrypt each object within the S3 bucket.
- H. Create a CMK with unique imported key material for each data classification type, and rotate them annually
- I. For the "Restricted" key material, define the MFA policy in the key policy
- J. Use S3 SSE-KMS to encrypt the objects.

**Answer:** A

**Explanation:**

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

**NEW QUESTION 198**

- (Exam Topic 3)

A company is planning to run a number of Admin related scripts using the IAM Lambda service. There is a need to understand if there are any errors encountered when the script runs. How can this be accomplished in the most effective manner. Please select:

- A. Use Cloudwatch metrics and logs to watch for errors
- B. Use Cloudtrail to monitor for errors
- C. Use the IAM Config service to monitor for errors
- D. Use the IAM inspector service to monitor for errors

**Answer:** A

**Explanation:**

The IAM Documentation mentions the following

IAM Lambda automatically monitors Lambda functions on your behalf, reporting metrics through Amazon CloudWatch. To help you troubleshoot failures in a function, Lambda logs all requests handled by your function and also automatically stores logs generated by your code through Amazon CloudWatch Logs.

Option B, C and D are all invalid because these services cannot be used to monitor for errors. For more information on Monitoring Lambda functions, please visit the following URL: <https://docs.aws.amazon.com/lambda/latest/dg/monitoring-functions.html>

The correct answer is: Use Cloudwatch metrics and logs to watch for errors Submit your Feedback/Queries to our Experts

**NEW QUESTION 199**

- (Exam Topic 3)

Your company has a set of EC2 Instances defined in IAM. They need to ensure that all traffic packets are monitored and inspected for any security threats. How can this be achieved? Choose 2 answers from the options given below

Please select:

- A. Use a host based intrusion detection system
- B. Use a third party firewall installed on a central EC2 instance

- C. Use VPC Flow logs
- D. Use Network Access control lists logging

**Answer:** AB

**Explanation:**

If you want to inspect the packets themselves, then you need to use custom based software A diagram representation of this is given in the IAM Security best practices

Option C is invalid because VPC Flow logs cannot conduct packet inspection. For more information on IAM Security best practices, please refer to below URL:  
 The correct answers are: Use a host based intrusion detection system. Use a third party firewall installed on a central EC2

Submit your Feedback/Queries to our Experts

**NEW QUESTION 203**

- (Exam Topic 3)

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

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

**Answer:** AD

**Explanation:**

The IAM Document mention the following which supports the requirement Option B is invalid because VPC peering is only used for connection between VPCs and cannot be used to connect On-premise infrastructure to the IAM Cloud.

Option C is invalid because NAT gateways is used to connect instances in a private subnet to the internet For more information on VPN Connections, please visit the following url

<https://docs.IAM.amazon.com/AmazonVPC/latest/UserGuideA/pn-connections.html>

The correct answers are: IAM VPN, IAM Direct Connect Submit your Feedback/Queries to our Experts

**NEW QUESTION 206**

- (Exam Topic 3)

There is a set of Ec2 Instances in a private subnet. The application hosted on these EC2 Instances need to access a DynamoDB table. It needs to be ensured that traffic does not flow out to the internet. How can this be achieved?

Please select:

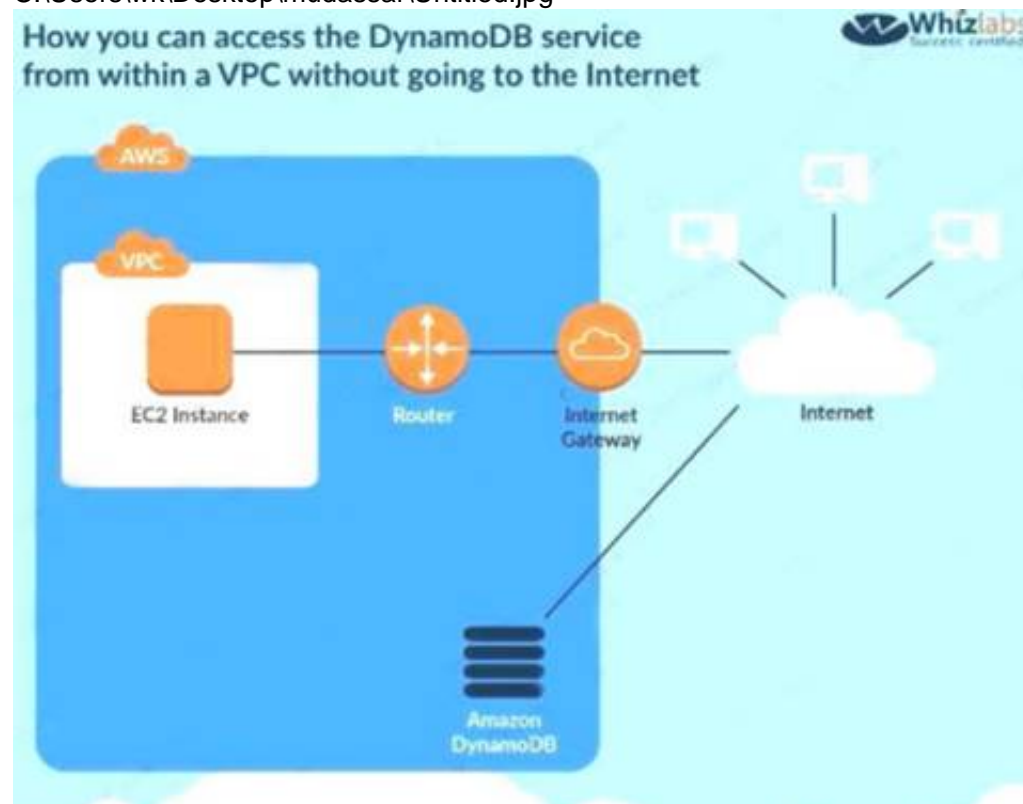
- A. Use a VPC endpoint to the DynamoDB table
- B. Use a VPN connection from the VPC
- C. Use a VPC gateway from the VPC
- D. Use a VPC Peering connection to the DynamoDB table

**Answer:** A

**Explanation:**

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

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



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

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

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

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

**NEW QUESTION 208**

- (Exam Topic 3)

You need to have a requirement to store objects in an S3 bucket with a key that is automatically managed and rotated. Which of the following can be used for this purpose?

Please select:

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

**Answer: B**

**Explanation:**

The IAM Documentation mentions the following

Server-side encryption protects data at rest. Server-side encryption with Amazon S3-managed encryption keys (SSE-S3) uses strong multi-factor encryption. Amazon S3 encrypts each object with a unique key. As an additional safeguard, it encrypts the key itself with a master key that it rotates regularly. Amazon S3 server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt your data.

All other options are invalid since here you need to ensure the keys are manually rotated since you manage the entire key set Using IAM S3 Server side encryption, IAM will manage the rotation of keys automatically.

For more information on Server side encryption, please visit the following URL:

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

The correct answer is: IAM S3 Server side encryption Submit your Feedback/Queries to our Experts

**NEW QUESTION 212**

- (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 217**

- (Exam Topic 3)

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

Please select:

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

**Answer: B**

**Explanation:**

The IAM Documentation mentions the following

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

Option A is invalid because its the cluster that needs to be encrypted

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

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

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

**NEW QUESTION 219**

- (Exam Topic 3)

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

Please select:

- A. The master keys encrypts the cluster ke
- B. The cluster key encrypts the database ke
- C. The database key encrypts the data encryption keys.
- D. The master keys encrypts the database ke
- E. The database key encrypts the data encryption keys.



- F. The master keys encrypts the data encryption key
- G. The data encryption keys encrypts the database key
- H. The master keys encrypts the cluster key, database key and data encryption keys

**Answer:** A

**Explanation:**

This is mentioned in the IAM Documentation

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

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

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

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

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

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

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

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

**NEW QUESTION 223**

- (Exam Topic 3)

Your company has a set of 1000 EC2 Instances defined in an IAM Account. They want to effectively automate several administrative tasks on these instances.

Which of the following would be an effective way to achieve this?

Please select:

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

**Answer:** B

**Explanation:**

The IAM Documentation mentions the following

IAM Systems Manager Run Command lets you remotely and securely manage the configuration of your managed instances. A managed instance is any Amazon EC2 instance or on-premises machine in your hybrid environment that has been configured for Systems Manager. Run Command enables you to automate common administrative tasks and perform ad hoc configuration changes at scale. You can use Run Command from the IAM console, the IAM Command Line Interface, IAM Tools for Windows PowerShell, or the IAM SDKs. Run Command is offered at no additional cost.

Option A is invalid because this service is used to store parameter Option C is invalid because this service is used to scan vulnerabilities in an EC2 Instance.

Option D is invalid because this service is used to check for configuration changes For more information on executing remote commands, please visit the below U <https://docs.IAM.amazon.com/systems-manageer/latest/useruide/execute-remote-commands.html> (

The correct answer is: Use the IAM Systems Manager Run Command Submit your Feedback/Queries to our Experts

**NEW QUESTION 228**

- (Exam Topic 3)

A company has a set of EC2 instances hosted in IAM. These instances have EBS volumes for storing critical information. There is a business continuity requirement and in order to boost the agility of the business and to ensure data durability which of the following options are not required.

Please select:

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

**Answer:** CD

**Explanation:**

Data stored in Amazon EBS volumes is redundantly stored in multiple physical locations as part of normal operation of those services and at no additional charge. However, Amazon EBS replication is stored within the same availability zone, not across multiple zones; therefore, it is highly recommended that you conduct regular snapshots to Amazon S3 for long-term data durability.

You can use Amazon Data Lifecycle Manager (Amazon DLM) to automate the creation, retention, and deletion of snapshots taken to back up your Amazon EBS volumes.

With lifecycle management, you can be sure that snapshots are cleaned up regularly and keep costs under control.

EBS Lifecycle Policies

A lifecycle policy consists of these core settings:

- Resource type—The IAM resource managed by the policy, in this case, EBS volumes.
- Target tag—The tag that must be associated with an EBS volume for it to be managed by the policy.
- Schedule—Defines how often to create snapshots and the maximum number of snapshots to keep. Snapshot creation starts within an hour of the specified start time. If creating a new snapshot exceeds the maximum number of snapshots to keep for the volume, the oldest snapshot is deleted.

Option C is correct. Each Amazon EBS volume is automatically replicated within its Availability Zone to protect you from component failure, offering high availability and durability. But it does not have an explicit feature like that.

Option D is correct Encryption does not ensure data durability

For information on security for Compute Resources, please visit the below URL <https://d1.IAMstatic.com/whitepapers/Security/Security Compute Services Whitepaper.pdf>

The correct answers are: Use EBS volume replication. Use EBS volume encryption Submit your Feedback/Queries to our Experts

#### NEW QUESTION 229

- (Exam Topic 3)

An application running on EC2 instances in a VPC must call an external web service via TLS (port 443). The instances run in public subnets.

Which configurations below allow the application to function and minimize the exposure of the instances? Select 2 answers from the options given below  
Please select:

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

**Answer:** BD

#### Explanation:

Since here the traffic needs to flow outbound from the Instance to a web service on Port 443, the outbound rules on both the Network and Security Groups need to allow outbound traffic. The Incoming traffic should be allowed on ephemeral ports for the Operating System on the Instance to allow a connection to be established on any desired or available port.

Option A is invalid because this rule alone is not enough. You also need to ensure incoming traffic on ephemeral ports

Option C is invalid because need to ensure incoming traffic on ephemeral ports and not only port 443 Option E and F are invalid since here you are allowing additional ports on Security groups which are not required

For more information on VPC Security Groups, please visit the below URL:

[https://docs.IAM.amazon.com/AmazonVPC/latest/UserGuideA/PC\\_SecurityGroups.html](https://docs.IAM.amazon.com/AmazonVPC/latest/UserGuideA/PC_SecurityGroups.html)

The correct answers are: A network ACL with rules that allow outgoing traffic on port 443 and incoming traffic on ephemeral ports, A security group with a rule that allows outgoing traffic on port 443

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 233

- (Exam Topic 3)

Your company has a set of EC2 Instances that are placed behind an ELB. Some of the applications hosted on these instances communicate via a legacy protocol.

There is a security mandate that all traffic between the client and the EC2 Instances need to be secure. How would you accomplish this?

Please select:

- A. Use an Application Load balancer and terminate the SSL connection at the ELB
- B. Use a Classic Load balancer and terminate the SSL connection at the ELB
- C. Use an Application Load balancer and terminate the SSL connection at the EC2 Instances
- D. Use a Classic Load balancer and terminate the SSL connection at the EC2 Instances

**Answer:** D

#### Explanation:

Since there are applications which work on legacy protocols, you need to ensure that the ELB can be used at the network layer as well and hence you should choose the Classic ELB. Since the traffic needs to be secure till the EC2 Instances, the SSL termination should occur on the Ec2 Instances.

Option A and C are invalid because you need to use a Classic Load balancer since this is a legacy application. Option B is incorrect since encryption is required until the EC2 Instance

For more information on HTTPS listeners for classic load balancers, please refer to below URL

<https://docs.IAM.ama20n.com/elasticloadbalancing/latest/classic/elb-https-load-balancers.html>

The correct answer is: Use a Classic Load balancer and terminate the SSL connection at the EC2 Instances Submit your Feedback/Queries to our Experts

#### NEW QUESTION 236

- (Exam Topic 3)

Your company has just started using IAM and created an IAM account. They are aware of the potential issues when root access is enabled. How can they best safeguard the account when it comes to root access? Choose 2 answers fro the options given below

Please select:

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

**Answer:** BD

#### Explanation:

The IAM Documentation mentions the following

All IAM accounts have root user credentials (that is, the credentials of the account owner). These credentials allow full access to all resources in the account.

Because you cant restrict permissions for root user credentials, we recommend that you delete your root user access keys. Then create IAM Identity and Access Management (IAM) user credentials for everyday interaction with IAM.

Option A is incorrect since you cannot delete the root access account

Option C is partially correct but cannot be used as the ideal solution for safeguarding the account For more information on root access vs admin IAM users, please refer to below URL: <https://docs.IAM.amazon.com/eeneral/latest/er/root-vs-iam.html>

The correct answers are: Create an Admin IAM user with the necessary permissions. Delete the root access keys Submit your Feedback/Queries to our Experts

#### NEW QUESTION 239

- (Exam Topic 3)

Every application in a company's portfolio has a separate IAM account for development and production. The security team wants to prevent the root user and all IAM users in the production accounts from accessing a specific set of unneeded services. How can they control this functionality?

Please select:

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

**Answer:** A

**Explanation:**

As an administrator of the master account of an organization, you can restrict which IAM services and individual API actions the users and roles in each member account can access. This restriction even overrides the administrators of member accounts in the organization. When IAM Organizations blocks access to a service or API action for a member account a user or role in that account can't access any prohibited service or API action, even if an administrator of a member account explicitly grants such permissions in an IAM policy. Organization permissions overrule account permissions.

Option B is invalid because service policies cannot be assigned to the root account at the account level. Option C and D are invalid because IAM policies alone at the account level would not be able to suffice the requirement

For more information, please visit the below URL id=docs\_orgs\_console [https://docs.IAM.amazon.com/IAM/latest/UserGi manage attach-policy.html](https://docs.IAM.amazon.com/IAM/latest/UserGi%20manage%20attach-policy.html)

The correct answer is: Create a Service Control Policy that denies access to the services. Assemble all production accounts in an organizational unit. Apply the policy to that organizational unit

Submit your Feedback/Queries to our Experts

**NEW QUESTION 243**

- (Exam Topic 3)

Your organization is preparing for a security assessment of your use of IAM. In preparation for this assessment, which three IAM best practices should you consider implementing?

Please select:

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

**Answer:** ABC

**Explanation:**

When you go to the security dashboard, the security status will show the best practices for initiating the first level of security.

Option D is invalid because as per the dashboard, this is not part of the security recommendation For more information on best security practices please visit the URL:

<https://IAM.amazon.com/whitepapers/IAM-security-best-practices;>

The correct answers are: Create individual IAM users, Configure MFA on the root account and for privileged IAM users. Assign IAM users and groups configured with policies granting least privilege access

Submit your Feedback/Queries to our Experts

**NEW QUESTION 244**

- (Exam Topic 3)

Your company is planning on IAM on hosting its IAM resources. There is a company policy which mandates that all security keys are completely managed within the company itself. Which of the following is the correct measure of following this policy?

Please select:

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

**Answer:** B

**Explanation:**

y ensuring that you generate the key pairs for EC2 Instances, you will have complete control of the access keys.

Options A,C and D are invalid because all of these processes means that IAM has ownership of the keys. And the question specifically mentions that you need ownership of the keys

For information on security for Compute Resources, please visit the below URL: [https://d1.IAMstatic.com/whitepapers/Security/Security Compute Services Whitepaper.pdf](https://d1.IAMstatic.com/whitepapers/Security/Security%20Compute%20Services%20Whitepaper.pdf)

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

**NEW QUESTION 249**

- (Exam Topic 3)

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

Please select:

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



**Answer:** B

**Explanation:**

If you want to use CloudFront signed URLs or signed cookies to provide access to objects in your Amazon S3 bucket you probably also want to prevent users from accessing your Amazon S3 objects using Amazon S3 URLs. If users access your objects directly in Amazon S3, they bypass the controls provided by CloudFront signed URLs or signed cookies, for example, control over the date and time that a user can no longer access your content and control over which IP addresses can be used to access content. In addition, if user's access objects both through CloudFront and directly by using Amazon S3 URLs, CloudFront access logs are less useful because they're incomplete.

Option A is invalid because you need to create a Origin Access Identity for Cloudfront and not an IAM user

Option C and D are invalid because using policies will not help fulfil the requirement For more information on Origin Access Identity please see the below Link:

<http://docs.IAM.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3>

The correct answer is: Create an Origin Access Identity (OAI) for CloudFront and grant access to the objects in your S3 bucket to that OAI.

(

Submit your Feedback/Queries to our Experts

**NEW QUESTION 253**

- (Exam Topic 3)

A web application runs in a VPC on EC2 instances behind an ELB Application Load Balancer. The application stores data in an RDS MySQL DB instance. A Linux bastion host is used to apply schema updates to the database - administrators connect to the host via SSH from a corporate workstation. The following security groups are applied to the infrastructure

\* sgLB - associated with the ELB

\* sgWeb - associated with the EC2 instances.

\* sgDB - associated with the database

\* sgBastion - associated with the bastion host Which security group configuration will allow the application to be secure and functional?

Please select:

A. sgLB :allow port 80 and 443 traffic from 0.0.0.0/0 sgWeb :allow port 80 and 443 traffic from 0.0.0.0/0 sgDB :allow port 3306 traffic from sgWeb and

sgBastion sgBastion: allow port 22 traffic from the corporate IP address range

B. sgLB :allow port 80 and 443 traffic from 0.0.0.0/0 sgWeb :allow port 80 and 443 traffic from sgLB sgDB :allow port 3306 traffic from sgWeb and sgLBsgBastion: allow port 22 traffic from the VPC IP address range

C. sgLB :allow port 80 and 443 traffic from 0.0.0.0/0 sgWeb :allow port 80 and 443 traffic from sgLBsgDB :allow port 3306 traffic from sgWeb and sgBastion sgBastion: allow port 22 traffic from the VPC IP address range

D. sgLB :allow port 80 and 443 traffic from 0.0.0.0/0 sgWeb :allow port 80 and 443 traffic from sgLBsgDB :allow port 3306 traffic from sgWeb and sgBastion sgBastion: allow port 22 traffic from the corporate IP address range

**Answer:** D

**Explanation:**

The Load Balancer should accept traffic on port 80 and 443 traffic from 0.0.0.0/0 The backend EC2 Instances should accept traffic from the Load Balancer

The database should allow traffic from the Web server

And the Bastion host should only allow traffic from a specific corporate IP address range Option A is incorrect because the Web group should only allow traffic from the Load balancer For more information on IAM Security Groups, please refer to below URL: <https://docs.IAM.amazon.com/IAM/EC2/latest/UserGuide/using-network-security.html>

The correct answer is: sgLB :allow port 80 and 443 traffic from 0.0.0.0/0 sgWeb :allow port 80 and 443 traffic from sgLB

sgDB :allow port 3306 traffic from sgWeb and sgBastion sgBastion: allow port 22 traffic from the corporate IP address range Submit your Feedback/Queries to our Experts

**NEW QUESTION 256**

- (Exam Topic 3)

You have an EC2 instance with the following security configured:

\* a. ICMP inbound allowed on Security Group

\* b. ICMP outbound not configured on Security Group

\* c. ICMP inbound allowed on Network ACL

\* d. ICMP outbound denied on Network ACL

If Flow logs is enabled for the instance, which of the following flow records will be recorded? Choose 3 answers from the options given below

Please select:

A. An ACCEPT record for the request based on the Security Group

B. An ACCEPT record for the request based on the NACL

C. A REJECT record for the response based on the Security Group

D. A REJECT record for the response based on the NACL

**Answer:** ABD

**Explanation:**

This example is given in the IAM documentation as well

For example, you use the ping command from your home computer (IP address is 203.0.113.12) to your instance (the network interface's private IP address is 172.31.16.139). Your security group's inbound rules allow ICMP traffic and the outbound rules do not allow ICMP traffic however, because security groups are stateful, the response ping from your instance is allowed. Your network ACL permits inbound ICMP traffic but does not permit outbound ICMP traffic. Because network ACLs are stateless, the response ping is dropped and will not reach your home computer. In a flow log, this is displayed as 2 flow log records:

An ACCEPT record for the originating ping that was allowed by both the network ACL and the security group, and therefore was allowed to reach your instance.

A REJECT record for the response ping that the network ACL denied.

Option C is invalid because the REJECT record would not be present For more information on Flow Logs, please refer to the below URL:

<http://docs.IAM.amazon.com/AmazonVPC/latest/UserGuide/flow-logs.html>

The correct answers are: An ACCEPT record for the request based on the Security Group, An ACCEPT record for the request based on the NACL, A REJECT record for the response based on the NACL

Submit your Feedback/Queries to our Experts

**NEW QUESTION 261**

- (Exam Topic 3)



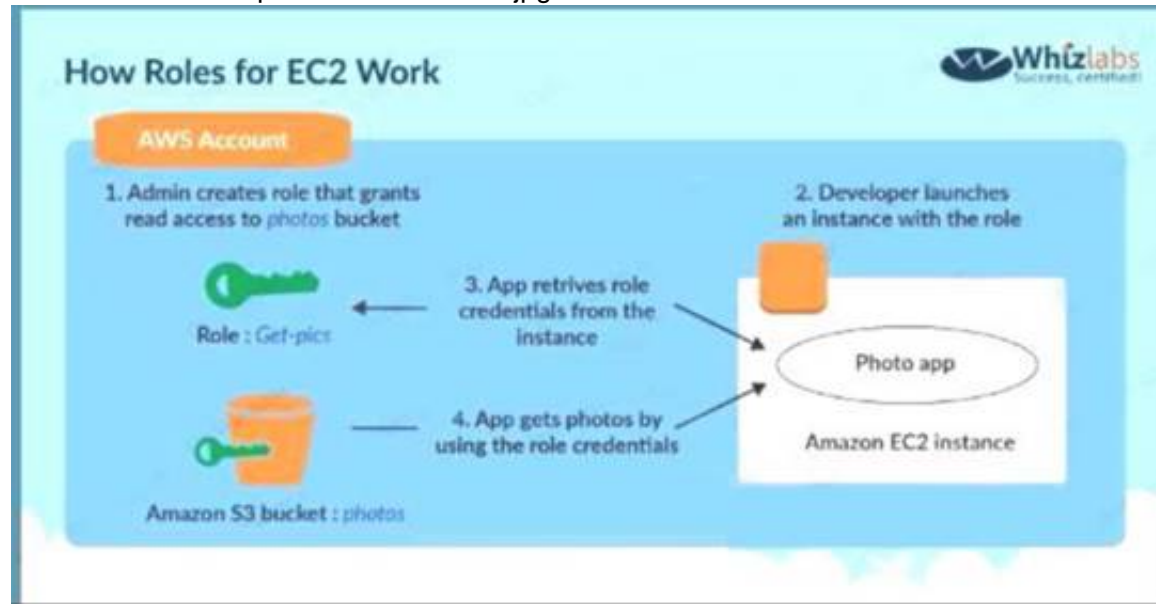
An application is designed to run on an EC2 Instance. The applications needs to work with an S3 bucket. From a security perspective , what is the ideal way for the EC2 instance/ application to be configured?  
 Please select:

- A. Use the IAM access keys ensuring that they are frequently rotated.
- B. Assign an IAM user to the application that has specific access to only that S3 bucket
- C. Assign an IAM Role and assign it to the EC2 Instance
- D. Assign an IAM group and assign it to the EC2 Instance

**Answer: C**

**Explanation:**

The below diagram from the IAM whitepaper shows the best security practice of allocating a role that has access to the S3 bucket  
 C:\Users\wk\Desktop\mudassar\Untitled.jpg



Options A,B and D are invalid because using users, groups or access keys is an invalid security practise when giving access to resources from other IAM resources.

For more information on the Security Best practices, please visit the following URL: <https://d1.IAMstatic.com/whitepapers/Security/IAM Security Best Practices.pdf>

The correct answer is: Assign an IAM Role and assign it to the EC2 Instance Submit your Feedback/Queries to our Experts

**NEW QUESTION 264**

- (Exam Topic 3)

Development teams in your organization use S3 buckets to store the log files for various applications hosted in development environments in IAM. The developers want to keep the logs for one month for troubleshooting purposes, and then purge the logs. What feature will enable this requirement?

Please select:

- A. Adding a bucket policy on the S3 bucket.
- B. Configuring lifecycle configuration rules on the S3 bucket.
- C. Creating an IAM policy for the S3 bucket.
- D. Enabling CORS on the S3 bucket.

**Answer: B**

**Explanation:**

The IAM Documentation mentions the following on lifecycle policies

Lifecycle configuration enables you to specify the lifecycle management of objects in a bucket. The configuration is a set of one or more rules, where each rule defines an action for Amazon S3 to apply to a group of objects. These actions can be classified as follows:

Transition actions - In which you define when objects transition to another . For example, you may choose to transition objects to the STANDARD\_IA (IA, for infrequent access) storage class 30 days after creation, or archive objects to the GLACIER storage class one year after creation.

Expiration actions - In which you specify when the objects expire. Then Amazon S3 deletes the expired objects on your behalf.

Option A and C are invalid because neither bucket policies neither IAM policy's can control the purging of logs Option D is invalid CORS is used for accessing objects across domains and not for purging of logs For more information on IAM S3 Lifecycle policies, please visit the following URL: [com/AmazonS3/latest/dg/](https://docs.aws.amazon.com/AmazonS3/latest/dg/bucket-lifecycle.html)

The correct answer is: Configuring lifecycle configuration rules on the S3 bucket. Submit your Feedback/Queries to our Experts

**NEW QUESTION 269**

- (Exam Topic 3)

Company policy requires that all insecure server protocols, such as FTP, Telnet, HTTP, etc be disabled on all servers. The security team would like to regularly check all servers to ensure compliance with this requirement by using a scheduled CloudWatch event to trigger a review of the current infrastructure. What process will check compliance of the company's EC2 instances?

Please select:

- A. Trigger an IAM Config Rules evaluation of the restricted-common-ports rule against every EC2 instance.
- B. Query the Trusted Advisor API for all best practice security checks and check for "action recommended" status.
- C. Enable a GuardDuty threat detection analysis targeting the port configuration on every EC2 instance.
- D. Run an Amazon Inspector assessment using the Runtime Behavior Analysis rules package against every EC2 instance.

**Answer: D**

**Explanation:**

Option B is incorrect because querying Trusted Advisor API's are not possible

Option C is incorrect because GuardDuty should be used to detect threats and not check the compliance of security protocols.

Option D states that Run Amazon Inspector using runtime behavior analysis rules which will analyze the behavior of your instances during an assessment run, and

provide guidance about how to make your EC2 instances more secure.

Insecure Server Protocols

This rule helps determine whether your EC2 instances allow support for insecure and unencrypted ports/services such as FTP, Telnet HTTP, IMAP, POP version 3, SMTP, SNMP versions 1 and 2, rsh, and rlogin.

For more information, please refer to below URL: [https://docs.IAM.amazon.eom/mspector/latest/userguide/inspector\\_runtime-behavior-analysis.html#insecure-pro](https://docs.IAM.amazon.eom/mspector/latest/userguide/inspector_runtime-behavior-analysis.html#insecure-pro)

The correct answer is: Run an Amazon Inspector assessment using the Runtime Behavior Analysis rules package against every EC2 instance.

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 272

- (Exam Topic 3)

The CFO of a company wants to allow one of his employees to view only the IAM usage report page. Which of the below mentioned IAM policy statements allows the user to have access to the IAM usage report page?

Please select:

- A. "Effect": "Allow", "Action": ["Describe"], "Resource": "Billing"
- B. "Effect": "Allow", "Action": ["AccountUsage"], "Resource": "\*\*"
- C. "Effect": "Allow", "Action": ["IAM-portal:ViewUsage", "IAM-portal:ViewBilling"], "Resource": "\*\*"
- D. "Effect": "Allow", "Action": ["IAM-portal: ViewBilling"], "Resource": "\*\*"

**Answer: C**

#### Explanation:

the IAM documentation, below is the access required for a user to access the Usage reports page and as per this, Option C is the right answer.

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



#### NEW QUESTION 277

- (Exam Topic 3)

A windows machine in one VPC needs to join the AD domain in another VPC. VPC Peering has been established. But the domain join is not working. What is the other step that needs to be followed to ensure that the AD domain join can work as intended

Please select:

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

**Answer: C**

#### Explanation:

In addition to VPC peering and setting the right route tables, the security groups for the AD EC2 instance needs to ensure the right rules are put in place for allowing incoming traffic.

Option A and B is invalid because changing the connection type will not help. This is a problem with the Security Groups.

Option D is invalid since the AD should not be placed in a public subnet

For more information on allowing ingress traffic for AD, please visit the following url

<https://docs.IAM.amazon.com/quickstart/latest/active-directory-ds/ingress.html>

The correct answer is: Ensure the security groups for the AD hosted subnet has the right rule for relevant subnets Submit your Feedback/Queries to our Experts

#### NEW QUESTION 281

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### SCS-C02 Practice Exam Features:

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

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The SCS-C02 Practice Test Here](#)**