



# Amazon-Web-Services

## Exam Questions SCS-C02

AWS Certified Security - Specialty

## About ExamBible

*[Your Partner of IT Exam](#)*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

### NEW QUESTION 1

- (Exam Topic 1)

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

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

The Security Engineer has verified the following:

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

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

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

**Answer:** CD

#### Explanation:

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

### NEW QUESTION 2

- (Exam Topic 1)

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

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

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

**Answer:** BC

### NEW QUESTION 3

- (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 4

- (Exam Topic 1)

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

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

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

**Answer:** AD

### NEW QUESTION 5

- (Exam Topic 1)

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

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

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

- A. IAM CloudFormation
- B. Amazon GuardDuty
- C. Amazon Inspector

- D. Amazon Macie
- E. IAM Step Functions

**Answer:** AE

#### NEW QUESTION 6

- (Exam Topic 1)

A 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 7

- (Exam Topic 1)

A company is outsourcing its operational support to an external company. The company's security officer must implement an access solution for delegating operational support that minimizes overhead.

Which approach should the security officer take to meet these requirements?

- A. implement Amazon Cognito identity pools with a role that uses a policy that denies the actions related to Amazon Cognito API management Allow the external company to federate through its identity provider
- B. Federate IAM identity and Access Management (IAM) with the external company's identity provider Create an IAM role and attach a policy with the necessary permissions
- C. Create an IAM group for the external company Add a policy to the group that denies IAM modifications Securely provide the credentials to the external company.
- D. Use IAM SSO with the external company's identity provider
- E. Create an IAM group to map to the identity provider user group, and attach a policy with the necessary permissions.

**Answer:** B

#### NEW QUESTION 8

- (Exam Topic 1)

Unapproved changes were previously made to a company's Amazon S3 bucket. A security engineer configured IAM Config to record configuration changes made to the company's S3 buckets. The engineer discovers there are S3 configuration changes being made, but no Amazon SNS notifications are being sent. The engineer has already checked the configuration of the SNS topic and has confirmed the configuration is valid.

Which combination of steps should the security engineer take to resolve the issue? (Select TWO.)

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

**Answer:** BE

#### NEW QUESTION 9

- (Exam Topic 1)

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

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

Which solution will meet these requirements?

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

**Answer:** A

#### NEW QUESTION 10

- (Exam Topic 1)

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 10

- (Exam Topic 1)

A Security Engineer is looking for a way to control access to data that is being encrypted under a CMK. The Engineer is also looking to use additional authenticated data (AAD) to prevent tampering with ciphertext.

Which action would provide the required functionality?

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

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 11

- (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 14

- (Exam Topic 1)

A company is trying to replace its on-premises bastion hosts used to access on-premises Linux servers with IAM Systems Manager Session Manager. A security engineer has installed the Systems Manager Agent on all servers. The security engineer verifies that the agent is running on all the servers, but Session Manager cannot connect to them. The security engineer needs to perform verification steps before Session Manager will work on the servers.

Which combination of steps should the security engineer perform? (Select THREE.)

- A. Open inbound port 22 to 0.0.0.0/0 on all Linux servers.
- B. Enable the advanced-instances tier in Systems Manager.
- C. Create a managed-instance activation for the on-premises servers.
- D. Reconfigure the Systems Manager Agent with the activation code and ID.
- E. Assign an IAM role to all of the on-premises servers.
- F. Initiate an inventory collection with Systems Manager on the on-premises servers

**Answer:** CEF

#### NEW QUESTION 17

- (Exam Topic 1)

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

What policy should the Engineer implement?

A

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

B

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

C

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



D

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

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

**Answer: B**

#### NEW QUESTION 22

- (Exam Topic 1)

While securing the connection between a company's VPC and its on-premises data center, a Security Engineer sent a ping command from an on-premises host (IP address 203.0.113.12) to an Amazon EC2 instance (IP address 172.31.16.139). The ping command did not return a response. The flow log in the VPC showed the following:

2 123456789010 eni-1235b8ca 203.0.113.12 172.31.16.139 0 0 1 4 336 1432917027 1432917142 ACCEPT OK

2 123456789010 eni-1235b8ca 172.31.16.139 203.0.113.12 0 0 1 4 336 1432917094 1432917142 REJECT OK

What action should be performed to allow the ping to work?

- A. In the security group of the EC2 instance, allow inbound ICMP traffic.
- B. In the security group of the EC2 instance, allow outbound ICMP traffic.
- C. In the VPC's NACL, allow inbound ICMP traffic.
- D. In the VPC's NACL, allow outbound ICMP traffic.

**Answer: D**

#### NEW QUESTION 23

- (Exam Topic 1)

A company's web application is hosted on Amazon EC2 instances running behind an Application Load Balancer (ALB) in an Auto Scaling group. An IAM WAF web ACL is associated with the ALB. IAM CloudTrail is enabled, and stores logs in Amazon S3 and Amazon CloudWatch Logs.

The operations team has observed some EC2 instances reboot at random. After rebooting, all access logs on the instances have been deleted. During an investigation, the operations team found that each reboot happened just after a PHP error occurred on the new-user-creation.php file. The operations team needs to view log information to determine if the company is being attacked.

Which set of actions will identify the suspect attacker's IP address for future occurrences?

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

**Answer: D**

#### Explanation:

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

#### NEW QUESTION 25

- (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 30

- (Exam Topic 1)

A company's Security Officer is concerned about the risk of IAM account root user logins and has assigned a Security Engineer to implement a notification solution for near-real-time alerts upon account root user logins.

How should the Security Engineer meet these requirements?

- A. Create a cron job that runs a script to download the IAM IAM security credentials W
- B. parse the file for account root user logins and email the Security team's distribution list
- C. Run IAM CloudTrail logs through Amazon CloudWatch Events to detect account root user logins and trigger an IAM Lambda function to send an Amazon SNS notification to the Security team's distribution list.
- D. Save IAM CloudTrail logs to an Amazon S3 bucket in the Security team's account Process the CloudTrail logs with the Security Engineer's logging solution for account root user logins Send an Amazon SNS notification to the Security team upon encountering the account root user login events
- E. Save VPC Flow Logs to an Amazon S3 bucket in the Security team's account and process the VPC Flow Logs with their logging solutions for account root user logins Send an Amazon SNS notification to the Security team upon encountering the account root user login events

**Answer:** B

#### NEW QUESTION 34

- (Exam Topic 1)

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

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

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

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

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

**Answer:** B

#### NEW QUESTION 36

- (Exam Topic 1)

A company has a VPC with an IPv6 address range and a public subnet with an IPv6 address block. The VPC currently hosts some public Amazon EC2 instances but a Security Engineer needs to migrate a second application into the VPC that also requires IPv6 connectivity.

This new application will occasionally make API requests to an external, internet-accessible endpoint to receive updates However, the Security team does not want the application's EC2 instance exposed directly to the internet The Security Engineer intends to create a private subnet with a custom route table and to associate the route table with the private subnet

What else does the Security Engineer need to do to ensure the application will not be exposed directly to the internet, but can still communicate as required"

- A. Launch a NAT instance in the public subnet Update the custom route table with a new route to the NAT instance
- B. Remove the internet gateway, and add IAM PrivateLink to the VPC Then update the custom route table with a new route to IAM PrivateLink
- C. Add a managed NAT gateway to the VPC Update the custom route table with a new route to the gateway
- D. Add an egress-only internet gateway to the VP
- E. Update the custom route table with a new route to the gateway

**Answer:** D

#### NEW QUESTION 38

- (Exam Topic 1)

The Development team receives an error message each time the team members attempt to encrypt or decrypt a Secure String parameter from the SSM Parameter Store by using an IAM KMS customer managed key (CMK).

Which CMK-related issues could be responsible? (Choose two.)

- A. The CMK specified in the application does not exist.
- B. The CMK specified in the application is currently in use.
- C. The CMK specified in the application is using the CMK KeyID instead of CMK Amazon Resource Name.
- D. The CMK specified in the application is not enabled.
- E. The CMK specified in the application is using an alias.

**Answer:** AD

#### Explanation:

[https://docs.amazonaws.cn/en\\_us/kms/latest/developerguide/services-parameter-store.html](https://docs.amazonaws.cn/en_us/kms/latest/developerguide/services-parameter-store.html)

#### NEW QUESTION 40

- (Exam Topic 1)

A company is running an application on Amazon EC2 instances in an Auto Scaling group. The application stores logs locally A security engineer noticed that logs were lost after a scale-in event. The security engineer needs to recommend a solution to ensure the durability and availability of log data All logs must be kept for a minimum of 1 year for auditing purposes



What should the security engineer recommend?

- A. Within the Auto Scaling lifecycle, add a hook to create and attach an Amazon Elastic Block Store (Amazon EBS) log volume each time an EC2 instance is create
- B. When the instance is terminated, the EBS volume can be reattached to another instance for log review.
- C. Create an Amazon Elastic File System (Amazon EFS) file system and add a command in the user data section of the Auto Scaling launch template to mount the EFS file system during EC2 instance creation Configure a process on the instance to copy the logs once a day from an instance Amazon Elastic Block Store (Amazon EBS) volume to a directory in the EFS file system.
- D. Build the Amazon CloudWatch agent into the AMI used in the Auto Scaling grou
- E. Configure the CloudWatch agent to send the logs to Amazon CloudWatch Logs for review.
- F. Within the Auto Scaling lifecycle, add a lifecycle hook at the terminating state transition and alert the engineering team by using a lifecycle notification to Amazon Simple Notification Service (Amazon SNS). Configure the hook to remain in the Terminating:Wait state for 1 hour to allow manual review of the security logs prior to instance termination.

**Answer: B**

#### NEW QUESTION 42

- (Exam Topic 1)

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

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

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

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

**Answer: DEF**

#### NEW QUESTION 44

- (Exam Topic 1)

A company hosts its public website on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances are in an EC2 Auto Scaling group across multiple Availability Zones. The website is under a DDoS attack by a specific IoT device brand that is visible in the user agent A security engineer needs to mitigate the attack without impacting the availability of the public website.

What should the security engineer do to accomplish this?

- A. Configure a web ACL rule for IAM WAF to block requests with a string match condition for the user agent of the IoT devic
- B. Associate the v/eb ACL with the ALB.
- C. Configure an Amazon CloudFront distribution to use the ALB as an origi
- D. Configure a web ACL rule for IAM WAF to block requests with a string match condition for the user agent of the IoT devic
- E. Associate the web ACL with the ALB Change the public DNS entry of the website to point to the CloudFront distribution.
- F. Configure an Amazon CloudFront distribution to use a new ALB as an origi
- G. Configure a web ACL rule for IAM WAF to block requests with a string match condition for the user agent of the IoT devic
- H. Change the ALB security group to alow access from CloudFront IP address ranges only Change the public DNS entry of the website to point to the CloudFront distribution.
- I. Activate IAM Shield Advanced to enable DDoS protectio
- J. Apply an IAM WAF ACL to the AL
- K. andconfigure a listener rule on the ALB to block IoT devices based on the user agent.

**Answer: D**

#### NEW QUESTION 45

- (Exam Topic 1)

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

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

- A. One in the US West (Oregon) region and one in the US East (Virginia) region.
- B. Two in the US West (Oregon) region and none in the US East (Virginia) region.
- C. One in the US West (Oregon) region and none in the US East (Virginia) region.
- D. Two in the US East (Virginia) region and none in the US West (Oregon) region.

**Answer: A**

#### Explanation:

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

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

#### NEW QUESTION 50

- (Exam Topic 1)

A security engineer has noticed that VPC Flow Logs are getting a lot REJECT traffic originating from a single Amazon EC2 instance in an Auto Scaling group. The security engineer is concerned that this EC2 instance may be compromised.

What immediate action should the security engineer take? What immediate action should the security engineer take?

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

**Answer: B**

#### NEW QUESTION 52

- (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 role.
- 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 55

- (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 classificatio
- D. For identified objects that contain PII, use the research function for auditing IAM CloudTrail logs and S3 bucket logs for GET operations.
- E. Enable Amazon GuardDuty and enable the PII rule set on the S3 buckets that were impacted, then perform data classificatio
- F. Using the PII findings report from GuardDuty, query the S3 bucket logs by using Athena for GET operations.
- G. Enable Amazon Inspector on the S3 buckets that were impacted, then perform data classificatio
- H. For identified objects that contain PII, query the S3 bucket logs by using Athena for GET operations.

**Answer:** B

#### NEW QUESTION 57

- (Exam Topic 2)

A company has enabled Amazon GuardDuty in all Regions as part of its security monitoring strategy. In one of the VPCs, the company hosts an Amazon EC2 instance working as an FTP server that is contacted by a high number of clients from multiple locations. This is identified by GuardDuty as a brute force attack due to the high number of connections that happen every hour.

The finding has been flagged as a false positive. However, GuardDuty keeps raising the issue. A Security Engineer has been asked to improve the signal-to-noise ratio. The Engineer needs to ensure that changes do not compromise the visibility of potential anomalous behavior.

How can the Security Engineer address the issue?

- A. Disable the FTP rule in GuardDuty in the Region where the FTP server is deployed
- B. Add the FTP server to a trusted IP list and deploy it to GuardDuty to stop receiving the notifications
- C. Use GuardDuty filters with auto archiving enabled to close the findings
- D. Create an IAM Lambda function that closes the finding whenever a new occurrence is reported

**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.

#### NEW QUESTION 58

- (Exam Topic 2)

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

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

Why did GuardDuty fail to alert to this behavior?

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 62

- (Exam Topic 2)

A security team must present a daily briefing to the CISO that includes a report of which of the company's thousands of EC2 instances and on-premises servers are missing the latest security patches. All instances/servers must be brought into compliance within 24 hours so they do not show up on the next day's report.

How can the security team fulfill these requirements?

Please select:

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

**Answer:** B

#### Explanation:

Use the Systems Manger Patch Manger to generate the report and also install the missing patches The IAM Documentation mentions the following

IAM Systems Manager Patch Manager automates the process of patching managed instances with

security-related updates. For Linux-based instances, you can also install patches for non-security updates. You can patch fleets of Amazon EC2 instances or your on-premises servers and virtual machines (VMs) by operating system type. This includes supported versions of Windows, Ubuntu Server, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), and Amazon Linux. You can scan instances to see only a report of missing patches, or you can scan and automatically install all missing patches.

Option A is invalid because Amazon QuickSight and Cloud Trail cannot be used to generate the list of servers that don't meet compliance needs.

Option C is wrong because deploying instances via new AMI'S would impact the applications hosted on these servers

Option D is invalid because Amazon Trusted Advisor cannot be used to generate the list of servers that don't meet compliance needs.

For more information on the IAM Patch Manager, please visit the below URL: <https://docs.IAM.amazon.com/systems-manager/latest/userguide/systems-manager-patch.html> (

The correct answer is: Use Systems Manger Patch Manger to generate the report of out of compliance instances/ servers. Use Systems Manager Patch Manger to install the missing patches.

Submit your Feedback/Queries to our Experts



#### NEW QUESTION 66

- (Exam Topic 2)

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

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

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 68

- (Exam Topic 2)

An organization wants to deploy a three-tier web application whereby the application servers run on Amazon EC2 instances. These EC2 instances need access to credentials that they will use to authenticate their SQL connections to an Amazon RDS DB instance. Also, IAM Lambda functions must issue queries to the RDS database by using the same database credentials.

The credentials must be stored so that the EC2 instances and the Lambda functions can access them. No other access is allowed. The access logs must record when the credentials were accessed and by whom.

What should the Security Engineer do to meet these requirements?

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

**Answer:** D

#### NEW QUESTION 71

- (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 75

- (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 79

- (Exam Topic 2)

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

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

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

Answer: AE

#### Explanation:

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

#### NEW QUESTION 81

- (Exam Topic 2)

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

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

The IAM user policy is as follows:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        <Action>
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:012345678910:key/ebs-encryption-key"
      ]
    },
    {
      "Effect": "Deny",
      "Action": [
        "ec2:StartInstances"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "Bool": {
          "aws:SecureTransport": "false"
        }
      }
    }
  ]
}
```

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

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

Answer: CE

#### Explanation:

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

#### NEW QUESTION 85

- (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 monitoring.

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 87

- (Exam Topic 2)

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

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

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

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 92

- (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.amazonaws.com/kms/latest/developerguide/importing-keys-delete-key-material.html>

#### NEW QUESTION 94

- (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:

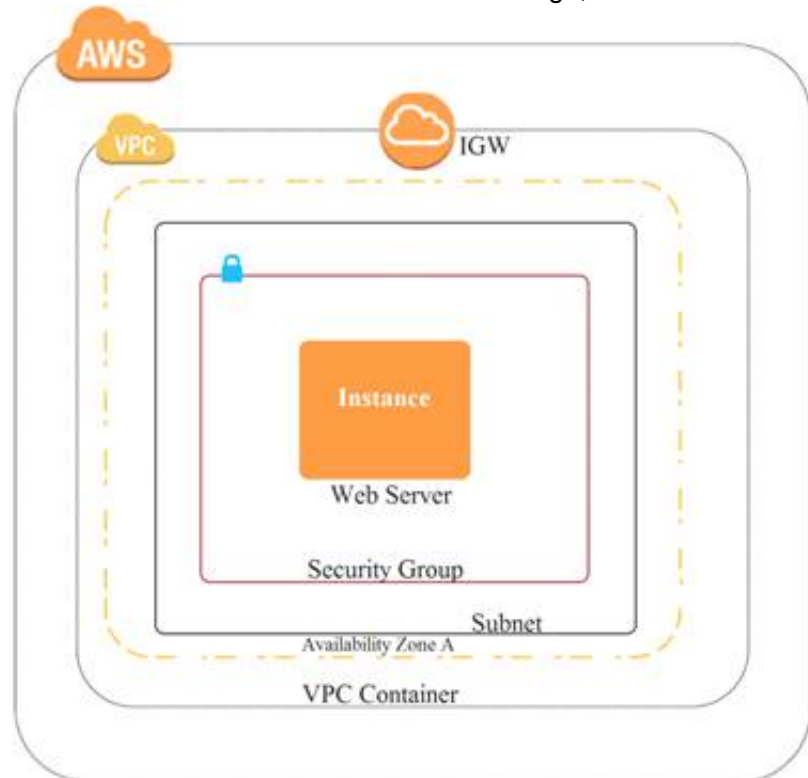
<https://docs.IAM.amazonaws.com/AmazonCloudWatch/latest/monitoring/cloudwatch-and-interface-VPC.html>

#### NEW QUESTION 97

- (Exam Topic 2)

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

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



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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 100**

- (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 104**

- (Exam Topic 2)

Your company has mandated that all calls to the IAM KMS service be recorded. How can this be achieved? Please select:

- A. Enable logging on the KMS service
- B. Enable a trail in CloudTrail
- C. Enable CloudWatch logs
- D. Use CloudWatch metrics

**Answer:** B

**Explanation:**

The IAM Documentation states the following

IAM KMS is integrated with CloudTrail, a service that captures API calls made by or on behalf of IAM KMS in your IAM account and delivers the log files to an Amazon S3 bucket that you specify. CloudTrail captures

API calls from the IAM KMS console or from the IAM KMS API. Using the information collected by CloudTrail, you can determine what request was made, the source IP address from which the request was made, who made the request when it was made, and so on.

Option A is invalid because logging is not possible in the KMS service

Option C and D are invalid because CloudWatch cannot be used to monitor API calls For more information on logging using CloudTrail please visit the below URL

<https://docs.IAM.amazon.com/kms/latest/developerguide/logging-using-cloudtrail.html> The correct answer is: Enable a trail in CloudTrail

Submit your Feedback/Queries to our Experts

**NEW QUESTION 108**

- (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 113**

- (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 114

- (Exam Topic 2)

You are hosting a web site via website hosting on an S3 bucket - [http://demo.s3-website-us-east-1](http://demo.s3-website-us-east-1.amazonaws.com)

.amazon.com. You have some web pages that use Javascript that access resources in another bucket which has web site hosting also enabled. But when users access the web pages, they are getting a blocked Javascript error. How can you rectify this?

Please select:

- A. Enable CORS for the bucket
- B. Enable versioning for the bucket
- C. Enable MFA for the bucket
- D. Enable CRR for the bucket

**Answer:** A

#### Explanation:

Your answer is incorrect Answer-A

Such a scenario is also given in the IAM Documentation Cross-Origin Resource Sharing: Use-case Scenarios The following are example scenarios for using CORS:

- Scenario 1: Suppose that you are hosting a website in an Amazon S3 bucket named website as described in Hosting a Static Website on Amazon S3. Your users load the website endpoint <http://website.s3-website-us-east-1.amazonaws.com>. Now you want to use JavaScript on the webpages that are stored in this bucket to be able to make authenticated GET and PUT requests against the same bucket by using the Amazon S3 API endpoint for the bucket [website.s3.amazonaws.com](http://website.s3.amazonaws.com). A browser would normally block JavaScript from allowing those requests, but with CORS you can configure your bucket to explicitly enable cross-origin requests from [website.s3-website-us-east-1.amazonaws.com](http://website.s3-website-us-east-1.amazonaws.com).
- Scenario 2: Suppose that you want to host a web font from your S3 bucket. Again, browsers require a CORS check (also called a preflight check) for loading web fonts. You would configure the bucket that is hosting the web font to allow any origin to make these requests.

Option B is invalid because versioning is only to create multiple versions of an object and can help in accidental deletion of objects

Option C is invalid because this is used as an extra measure of caution for deletion of objects Option D is invalid because this is used for Cross region replication of objects

For more information on Cross Origin Resource sharing, please visit the following URL

- <https://docs.IAM.amazonaws.com/AmazonS3/latest/dev/cors.html> The correct answer is: Enable CORS for the bucket

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 115

- (Exam Topic 2)

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

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

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

**Answer:** ACE

#### Explanation:

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

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

#### NEW QUESTION 117

- (Exam Topic 2)

A company runs an application on IAM that needs to be accessed only by employees. Most employees work from the office, but others work remotely or travel. How can the Security Engineer protect this workload so that only employees can access it?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 120**

- (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 121**

- (Exam Topic 2)

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 125**

- (Exam Topic 2)

A Developer's laptop was stolen. The laptop was not encrypted, and it contained the SSH key used to access multiple Amazon EC2 instances. A Security Engineer has verified that the key has not been used, and has blocked port 22 to all EC2 instances while developing a response plan. How can the Security Engineer further protect currently running instances?

- A. Delete the key-pair key from the EC2 console, then create a new key pair.
- B. Use the modify-instance-attribute API to change the key on any EC2 instance that is using the key.
- C. Use the EC2 RunCommand to modify the authorized\_keys file on any EC2 instance that is using the key.
- D. Update the key pair in any AMI used to launch the EC2 instances, then restart the EC2 instances.

**Answer:** C

**NEW QUESTION 126**

- (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 127**

- (Exam Topic 2)

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

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



required.  
E. Store the encrypted data key alongside the encrypted data  
F. Use the Decrypt API to retrieve the data key to decrypt the data when required.

**Answer: D**

**Explanation:**

We recommend that you use the following pattern to locally encrypt data: call the GenerateDataKey API, use the key returned in the Plaintext response field to locally encrypt data, and then erase the plaintext data key from memory. Store the encrypted data key (contained in the CiphertextBlob field) alongside of the locally encrypted data. The Decrypt API returns the plaintext key from the encrypted key.

<https://docs.IAM.amazon.com/sdkfornet/latest/apidocs/items/MKeyManagementServiceKeyManagementService>

**NEW QUESTION 132**

- (Exam Topic 2)

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

Please select:

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

**Answer: D**

**Explanation:**

The IAM Documentation states the following

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

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

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

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

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

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

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

- IAM/elasticfilesystem 1 IAM/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 CMK

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

Rotation period for CMKs is as follows:

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

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

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

Submit your Feedback/Queries to our Experts

**NEW QUESTION 136**

- (Exam Topic 2)

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

A user is unable to assume the IAM role in the target account. The policy attached to the role in the identity account is:

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

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



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

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

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

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

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

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

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

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

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

**Answer: A**

#### NEW QUESTION 139

- (Exam Topic 2)

Your company has defined privileged users for their IAM Account. These users are administrators for key resources defined in the company. There is now a mandate to enhance the security authentication for these users. How can this be accomplished?

Please select:

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

**Answer: A**

**Explanation:**

The IAM Documentation mentions the following as a best practices for IAM users. For extra security, enable multi-factor authentication (MFA) for privileged IAM users (users who are allowed access to sensitive resources or APIs). With MFA, users have a device that generates unique authentication code (a one-time password, or OTP). Users must provide both their normal credentials (like their user name and password) and the OTP. The MFA device can either be a special piece of hardware, or it can be a virtual device (for example, it can run in an app on a smartphone).

Option B,C and D are invalid because no such security options are available in IAM For more information on IAM best practices, please visit the below URL

<https://docs.IAM.amazon.com/IAM/latest/UserGuide/best-practices.html> The correct answer is: Enable MFA for these user accounts

Submit your Feedback/Queries to our Experts

**NEW QUESTION 143**

- (Exam Topic 2)

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

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

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

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

**Answer:** ACE

**NEW QUESTION 145**

- (Exam Topic 2)

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

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

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

**Answer:** D

**Explanation:**

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

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

**NEW QUESTION 146**

- (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 148**

- (Exam Topic 2)

You have just recently set up a web and database tier in a VPC and hosted the application. When testing the app , you are not able to reach the home page for the app. You have verified the security groups. What can help you diagnose the issue.

Please select:

- A. Use the IAM Trusted Advisor to see what can be done.
- B. Use VPC Flow logs to diagnose the traffic
- C. Use IAM WAF to analyze the traffic
- D. Use IAM Guard Duty to analyze the traffic

**Answer:** B

**Explanation:**

Option A is invalid because this can be used to check for security issues in your account, but not verify as to why you cannot reach the home page for your application

Option C is invalid because this used to protect your app against application layer attacks, but not verify as to why you cannot reach the home page for your application

Option D is invalid because this used to protect your instance against attacks, but not verify as to why you cannot reach the home page for your application

The IAM Documentation mentions the following

VPC Flow Logs capture network flow information for a VPC, subnet or network interface and stores it in Amazon CloudWatch Logs. Flow log data can help customers troubleshoot network issues; for example, to diagnose why specific traffic is not reaching an instance, which might be a result of overly restrictive security group rules. Customers can also use flow logs as a security tool to monitor the traffic that reaches their instances, to profile network traffic, and to look for abnormal traffic behaviors.

For more information on IAM Security, please visit the following URL: <https://IAM.amazon.com/answers/networking/vpc-security-capabilities>

The correct answer is: Use VPC Flow logs to diagnose the traffic Submit your Feedback/Queries to our Experts

**NEW QUESTION 149**

- (Exam Topic 2)

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

Please select:

A. Consider using the IAM Shield Service

B. Consider using VPC Flow logs to monitor traffic for DDos attack and quickly take actions on a trigger of a potential attack.

C. Consider using the IAM Shield Advanced Service

D. Consider using Cloudwatch logs to monitor traffic for DDos attack and quickly take actions on a trigger of a potential attack.

**Answer: C**

**Explanation:**

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

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

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

The IAM Documentation mentions the following

IAM Shield Advanced provides enhanced protections for your applications running on Amazon EC2. Elastic Load Balancing (ELB), Amazon CloudFront and Route 53 against larger and more sophisticated attacks. IAM Shield Advanced is available to IAM Business Support and IAM Enterprise Support customers. IAM Shield Advanced protection provides always-on, flow-based monitoring of network traffic and active application monitoring to provide near real-time notifications of DDos attacks. IAM Shield Advanced also gives customers highly flexible controls over attack mitigations to take actions instantly. Customers can also engage the DDos Response Team (DRT) 24X7 to manage and mitigate their application layer DDos attacks.

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

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

**NEW QUESTION 154**

- (Exam Topic 2)

An organization receives an alert that indicates that an EC2 instance behind an ELB Classic Load Balancer has been compromised.

What techniques will limit lateral movement and allow evidence gathering?

A. Remove the instance from the load balancer and terminate it.

B. Remove the instance from the load balancer, and shut down access to the instance by tightening the security group.

C. Reboot the instance and check for any Amazon CloudWatch alarms.

D. Stop the instance and make a snapshot of the root EBS volume.

**Answer: B**

**Explanation:**

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

**NEW QUESTION 157**

- (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 161**

- (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 165

- (Exam Topic 2)

Amazon CloudWatch Logs agent is successfully delivering logs to the CloudWatch Logs service. However, logs stop being delivered after the associated log stream has been active for a specific number of hours.

What steps are necessary to identify the cause of this phenomenon? (Choose two.)

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

**Answer:** AB

**Explanation:**

[https://acloud.guru/forums/IAM-certified-security-specialty/discussion/-Lm5A3w6\\_NybQPhh6tRP/Cloudwatch](https://acloud.guru/forums/IAM-certified-security-specialty/discussion/-Lm5A3w6_NybQPhh6tRP/Cloudwatch)

#### NEW QUESTION 167

- (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-volurnn

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 169

- (Exam Topic 3)

An auditor needs access to logs that record all API events on IAM. The auditor only needs read-only access to the log files and does not need access to each IAM account. The company has multiple IAM accounts, and the auditor needs access to all the logs for all the accounts. What is the best way to configure access for the auditor to view event logs from all accounts? Choose the correct answer from the options below

Please select:

- A. Configure the CloudTrail service in each IAM account, and have the logs delivered to an IAM bucket on each account, while granting the auditor permissions to the bucket via roles in the secondary accounts and a single primary IAM account that can assume a read-only role in the secondary IAM accounts.
- B. Configure the CloudTrail service in the primary IAM account and configure consolidated billing for all the secondary account
- C. Then grant the auditor access to the S3 bucket that receives the CloudTrail log files.
- D. Configure the CloudTrail service in each IAM account and enable consolidated logging inside of CloudTrail.
- E. Configure the CloudTrail service in each IAM account and have the logs delivered to a single IAM bucket in the primary account and erant the auditor access to that single bucket in the orimarv account.

**Answer:** D

**Explanation:**

Given the current requirements, assume the method of "least privilege" security design and only allow the auditor access to the minimum amount of IAM resources as possibli

IAM CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your IAM account. With CloudTrail, you can log, continuously monitor, and retain events related to API calls across your IAM infrastructure. CloudTrail provides a history of IAM API calls for your account including API calls made through the IAM Management Console, IAM SDKs, command line tools, and other IAM services. This history simplifies security analysis, resource change tracking, and troubleshooting



only be granted access in one location

Option Option A is incorrect since the auditor should B is incorrect since consolidated billing is not a key requirement as part of the question

Option C is incorrect since there is not consolidated logging

For more information on Cloudtrail please refer to the below URL: <https://IAM.amazon.com/cloudtrail>

(

The correct answer is: Configure the CloudTrail service in each IAM account and have the logs delivered to a single IAM bud in the primary account and grant the auditor access to that single bucket in the primary account.

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 173

- (Exam Topic 3)

Your company has the following setup in IAM

\* a. A set of EC2 Instances hosting a web application

\* b. An application load balancer placed in front of the EC2 Instances

There seems to be a set of malicious requests coming from a set of IP addresses. Which of the following can be used to protect against these requests?

Please select:

A. Use Security Groups to block the IP addresses

B. Use VPC Flow Logs to block the IP addresses

C. Use IAM inspector to block the IP addresses

D. Use IAM WAF to block the IP addresses

**Answer: D**

#### Explanation:

Your answer is incorrect Answer -D

The IAM Documentation mentions the following on IAM WAF which can be used to protect Application Load Balancers and Cloud front

A web access control list (web ACL) gives you fine-grained control over the web requests that your Amazon CloudFront distributions or Application Load Balancers respond to. You can allow or block the following types of requests:

Originate from an IP address or a range of IP addresses Originate from a specific country or countries

Contain a specified string or match a regular expression (regex) pattern in a particular part of requests Exceed a specified length

Appear to contain malicious SQL code (known as SQL injection) Appear to contain malicious scripts (known as cross-site scripting)

Option A is invalid because by default Security Groups have the Deny policy

Options B and C are invalid because these services cannot be used to block IP addresses For information on IAM WAF, please visit the below URL:

<https://docs.IAM.amazon.com/waf/latest/developerguide/web-acl.html>

The correct answer is: Use IAM WAF to block the IP addresses Submit your Feedback/Queries to our Experts

#### NEW QUESTION 174

- (Exam Topic 3)

What is the result of the following bucket policy?

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

Choose the correct Answer Please select:

A. It will allow all access to the bucket mybucket

B. It will allow the user mark from IAM account number 111111111 all access to the bucket but deny everyone else all access to the bucket

C. It will deny all access to the bucket mybucket

D. None of these

**Answer: C**



**Explanation:**

The policy consists of 2 statements, one is the allow for the user mark to the bucket and the next is the deny policy for all other users. The deny permission will override the allow and hence all users will not have access to the bucket.

Options A,B and D are all invalid because this policy is used to deny all access to the bucket mybucket For examples on S3 bucket policies, please refer to the below Link: <http://docs.IAM.amazon.com/AmazonS3/latest/dev/example-bucket-policies.html>

The correct answer is: It will deny all access to the bucket mybucket Submit your Feedback/Quenes to our Experts

**NEW QUESTION 179**

- (Exam Topic 3)

An employee keeps terminating EC2 instances on the production environment. You've determined the best way to ensure this doesn't happen is to add an extra layer of defense against terminating the instances. What is the best method to ensure the employee does not terminate the production instances? Choose the 2 correct answers from the options below

Please select:

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

**Answer:** AB

**Explanation:**

Tags enable you to categorize your IAM resources in different ways, for example, by purpose, owner, or environment. This is useful when you have many resources of the same type — you can quickly identify a specific resource based on the tags you've assigned to it. Each tag consists of a key and an optional value, both of which you define

Options C&D are incorrect because it will not ensure that the employee cannot terminate the instance. For more information on tagging answer resources please refer to the below URL:

[http://docs.IAM.amazon.com/IAMEC2/latest/UserGuide/Usins\\_Tags.html](http://docs.IAM.amazon.com/IAMEC2/latest/UserGuide/Usins_Tags.html)

The correct answers are: Tag the instance with a production-identifying tag and add resource-level permissions to the employe user with an explicit deny on the terminate API call to instances with the production tag.. Tag the instance with a production-identifying tag and modify the employees group to allow only start stop, and reboot API calls and not the terminate instance

Submit your Feedback/Queries to our Experts

**NEW QUESTION 181**

- (Exam Topic 3)

A company hosts data in S3. There is a requirement to control access to the S3 buckets. Which are the 2 ways in which this can be achieved?

Please select:

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

**Answer:** AC

**Explanation:**

The IAM Documentation mentions the following

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

Option B and D are invalid because these cannot be used to control access to S3 buckets For more information on S3 access control, please refer to the below Link: <https://docs.IAM.amazon.com/AmazonS3/latest/dev/s3-access-control.html>

The correct answers are: Use Bucket policies. Use IAM user policies Submit your Feedback/Queries to our Experts

**NEW QUESTION 185**

- (Exam Topic 3)

Your company is planning on developing an application in IAM. This is a web based application. The application users will use their facebook or google identities for authentication. You want to have the ability to manage user profiles without having to add extra coding to manage this. Which of the below would assist in this. Please select:

- A. Create an OIDC identity provider in IAM
- B. Create a SAML provider in IAM
- C. Use IAM Cognito to manage the user profiles
- D. Use IAM users to manage the user profiles

**Answer:** B

**Explanation:**

The IAM Documentation mentions the following The IAM Documentation mentions the following

OIDC identity providers are entities in IAM that describe an identity provider (IdP) service that supports the OpenID Connect (OIDC) standard. You use an OIDC identity provider when you want to establish trust between an OIDC-compatible IdP—such as Google, Salesforce, and many others—and your IAM account This is useful if you are creating a mobile app or web application that requires access to IAM resources, but you don't want to create custom sign-in code or manage your own user identities

Option A is invalid because in the security groups you would not mention this information/ Option C is invalid because SAML is used for federated authentication

Option D is invalid because you need to use the OIDC identity provider in IAM For more information on ODIC identity providers, please refer to the below Link:

[https://docs.IAM.amazon.com/IAM/latest/UserGuide/id\\_roles\\_providers\\_create\\_oidc.html](https://docs.IAM.amazon.com/IAM/latest/UserGuide/id_roles_providers_create_oidc.html) The correct answer is: Create an OIDC identity provider in IAM

**NEW QUESTION 189**

- (Exam Topic 3)

You need to establish a secure backup and archiving solution for your company, using IAM. Documents should be immediately accessible for three months and available for five years for compliance reasons. Which IAM service fulfills these requirements in the most cost-effective way? Choose the correct Answer Please select:

- A. Upload data to S3 and use lifecycle policies to move the data into Glacier for long-term archiving.
- B. Upload the data on EBS, use lifecycle policies to move EBS snapshots into S3 and later into Glacier for long-term archiving.
- C. Use Direct Connect to upload data to S3 and use IAM policies to move the data into Glacier for long-term archiving.
- D. Use Storage Gateway to store data to S3 and use lifecycle policies to move the data into Redshift for long-term archiving.

**Answer:** A

**Explanation:**

amazon Glacier is a secure, durable, and extremely low-cost cloud storage service for data archiving and long-term backup. Customers can reliably store large or small amounts of data for as little as \$0,004 per gigabyte per month, a significant savings compared to on-premises solutions.

With Amazon lifecycle policies you can create transition actions in which you define when objects transition to another Amazon S3 storage class. For example, you may choose to transition objects to the STANDARD\_IA (IA, for infrequent access) storage class 30 days after creation, or archive objects to the GLACIER storage class one year after creation.

Option B is invalid because lifecycle policies are not available for EBS volumes Option C is invalid because IAM policies cannot be used to move data to Glacier

Option D is invalid because lifecycle policies is not used to move data to Redshift For more information on S3 lifecycle policies, please visit the URL:

<http://docs.IAM.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html>

The correct answer is: Upload data to S3 and use lifecycle policies to move the data into Glacier for long-term archiving.

Submit your Feedback/Queries to our Experts

**NEW QUESTION 190**

- (Exam Topic 3)

A company has an existing IAM account and a set of critical resources hosted in that account. The employee who was in-charge of the root account has left the company. What must be now done to secure the account. Choose 3 answers from the options given below.

Please select:

- A. Change the access keys for all IAM users.
- B. Delete all custom created IAM policies
- C. Delete the access keys for the root account
- D. Confirm MFA to a secure device
- E. Change the password for the root account
- F. Change the password for all IAM users

**Answer:** CDE

**Explanation:**

Now if the root account has a chance to be compromised, then you have to carry out the below steps

\* 1. Delete the access keys for the root account

\* 2. Confirm MFA to a secure device

\* 3. Change the password for the root account

This will ensure the employee who has left has no change to compromise the resources in IAM. Option A is invalid because this would hamper the working of the current IAM users

Option B is invalid because this could hamper the current working of services in your IAM account Option F is invalid because this would hamper the working of the current IAM users

For more information on IAM root user, please visit the following URL: <https://docs.IAM.amazon.com/IAM/latest/UserGuide/id-root-user.html>

The correct answers are: Delete the access keys for the root account Confirm MFA to a secure device. Change the password for the root account

Submit Your Feedback/Queries to our Experts

**NEW QUESTION 191**

- (Exam Topic 3)

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

Please select:

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

**Answer:** CD

**Explanation:**

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

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

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

EBS Lifecycle Policies

A lifecycle policy consists of these core settings:

- Resource type—The IAM resource managed by the policy, in this case, EBS volumes.

- Target tag—The tag that must be associated with an EBS volume for it to be managed by the policy.

- Schedule—Defines how often to create snapshots and the maximum number of snapshots to keep. Snapshot creation starts within an hour of the specified start time. If creating a new snapshot exceeds the maximum number of snapshots to keep for the volume, the oldest snapshot is deleted.

Option C is correct. Each Amazon EBS volume is automatically replicated within its Availability Zone to protect you from component failure, offering high availability

and durability. But it does not have an explicit feature like that.

Option D is correct Encryption does not ensure data durability

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

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

#### NEW QUESTION 195

- (Exam Topic 3)

You have a set of application , database and web servers hosted in IAM. The web servers are placed behind an ELB. There are separate security groups for the application, database and web servers. The network security groups have been defined accordingly. There is an issue with the communication between the application and database servers. In order to troubleshoot the issue between just the application and database server, what is the ideal set of MINIMAL steps you would take?

Please select:

- A. Check the Inbound security rules for the database security group Check the Outbound security rules for the application security group
- B. Check the Outbound security rules for the database security group I Check the inbound security rules for the application security group
- C. Check the both the Inbound and Outbound security rules for the database security group Check the inbound security rules for the application security group
- D. Check the Outbound security rules for the database security group Check the both the Inbound and Outbound security rules for the application security group

**Answer: A**

#### Explanation:

Here since the communication would be established inward to the database server and outward from the application server, you need to ensure that just the Outbound rules for application server security groups are checked. And then just the Inbound rules for database server security groups are checked.

Option B can't be the correct answer. It says that we need to check the outbound security group which is not needed.

We need to check the inbound for DB SG and outbound of Application SG. Because, this two group need to communicate with each other to function properly.

Option C is invalid because you don't need to check for Outbound security rules for the database security group

Option D is invalid because you don't need to check for Inbound security rules for the application security group

For more information on Security Groups, please refer to below URL:

The correct answer is: Check the Inbound security rules for the database security group Check the Outbound security rules for the application security group

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 197

- (Exam Topic 3)

You want to ensure that you keep a check on the Active EBS Volumes, Active snapshots and Elastic IP addresses you use so that you don't go beyond the service limit. Which of the below services can help in this regard?

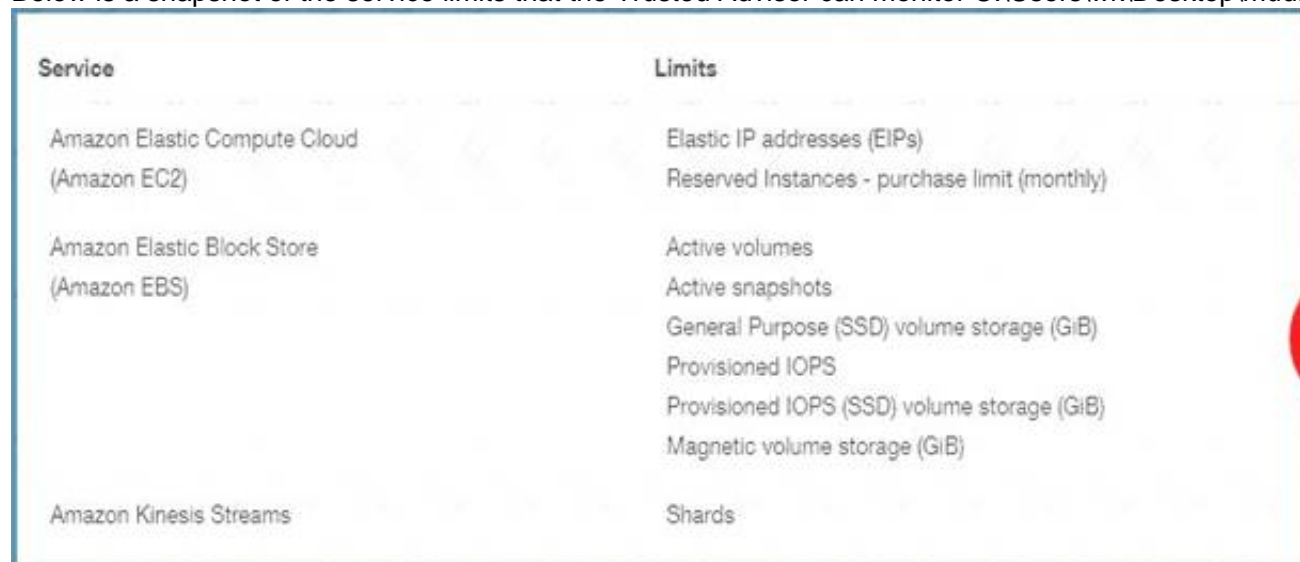
Please select:

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

**Answer: C**

#### Explanation:

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



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

Option A is invalid because even though you can monitor resources, it cannot be checked against the service limit.

Option B is invalid because this is the Elastic Compute cloud service Option D is invalid because it can be send notification but not check on service limit For more information on the Trusted Advisor monitoring, please visit the below URL:

<https://IAM.amazon.com/premiumsupport/ta-faqs>> The correct answer is: IAM Trusted Advisor Submit your Feedback/Queries to our Experts

#### NEW QUESTION 202

- (Exam Topic 3)

One of the EC2 Instances in your company has been compromised. What steps would you take to ensure that you could apply digital forensics on the Instance.

Select 2 answers from the options given below

Please select:

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

**Answer:** BC

**Explanation:**

Option A is invalid because removing the role will not help completely in such a situation

Option D is invalid because terminating the instance means that you cannot conduct forensic analysis on the instance

One way to isolate an affected EC2 instance for investigation is to place it in a Security Group that only the forensic investigators can access. Close all ports except to receive inbound SSH or RDP traffic from one single IP address from which the investigators can safely examine the instance.

For more information on security scenarios for your EC2 Instance, please refer to below URL: <https://d1.IAMstatic.com/Marketplace/scenarios/security/SEC 11 TSB Final.pdf>

The correct answers are: Create a separate forensic instance. Ensure that the security groups only allow communication to this forensic instance

Submit your Feedback/Queries to our Experts

**NEW QUESTION 204**

- (Exam Topic 3)

A company hosts critical data in an S3 bucket. Even though they have assigned the appropriate permissions to the bucket, they are still worried about data deletion. What measures can be taken to restrict the risk of data deletion on the bucket. Choose 2 answers from the options given below

Please select:

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

**Answer:** AC

**Explanation:**

One of the IAM Security blogs mentions the following

Versioning keeps multiple versions of an object in the same bucket. When you enable it on a bucket Amazon S3 automatically adds a unique version ID to every object stored in the bucket. At that point, a simple DELETE action does not permanently delete an object version; it merely associates a delete marker with the object. If you want to permanently delete an object version, you must specify its version ID in your DELETE request.

You can add another layer of protection by enabling MFA Delete on a versioned bucket. Once you do so, you must provide your IAM accounts access keys and a valid code from the account's MFA device in order to permanently delete an object version or suspend or reactivate versioning on the bucket.

Option B is invalid because enabling encryption does not guarantee risk of data deletion. Option D is invalid because this option does not guarantee risk of data deletion.

For more information on IAM S3 versioning and MFA please refer to the below URL: <https://IAM.amazon.com/blogs/security/securing-access-to-IAM-using-mfa-part-3/>

The correct answers are: Enable versioning on the S3 bucket Enable MFA Delete in the bucket policy Submit your Feedback/Queries to our Experts

**NEW QUESTION 208**

- (Exam Topic 3)

Your current setup in IAM consists of the following architecture. 2 public subnets, one subnet which has the web servers accessed by users across the internet and the other subnet for the database server. Which of the following changes to the architecture would add a better security boundary to the resources hosted in your setup

Please select:

- A. Consider moving the web server to a private subnet
- B. Consider moving the database server to a private subnet
- C. Consider moving both the web and database server to a private subnet
- D. Consider creating a private subnet and adding a NAT instance to that subnet

**Answer:** B

**Explanation:**

The ideal setup is to ensure that the web server is hosted in the public subnet so that it can be accessed by users on the internet. The database server can be hosted in the private subnet.

The below diagram from the IAM Documentation shows how this can be setup

Option A and C are invalid because if you move the web server to a private subnet, then it cannot be accessed by users Option D is invalid because NAT instances should be present in the public subnet

For more information on public and private subnets in IAM, please visit the following url [com/AmazonVPC/latest/UserGuide/VPC Scenario2](https://com/AmazonVPC/latest/UserGuide/VPC%20Scenario2).

The correct answer is: Consider moving the database server to a private subnet Submit your Feedback/Queries to our Experts

**NEW QUESTION 213**

- (Exam Topic 3)

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

Please select:

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

**Answer:** BD

**Explanation:**

The IAM Documentation mentions the following

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

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

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



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

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

**NEW QUESTION 217**

- (Exam Topic 3)

An organization has setup multiple IAM users. The organization wants that each IAM user accesses the IAM console only within the organization and not from outside. How can it achieve this?

Please select:

- A. Create an IAM policy with the security group and use that security group for IAM console login
- B. Create an IAM policy with a condition which denies access when the IP address range is not from the organization
- C. Configure the EC2 instance security group which allows traffic only from the organization's IP range
- D. Create an IAM policy with VPC and allow a secure gateway between the organization and IAM Console

**Answer: B**

**Explanation:**

You can actually use a Deny condition which will not allow the person to log in from outside. The below example shows the Deny condition to ensure that any address specified in the source address is not allowed to access the resources in IAM.

Option A is invalid because you don't mention the security group in the IAM policy Option C is invalid because security groups by default don't allow traffic

Option D is invalid because the IAM policy does not have such an option For more information on IAM policy conditions, please visit the URL:

<http://docs.IAM.amazon.com/IAM/latest/UserGuide/access>

pol examples.htm l#iam-policy-example-ec2-two-condition!

The correct answer is: Create an IAM policy with a condition which denies access when the IP address range is not from the organization

Submit your Feedback/Queries to our Experts

**NEW QUESTION 222**

- (Exam Topic 3)

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

Please select:

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

**Answer: ABC**

**Explanation:**

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

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

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

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

Submit your Feedback/Queries to our Experts

**NEW QUESTION 227**

- (Exam Topic 3)

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

Please select:

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

**Answer: B**

**Explanation:**

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

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

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

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

**NEW QUESTION 231**

- (Exam Topic 3)

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

Please select:

- A. Create an Identity and Access Management (IAM) user for CloudFront and grant access to the objects in your S3 bucket to that IAM User.
- B. Create an Origin Access Identity (OAI) for CloudFront and grant access to the objects in your S3 bucket to that OAI.



- C. Create individual policies for each bucket the documents are stored in and in that policy grant access to only CloudFront.  
D. Create an S3 bucket policy that lists the CloudFront distribution ID as the Principal and the target bucket as the Amazon Resource Name (ARN).

**Answer:** B

**Explanation:**

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

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

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

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

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

(

Submit your Feedback/Queries to our Experts

**NEW QUESTION 232**

- (Exam Topic 3)

A user has enabled versioning on an S3 bucket. The user is using server side encryption for data at Rest. If the user is supplying his own keys for encryption SSE-C, which of the below mentioned statements is true?

Please select:

- A. The user should use the same encryption key for all versions of the same object  
B. It is possible to have different encryption keys for different versions of the same object  
C. IAM S3 does not allow the user to upload his own keys for server side encryption  
D. The SSE-C does not work when versioning is enabled

**Answer:** B

**Explanation:**

Managing your own encryption keys, you

You can encrypt the object and send it across to S3

Option A is invalid because ideally you should use different encryption keys Option C is invalid because you can use your own encryption keys Option D is invalid because encryption works even if versioning is enabled For more information on client side encryption please visit the below Link:

""Keys.html <https://docs.IAM.amazonaws.com/AmazonS3/latest/dev/UsingClientSideEncryption.html>

The correct answer is: It is possible to have different encryption keys for different versions of the same object Submit your Feedback/Queries to our Experts

**NEW QUESTION 236**

- (Exam Topic 3)

You need to inspect the running processes on an EC2 Instance that may have a security issue. How can you achieve this in the easiest way possible. Also you need to ensure that the process does not interfere with the continuous running of the instance.

Please select:

- A. Use IAM Cloudtrail to record the processes running on the server to an S3 bucket.  
B. Use IAM Cloudwatch to record the processes running on the server  
C. Use the SSM Run command to send the list of running processes information to an S3 bucket.  
D. Use IAM Config to see the changed process information on the server

**Answer:** C

**Explanation:**

The SSM Run command can be used to send OS specific commands to an Instance. Here you can check and see the running processes on an instance and then send the output to an S3 bucket.

Option A is invalid because this is used to record API activity and cannot be used to record running processes. Option B is invalid because Cloudwatch is a logging and metric service and cannot be used to record running processes.

Option D is invalid because IAM Config is a configuration service and cannot be used to record running processes.

For more information on the Systems Manager Run command, please visit the following URL: <https://docs.IAM.amazonaws.com/systems-manager/latest/userguide/execute-remote-commands.html>

The correct answer is: Use the SSM Run command to send the list of running processes information to an S3 bucket. Submit your Feedback/Queries to our Experts

**NEW QUESTION 239**

- (Exam Topic 3)

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

Please select:

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

**Answer:** D

**Explanation:**

One important security aspect is to never give access to actual servers, hence Option A.B and C are just totally wrong from a security perspective.

The best option is to have a central logging server that can be used to archive logs. These logs can then be stored in S3.

Options A,B and C are all invalid because you should not give access to the developers on the Apache se  
For more information on S3, please refer to the below link <https://IAM.amazon.com/documentation/s3j>  
The correct answer is: Set up a central logging server that you can use to archive your logs; archive these logs to an S3 bucket for developer-access.  
Submit your Feedback/Queries to our Experts

#### NEW QUESTION 242

- (Exam Topic 3)

Your company is hosting a set of EC2 Instances in IAM. They want to have the ability to detect if any port scans occur on their IAM EC2 Instances. Which of the following can help in this regard?  
Please select:

- A. Use IAM inspector to consciously inspect the instances for port scans
- B. Use IAM Trusted Advisor to notify of any malicious port scans
- C. Use IAM Config to notify of any malicious port scans
- D. Use IAM Guard Duty to monitor any malicious port scans

**Answer:** D

#### Explanation:

The IAM blogs mention the following to support the use of IAM GuardDuty

GuardDuty voraciously consumes multiple data streams, including several threat intelligence feeds, staying aware of malicious addresses, devious domains, and more importantly, learning to accurately identify malicious or unauthorized behavior in your IAM accounts. In combination with information gleaned from your VPC Flow Logs, IAM CloudTrail Event Logs, and DNS logs, th allows GuardDuty to detect many different types of dangerous and mischievous behavior including probes for known vulnerabilities, port scans and probes, and access from unusual locations. On the IAM side, it looks for suspicious IAM account activity such as unauthorized deployments, unusual CloudTrail activity, patterns of access to IAM API functions, and attempts to exceed multiple service limits. GuardDuty will also look for compromised EC2 instances talking to malicious entities or services, data exfiltration attempts, and instances that are mining cryptocurrency.

Options A, B and C are invalid because these services cannot be used to detect port scans For more information on IAM Guard Duty, please refer to the below Link:

<https://IAM.amazon.com/blogs/IAM/amazon-guardduty-continuous-security-monitoring-threat-detection/>; (

The correct answer is: Use IAM Guard Duty to monitor any malicious port scans Submit your Feedback/Queries to our Experts

#### NEW QUESTION 245

- (Exam Topic 3)

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

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

**Answer:** C

#### Explanation:

So definitely the case here is that the incident response plan is not catering to newly created services. IAM keeps on changing and adding new services and hence the response plan must cater to these new services.

Option A and B are invalid because we don't know this for a fact.

Option D is invalid because we know that the response plan is not complete, because it does not cater to new features of IAM

For more information on incident response plan please visit the following URL: <https://IAM.amazon.com/blogs/publicsector/buildins-a-cloud-specific-incident-response-plan/>;

The correct answer is: The response plan does not cater to new services Submit your Feedback/Queries to our Experts

#### NEW QUESTION 248

.....

## Relate Links

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

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

## Contact us

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

Viste - <https://www.exambible.com/>