



# Amazon-Web-Services

## Exam Questions SCS-C02

AWS Certified Security - Specialty

### NEW QUESTION 1

- (Exam Topic 1)

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

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

The Security Engineer has verified the following:

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

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

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

**Answer:** CD

#### Explanation:

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

### NEW QUESTION 2

- (Exam Topic 1)

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

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

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

**Answer:** CD

### NEW QUESTION 3

- (Exam Topic 1)

A Developer is building a serverless application that uses Amazon API Gateway as the front end. The application will not be publicly accessible. Other legacy applications running on Amazon EC2 will make calls to the application A Security Engineer Has been asked to review the security controls for authentication and authorization of the application

Which combination of actions would provide the MOST secure solution? (Select TWO )

- A. Configure an IAM policy that allows the least permissive actions to communicate with the API Gateway Attach the policy to the role used by the legacy EC2 instances
- B. Enable IAM WAF for API Gateway Configure rules to explicitly allow connections from the legacy EC2 instances
- C. Create a VPC endpoint for API Gateway Attach an IAM resource policy that allows the role of the legacy EC2 instances to call specific APIs
- D. Create a usage plan Generate a set of API keys for each application that needs to call the API.
- E. Configure cross-origin resource sharing (CORS) in each API Share the CORS information with the applications that call the API.

**Answer:** AE

### NEW QUESTION 4

- (Exam Topic 1)

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

What should the Security Engineer do to meet these requirements?

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

**Answer:** B

### NEW QUESTION 5

- (Exam Topic 1)

A city is implementing an election results reporting website that will use Amazon GoudFront The website runs on a fleet of Amazon EC2 instances behind an

Application Load Balancer (ALB) in an Auto Scaling group. Election results are updated hourly and are stored as .pdf tiles in an Amazon S3 bucket. A Security Engineer needs to ensure that all external access to the website goes through CloudFront. Which solution meets these requirements?

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

**Answer:** C

#### NEW QUESTION 6

- (Exam Topic 1)

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

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

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

**Answer:** BDF

#### NEW QUESTION 7

- (Exam Topic 1)

The Security Engineer is managing a traditional three-tier web application that is running on Amazon EC2 instances. The application has become the target of increasing numbers of malicious attacks from the Internet.

What steps should the Security Engineer take to check for known vulnerabilities and limit the attack surface? (Choose two.)

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

**Answer:** BD

#### NEW QUESTION 8

- (Exam Topic 1)

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

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

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

**Answer:** BC

#### NEW QUESTION 9

- (Exam Topic 1)

A company has implemented centralized logging and monitoring of IAM CloudTrail logs from all Regions in an Amazon S3 bucket. The logs are encrypted using IAM KMS. A Security Engineer is attempting to review the log files using a third-party tool hosted on an Amazon EC2 instance. The Security Engineer is unable to access the logs in the S3 bucket and receives an access denied error message.

What should the Security Engineer do to fix this issue?

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

Answer: C

#### NEW QUESTION 10

- (Exam Topic 1)

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

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

Answer: BE

#### NEW QUESTION 10

- (Exam Topic 1)

A company requires that SSH commands used to access its IAM instance be traceable to the user who executed each command. How should a Security Engineer accomplish this?

- A. Allow inbound access on port 22 at the security group attached to the instance Use IAM Systems Manager Session Manager for shell access to Amazon EC2 instances with the user tag defined Enable Amazon CloudWatch logging for Systems Manager sessions
- B. Use Amazon S3 to securely store one Privacy Enhanced Mail Certificate (PEM file) for each user Allow Amazon EC2 to read from Amazon S3 and import every user that wants to use SSH to access EC2 instances Allow inbound access on port 22 at the security group attached to the instance Install the Amazon CloudWatch agent on the EC2 instance and configure it to ingest audit logs for the instance
- C. Deny inbound access on port 22 at the security group attached to the instance Use IAM Systems Manager Session Manager for shell access to Amazon EC2 instances with the user tag defined Enable Amazon CloudWatch logging for Systems Manager sessions
- D. Use Amazon S3 to securely store one Privacy Enhanced Mail Certificate (PEM file) for each team or group Allow Amazon EC2 to read from Amazon S3 and import every user that wants to use SSH to access EC2 instances Allow inbound access on port 22 at the security group attached to the instance Install the Amazon CloudWatch agent on the EC2 instance and configure it to ingest audit logs for the instance

Answer: C

#### NEW QUESTION 13

- (Exam Topic 1)

A security engineer is responsible for providing secure access to IAM resources for thousands of developer in a company's corporate identity provider (idp). The developers access a set of IAM services from the corporate premises using IAM credential. Due to the volume of requests for provisioning new IAM users, it is taking a long time to grant access permissions. The security engineer receives reports that developer are sharing their IAM credentials with others to avoid provisioning delays. The causes concern about overall security for the security engineer. Which actions will meet the program requirements that address security?

- A. Create an Amazon CloudWatch alarm for IAM CloudTrail Events Create a metric filter to send a notification when the same set of IAM credentials is used by multiple developer
- B. Create a federation between IAM and the existing corporate IdP Leverage IAM roles to provide federated access to IAM resources
- C. Create a VPN tunnel between the corporate premises and the VPC Allow permissions to all IAM services only if it originates from corporate premises.
- D. Create multiple IAM roles for each IAM user Ensure that users who use the same IAM credentials cannot assume the same IAM role at the same time.

Answer: B

#### NEW QUESTION 18

- (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 21

- (Exam Topic 1)

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

Which solution will meet these requirements?

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

**Answer:** C

#### NEW QUESTION 25

- (Exam Topic 1)

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

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

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

**Answer:** BCE

#### NEW QUESTION 26

- (Exam Topic 1)

A company's on-premises data center forwards DNS logs to a third-party security incident events management (SIEM) solution that alerts on suspicious behavior. The company wants to introduce a similar capability to its IAM accounts that includes automatic remediation. The company expects to double in size within the next few months.

Which solution meets the company's current and future logging requirements?

- A. Enable Amazon GuardDuty and IAM Security Hub in all Regions and all account
- B. Designate a master security account to receive all alerts from the child account
- C. Set up specific rules within Amazon EventBridge to trigger an IAM Lambda function for remediation steps.
- D. Ingest all IAM CloudTrail logs, VPC Flow Logs, and DNS logs into a single Amazon S3 bucket in a designated security account
- E. Use the current on-premises SIEM to monitor the logs and send a notification to an Amazon SNS topic to alert the security team of remediation steps.
- F. Ingest all IAM CloudTrail logs, VPC Flow Logs, and DNS logs into a single Amazon S3 bucket in a designated security account
- G. Launch an Amazon EC2 instance and install the current SIEM to monitor the logs and send a notification to an Amazon SNS topic to alert the security team of remediation steps.
- H. Enable Amazon GuardDuty and IAM Security Hub in all Regions and all account
- I. Designate a master security account to receive all alerts from the child account
- J. Create an IAM Organizations SCP that denies access to certain API calls that are on an ignore list.

**Answer:** A

#### NEW QUESTION 31

- (Exam Topic 1)

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

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

Which solution should the security engineer recommend?

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

**Answer:** B

#### NEW QUESTION 33

- (Exam Topic 1)

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

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

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

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

**Answer:** AD

#### NEW QUESTION 34

- (Exam Topic 1)

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

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

**Answer:** B

#### NEW QUESTION 37

- (Exam Topic 1)

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

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

**Answer:** B

#### NEW QUESTION 40

- (Exam Topic 1)

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

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

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

**Answer:** D

#### NEW QUESTION 44

- (Exam Topic 1)

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

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

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 45

- (Exam Topic 1)

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

What could be causing these terminations?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 49**

- (Exam Topic 1)

A company is setting up products to deploy in IAM Service Catalog. Management is concerned that when users launch products, elevated IAM privileges will be required to create resources. How should the company mitigate this concern?

- A. Add a template constraint to each product in the portfolio.
- B. Add a launch constraint to each product in the portfolio.
- C. Define resource update constraints for each product in the portfolio.
- D. Update the IAM CloudFormation template backing the product to include a service role configuration.

**Answer:** B

**Explanation:**

<https://docs.IAM.amazon.com/servicecatalog/latest/adminguide/constraints-launch.html>

Launch constraints apply to products in the portfolio (product-portfolio association). Launch constraints do not apply at the portfolio level or to a product across all portfolios. To associate a launch constraint with all products in a portfolio, you must apply the launch constraint to each product individually.

**NEW QUESTION 51**

- (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 54**

- (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 59**

- (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 created.
- 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 group.
- 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 61

- (Exam Topic 1)

A company is using IAM Organizations to manage multiple IAM accounts. The company has an application that allows users to assume the AppUser IAM role to download files from an Amazon S3 bucket that is encrypted with an IAM KMS CMK. However, when users try to access the files in the S3 bucket, they get an access denied error.

What should a Security Engineer do to troubleshoot this error? (Select THREE )

- A. Ensure the KMS policy allows the AppUser role to have permission to decrypt for the CMK
- B. Ensure the S3 bucket policy allows the AppUser role to have permission to get objects for the S3 bucket
- C. Ensure the CMK was created before the S3 bucket.
- D. Ensure the S3 block public access feature is enabled for the S3 bucket.
- E. Ensure that automatic key rotation is disabled for the CMK
- F. Ensure the SCPs within Organizations allow access to the S3 bucket.

**Answer:** ABF

#### NEW QUESTION 62

- (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 device
- B. Associate the v/eb ACL with the ALB.
- C. Configure an Amazon CloudFront distribution to use the ALB as an origin
- D. Configure a web ACL rule for IAM WAF to block requests with a string match condition for the user agent of the IoT device
- 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 origin
- G. Configure a web ACL rule for IAM WAF to block requests with a string match condition for the user agent of the IoT device
- H. Change the ALB security group to allow 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 protection
- J. Apply an IAM WAF ACL to the ALB
- K. and configure a listener rule on the ALB to block IoT devices based on the user agent.

**Answer:** D

#### NEW QUESTION 67

- (Exam Topic 1)

A company is operating an open-source software platform that is internet-facing. The legacy software platform no longer receives security updates. The software platform operates using Amazon Route 53 weighted load balancing to send traffic to two Amazon EC2 instances that connect to an Amazon RDS database. A recent report suggests this software platform is vulnerable to SQL injection attacks, with samples of attacks provided. The company's security engineer must secure this system against SQL injection attacks within 24 hours. The security engineer's solution involves the least amount of effort and maintains normal operations during implementation.

What should the security engineer do to meet these requirements?

- A. Create an Application Load Balancer with the existing EC2 instances as a target group. Create an IAM WAF web ACL containing rules that protect the application from this attack.
- B. Then apply it to the ALB. Test to ensure the vulnerability has been mitigated, then redirect the Route 53 records to point to the ALB. Update security groups on the EC2 instances to prevent direct access from the internet.
- C. Create an Amazon CloudFront distribution specifying one EC2 instance as an origin. Create an IAM WAF web ACL containing rules that protect the application from this attack, then apply it to the distribution. Test to ensure the vulnerability has been mitigated, then redirect the Route 53 records to point to CloudFront.
- D. Obtain the latest source code for the platform and make the necessary updates. Test the updated code to ensure that the vulnerability has been mitigated, then deploy the patched version of the platform to the EC2 instances.
- E. Update the security group that is attached to the EC2 instances, removing access from the internet to the TCP port used by the SQL database. Create an IAM WAF web ACL containing rules that protect the application from this attack, then apply it to the EC2 instances. Test to ensure the vulnerability has been mitigated.
- F. Then restore the security group to the original setting.

**Answer:** A

#### NEW QUESTION 68

- (Exam Topic 1)

A company's Security Engineer has been asked to monitor and report all IAM account root user activities. Which of the following would enable the Security Engineer to monitor and report all root user activities?

(Select TWO)

- A. Configuring IAM Organizations to monitor root user API calls on the paying account
- B. Creating an Amazon CloudWatch Events rule that will trigger when any API call from the root user is reported
- C. Configuring Amazon Inspector to scan the IAM account for any root user activity
- D. Configuring IAM Trusted Advisor to send an email to the Security team when the root user logs in to the console
- E. Using Amazon SNS to notify the target group

**Answer:** BE

#### NEW QUESTION 72

- (Exam Topic 2)

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

Please select:

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

**Answer:** A

**Explanation:**

The IAM Documentation mentions the following on IAM KMS

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

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

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

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

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

Submit your Feedback/Queries to our Experts

**NEW QUESTION 76**

- (Exam Topic 2)

The Security Engineer implemented a new vault lock policy for 10TB of data and called initiate-vault-lock 12 hours ago. The Audit team identified a typo that is allowing incorrect access to the vault.

What is the MOST cost-effective way to correct this?

- A. Call the abort-vault-lock operation, fix the typo, and call the initiate-vault-lock again.
- B. Copy the vault data to Amazon S3, delete the vault, and create a new vault with the data.
- C. Update the policy, keeping the vault lock in place.
- D. Update the policy and call initiate-vault-lock again to apply the new policy.

**Answer:** A

**Explanation:**

Initiate the lock by attaching a vault lock policy to your vault, which sets the lock to an in-progress state and returns a lock ID. While in the in-progress state, you have 24 hours to validate your vault lock policy before the lock ID expires. Use the lock ID to complete the lock process. If the vault lock policy doesn't work as expected, you can abort the lock and restart from the beginning. For information on how to use the S3 Glacier API to lock a vault, see Locking a Vault by Using the Amazon S3 Glacier API. <https://docs.IAM.amazon.com/amazonglacier/latest/dev/vault-lock-policy.html>

**NEW QUESTION 77**

- (Exam Topic 2)

Your company has an EC2 Instance that is hosted in an IAM VPC. There is a requirement to ensure that logs files from the EC2 Instance are stored accordingly. The access should also be limited for the destination of the log files. How can this be accomplished? Choose 2 answers from the options given below. Each answer forms part of the solution

Please select:

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

**Answer:** BD

**Explanation:**

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

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

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

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

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

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

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

Submit your Feedback/Queries to our Experts

**NEW QUESTION 79**

- (Exam Topic 2)

You have an S3 bucket hosted in IAM. This is used to host promotional videos uploaded by yourself. You need to provide access to users for a limited duration of time. How can this be achieved?

Please select:

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

**Answer:** B

**Explanation:**

The IAM Documentation mentions the following

All objects by default are private. Only the object owner has permission to access these objects. However, the object owner can optionally share objects with others by creating a pre-signed URL using their own security credentials, to grant time-limited permission to download the objects.

Option A is invalid because this can be used to prevent accidental deletion of objects Option C is invalid because timestamps are not possible for Roles

Option D is invalid because policies is not the right way to limit access based on time For more information on pre-signed URL's, please visit the URL:

<https://docs.IAM.ama2on.com/AmazonS3/latest/dev/ShareObjectPreSignedURL.html>

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

**NEW QUESTION 83**

- (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 85**

- (Exam Topic 2)

Example.com hosts its internal document repository on Amazon EC2 instances. The application runs on EC2 instances and previously stored the documents on encrypted Amazon EBS volumes. To optimize the application for scale, example.com has moved the files to Amazon S3. The security team has mandated that all the files are securely deleted from the EBS volume, and it must certify that the data is unreadable before releasing the underlying disks.

Which of the following methods will ensure that the data is unreadable by anyone else?

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

**Answer:** D

**Explanation:**

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

<https://d0.IAMstatic.com/whitepapers/IAM-security-whitepaper.pdf>

**NEW QUESTION 87**

- (Exam Topic 2)

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

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

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

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

- A. Remove the sensitive data from the object name, and store the sensitive data using S3 user-defined metadata.
- B. Add an S3 bucket policy that denies the action s3:GetObject
- C. Use a random and unique S3 object key, and create an S3 metadata index in Amazon DynamoDB using client-side encrypted attributes.
- D. Store all sensitive objects in Binary Large Objects (BLOBS) in an encrypted Amazon RDS instance.

**Answer:** C

**Explanation:**

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

**NEW QUESTION 90**

- (Exam Topic 2)

An organization has three applications running on IAM, each accessing the same data on Amazon S3. The data on Amazon S3 is server-side encrypted by using

an IAM KMS Customer Master Key (CMK).

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

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

**Answer:** C

#### NEW QUESTION 94

- (Exam Topic 2)

The Security Engineer for a mobile game has to implement a method to authenticate users so that they can save their progress. Because most of the users are part of the same OpenID-Connect compatible social media website, the Security Engineer would like to use that as the identity provider.

Which solution is the SIMPLEST way to allow the authentication of users using their social media identities?

- A. Amazon Cognito
- B. AssumeRoleWithWebIdentity API
- C. Amazon Cloud Directory
- D. Active Directory (AD) Connector

**Answer:** A

#### NEW QUESTION 96

- (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 99

- (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 103

- (Exam Topic 2)

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

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

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 108

- (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 112

- (Exam Topic 2)

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

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

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

**Answer: AD**

#### NEW QUESTION 113

- (Exam Topic 2)

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

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

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

**Answer: AC**

#### Explanation:

The IAM Documentation mentions the following

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

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

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

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

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

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

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 117

- (Exam Topic 2)

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

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

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

**Answer: AE**

#### Explanation:

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

#### NEW QUESTION 121

- (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 124

- (Exam Topic 2)

The Information Technology department has stopped using Classic Load Balancers and switched to Application Load Balancers to save costs. After the switch, some users on older devices are no longer able to connect to the website.

What is causing this situation?

- A. Application Load Balancers do not support older web browsers.
- B. The Perfect Forward Secrecy settings are not configured correctly.
- C. The intermediate certificate is installed within the Application Load Balancer.
- D. The cipher suites on the Application Load Balancers are blocking connections.

**Answer:** D

**Explanation:**

<https://docs.IAM.amazonaws.com/elasticloadbalancing/latest/application/create-https-listener.html>

#### NEW QUESTION 127

- (Exam Topic 2)

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

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

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

**Answer:** D

**Explanation:**

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

The IAM Documentation additionally mentions the following

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

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

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

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

Option B is invalid because resource policies are present for resources such as S3 and KMS, but not IAM Lambda

Option C is invalid because IAM Roles should be used and not IAM Users

For more information on the Lambda permission model, please visit the below URL: <https://docs.IAM.amazonaws.com/lambda/latest/dg/intro-permission-model.html>

The correct answer is: Create an IAM service role with permissions to write to the DynamoDB table. Associate that role with the Lambda function.

Submit your Feedback/Queries to our Exp

#### NEW QUESTION 129

- (Exam Topic 2)

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

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

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

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

Which buckets can user “alice” access?

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

**Answer:** C

**Explanation:**

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

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

**NEW QUESTION 130**

- (Exam Topic 2)

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

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

**Answer:** A

**Explanation:**

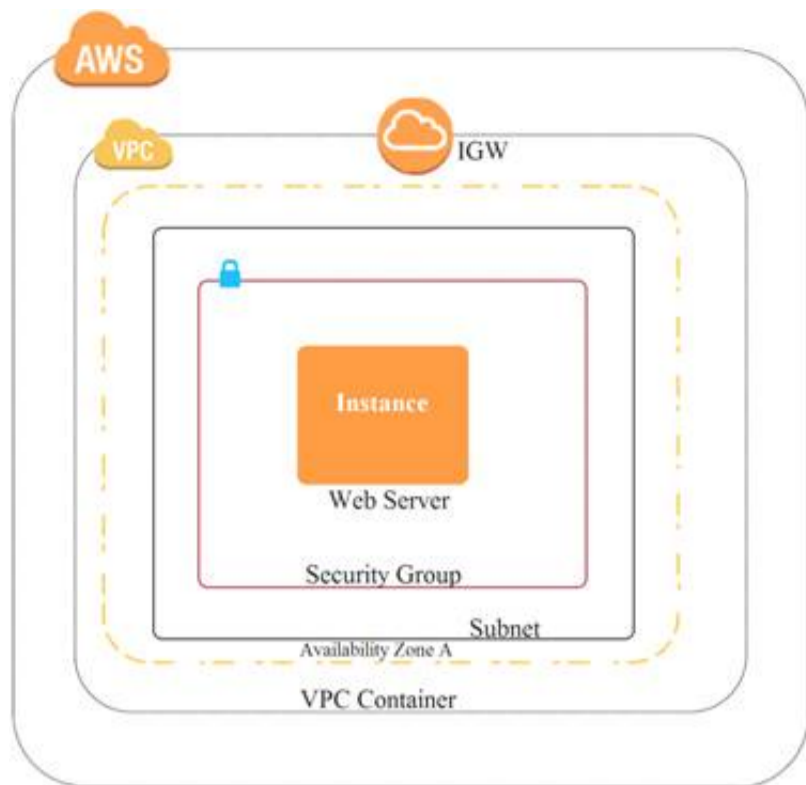
<https://IAM.amazon.com/answers/networking/vpc-security-capabilities/> Security Group is stateful and hypervisor level.

**NEW QUESTION 132**

- (Exam Topic 2)

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

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



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

**Answer:** D

**Explanation:**

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

#### NEW QUESTION 133

- (Exam Topic 2)

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

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

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

**Answer:** AC

**Explanation:**

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

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

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

#### NEW QUESTION 134

- (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 139

- (Exam Topic 2)

Due to new compliance requirements, a Security Engineer must enable encryption with customer-provided keys on corporate data that is stored in DynamoDB. The company wants to retain full control of the encryption keys.

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

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

**Answer:** D

**Explanation:**

Follow the link:

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

**NEW QUESTION 141**

- (Exam Topic 2)

A Security Engineer is trying to determine whether the encryption keys used in an IAM service are in compliance with certain regulatory standards. Which of the following actions should the Engineer perform to get further guidance?

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

**Answer:** B

**Explanation:**

<https://IAM.amazon.com/artifact/>

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

**NEW QUESTION 146**

- (Exam Topic 2)

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

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

**Answer:** A

**Explanation:**

The IAM Documentation mentions the following

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

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

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

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

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

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

**NEW QUESTION 151**

- (Exam Topic 2)

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 155**

- (Exam Topic 2)

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

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

- A. Create a new S3 bucket in a separate IAM account for centralized storage of CloudTrail logs, and enable “Log File Validation” on all trails.

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

**Answer:** ACE

**Explanation:**

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

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

**NEW QUESTION 157**

- (Exam Topic 2)

A 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 policies
- 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 162**

- (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 CMKs: 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 the 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 163

- (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 167

- (Exam Topic 2)

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

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

Security Engineer

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

Lambda function execution role

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

What is causing the error?

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

**Answer:** D

#### NEW QUESTION 168

- (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 171

- (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 172

- (Exam Topic 2)

IAM CloudTrail is being used to monitor API calls in an organization. An audit revealed that CloudTrail is failing to deliver events to Amazon S3 as expected. What initial actions should be taken to allow delivery of CloudTrail events to S3? (Select two.)

- A. Verify that the S3 bucket policy allow CloudTrail to write objects.
- B. Verify that the IAM role used by CloudTrail has access to write to Amazon CloudWatch Logs.
- C. Remove any lifecycle policies on the S3 bucket that are archiving objects to Amazon Glacier.
- D. Verify that the S3 bucket defined in CloudTrail exists.
- E. Verify that the log file prefix defined in CloudTrail exists in the S3 bucket.

**Answer: BD**

#### Explanation:

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

#### NEW QUESTION 175

- (Exam Topic 2)

Your IT Security team has advised to carry out a penetration test on the resources in their company's IAM Account. This is as part of their capability to analyze the security of the Infrastructure. What should be done first in this regard?

Please select:

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

**Answer: C**

#### Explanation:

This concept is given in the IAM Documentation

How do I submit a penetration testing request for my IAM resources? Issue

I want to run a penetration test or other simulated event on my IAM architecture. How do I get permission from IAM to do that?

Resolution

Before performing security testing on IAM resources, you must obtain approval from IAM. After you submit your request IAM will reply in about two business days. IAM might have additional questions about your test which can extend the approval process, so plan accordingly and be sure that your initial request is as detailed as possible.

If your request is approved, you'll receive an authorization number.

Option A,B and D are all invalid because the first step is to get prior authorization from IAM for penetration tests

For more information on penetration testing, please visit the below URL

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

\* <https://IAM.amazon.com/premiumsupport/knowledge-center/penetration-testing/> (

The correct answer is: Submit a request to IAM Support Submit your Feedback/Queries to our Experts

#### NEW QUESTION 180

- (Exam Topic 2)

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

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

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

**Answer:** D

#### Explanation:

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

#### NEW QUESTION 181

- (Exam Topic 2)

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

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

**Answer:** AB

#### Explanation:

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

#### NEW QUESTION 184

- (Exam Topic 2)

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

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

Which of the following troubleshooting steps should the Analyst perform?

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

**Answer:** B

#### Explanation:

MetricFilter:

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

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

|| (\$eventName = CreateSecurityGroup) || (\$eventName = DeleteSecurityGroup) }

MetricTransformations:

- MetricValue: '1'

MetricNamespace: CloudTrailMetrics MetricName: SecurityGroupEventCount

#### NEW QUESTION 188

- (Exam Topic 2)

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

Please select:

- A. Port 443 coming from 0.0.0.0/0
- B. Port 443 coming from 10.0.0.0/16

- C. Port 22 coming from 0.0.0.0/0
- D. Port 22 coming from 203.0.113.1/32

**Answer:** AD

**Explanation:**

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

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

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

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

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

**NEW QUESTION 190**

- (Exam Topic 2)

The Security team believes that a former employee may have gained unauthorized access to IAM resources sometime in the past 3 months by using an identified access key.

What approach would enable the Security team to find out what the former employee may have done within IAM?

- A. Use the IAM CloudTrail console to search for user activity.
- B. Use the Amazon CloudWatch Logs console to filter CloudTrail data by user.
- C. Use IAM Config to see what actions were taken by the user.
- D. Use Amazon Athena to query CloudTrail logs stored in Amazon S3.

**Answer:** A

**Explanation:**

You can use CloudTrail to search event history for the last 90 days. You can use CloudWatch queries to search API history beyond the last 90 days. You can use Athena to query CloudTrail logs over the last 90 days. <https://IAM.amazon.com/premiumsupport/knowledge-center/view-iam-history/>

**NEW QUESTION 195**

- (Exam Topic 2)

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 199**

- (Exam Topic 2)

A company will store sensitive documents in three Amazon S3 buckets based on a data classification scheme of "Sensitive," "Confidential," and "Restricted."

The security solution must meet all of the following requirements:

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

Which of the following meets these requirements?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 204**

- (Exam Topic 2)

Your company is planning on hosting an internal network in IAM. They want machines in the VPC to authenticate using private certificates. They want to minimize

the work and maintenance in working with certificates. What is the ideal way to fulfil this requirement.  
Please select:

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

**Answer: B**

**Explanation:**

The IAM Documentation mentions the following

ACM is tightly linked with IAM Certificate Manager Private Certificate Authority. You can use ACM PCA to create a private certificate authority (CA) and then use ACM to issue private certificates. These are SSL/TLS X.509 certificates that identify users, computers, applications, services, servers, and other devices internally. Private certificates cannot be publicly trusted

Option A is partially invalid. Windows Server 2016 Certificate Manager can be used but since there is a requirement to "minimize the work and maintenance", IAM Certificate Manager should be used

Option C and D are invalid because these cannot be used for managing certificates. For more information on ACM, please visit the below URL:

<https://docs.IAM.amazon.com/acm/latest/userguide/acm-overview.html>

The correct answer is: Consider using IAM Certificate Manager Submit your Feedback/Queries to our Experts

**NEW QUESTION 206**

- (Exam Topic 3)

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

Please select:

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

**Answer: A**

**Explanation:**

The IAM Documentation mentions the following

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

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

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

**NEW QUESTION 210**

- (Exam Topic 3)

Your company has an EC2 Instance hosted in IAM. This EC2 Instance hosts an application. Currently this application is experiencing a number of issues. You need to inspect the network packets to see what the type of error that is occurring? Which one of the below steps can help address this issue?

Please select:

- A. Use the VPC Flow Logs.
- B. Use a network monitoring tool provided by an IAM partner.
- C. Use another instanc
- D. Setup a port to "promiscuous mode" and sniff the traffic to analyze the packet
- E. Use Cloudwatch metric

**Answer: B**

**NEW QUESTION 212**

- (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 215

- (Exam Topic 3)

You are working in the media industry and you have created a web application where users will be able to upload photos they create to your website. This web application must be able to call the S3 API in order to be able to function. Where should you store your API credentials whilst maintaining the maximum level of security?

Please select:

- A. Save the API credentials to your PHP files.
- B. Don't save your API credentials, instead create a role in IAM and assign this role to an EC2 instance when you first create it.
- C. Save your API credentials in a public Github repository.
- D. Pass API credentials to the instance using instance userdata.

**Answer: B**

#### Explanation:

Applications must sign their API requests with IAM credentials. Therefore, if you are an application developer, you need a strategy for managing credentials for your applications that run on EC2 instances. For example, you can securely distribute your IAM credentials to the instances, enabling the applications on those instances to use your credentials to sign requests, while protecting your credentials from other users. However, it's challenging to securely distribute credentials to each instance. especially those that IAM creates on your behalf, such as Spot Instances or instances in Auto Scaling groups. You must also be able to update the credentials on each instance when you rotate your IAM credentials. IAM roles are designed so that your applications can securely make API requests from your instances, without requiring you manage the security credentials that the applications use.

Option A.C and D are invalid because using IAM Credentials in an application in production is a direct no recommendation 1 secure access

For more information on IAM Roles, please visit the below URL:

<http://docs.IAM.amazon.com/IAMEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html>

The correct answer is: Don't save your API credentials. Instead create a role in IAM and assign this role to an EC2 instance when you first create it

Submit your Feedback/Queries to our Experts

### NEW QUESTION 218

- (Exam Topic 3)

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

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

Please select:

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

**Answer: BD**

#### Explanation:

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

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

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

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

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

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

Submit your Feedback/Queries to our Experts

### NEW QUESTION 219

- (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 224

- (Exam Topic 3)

A company has hired a third-party security auditor, and the auditor needs read-only access to all IAM resources and logs of all VPC records and events that have occurred on IAM. How can the company meet the auditor's requirements without comprising security in the IAM environment? Choose the correct answer from the options below

Please select:

- A. Create a role that has the required permissions for the auditor.
- B. Create an SNS notification that sends the CloudTrail log files to the auditor's email when CloudTrail delivers the logs to S3, but do not allow the auditor access to the IAM environment.
- C. The company should contact IAM as part of the shared responsibility model, and IAM will grant required access to the third-party auditor.
- D. Enable CloudTrail logging and create an IAM user who has read-only permissions to the required IAM resources, including the bucket containing the CloudTrail logs.

**Answer:** D

#### Explanation:

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.

Option A and C are incorrect since Cloudtrail needs to be used as part of the solution Option B is incorrect since the auditor needs to have access to Cloudtrail

For more information on cloudtrail, please visit the below URL: <https://IAM.amazon.com/cloudtrail>

The correct answer is: Enable CloudTrail logging and create an IAM user who has read-only permissions to the required IAM resources, including the bucket containing the CloudTrail logs.

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 227

- (Exam Topic 3)

You have a set of Customer keys created using the IAM KMS service. These keys have been used for around 6 months. You are now trying to use the new KMS features for the existing set of key's but are not able to do so. What could be the reason for this.

Please select:

- A. You have not explicitly given access via the key policy
- B. You have not explicitly given access via the IAM policy
- C. You have not given access via the IAM roles
- D. You have not explicitly given access via IAM users

**Answer:** A

#### Explanation:

By default, keys created in KMS are created with the default key policy. When features are added to KMS, you need to explicitly update the default key policy for these keys.

Option B,C and D are invalid because the key policy is the main entity used to provide access to the keys For more information on upgrading key policies please visit the following URL: <https://docs.IAM.amazonaws.com/kms/latest/developerguide/key-policy-upgrading.html>

(

The correct answer is: You have not explicitly given access via the key policy Submit your Feedback/Queries to our Experts

#### NEW QUESTION 232

- (Exam Topic 3)

A customer has an instance hosted in the IAM Public Cloud. The VPC and subnet used to host the Instance have been created with the default settings for the Network Access Control Lists. They need to provide an IT Administrator secure access to the underlying instance. How can this be accomplished.

Please select:

- A. Ensure the Network Access Control Lists allow Inbound SSH traffic from the IT Administrator's Workstation
- B. Ensure the Network Access Control Lists allow Outbound SSH traffic from the IT Administrator's Workstation
- C. Ensure that the security group allows Inbound SSH traffic from the IT Administrator's Workstation
- D. Ensure that the security group allows Outbound SSH traffic from the IT Administrator's Workstation

**Answer:** C

#### Explanation:

Options A & B are invalid as default NACL rule will allow all inbound and outbound traffic.

The requirement is that the IT administrator should be able to access this EC2 instance from his workstation. For that we need to enable the Security Group of EC2 instance to allow traffic from the IT administrator's workstation. Hence option C is correct.

Option D is incorrect as we need to enable the Inbound SSH traffic on the EC2 instance Security Group since the traffic originates from the IT admin's workstation.

The correct answer is: Ensure that the security group allows Inbound SSH traffic from the IT Administrator's Workstation Submit your Feedback/Queries to our Experts

#### NEW QUESTION 236

- (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 239**

- (Exam Topic 3)

Which technique can be used to integrate IAM IAM (Identity and Access Management) with an on-premise LDAP (Lightweight Directory Access Protocol) directory service?

Please select:

- A. Use an IAM policy that references the LDAP account identifiers and the IAM credentials.
- B. Use SAML (Security Assertion Markup Language) to enable single sign-on between IAM and LDAP.
- C. Use IAM Security Token Service from an identity broker to issue short-lived IAM credentials.
- D. Use IAM roles to automatically rotate the IAM credentials when LDAP credentials are updated.

**Answer:** B

**Explanation:**

On the IAM Blog site the following information is present to help on this context

The newly released whitepaper. Single Sign-On: Integrating IAM, OpenLDAP, and Shibboleth, will help you integrate your existing LDAP-based user directory with IAM. When you integrate your existing directory with IAM, your users can access IAM by using their existing credentials. This means that your users don't need to maintain yet another user name and password just to access IAM resources.

Option A.C and D are all invalid because in this sort of configuration, you have to use SAML to enable single sign on.

For more information on integrating IAM with LDAP for Single Sign-On, please visit the following URL:

<https://IAM.amazon.com/blogs/security/new-whitepaper-single-sign-on-integrating-IAM-openldap-and-shibboleth/>

The correct answer is: Use SAML (Security Assertion Markup Language) to enable single sign-on between IAM and LDAP. Submit your Feedback/Queries to our Experts

**NEW QUESTION 240**

- (Exam Topic 3)

You are designing a connectivity solution between on-premises infrastructure and Amazon VPC. Your server's on-premises will be communicating with your VPC instances. You will be establishing IPsec tunnels over the internet. You will be using VPN gateways and terminating the IPsec tunnels on IAM-supported customer gateways. Which of the following objectives would you achieve by implementing an IPsec tunnel as outlined above? Choose 4 answers from the options below

Please select:

- A. End-to-end protection of data in transit
- B. End-to-end Identity authentication
- C. Data encryption across the internet
- D. Protection of data in transit over the Internet
- E. Peer identity authentication between VPN gateway and customer gateway
- F. Data integrity protection across the Internet

**Answer:** CDEF

**Explanation:**

IPSec is a widely adopted protocol that can be used to provide end to end protection for data

**NEW QUESTION 242**

- (Exam Topic 3)

Your company currently has a set of EC2 Instances hosted in a VPC. The IT Security department is suspecting a possible DDos attack on the instances. What can you do to zero in on the IP addresses which are receiving a flurry of requests.

Please select:

- A. Use VPC Flow logs to get the IP addresses accessing the EC2 Instances
- B. Use IAM Cloud trail to get the IP addresses accessing the EC2 Instances
- C. Use IAM Config to get the IP addresses accessing the EC2 Instances
- D. Use IAM Trusted Advisor to get the IP addresses accessing the EC2 Instances

**Answer:** A

**Explanation:**

With VPC Flow logs you can get the list of IP addresses which are hitting the Instances in your VPC You can then use the information in the logs to see which external IP addresses are sending a flurry of requests which could be the potential threat for a DDos attack.

Option B is incorrect Cloud Trail records IAM API calls for your account. VPC Flowlogs logs network traffic for VPC, subnets. Network interfaces etc.

As per IAM,

VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC where as IAM CloudTrail, is a service that captures API calls and delivers the log files to an Amazon S3 bucket that you specify.

Option C is invalid this is a config service and will not be able to get the IP addresses

Option D is invalid because this is a recommendation service and will not be able to get the IP addresses For more information on VPC Flow Logs, please visit the

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

The correct answer is: Use VPC Flow logs to get the IP addresses accessing the EC2 Instances Submit your Feedback/Queries to our Experts

#### NEW QUESTION 243

- (Exam Topic 3)

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

\* sgLB - associated with the ELB

\* sgWeb - associated with the EC2 instances.

\* sgDB - associated with the database

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

Please select:

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

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

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

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

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

**Answer: D**

#### Explanation:

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

The database should allow traffic from the Web server

And the Bastion host should only allow traffic from a specific corporate IP address range Option A is incorrect because the Web group should only allow traffic from the Load balancer For more information on IAM Security Groups, please refer to below URL: <https://docs.IAM.amazon.com/IAMEC2/latest/UserGuide/usins-network-security.html>

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

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

#### NEW QUESTION 245

- (Exam Topic 3)

You have an EC2 instance with the following security configured:

\* a. ICMP inbound allowed on Security Group

\* b. ICMP outbound not configured on Security Group

\* c. ICMP inbound allowed on Network ACL

\* d. ICMP outbound denied on Network ACL

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

Please select:

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

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

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

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

**Answer: ABD**

#### Explanation:

This example is given in the IAM documentation as well

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

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

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

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

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

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

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 247

- (Exam Topic 3)

Which of the following is the responsibility of the customer? Choose 2 answers from the options given below. Please select:

A. Management of the Edge locations

B. Encryption of data at rest

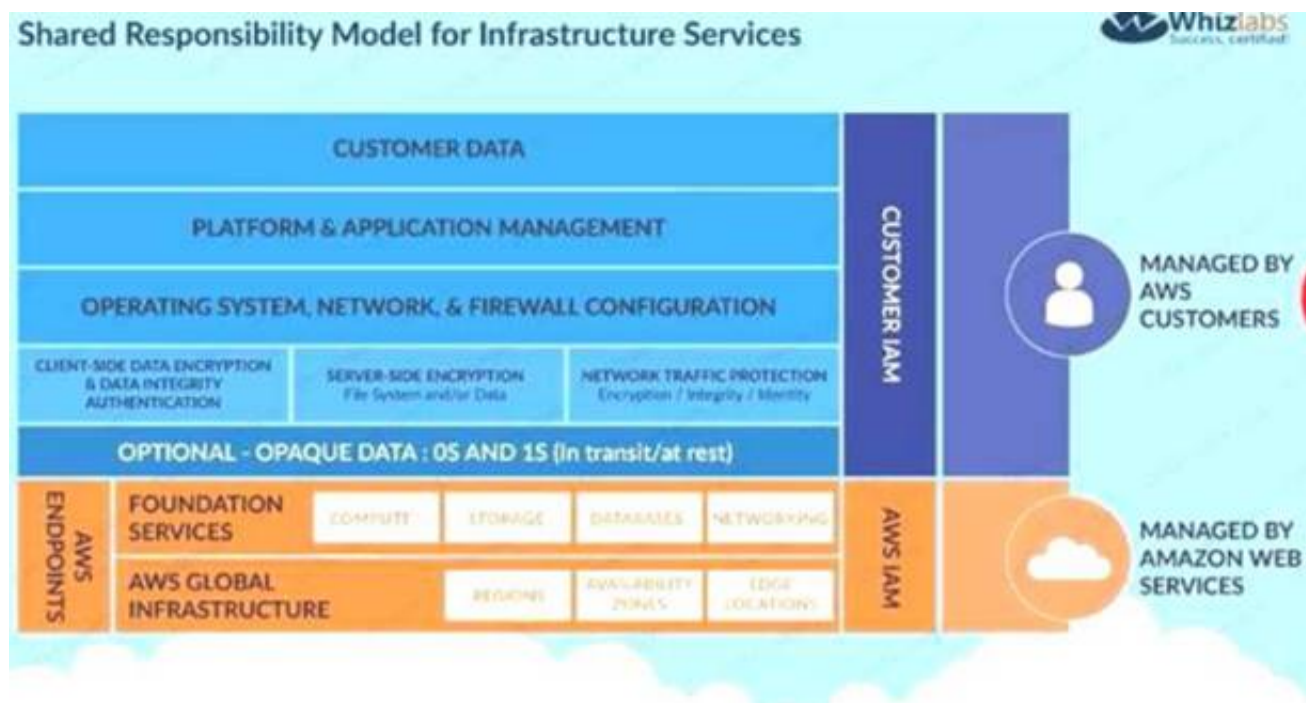
C. Protection of data in transit

D. Decommissioning of old storage devices

**Answer: BC**

#### Explanation:

Below is the snapshot of the Shared Responsibility Model C:\Users\wk\Desktop\mudassar\Untitled.jpg



For more information on IAM Security best practises, please refer to below URL [IAMStatic corn/whitepapers/Security/IAM Practices](https://static.amazonaws.com/public/static/IAMStaticContent/whitepapers/Security/IAMPractices.pdf).  
 The correct answers are: Encryption of data at rest Protection of data in transit Submit your Feedback/Queries to our Experts

### NEW QUESTION 251

- (Exam Topic 3)

You are creating a Lambda function which will be triggered by a Cloudwatch Event. The data from these events needs to be stored in a DynamoDB table. How should the Lambda function be given access to the DynamoDB table?

Please select:

- A. Put the IAM Access keys in the Lambda function since the Lambda function by default is secure
- B. Use an IAM role which has permissions to the DynamoDB table and attach it to the Lambda function.
- C. Use the IAM Access keys which has access to DynamoDB and then place it in an S3 bucket.
- D. Create a VPC endpoint for the DynamoDB tabl
- E. Access the VPC endpoint from the Lambda function.

**Answer: B**

#### Explanation:

IAM Lambda functions uses roles to interact with other IAM services. So use an IAM role which has permissions to the DynamoDB table and attach it to the Lambda function.

Options A and C are all invalid because you should never use IAM keys for access. Option D is invalid because the VPC endpoint is used for VPCs

For more information on Lambda function Permission model, please visit the URL <https://docs.IAM.amazon.com/lambda/latest/dg/intro-permission-model.html>

The correct answer is: Use an IAM role which has permissions to the DynamoDB table and attach it to the Lambda function. Submit your Feedback/Queries to our Experts

### NEW QUESTION 252

- (Exam Topic 3)

You need to create a Linux EC2 instance in IAM. Which of the following steps is used to ensure secure authentication the EC2 instance from a windows machine. Choose 2 answers from the options given below.

Please select:

- A. Ensure to create a strong password for logging into the EC2 Instance
- B. Create a key pair using putty
- C. Use the private key to log into the instance
- D. Ensure the password is passed securely using SSL

**Answer: BC**

#### Explanation:

The IAM Documentation mentions the following

You can use Amazon EC2 to create your key pair. Alternatively, you could use a third-party tool and then import the public key to Amazon EC2. Each key pair requires a name. Be sure to choose a name that is easy to remember. Amazon EC2 associates the public key with the name that you specify as the key name. Amazon EC2 stores the public key only, and you store the private key. Anyone who possesses your private key can decrypt login information, so it's important that you store your private keys in a secure place.

Options A and D are incorrect since you should use key pairs for secure access to Ec2 Instances For more information on EC2 key pairs, please refer to below URL: <https://docs.IAM.amazon.com/IAMEC2/latest/UserGuide/ec2-key-pairs.html>

The correct answers are: Create a key pair using putty. Use the private key to log into the instance Submit your Feedback/Queries to our Experts

### NEW QUESTION 256

- (Exam Topic 3)

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

Please select:

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

**Answer:** B

**Explanation:**

The IAM Documentation mentions the following on lifecycle policies

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

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

archive objects to the GLACIER storage class one year after creation.

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

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

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

**NEW QUESTION 257**

.....

## Thank You for Trying Our Product

### We offer two products:

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

2nd - Questions and Answers in PDF Format

### SCS-C02 Practice Exam Features:

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

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