

# Amazon-Web-Services

## Exam Questions SCS-C02

AWS Certified Security - Specialty



#### NEW QUESTION 1

- (Exam Topic 1)

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

- A. 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 2

- (Exam Topic 1)

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

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

**Answer:** A

#### NEW QUESTION 3

- (Exam Topic 1)

A company has a serverless application for internal users deployed on IAM. The application uses IAM Lambda for the front end and for business logic. The Lambda function accesses an Amazon RDS database inside a VPC. The company uses IAM Systems Manager Parameter Store for storing database credentials. A recent security review highlighted the following issues:

- > The Lambda function has internet access.
- > The relational database is publicly accessible.
- > The database credentials are not stored in an encrypted state.

Which combination of steps should the company take to resolve these security issues? (Select THREE)

- A. Disable public access to the RDS database inside the VPC.
- B. Move all the Lambda functions inside the VPC.
- C. Edit the IAM role used by Lambda to restrict internet access.
- D. Create a VPC endpoint for Systems Manager.
- E. Store the credentials as a string parameter.
- F. Change the parameter type to an advanced parameter.
- G. Edit the IAM role used by RDS to restrict internet access.
- H. Create a VPC endpoint for Systems Manager.
- I. Store the credentials as a SecureString parameter.

**Answer:** ABE

#### NEW QUESTION 4

- (Exam Topic 1)

Which of the following are valid configurations for using SSL certificates with Amazon CloudFront? (Select THREE)

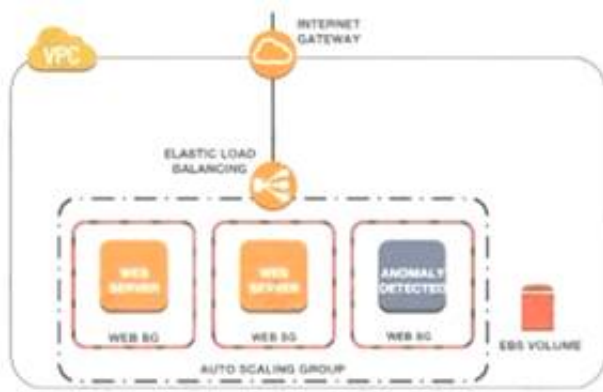
- A. Default IAM Certificate Manager certificate
- B. Custom SSL certificate stored in IAM KMS
- C. Default CloudFront certificate
- D. Custom SSL certificate stored in IAM Certificate Manager
- E. Default SSL certificate stored in IAM Secrets Manager
- F. Custom SSL certificate stored in IAM IAM

**Answer:** ACD

#### NEW QUESTION 5

- (Exam Topic 1)

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



- A. Remove the instance from the Auto Scaling group Place the instance within an isolation security group, detach the EBS volume launch an EC2 instance with a forensic toolkit and attach the E8S volume to investigate
- B. Remove the instance from the Auto Scaling group and the Elastic Load Balancer Place the instance within an isolation security group, launch an EC2 instance with a forensic toolkit, and allow the forensic toolkit image to connect to the suspicious Instance to perform the Investigation.
- C. Remove the instance from the Auto Scaling group Place the Instance within an isolation security group, launch an EC2 Instance with a forensic toolkit and use the forensic toolkit imago to deploy an ENI as a network span port to inspect all traffic coming from the suspicious instance.
- D. Remove the instance from the Auto Scaling group and the Elastic Load Balancer Place the instance within an isolation security group, make a copy of the EBS volume from a new snapshot, launch an EC2 Instance with a forensic toolkit and attach the copy of the EBS volume to investigate.

**Answer: B**

#### NEW QUESTION 6

- (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 7

- (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 8

- (Exam Topic 1)

A company's development team is designing an application using IAM Lambda and Amazon Elastic Container Service (Amazon ECS). The development team needs to create IAM roles to support these systems. The company's security team wants to allow the developers to build IAM roles directly, but the security team wants to retain control over the permissions the developers can delegate to those roles. The development team needs access to more permissions than those required for the application's IAM services. The solution must minimize management overhead.

How should the security team prevent privilege escalation for both teams?

- A. Enable IAM CloudTrail
- B. Create a Lambda function that monitors the event history for privilege escalation events and notifies the security team.
- C. Create a managed IAM policy for the permissions require
- D. Reference the IAM policy as a permissions boundary within the development team's IAM role.
- E. Enable IAM Organizations Create an SCP that allows the IAM CreateUser action but that has a condition that prevents API calls other than those required by the development team
- F. Create an IAM policy with a deny on the IAMCreateUser action and assign the policy to the development tea
- G. Use a ticket system to allow the developers to request new IAM roles for their application
- H. The IAM roles will then be created by the security team.

**Answer: A**

#### NEW QUESTION 9

- (Exam Topic 1)

A company has implemented centralized logging and monitoring of IAM CloudTrail logs from all Regions in an Amazon S3 bucket. The log Hies are encrypted

using IAM KMS. A Security Engineer is attempting to review the log files using a third-party tool hosted on an Amazon EC2 instance. The Security Engineer is unable to access the logs in the S3 bucket and receives an access denied error message. What should the Security Engineer do to fix this issue?

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

**Answer: C**

#### NEW QUESTION 10

- (Exam Topic 1)

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 days.
- 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.amazonaws.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.amazonaws.com/blogs/security/how-to-record-and-govern-your-iam-resource-configurations-using-IAM>

#### NEW QUESTION 10

- (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 all public S3 buckets without causing any outages on the existing websites. The engineer has set up an Amazon CloudFront distribution (one for each website).

Which set of steps should the security engineer implement next?

- A. Configure an S3 bucket as the origin and origin access identity (OAI) for the CloudFront distribution. Switch the DNS records from websites to point to the CloudFront distribution. Enable block 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 DNS records for the websites to point to the CloudFront distribution. Then, for 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 the 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 the account level.

**Answer: A**

#### NEW QUESTION 15

- (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 Service (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.amazonaws.com/systems-manager/latest/userguide/sysman-paramstore-access.html>

#### NEW QUESTION 20

- (Exam Topic 1)

A company wants to encrypt the private network between its on-premises environment and IAM. The company also wants a consistent network experience for its employees.

What should the company do to meet these requirements?

- A. Establish an IAM Direct Connect connection with IAM and set up a Direct Connect gateway.
- B. In the Direct Connect gateway configuration, enable IPsec and BGP, and then leverage native IAM network encryption between Availability Zones and Regions.
- C. Establish an IAM Direct Connect connection with IAM and set up a Direct Connect gateway.

- D. Using the Direct Connect gateway, create a private virtual interface and advertise the customer gateway private IP address
- E. Create a VPN connection using the customer gateway and the virtual private gateway
- F. Establish a VPN connection with the IAM virtual private cloud over the internet
- G. Establish an IAM Direct Connect connection with IAM and establish a public virtual interface
- H. For prefixes that need to be advertised, enter the customer gateway public IP address
- I. Create a VPN connection over Direct Connect using the customer gateway and the virtual private gateway.

**Answer: D**

#### NEW QUESTION 22

- (Exam Topic 1)

After a recent security audit involving Amazon S3, a company has asked assistance reviewing its S3 buckets to determine whether data is properly secured. The first S3 bucket on the list has the following bucket policy.

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

Is this bucket policy sufficient to ensure that the data is not publicly accessible?

- A. Yes, the bucket policy makes the whole bucket publicly accessible despite now the S3 bucket ACL or object ACLs are configured.
- B. Yes, none of the data in the bucket is publicly accessible, regardless of how the S3 bucket ACL and object ACLs are configured.
- C. No, the IAM user policy would need to be examined first to determine whether any data is publicly accessible.
- D. No, the S3 bucket ACL and object ACLs need to be examined first to determine whether any data is publicly accessible.

**Answer: A**

#### NEW QUESTION 27

- (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 29

- (Exam Topic 1)

A company's application runs on Amazon EC2 and stores data in an Amazon S3 bucket The company wants additional security controls in place to limit the likelihood of accidental exposure of data to external parties

Which combination of actions will meet this requirement? (Select THREE.)

- A. Encrypt the data in Amazon S3 using server-side encryption with Amazon S3 managed encryption keys (SSE-S3)
- B. Encrypt the data in Amazon S3 using server-side encryption with IAM KMS managed encryption keys (SSE-KMS)
- C. Create a new Amazon S3 VPC endpoint and modify the VPC's routing tables to use the new endpoint
- D. Use the Amazon S3 Block Public Access feature.
- E. Configure the bucket policy to allow access from the application instances only
- F. Use a NACL to filter traffic to Amazon S3

**Answer: BCE**

#### NEW QUESTION 31

- (Exam Topic 1)

A security engineer need to ensure their company's uses of IAM meets IAM security best practices. As part of this, the IAM account root user must not be used for daily work. The root user must be monitored for use, and the Security team must be alerted as quickly as possible if the root user is used.

Which solution meets these requirements?

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

**Answer: A**



#### NEW QUESTION 35

- (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 uses multiple IAM accounts managed with IAM Organizations Security engineers have created a standard set of security groups for all these accounts. The security policy requires that these security groups be used for all applications and delegates modification authority to the security team only.

A recent security audit found that the security groups are inconsistency implemented across accounts and that unauthorized changes have been made to the security groups. A security engineer needs to recommend a solution to improve consistency and to prevent unauthorized changes in the individual accounts in the future.

Which solution should the security engineer recommend?

- A. Use IAM Resource Access Manager to create shared resources for each required security group and apply an IAM policy that permits read-only access to the security groups only.
- B. Create an IAM CloudFormation template that creates the required security groups Execute the template as part of configuring new accounts Enable Amazon Simple Notification Service (Amazon SNS) notifications when changes occur
- C. Use IAM Firewall Manager to create a security group policy, enable the policy feature to identify and revert local changes, and enable automatic remediation
- D. Use IAM Control Tower to edit the account factory template to enable the share security groups option Apply an SCP to the OU or individual accounts that prohibits security group modifications from local account users

**Answer: B**

#### NEW QUESTION 43

- (Exam Topic 1)

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

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

**Answer: B**

#### NEW QUESTION 47

- (Exam Topic 1)

A company has several critical applications running on a large fleet of Amazon EC2 instances. As part of a security operations review, the company needs to apply a critical operating system patch to EC2 instances within 24 hours of the patch becoming available from the operating system vendor. The company does not have a patching solution deployed on IAM, but does have IAM Systems Manager configured. The solution must also minimize administrative overhead.

What should a security engineer recommend to meet these requirements?

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

**Answer: B**

#### NEW QUESTION 51

- (Exam Topic 1)

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

Which policy should the security engineer apply?

A. 

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

B. 

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

C. 

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

D. 

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

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

**Answer:** A

### NEW QUESTION 53

- (Exam Topic 1)

A company has multiple production IAM accounts. Each account has IAM CloudTrail configured to log to a single Amazon S3 bucket in a central account. Two of the production accounts have trails that are not logging anything to the S3 bucket.

Which steps should be taken to troubleshoot the issue? (Choose three.)

- A. Verify that the log file prefix is set to the name of the S3 bucket where the logs should go.
- B. Verify that the S3 bucket policy allows access for CloudTrail from the production IAM account IDs.
- C. Create a new CloudTrail configuration in the account, and configure it to log to the account's S3 bucket.
- D. Confirm in the CloudTrail Console that each trail is active and healthy.
- E. Open the global CloudTrail configuration in the master account, and verify that the storage location is set to the correct S3 bucket.
- F. Confirm in the CloudTrail Console that the S3 bucket name is set correctly.

**Answer:** BDF

### NEW QUESTION 58

- (Exam Topic 1)

A company has decided to migrate sensitive documents from on-premises data centers to Amazon S3. Currently, the hard drives are encrypted to meet a compliance requirement regarding data encryption. The CISO wants to improve security by encrypting each file using a different key instead of a single key. Using a different key would limit the security impact of a single exposed key.

Which of the following requires the LEAST amount of configuration when implementing this approach?

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

- F. Place all the files in the same S3 bucket
- G. Use server-side encryption with IAM KMS-managed keys (SSE-KMS) to encrypt the data

**Answer:** D

**Explanation:**

References:

<https://docs.IAM.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html>

Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3) When you use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3), each object is encrypted with a unique key. Server-Side Encryption with Customer Master Keys (CMKs) Stored in IAM Key Management Service (SSE-KMS) is similar to SSE-S3, but with some additional benefits and charges for using this service.

When you use SSE-KMS to protect your data without an S3 Bucket Key, Amazon S3 uses an individual IAM KMS data key for every object. It makes a call to IAM KMS every time a request is made against a

KMS-encrypted object. <https://docs.IAM.amazon.com/AmazonS3/latest/dev/bucket-key.html>

<https://docs.IAM.amazon.com/kms/latest/developerguide/symmetric-asymmetric.html>

**NEW QUESTION 60**

- (Exam Topic 1)

A Security Engineer is setting up an IAM CloudTrail trail for all regions in an IAM account. For added security, the logs are stored using server-side encryption with IAM KMS-managed keys (SSE-KMS) and have log integrity validation enabled.

While testing the solution, the Security Engineer discovers that the digest files are readable, but the log files are not. What is the MOST likely cause?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 65**

- (Exam Topic 1)

A company hosts a web-based application that captures and stores sensitive data in an Amazon DynamoDB table. A security audit reveals that the application does not provide end-to-end data protection or the ability to detect unauthorized data changes. The software engineering team needs to make changes that will address the audit findings.

Which set of steps should the software engineering team take?

- A. Use an IAM Key Management Service (IAM KMS) CM
- B. Encrypt the data at rest.
- C. Use IAM Certificate Manager (ACM) Private Certificate Authority. Encrypt the data in transit.
- D. Use a DynamoDB encryption client
- E. Use client-side encryption and sign the table items
- F. Use the IAM Encryption SDK
- G. Use client-side encryption and sign the table items.

**Answer:** A

**NEW QUESTION 69**

- (Exam Topic 1)

Authorized Administrators are unable to connect to an Amazon EC2 Linux bastion host using SSH over the internet. The connection either fails to respond or generates the following error message:

Network error: Connection timed out.

What could be responsible for the connection failure? (Select THREE )

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

**Answer:** BDF

**NEW QUESTION 72**

- (Exam Topic 1)

A Security Engineer is troubleshooting a connectivity issue between a web server that is writing log files to the logging server in another VPC. The Engineer has confirmed that a peering relationship exists between the two VPCs. VPC flow logs show that requests sent from the web server are accepted by the logging server but the web server never receives a reply.

Which of the following actions could fix this issue?

- A. Add an inbound rule to the security group associated with the logging server that allows requests from the web server
- B. Add an outbound rule to the security group associated with the web server that allows requests to the logging server.
- C. Add a route to the route table associated with the subnet that hosts the logging server that targets the peering connection
- D. Add a route to the route table associated with the subnet that hosts the web server that targets the peering connection

**Answer:** C



#### NEW QUESTION 77

- (Exam Topic 1)

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 81

- (Exam Topic 1)

A global company that deals with International finance is investing heavily in cryptocurrencies and wants to experiment with mining technologies using IAM. The company's security team has enabled Amazon GuardDuty and is concerned by the number of findings being generated by the accounts. The security team wants to minimize the possibility of GuardDuty finding false negatives for compromised instances that are performing mining. How can the security team continue using GuardDuty while meeting these requirements?

- A. In the GuardDuty console, select the CryptoCurrency:EC2/BitcoinTool B'DNS finding and use the suppress findings option
- B. Create a custom IAM Lambda function to process newly detected GuardDuty alerts Process the CryptoCurrency EC2/BitcoinTool BIDNS alert and filter out the high-severity finding types only.
- C. When creating a new Amazon EC2 Instance, provide the instance with a specific tag that indicates it is performing mining operations Create a custom IAM Lambda function to process newly detected GuardDuty alerts and filter for the presence of this tag
- D. When GuardDuty produces a cryptocurrency finding, process the finding with a custom IAM Lambda function to extract the instance ID from the finding Then use the IAM Systems Manager Run Command to check for a running process performing mining operations

**Answer:** A

#### NEW QUESTION 85

- (Exam Topic 1)

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

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

**Answer:** D

#### NEW QUESTION 90

- (Exam Topic 1)

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

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

**Answer:** A

#### NEW QUESTION 94

- (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 98

- (Exam Topic 1)

A convays data lake uses Amazon S3 and Amazon Athena. The company's security engineer has been asked to design an encryption solution that meets the company's data protection requirements. The encryption solution must work with Amazon S3 and keys managed by the company. The encryption solution must be protected in a hardware security module that is validated id Federal information Processing Standards (FPS) 140-2 Level 3. Which solution meets these requirements?

- A. Use client-side encryption with an IAM KMS customer-managed key implemented with the IAM Encryption SDK
- B. Use IAM CloudHSM to store the keys and perform cryptographic operations Save the encrypted text in Amazon S3
- C. Use an IAM KMS customer-managed key that is backed by a custom key store using IAM CloudHSM
- D. Use an IAM KMS customer-managed key with the bring your own key (BYOK) feature to import a key stored in IAM CloudHSM

**Answer:** B

#### NEW QUESTION 102

- (Exam Topic 1)

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

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

**Answer:** A

#### NEW QUESTION 107

- (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 108

- (Exam Topic 1)

A Developer signed in to a new account within an IAM Organizations organizations unit (OU) containing multiple accounts. Access to the Amazon S3 service is restricted with the following SCP:

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

How can the Security Engineer provide the Developer with Amazon S3 access without affecting other accounts?

- A. Move the SCP to the root OU of Organizations to remove the restriction to access Amazon S3.
- B. Add an IAM policy for the Developer, which grants S3 access.
- C. Create a new OU without applying the SCP restricting S3 access.
- D. Move the Developer account to this new OU.
- E. Add an allow list for the Developer account for the S3 service.

**Answer: C**

#### NEW QUESTION 113

- (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.amazonaws.com/AmazonCloudFront/latest/DeveloperGuide/cnames-and-https-requirements.html>

#### NEW QUESTION 118

- (Exam Topic 1)

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

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

**Answer: C**

#### NEW QUESTION 122

- (Exam Topic 1)

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

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

**Answer: D**

#### NEW QUESTION 125

- (Exam Topic 1)

A company plans to use custom AMIs to launch Amazon EC2 instances across multiple IAM accounts in a single Region to perform security monitoring and analytics tasks. The EC2 instances are launched in EC2 Auto Scaling groups. To increase the security of the solution, a Security Engineer will manage the lifecycle of the custom AMIs in a centralized account and will encrypt them with a centrally managed IAM KMS CMK. The Security Engineer configured the KMS key policy to allow cross-account access. However, the EC2 instances are still not being properly launched by the EC2 Auto Scaling groups. Which combination of configuration steps should the Security Engineer take to ensure the EC2 Auto Scaling groups have been granted the proper permissions to execute tasks?

- A. Create a customer-managed CMK in the centralized account

- B. Allow other applicable accounts to use that key for cryptographic operations by applying proper cross-account permissions in the key policy
- C. Create an IAM role in all applicable accounts and configure its access policy to allow the use of the centrally managed CMK for cryptographic operation
- D. Configure EC2 Auto Scaling groups within each applicable account to use the created IAM role to launch EC2 instances.
- E. Create a customer-managed CMK in the centralized account
- F. Allow other applicable accounts to use that key for cryptographic operations by applying proper cross-account permissions in the key policy
- G. Create an IAM role in all applicable accounts and configure its access policy with permissions to create grants for the centrally managed CM
- H. Use this IAM role to create a grant for the centrally managed CMK with permissions to perform cryptographic operations and with the EC2 Auto Scaling service-linked role defined as the grantee principal.
- I. Create a customer-managed CMK or an IAM managed CMK in the centralized account
- J. Allow other applicable accounts to use that key for cryptographic operations by applying proper cross-account permissions in the key policy
- K. Use the CMK administrator to create a CMK grant that includes permissions to perform cryptographic operations that define EC2 Auto Scaling service-linked roles from all other accounts as the grantee principal.
- L. Create a customer-managed CMK or an IAM managed CMK in the centralized account
- M. Allow other applicable accounts to use that key for cryptographic operations by applying proper cross-account permissions in the key policy
- N. Modify the access policy for the EC2 Auto Scaling roles to perform cryptographic operations against the centrally managed CMK.

**Answer: B**

#### NEW QUESTION 130

- (Exam Topic 1)

A security engineer is auditing a production system and discovers several additional IAM roles that are not required and were not previously documented during the last audit 90 days ago. The engineer is trying to find out who created these IAM roles and when they were created. The solution must have the lowest operational overhead.

Which solution will meet this requirement?

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

**Answer: A**

#### NEW QUESTION 133

- (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/developerguide/overview.html> The correct answer is:

IAM KMS API

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 135

- (Exam Topic 2)

A company wants to control access to its IAM resources by using identities and groups that are defined in its existing Microsoft Active Directory.

What must the company create in its IAM account to map permissions for IAM services to Active Directory user attributes?

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

**Answer: C**

#### Explanation:

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

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

#### NEW QUESTION 136

- (Exam Topic 2)

You have a web site that is sitting behind IAM Cloudfront. You need to protect the web site against threats



such as SQL injection and Cross site scripting attacks. Which of the following service can help in such a scenario Please select:

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

**Answer:** B

**Explanation:**

The IAM Documentation mentions the following

IAM WAF is a web application firewall that helps detect and block malicious web requests targeted at your web applications. IAM WAF allows you to create rules that can help protect against common web exploits like SQL injection and cross-site scripting. With IAM WAF you first identify the resource (either an Amazon CloudFront distribution or an Application Load Balancer) that you need to protect.

Option A is invalid because this will only give advise on how you can better the security in your IAM account but not protect against threats mentioned in the question.

Option C is invalid because this can be used to scan EC2 Instances for vulnerabilities but not protect against threats mentioned in the question.

Option D is invalid because this can be used to check config changes but not protect against threats mentioned in the quest

For more information on IAM WAF, please visit the following URL: <https://IAM.amazon.com/waf/details>;

The correct answer is: IAM WAF

Submit your Feedback/Queries to our Experts

**NEW QUESTION 137**

- (Exam Topic 2)

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

Please select:

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

**Answer:** CD

**Explanation:**

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

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

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

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

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

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

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

Submit your Feedback/Queries to our Experts

**NEW QUESTION 139**

- (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 142

- (Exam Topic 2)

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

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

**Answer: B**

#### Explanation:

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

Option A, C and D are all invalid because this would affect the application running on the server. The easiest way is just to remove the rule for access on port 22. For more information on authorizing access to an instance, please visit the below URL: <https://docs.IAM.amazon.com/IAMEC2/latest/UserGuide/authorizing-access-to-an-instance.html>

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

#### NEW QUESTION 146

- (Exam Topic 2)

An organization has three applications running on IAM, each accessing the same data on Amazon S3. The data on Amazon S3 is server-side encrypted by using an IAM KMS Customer Master Key (CMK).

What is the recommended method to ensure that each application has its own programmatic access control permissions on the KMS CMK?

- A. Change the key policy permissions associated with the KMS CMK for each application when it must access the data in Amazon S3.
- B. Have each application assume an IAM role that provides permissions to use the IAM Certificate Manager CMK.
- C. Have each application use a grant on the KMS CMK to add or remove specific access controls on the KMS CMK.
- D. Have each application use an IAM policy in a user context to have specific access permissions on the KMS CMK.

**Answer: C**

#### NEW QUESTION 150

- (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 attacks by simply denying traffic with the header match. HTH ExampleGame/1.22; Mobile/1.0)

#### NEW QUESTION 152

- (Exam Topic 2)

A Security Engineer is working with a Product team building a web application on IAM. The application uses Amazon S3 to host the static content, Amazon API Gateway to provide RESTful services; and Amazon DynamoDB as the backend data store. The users already exist in a directory that is exposed through a SAML identity provider.

Which combination of the following actions should the Engineer take to enable users to be authenticated into the web application and call APIs? (Choose three.)

- A. Create a custom authorization service using IAM Lambda.
- B. Configure a SAML identity provider in Amazon Cognito to map attributes to the Amazon Cognito user pool attributes.

- C. Configure the SAML identity provider to add the Amazon Cognito user pool as a relying party.
- D. Configure an Amazon Cognito identity pool to integrate with social login providers.
- E. Update DynamoDB to store the user email addresses and passwords.
- F. Update API Gateway to use a COGNITO\_USER\_POOLS authorizer.

**Answer:** BDE

#### NEW QUESTION 155

- (Exam Topic 2)

A Security Engineer must implement mutually authenticated TLS connections between containers that communicate inside a VPC.

Which solution would be MOST secure and easy to maintain?

- A. Use IAM Certificate Manager to generate certificates from a public certificate authority and deploy them to all the containers.
- B. Create a self-signed certificate in one container and use IAM Secrets Manager to distribute the certificate to the other containers to establish trust.
- C. Use IAM Certificate Manager Private Certificate Authority (ACM PCA) to create a subordinate certificate authority, then create the private keys in the containers and sign them using the ACM PCA API.
- D. Use IAM Certificate Manager Private Certificate Authority (ACM PCA) to create a subordinate certificate authority, then use IAM Certificate Manager to generate the private certificates and deploy them to all the containers.

**Answer:** D

#### NEW QUESTION 160

- (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 161

- (Exam Topic 2)

A Security Engineer is defining the logging solution for a newly developed product. Systems Administrators and Developers need to have appropriate access to event log files in IAM CloudTrail to support and troubleshoot the product.

Which combination of controls should be used to protect against tampering with and unauthorized access to log files? (Choose two.)

- A. Ensure that the log file integrity validation mechanism is enabled.
- B. Ensure that all log files are written to at least two separate Amazon S3 buckets in the same account.
- C. Ensure that Systems Administrators and Developers can edit log files, but prevent any other access.
- D. Ensure that Systems Administrators and Developers with job-related need-to-know requirements only are capable of viewing—but not modifying—the log files.
- E. Ensure that all log files are stored on Amazon EC2 instances that allow SSH access from the internal corporate network only.

**Answer:** AD

#### NEW QUESTION 164

- (Exam Topic 2)

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

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

Please select:

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

**Answer:** AC

#### Explanation:

The IAM Documentation mentions the following

To determine whether a log file was modified, deleted, or unchanged after CloudTrail delivered it you can use CloudTrail log file integrity validation. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete

or forge CloudTrail log files without detection.

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

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

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

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

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

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 165

- (Exam Topic 2)

An application outputs logs to a text file. The logs must be continuously monitored for security incidents. Which design will meet the requirements with MINIMUM effort?

- A. Create a scheduled process to copy the component's logs into Amazon S3. Use S3 events to trigger a Lambda function that updates Amazon CloudWatch metrics with the log data
- B. Set up CloudWatch alerts based on the metrics.
- C. Install and configure the Amazon CloudWatch Logs agent on the application's EC2 instance
- D. Create a CloudWatch metric filter to monitor the application log
- E. Set up CloudWatch alerts based on the metrics.
- F. Create a scheduled process to copy the application log files to IAM CloudTrail
- G. Use S3 events to trigger Lambda functions that update CloudWatch metrics with the log data
- H. Set up CloudWatch alerts based on the metrics.
- I. Create a file watcher that copies data to Amazon Kinesis when the application writes to the log file. Have Kinesis trigger a Lambda function to update Amazon CloudWatch metrics with the log data
- J. Set up CloudWatch alerts based on the metrics.

**Answer: B**

**Explanation:**

<https://docs.IAM.amazon.com/AmazonCloudWatch/latest/logs/QuickStartEC2Instance.html>

#### NEW QUESTION 170

- (Exam Topic 2)

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

How can this be accomplished? (Choose two.)



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

**Answer: BD**

**Explanation:**

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

#### NEW QUESTION 171

- (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 174

- (Exam Topic 2)

Some highly sensitive analytics workloads are to be moved to Amazon EC2 hosts. Threat modeling has found that a risk exists where a subnet could be maliciously or accidentally exposed to the internet.

Which of the following mitigations should be recommended?

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

**Answer: A**

#### Explanation:

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

#### NEW QUESTION 175

- (Exam Topic 2)

The Security Engineer is given the following requirements for an application that is running on Amazon EC2 and managed by using IAM CloudFormation templates with EC2 Auto Scaling groups:

- Have the EC2 instances bootstrapped to connect to a backend database.
- Ensure that the database credentials are handled securely.
- Ensure that retrievals of database credentials are logged.

Which of the following is the MOST efficient way to meet these requirements?

- A. Pass databases credentials to EC2 by using CloudFormation stack parameters with the property set to tru
- B. Ensure that the instance is configured to log to Amazon CloudWatch Logs.
- C. Store database passwords in IAM Systems Manager Parameter Store by using SecureString parameters. Set the IAM role for the EC2 instance profile to allow access to the parameters.
- D. Create an IAM Lambda that ingests the database password and persists it to Amazon S3 with server-side encryptio
- E. Have the EC2 instances retrieve the S3 object on startup, and log all script invocations to syslog.
- F. Write a script that is passed in as UserData so that it is executed upon launch of the EC2 instance. Ensure that the instance is configured to log to Amazon CloudWatch Logs.

**Answer: B**

**NEW QUESTION 176**

- (Exam Topic 2)

An organization has tens of applications deployed on thousands of Amazon EC2 instances. During testing, the Application team needs information to let them know whether the network access control lists (network ACLs) and security groups are working as expected.

How can the Application team's requirements be met?

- A. Turn on VPC Flow Logs, send the logs to Amazon S3, and use Amazon Athena to query the logs.
- B. Install an Amazon Inspector agent on each EC2 instance, send the logs to Amazon S3, and use Amazon EMR to query the logs.
- C. Create an IAM Config rule for each network ACL and security group configuration, send the logs to Amazon S3, and use Amazon Athena to query the logs.
- D. Turn on IAM CloudTrail, send the trails to Amazon S3, and use IAM Lambda to query the trails.

**Answer:** A

**NEW QUESTION 179**

- (Exam Topic 2)

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

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

**Answer:** A

**Explanation:**

"automatic key rotation has no effect on the data that the CMK protects. It does not rotate the data keys that the CMK generated or re-encrypt any data protected by the CMK, and it will not mitigate the effect of a compromised data key. You might decide to create a new CMK and use it in place of the original CMK. This has the same effect as rotating the key material in an existing CMK, so it's often thought of as manually rotating the key."

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

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

**NEW QUESTION 182**

- (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 187**

- (Exam Topic 2)

A Software Engineer wrote a customized reporting service that will run on a fleet of Amazon EC2 instances. The company security policy states that application logs for the reporting service must be centrally collected.

What is the MOST efficient way to meet these requirements?

- A. Write an IAM Lambda function that logs into the EC2 instance to pull the application logs from the EC2 instance and persists them into an Amazon S3 bucket.
- B. Enable IAM CloudTrail logging for the IAM account, create a new Amazon S3 bucket, and then configure Amazon CloudWatch Logs to receive the application logs from CloudTrail.
- C. Create a simple cron job on the EC2 instances that synchronizes the application logs to an Amazon S3 bucket by using rsync.
- D. Install the Amazon CloudWatch Logs Agent on the EC2 instances, and configure it to send the application logs to CloudWatch Logs.

**Answer:** D

**Explanation:**

<https://IAM.amazon.com/blogs/IAM/cloudwatch-log-service/>

**NEW QUESTION 189**

- (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.amazon.com/AmazonCloudWatch/latest/monitoring/permissions-reference-cw.html>

**NEW QUESTION 192**

- (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 195**

- (Exam Topic 2)

A Security Engineer is implementing a solution to allow users to seamlessly encrypt Amazon S3 objects without having to touch the keys directly. The solution must be highly scalable without requiring continual management. Additionally, the organization must be able to immediately delete the encryption keys.

Which solution meets these requirements?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 198**

- (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 199**

- (Exam Topic 2)

Which of the following minimizes the potential attack surface for applications?

- A. Use security groups to provide stateful firewalls for Amazon EC2 instances at the hypervisor level.
- B. Use network ACLs to provide stateful firewalls at the VPC level to prevent access to any specific IAM resource.
- C. Use IAM Direct Connect for secure trusted connections between EC2 instances within private subnets.
- D. Design network security in a single layer within the perimeter network (also known as DMZ, demilitarized zone, and screened subnet) to facilitate quicker responses to threats.

**Answer:** A

**Explanation:**

<https://IAM.amazon.com/answers/networking/vpc-security-capabilities/> Security Group is stateful and hypervisor level.

**NEW QUESTION 203**

- (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 206**

- (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 207**

- (Exam Topic 2)

A corporate cloud security policy states that communications between the company's VPC and KMS must travel entirely within the IAM network and not use public service endpoints.

Which combination of the following actions MOST satisfies this requirement? (Choose two.)

- A. Add the IAM:sourceVpce condition to the IAM KMS key policy referencing the company's VPC endpoint ID.
- B. Remove the VPC internet gateway from the VPC and add a virtual private gateway to the VPC to prevent direct, public internet connectivity.
- C. Create a VPC endpoint for IAM KMS with private DNS enabled.
- D. Use the KMS Import Key feature to securely transfer the IAM KMS key over a VPN.
- E. Add the following condition to the IAM KMS key policy: "IAM:SourceIp": "10.0.0.0/16".

**Answer:** AC



**Explanation:**

An IAM policy can deny access to KMS except through your VPC endpoint with the following condition statement:

```
"Condition": { "StringNotEquals": {  
  "IAM:sourceVpce": "vpce-0295a3caf8414c94a"  
}  
}
```

If you select the Enable Private DNS Name option, the standard IAM KMS DNS hostname (<https://kms.<region>.amazonIAM.com>) resolves to your VPC endpoint.

**NEW QUESTION 211**

- (Exam Topic 2)

An organization has a system in IAM that allows a large number of remote workers to submit data files. File sizes vary from a few kilobytes to several megabytes.

A recent audit highlighted a concern that data files are not encrypted while in transit over untrusted networks.

Which solution would remediate the audit finding while minimizing the effort required?

- A. Upload an SSL certificate to IAM, and configure Amazon CloudFront with the passphrase for the private key.
- B. Call KMS.Encrypt() in the client, passing in the data file contents, and call KMS.Decrypt() server-side.
- C. Use IAM Certificate Manager to provision a certificate on an Elastic Load Balancing in front of the web service's servers.
- D. Create a new VPC with an Amazon VPC VPN endpoint, and update the web service's DNS record.

**Answer: C**

**NEW QUESTION 212**

- (Exam Topic 2)

Due to new compliance requirements, a Security Engineer must enable encryption with customer-provided keys on corporate data that is stored in DynamoDB.

The company wants to retain full control of the encryption keys.

Which DynamoDB feature should the Engineer use to achieve compliance'?

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

**Answer: D**

**Explanation:**

Follow the link:

<https://docs.IAM.amazon.com/dynamodb-encryption-client/latest/devguide/what-is-ddb-encrypt.html>

**NEW QUESTION 217**

- (Exam Topic 2)

Your company has a set of resources defined in the IAM Cloud. Their IT audit department has requested to get a list of resources that have been defined across the account. How can this be achieved in the easiest manner?

Please select:







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

**Answer: D**

**Explanation:**

The most feasible option is to use IAM Config. When you turn on IAM Config, you will get a list of resources defined in your IAM Account.

A sample snapshot of the resources dashboard in IAM Config is shown below C:\Users\wk\Desktop\mudassar\Untitled.jpg

Resources	
Total resource count	131
Top 10 resource types	Total
 IAM Policy	45
 IAM Role	40
 EC2 Subnet	7
 EC2 SecurityGroup	6
 EC2 RouteTable	6
 EC2 VPC	4
 EC2 NetworkAcl	4

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

#### NEW QUESTION 221

- (Exam Topic 2)

A threat assessment has identified a risk whereby an internal employee could exfiltrate sensitive data from production host running inside IAM (Account 1). The threat was documented as follows:

Threat description: A malicious actor could upload sensitive data from Server X by configuring credentials for an IAM account (Account 2) they control and uploading data to an Amazon S3 bucket within their control.

Server X has outbound internet access configured via a proxy server. Legitimate access to S3 is required so that the application can upload encrypted files to an S3 bucket. Server X is currently using an IAM instance role. The proxy server is not able to inspect any of the server communication due to TLS encryption.

Which of the following options will mitigate the threat? (Choose two.)

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

**Answer: AB**

#### NEW QUESTION 223

- (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 224

- (Exam Topic 2)

A Security Administrator has a website hosted in Amazon S3. The Administrator has been given the following requirements:

- > Users may access the website by using an Amazon CloudFront distribution.
- > Users may not access the website directly by using an Amazon S3 URL.

Which configurations will support these requirements? (Choose two.)

- A. Associate an origin access identity with the CloudFront distribution.
- B. Implement a "Principal": "cloudfront.amazonaws.com" condition in the S3 bucket policy.

- C. Modify the S3 bucket permissions so that only the origin access identity can access the bucket contents.
- D. Implement security groups so that the S3 bucket can be accessed only by using the intended CloudFront distribution.
- E. Configure the S3 bucket policy so that it is accessible only through VPC endpoints, and place the CloudFront distribution into the specified VPC.

**Answer:** AC

#### NEW QUESTION 226

- (Exam Topic 2)

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

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

**Answer:** C

#### Explanation:

<https://docs.IAM.amazonaws.com/ses/latest/DeveloperGuide/smtp-connect.html>

#### NEW QUESTION 230

- (Exam Topic 2)

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 235

- (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 240

- (Exam Topic 2)

An organization is using Amazon CloudWatch Logs with agents deployed on its Linux Amazon EC2 instances. The agent configuration files have been checked and the application log files to be pushed are configured correctly. A review has identified that logging from specific instances is missing. Which steps should be taken to troubleshoot the issue? (Choose two.)

- A. Use an EC2 run command to confirm that the "IAMLogs" service is running on all instances.
- B. Verify that the permissions used by the agent allow creation of log groups/streams and to put log events.
- C. Check whether any application log entries were rejected because of invalid time stamps by reviewing /var/cwlogs/rejects.log.
- D. Check that the trust relationship grants the service "cwlogs.amazonaws.com" permission to write objects to the Amazon S3 staging bucket.
- E. Verify that the time zone on the application servers is in UTC.

**Answer:** AB

#### Explanation:

EC2 run command - can run scripts, install software, collect metrics and log files, manage patches and more. Bringing these two services together - can create CloudWatch Events rules that use EC2 Run Command to perform actions on EC2 instances or on-premises servers.

#### NEW QUESTION 241

- (Exam Topic 2)

Your development team has started using IAM resources for development purposes. The IAM account has just been created. Your IT Security team is worried about possible leakage of IAM keys. What is the first level of measure that should be taken to protect the IAM account. Please select:

- A. Delete the IAM keys for the root account
- B. Create IAM Groups
- C. Create IAM Roles

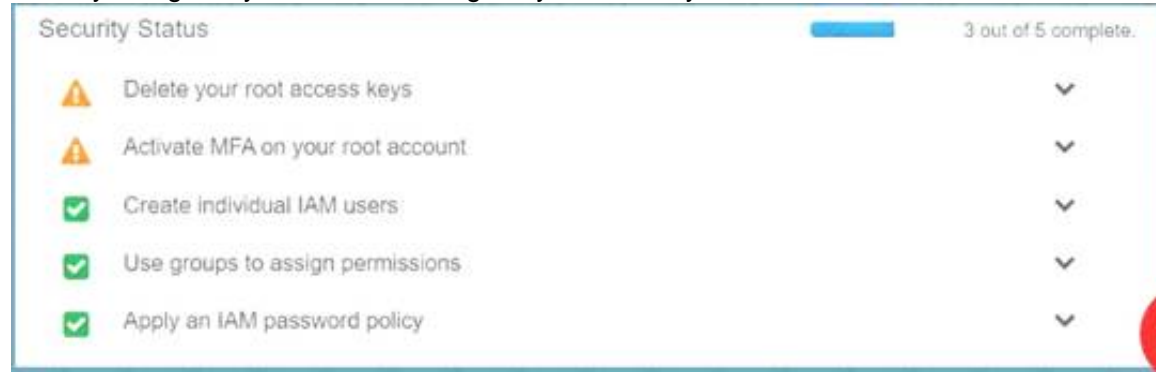
D. Restrict access using IAM policies

**Answer:** A

**Explanation:**

The first level or measure that should be taken is to delete the keys for the IAM root user

When you log into your account and go to your Security Access dashboard, this is the first step that can be seen C:\Users\wk\Desktop\mudassar\Untitled.jpg



Option B and C are wrong because creation of IAM groups and roles will not change the impact of leakage of IAM root access keys

Option D is wrong because the first key aspect is to protect the access keys for the root account For more information on best practises for Security Access keys, please visit the below URL:

<https://docs.IAM.amazon.com/eeneral/latest/gr/IAM-access-keys-best-practices.html>

The correct answer is: Delete the IAM keys for the root account Submit your Feedback/Queries to our Experts

**NEW QUESTION 242**

- (Exam Topic 2)

A Security Engineer received an IAM Abuse Notice listing EC2 instance IDs that are reportedly abusing other hosts.

Which action should the Engineer take based on this situation? (Choose three.)

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

**Answer:** BEF

**NEW QUESTION 245**

- (Exam Topic 2)

A Security Engineer must design a solution that enables the Incident Response team to audit for changes to a user's IAM permissions in the case of a security incident.

How can this be accomplished?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 247**

- (Exam Topic 2)

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

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

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

**Answer:** A

**NEW QUESTION 252**

- (Exam Topic 2)

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

Please select:

- A. After 30 days



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

**Answer: D**

**Explanation:**

The IAM Documentation states the following

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

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

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

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

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

You can login to you IAM dashbaord . Click on "Encryption Keys"

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

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

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

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

Rotation period for CMKs is as follows:

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

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

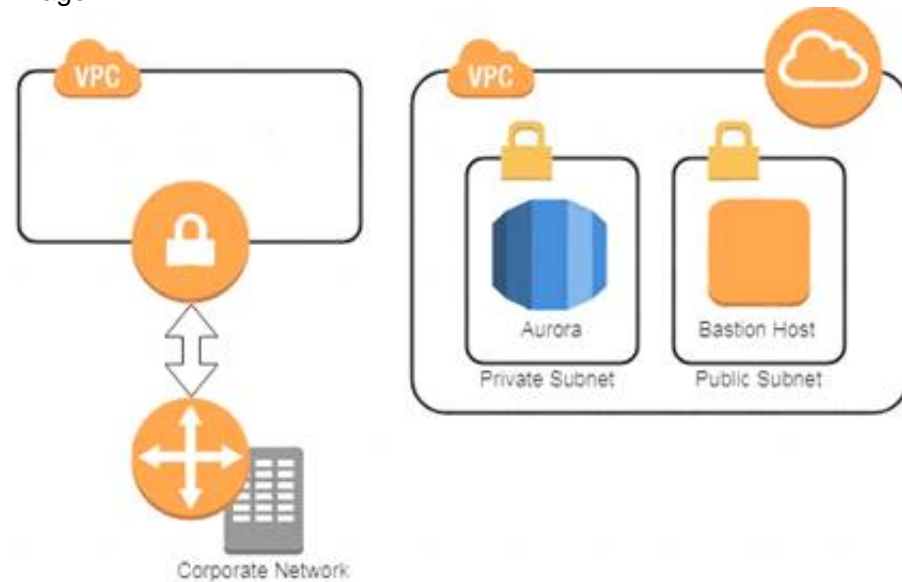
For more details, please check below IAM Docs: <https://docs.IAM.amazon.com/kms/latest/developerguide/concepts.html> The correct answer is: After 3 years

Submit your Feedback/Queries to our Experts

**NEW QUESTION 256**

- (Exam Topic 2)

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



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

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

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

**Answer: A**

**NEW QUESTION 260**

- (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 262**

- (Exam Topic 2)

A Security Engineer has created an Amazon CloudWatch event that invokes an IAM Lambda function daily. The Lambda function runs an Amazon Athena query that checks IAM CloudTrail logs in Amazon S3 to detect whether any IAM user accounts or credentials have been created in the past 30 days. The results of the Athena query are created in the same S3 bucket. The Engineer runs a test execution of the Lambda function via the IAM Console, and the function runs successfully.

After several minutes, the Engineer finds that his Athena query has failed with the error message: "Insufficient Permissions". The IAM permissions of the Security Engineer and the Lambda function are shown below:

Security Engineer

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:*",
        "iam:*",
        "lambda:*",
        "athena:Get*",
        "athena:List*",
        "cloudwatch:*"
      ],
      "Resource": "*"
    }
  ]
}
```

Lambda function execution role

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "athena:*",
        "cloudwatch:*"
      ],
      "Resource": "*"
    }
  ]
}
```

What is causing the error?

- A. The Lambda function does not have permissions to start the Athena query execution.
- B. The Security Engineer does not have permissions to start the Athena query execution.
- C. The Athena service does not support invocation through Lambda.
- D. The Lambda function does not have permissions to access the CloudTrail S3 bucket.

**Answer:** D

**NEW QUESTION 263**

- (Exam Topic 2)

A Security Engineer must enforce the use of only Amazon EC2, Amazon S3, Amazon RDS, Amazon DynamoDB, and IAM STS in specific accounts.

What is a scalable and efficient approach to meet this requirement?

- A Set up an AWS Organizations hierarchy, and replace the FullAWSAccess policy with the following Service Control Policy for the governed organization units:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "dynamodb:*", "rds:*", "ec2:*",
        "s3:*", "sts:*"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

- B Create multiple IAM users for the regulated accounts, and attach the following policy statement to restrict services as required:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": *
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "NotAction": [
        "dynamodb:*", "rds:*", "ec2:*",
        "s3:*", "sts:*"
      ],
      "Effect": "Deny ",
      "Resource": "*"
    }
  ]
}
```

- C Set up an Organizations hierarchy, replace the global FullAWSAccess with the following Service Control Policy at the top level:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "dynamodb:*", "rds:*", "ec2:*",
        "s3:*", "sts:*"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

- D Set up all users in the Active Directory for federated access to all accounts in the company. Associate Active Directory groups with IAM groups, and attach the following policy statement to restrict services as required:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": *
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "NotAction": [
        "dynamodb:*", "rds:*", "ec2:*",
        "s3:*", "sts:*"
      ],
      "Effect": "Deny ",
      "Resource": "*"
    }
  ]
}
```

A. Option A

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

**Answer:** A

**Explanation:**

It says specific accounts which mean specific governed OUs under your organization and you apply specific service control policy to these OUs.

**NEW QUESTION 264**

- (Exam Topic 2)

A company's database developer has just migrated an Amazon RDS database credential to be stored and managed by IAM Secrets Manager. The developer has also enabled rotation of the credential within the Secrets Manager console and set the rotation to change every 30 days.

After a short period of time, a number of existing applications have failed with authentication errors. What is the MOST likely cause of the authentication errors?

- A. Migrating the credential to RDS requires that all access come through requests to the Secrets Manager.
- B. Enabling rotation in Secrets Manager causes the secret to rotate immediately, and the applications are using the earlier credential.
- C. The Secrets Manager IAM policy does not allow access to the RDS database.
- D. The Secrets Manager IAM policy does not allow access for the applications.

**Answer:** B

**Explanation:**

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

**NEW QUESTION 267**

- (Exam Topic 2)

The InfoSec team has mandated that in the future only approved Amazon Machine Images (AMIs) can be used.

How can the InfoSec team ensure compliance with this mandate?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 268**

- (Exam Topic 2)

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

Which of the following solutions will meet these requirements?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 272**

- (Exam Topic 2)

A distributed web application is installed across several EC2 instances in public subnets residing in two Availability Zones. Apache logs show several intermittent brute-force attacks from hundreds of IP addresses at the layer 7 level over the past six months.

What would be the BEST way to reduce the potential impact of these attacks in the future?

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 277**

- (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 279

- (Exam Topic 2)

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

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

**Answer:** A

#### Explanation:

<https://docs.IAM.amazon.com/IAMcloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail.html#cloudwatc> Open the CloudWatch console at <https://console.IAM.amazon.com/cloudwatch/>. In the navigation pane, choose Logs. In the list of log groups, select the check box next to the log group that you created for CloudTrail log events. Choose Create Metric Filter. On the Define Logs Metric Filter screen, choose Filter Pattern and then type the following: { (\$errorCode = "\*UnauthorizedOperation") || (\$errorCode = "AccessDenied")} Choose Assign Metric. For Filter Name, type AuthorizationFailures. For Metric Namespace, type CloudTrailMetrics. For Metric Name, type AuthorizationFailureCount.

#### NEW QUESTION 280

- (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 283

- (Exam Topic 2)

An application has been built with Amazon EC2 instances that retrieve messages from Amazon SQS. Recently, IAM changes were made and the instances can no longer retrieve messages.

What actions should be taken to troubleshoot the issue while maintaining least privilege. (Select two.)

- A. Configure and assign an MFA device to the role used by the instances.
- B. Verify that the SQS resource policy does not explicitly deny access to the role used by the instances.
- C. Verify that the access key attached to the role used by the instances is active.
- D. Attach the AmazonSQSFullAccess managed policy to the role used by the instances.
- E. Verify that the role attached to the instances contains policies that allow access to the queue.

**Answer:** BE

#### NEW QUESTION 288

- (Exam Topic 2)

A Security Analyst attempted to troubleshoot the monitoring of suspicious security group changes. The Analyst was told that there is an Amazon CloudWatch alarm in place for these IAM CloudTrail log events.

The Analyst tested the monitoring setup by making a configuration change to the security group but did not receive any alerts.

Which of the following troubleshooting steps should the Analyst perform?

- A. Ensure that CloudTrail and S3 bucket access logging is enabled for the Analyst's IAM account.
- B. Verify that a metric filter was created and then mapped to an alarm.
- C. Check the alarm notification action.
- D. Check the CloudWatch dashboards to ensure that there is a metric configured with an appropriate dimension for security group changes.
- E. Verify that the Analyst's account is mapped to an IAM policy that includes permissions for cloudwatch: GetMetricStatistics and Cloudwatch: ListMetrics.

**Answer:** B

#### Explanation:

MetricFilter:

Type: 'IAM::Logs::MetricFilter' Properties:

LogGroupName: " FilterPattern: >{ (\$eventName = AuthorizeSecurityGroupIngress) || (\$eventName = AuthorizeSecurityGroupEgress) || (\$eventName = RevokeSecurityGroupIngress) || (\$eventName = RevokeSecurityGroupEgress) || (\$eventName = CreateSecurityGroup) || (\$eventName = DeleteSecurityGroup) }

MetricTransformations:

- MetricValue: '1'

MetricNamespace: CloudTrailMetrics MetricName: SecurityGroupEventCount

#### NEW QUESTION 289

- (Exam Topic 2)

A pharmaceutical company has digitized versions of historical prescriptions stored on premises. The company would like to move these prescriptions to IAM and perform analytics on the data in them. Any operation with this data requires that the data be encrypted in transit and at rest.

Which application flow would meet the data protection requirements on IAM?

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

**Answer:** A

#### Explanation:

(Amazon Kinesis Data Analytics is the easiest way to analyze streaming data, also provide encryption at rest and in-transit)

-<https://docs.IAM.amazon.com/kinesisanalytics/latest/dev/data-protection.html>

#### NEW QUESTION 293

- (Exam Topic 2)

A company plans to move most of its IT infrastructure to IAM. The company wants to leverage its existing on-premises Active Directory as an identity provider for IAM.

Which steps should be taken to authenticate to IAM services using the company's on-premises Active Directory? (Choose three).

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

**Answer:** ACE

#### Explanation:

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

#### NEW QUESTION 296

- (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 298

- (Exam Topic 2)

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

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

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

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

**Answer:** D

#### Explanation:

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

#### NEW QUESTION 299

- (Exam Topic 2)

You have a vendor that needs access to an IAM resource. You create an IAM user account. You want to restrict access to the resource using a policy for just that user over a brief period. Which of the following would be an ideal policy to use?

Please select:

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

**Answer:** B

#### Explanation:

The IAM Documentation gives an example on such a case

Inline policies are useful if you want to maintain a strict one-to-one relationship between a policy and the principal entity that it is applied to. For example, you want to be sure that the permissions in a policy are not inadvertently assigned to a principal entity other than the one they're intended for. When you use an inline policy, the permissions in the policy cannot be inadvertently attached to the wrong principal entity. In addition, when you use the IAM Management Console to delete that principal entity the policies embedded in the principal entity are deleted as well. That's because they are part of the principal entity.

Option A is invalid because IAM Managed Policies are ok for a group of users, but for individual users, inline policies are better.

Option C and D are invalid because they are specifically meant for access to S3 buckets. For more information on policies, please visit the following URL:

<https://docs.IAM.amazon.com/IAM/latest/UserGuide/access-managed-vs-inline>

The correct answer is: An Inline Policy. Submit your Feedback/Queries to our Experts

#### NEW QUESTION 304

- (Exam Topic 2)

You have just received an email from IAM Support stating that your IAM account might have been compromised. Which of the following steps would you look to carry out immediately. Choose 3 answers from the options below.

Please select:

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

**Answer:** ABD

#### Explanation:

One of the articles from IAM mentions what should be done in such a scenario

If you suspect that your account has been compromised, or if you have received a notification from IAM that the account has been compromised, perform the following tasks:

Change your IAM root account password and the passwords of any IAM users.

Delete or rotate all root and IAM Identity and Access Management (IAM) access keys.

Delete any resources on your account you didn't create, especially running EC2 instances, EC2 spot bids, or IAM users.

Respond to any notifications you received from IAM Support through the IAM Support Center.

Option C is invalid because there could be compromised instances or resources running on your environment. They should be shutdown or stopped immediately.

For more information on the article, please visit the below URL: <https://IAM.amazon.com/premiumsupport/knowledge-center/potential-account-compromise>

The correct answers are: Change the root account password. Rotate all IAM access keys. Change the password for all IAM users. Submit your Feedback/Queries to our Experts

#### NEW QUESTION 309

- (Exam Topic 3)

Your company has a set of EBS volumes defined in IAM. The security mandate is that all EBS volumes are encrypted. What can be done to notify the IT admin staff if there are any unencrypted volumes in the account.

Please select:

- A. Use IAM Inspector to inspect all the EBS volumes
- B. Use IAM Config to check for unencrypted EBS volumes
- C. Use IAM Guard duty to check for the unencrypted EBS volumes
- D. Use IAM Lambda to check for the unencrypted EBS volumes

**Answer:** B

**Explanation:**

The enc

config rule for IAM Config can be used to check for unencrypted volumes. encrypted-volurn

5 volumes that are in an attached state are encrypted. If you specify the ID of a KMS key for encryptio using the kmsId parameter, the rule checks if the EBS volumes in an attached state are encrypted with that KMS key\*1.

Options A and C are incorrect since these services cannot be used to check for unencrypted EBS volumes

Option D is incorrect because even though this is possible, trying to implement the solution alone with just the Lambda servk would be too difficult

For more information on IAM Config and encrypted volumes, please refer to below URL:

> <https://docs.IAM.amazon.com/config/latest/developerguide/encrypted-volumes.html>

Submit your Feedback/Queries to our Experts

**NEW QUESTION 313**

.....



## 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](#)**