

# Amazon

## Exam Questions AWS-Certified-Security-Specialty

Amazon AWS Certified Security - Specialty



### NEW QUESTION 1

- (Exam Topic 1)

A company has an encrypted Amazon S3 bucket. An Application Developer has an IAM policy that allows access to the S3 bucket, but the Application Developer is unable to access objects within the bucket.

What is a possible cause of the issue?

- A. The S3 ACL for the S3 bucket fails to explicitly grant access to the Application Developer
- B. The AWS KMS key for the S3 bucket fails to list the Application Developer as an administrator
- C. The S3 bucket policy fails to explicitly grant access to the Application Developer
- D. The S3 bucket policy explicitly denies access to the Application Developer

**Answer: C**

### NEW QUESTION 2

- (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 AWS, but does have AWS Systems Manager configured. The solution must also minimize administrative overhead.

What should a security engineer recommend to meet these requirements?

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

**Answer: B**

### NEW QUESTION 3

- (Exam Topic 1)

A security engineer has created an Amazon Cognito user pool. The engineer needs to manually verify the ID and access token sent by the application for troubleshooting purposes

What is the MOST secure way to accomplish this?

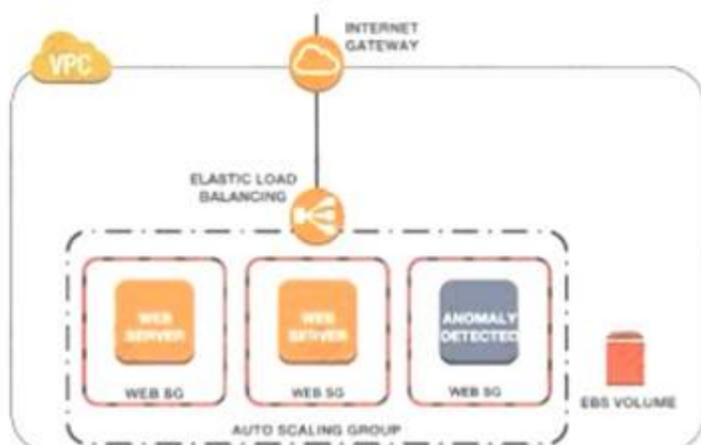
- A. Extract the subject (sub), audience (aud), and cognito:username from the ID token payload. Manually check the subject and audience for the user name in the user pool.
- B. Search for the public key with a key ID that matches the key ID in the header of the token.
- C. Then use a JSON Web Token (JWT)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

**Answer: A**

### NEW QUESTION 4

- (Exam Topic 1)

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



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

**Answer: B**

### NEW QUESTION 5

- (Exam Topic 1)

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

Network error: Connection timed out.

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

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

**Answer:** BDF

#### NEW QUESTION 6

- (Exam Topic 1)

A company uses a third-party identity provider and SAML-based SSO for its AWS accounts After the third-party identity provider renewed an expired signing certificate users saw the following message when trying to log in:

```
Error: Response Signature Invalid (Service: AWSSecurityTokenService; Status Code: 400; Error Code: InvalidIdentityToken)
```

A security engineer needs to provide a solution that corrects the error and minimizes operational overhead Which solution meets these requirements?

- A. Upload the third-party signing certificate's new private key to the AWS identity provider entity defined in AWS identity and Access Management (IAM) by using the AWS Management Console
- B. Sign the identity provider's metadata file with the new public key Upload the signature to the AWS identity provider entity defined in AWS Identity and Access Management (IAM) by using the AWS CLI.
- C. Download the updated SAML metadata tile from the identity service provider Update the file in the AWS identity provider entity defined in AWS Identity and Access Management (IAM) by using the AWS CLI
- D. Configure the AWS identity provider entity defined in AWS Identity and Access Management (IAM) to synchronously fetch the new public key by using the AWS Management Console.

**Answer:** C

#### NEW QUESTION 7

- (Exam Topic 1)

An application running on Amazon EC2 instances generates log files in a folder on a Linux file system. The instances block access to the console and file transfer utilities, such as Secure Copy Protocol (SCP) and Secure File Transfer Protocol (SFTP). The Application Support team wants to automatically monitor the application log files so the team can set up notifications in the future.

A Security Engineer must design a solution that meets the following requirements:

- Make the log files available through an AWS managed service.
- Allow for automatic monitoring of the logs.
- Provide an Interlace for analyzing logs.
- Minimize effort.

Which approach meets these requirements^

- A. Modify the application to use the AWS SD
- B. Write the application logs lo an Amazon S3 bucket
- C. install the unified Amazon CloudWatch agent on the instances Configure the agent to collect the application log dies on the EC2 tile system and send them to Amazon CloudWatch Logs
- D. Install AWS Systems Manager Agent on the instances Configure an automation document to copy the application log files to AWS DeepLens
- E. Install Amazon Kinesis Agent on the instances Stream the application log files to Amazon Kinesis Data Firehose and sot the destination to Amazon Elasticsearch Service

**Answer:** D

#### NEW QUESTION 8

- (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 AWS 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 9

- (Exam Topic 1)

A company's information security team wants to analyze Amazon EC2 performance and utilization data in the near-real time for anomalies. A Sec Engineer is responsible for log aggregation. The Engineer must collect logs from all of the company's AWS accounts in centralized location to perform the analysis.

How should the Security Engineer do this?

Log in to each account four te a day and filter the AWS CloudTrail log data, then copy and paste the logs in to the Amazon S3 bucket in the destination account.

- A. Set up Amazon CloudWatch to stream data to an Amazon S3 bucket in each source account
- B. Set up bucket replication for each source account into a centralized bucket owned by the security Engineer.
- C. Set up an AWS Config aggregator to collect AWS configuration data from multiple sources.
- D. Set up an AWS config aggregator to collect AWS configuration data from multiple sources.
- E. Set up Amazon CloudWatch cross-account log data sharing with subscriptions in each account
- F. Send the logs to Amazon Kinesis Data Firehose in the Security Engineer's account.

**Answer:** A

#### NEW QUESTION 10

- (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 AWS KMS to resolve the URL on-the-fly after the user is authenticated.

**Answer:** B

#### NEW QUESTION 10

- (Exam Topic 1)

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

Which solution will meet this requirement?

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

**Answer:** A

#### NEW QUESTION 11

- (Exam Topic 1)

A Security Engineer is setting up an AWS CloudTrail trail for all regions in an AWS account. For added security, the logs are stored using server-side encryption with AWS 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:** D

#### NEW QUESTION 15

- (Exam Topic 1)

A Security Engineer has launched multiple Amazon EC2 instances from a private AMI using an AWS 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 AWS KMS permissions.
- C. The instance profile used with the EC2 instances is unable to query instance metadata.
- D. AWS currently does not have sufficient capacity in the Region.

**Answer:** C

#### NEW QUESTION 18

- (Exam Topic 1)

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

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

**Answer:** BD

### NEW QUESTION 19

- (Exam Topic 1)

A website currently runs on Amazon EC2 with mostly static content on the site. Recently, the site was subjected to a ODoS attack, and a Security Engineer was tasked with redesigning the edge security to help mitigate this risk in the future

What are some ways the Engineer could achieve this? (Select THREE )

- A. Use AWS X-Ray to inspect the traffic going to the EC2 instances
- B. Move the static content to Amazon S3 and front this with an Amazon CloudFront distribution
- C. Change the security group configuration to block the source of the attack traffic
- D. Use AWS WAF security rules to inspect the inbound traffic
- E. Use Amazon Inspector assessment templates to inspect the inbound traffic
- F. Use Amazon Route 53 to distribute traffic

**Answer:** BDF

### NEW QUESTION 21

- (Exam Topic 1)

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

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

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

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

**Answer:** B

### NEW QUESTION 23

- (Exam Topic 1)

A Security Engineer launches two Amazon EC2 instances in the same Amazon VPC but in separate Availability Zones. Each instance has a public IP address and is able to connect to external hosts on the internet. The two instances are able to communicate with each other by using their private IP addresses, but they are not able to communicate with each other when using their public IP addresses.

Which action should the Security Engineer take to allow communication over the public IP addresses?

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

**Answer:** D

### Explanation:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/security-group-rules-reference.html#sg-rules-other-ins>

### NEW QUESTION 28

- (Exam Topic 1)

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

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

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

**Answer:** B

### NEW QUESTION 30

- (Exam Topic 1)

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

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

What should the security engineer do to resolve this issue?

- A. Set up an Amazon CloudWatch Event rule to forward all GuardDuty findings to the security account. Use an AWS Lambda function as a target to raise findings.
- B. Set up an Amazon CloudWatch Events rule to forward all GuardDuty findings to the security account. Use an AWS Lambda function as a target to raise findings.

in AWS Security Hub

- C. Check that GuardDuty in the security account is able to assume a role in the compromised account using the GuardDuty fast findings permission Schedule an Amazon CloudWatch Events rule and an AWS Lambda function to periodically check for GuardDuty findings
- D. Use the aws GuardDuty get-members AWS CLI command in the security account to see if the account is listed Send an invitation from GuardDuty in the security account to GuardDuty in the compromised account Accept the invitation to forward all future GuardDuty findings

**Answer: D**

### NEW QUESTION 33

- (Exam Topic 1)

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

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

**Answer: B**

### NEW QUESTION 35

- (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 cluster 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 secure, engineer's solution involve the least amount of effort and maintain 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 AWS 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 EC 2 instances to prevent direct access from the internet
- C. Create an Amazon CloudFront distribution specifying one EC2 instance as an origin Create an AWS 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 AWS 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 38

- (Exam Topic 1)

A security engineer has noticed an unusually high amount of traffic coming from a single IP address. This was discovered by analyzing the Application Load Balancer's access logs. How can the security engineer limit the number of requests from a specific IP address without blocking the IP address?

- A. Add a rule to the Application Load Balancer to route the traffic originating from the IP address in question and show a static webpage.
- B. Implement a rate-based rule with AWS WAF
- C. Use AWS Shield to limit the originating traffic hit rate.
- D. Implement the GeoLocation feature in Amazon Route 53.

**Answer: B**

### NEW QUESTION 40

- (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 44

- (Exam Topic 1)

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

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

**Answer:** ACD

#### NEW QUESTION 48

- (Exam Topic 1)

A company uses SAML federation with AWS Identity and Access Management (IAM) to provide internal users with SSO for their AWS accounts. The company's identity provider certificate was rotated as part of its normal lifecycle. Shortly after, users started receiving the following error when attempting to log in: "Error: Response Signature Invalid (Service: AWSSecurityTokenService; Status Code: 400; Error Code: InvalidIdentityToken)"

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

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

**Answer:** AD

#### NEW QUESTION 52

- (Exam Topic 1)

After multiple compromises of its Amazon EC2 instances, a company's Security Officer is mandating that memory dumps of compromised instances be captured for further analysis. A Security Engineer just received an EC2 abuse notification report from AWS stating that an EC2 instance running the most recent Windows Server 2019 Base AMI is compromised.

How should the Security Engineer collect a memory dump of the EC2 instance for forensic analysis?

- A. Give consent to the AWS Security team to dump the memory core on the compromised instance and provide it to AWS Support for analysis.
- B. Review memory dump data that the AWS Systems Manager Agent sent to Amazon CloudWatch Logs.
- C. Download and run the EC2Rescue for Windows Server utility from AWS.
- D. Reboot the EC2 Windows Server, enter safe mode, and select memory dump.

**Answer:** B

#### NEW QUESTION 54

- (Exam Topic 1)

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

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

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

**Answer:** C

#### NEW QUESTION 59

- (Exam Topic 1)

A company's Security Engineer has been asked to monitor and report all AWS 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 AWS 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 AWS account for any root user activity
- D. Configuring AWS 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 63

- (Exam Topic 1)

A global company must mitigate and respond to DDoS attacks at Layers 3, 4 and 7 All of the company's AWS 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 AWS WAF with an upgrade to the AWS Business support plan
- B. Use AWS Certificate Manager with an Application Load Balancer configured with an origin access identity
- C. Use AWS Shield Advanced
- D. Use AWS WAF to protect AWS Lambda functions encrypted with AWS KMS and a NACL restricting all Ingress traffic

**Answer: C**

#### NEW QUESTION 68

- (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 AWS 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 AWS Key Management Services to encrypt all the traffic between the client and application servers.

**Answer: BD**

#### NEW QUESTION 72

- (Exam Topic 1)

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

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

**Answer: B**

#### NEW QUESTION 77

- (Exam Topic 1)

Unapproved changes were previously made to a company's Amazon S3 bucket. A security engineer configured AWS 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 AWS Config to record changes to the buckets.
- B. Configure policies attached to S3 buckets to allow AWS 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 AWS Config actions.
- E. Assign the AWSConfigRole managed policy to the AWS Config role

**Answer: BE**

#### NEW QUESTION 81

- (Exam Topic 1)

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

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

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

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

**Answer: B**

#### NEW QUESTION 83

- (Exam Topic 1)

A Security Engineer for a large company is managing a data processing application used by 1,500 subsidiary companies. The parent and subsidiary companies all use AWS. The application uses TCP port 443 and runs on Amazon EC2 behind a Network Load Balancer (NLB). For compliance reasons, the application should only be accessible to the subsidiaries and should not be available on the public internet. To meet the compliance requirements for restricted access, the Engineer has received the public and private CIDR block ranges for each subsidiary

What solution should the Engineer use to implement the appropriate access restrictions for the application?

- A. Create a NACL to allow access on TCP port 443 from the 1,500 subsidiary CIDR block ranges. Associate the NACL to both the NLB and EC2 instances
- B. Create an AWS security group to allow access on TCP port 443 from the 1,500 subsidiary CIDR block range
- C. Associate the security group to the NL
- D. Create a second security group for EC2 instances with access on TCP port 443 from the NLB security group.
- E. Create an AWS PrivateLink endpoint service in the parent company account attached to the NL
- F. Create an AWS security group for the instances to allow access on TCP port 443 from the AWS PrivateLink endpoint
- G. Use AWS PrivateLink interface endpoints in the 1,500 subsidiary AWS accounts to connect to the data processing application.
- H. Create an AWS security group to allow access on TCP port 443 from the 1,500 subsidiary CIDR block range
- I. Associate the security group with EC2 instances.

**Answer: D**

#### NEW QUESTION 84

- (Exam Topic 1)

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

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

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

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

Answer: B

#### NEW QUESTION 88

- (Exam Topic 1)

A company is collecting AWS CloudTrail log data from multiple AWS 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 AWS Organizations trails, the company decided to further centralize management and automate deployment of the CloudTrail logging capability across all of its AWS accounts.

The company's security engineer created an AWS Organizations trail in the master account, enabled server-side encryption with AWS 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 cryptographic operations.

Answer: AD

#### NEW QUESTION 89

- (Exam Topic 1)

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

The engineer needs to block public S3 buckets without causing any outages on existing websites. The engineer has set up an Amazon CloudFront distribution for each website. Which set of steps should the security engineer implement next?

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

Answer: A

#### NEW QUESTION 90

- (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 AWS 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 95

- (Exam Topic 1)

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

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

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

Answer: BC

#### NEW QUESTION 99

- (Exam Topic 1)

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

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

- A. Update the password length policy in the on-premises Active Directory configuration.
- B. Update the password length policy in the IAM configuration.

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

**Answer:** AD

#### NEW QUESTION 104

- (Exam Topic 1)

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

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

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

**Answer:** AD

#### Explanation:

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

#### NEW QUESTION 106

- (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 AWS 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 110

- (Exam Topic 1)

A company has implemented centralized logging and monitoring of AWS CloudTrail logs from all Regions in

an Amazon S3 bucket. The log files are encrypted using AWS 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 114

- (Exam Topic 1)

A company is using AWS Organizations to manage multiple AWS 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 AWS 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 117

- (Exam Topic 1)

A company is designing the securely architecture (or a global latency-sensitive web application it plans to deploy to AWS. A Security Engineer needs to configure a highly available and secure two-tier architecture. The security design must include controls to prevent common attacks such as DDoS, cross-site scripting, and SQL injection.

Which solution meets these requirements?

- A. Create an Application Load Balancer (ALB) that uses public subnets across multiple Availability Zones within a single Region
- B. Point the ALB to an Auto Scaling group with Amazon EC2 instances in private subnets across multiple Availability Zones within the same Region
- C. Create an AmazonCloudFront distribution that uses the ALB as its origin

- D. Create appropriate AWS WAF ACLs and enable them on the CloudFront distribution.
- E. Create an Application Load Balancer (ALB) that uses private subnets across multiple Availability Zones within a single Region
- F. Point the ALB to an Auto Scaling group with Amazon EC2 instances in private subnets across multiple Availability Zones within the same Region
- G. Create an Amazon CloudFront distribution that uses the ALB as its origin
- H. Create appropriate AWS WAF ACLs and enable them on the CloudFront distribution.
- I. Create an Application Load Balancer (ALB) that uses public subnets across multiple Availability Zones within a single Region
- J. Point the ALB to an Auto Scaling group with Amazon EC2 instances in private subnets across multiple Availability Zones within the same Region
- K. Create appropriate AWS WAF ACLs and enable them on the ALB.
- L. Create an Application Load Balancer (ALB) that uses private subnets across multiple Availability Zones within a single Region
- M. Point the ALB to an Auto Scaling group with Amazon EC2 instances in private subnets across multiple Availability Zones within the same Region
- N. Create appropriate AWS WAF ACLs and enable them on the ALB.

**Answer: A**

#### NEW QUESTION 121

- (Exam Topic 1)

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

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

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

**Answer: B**

#### NEW QUESTION 125

- (Exam Topic 1)

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

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

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

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

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

**Answer: D**

#### NEW QUESTION 129

- (Exam Topic 1)

A security engineer has been tasked with implementing a solution that allows the company's development team to have interactive command line access to Amazon EC2 Linux instances using the AWS Management Console.

Which steps should the security engineer take to satisfy this requirement while maintaining least privilege?

- A. Enable AWS Systems Manager in the AWS Management Console and configure for access to EC2 instances using the default AmazonEC2RoleforSSM role.
- B. Install the Systems Manager Agent on all EC2 Linux instances that need interactive access.
- C. Configure IAM user policies to allow development team access to the Systems Manager Session Manager and attach to the team's IAM users.
- D. Enable console SSH access in the EC2 console.
- E. Configure IAM user policies to allow development team access to the AWS Systems Manager Session Manager and attach to the development team's IAM users.
- F. Enable AWS Systems Manager in the AWS Management Console and configure to access EC2 instances using the default AmazonEC2RoleforSSM role.
- G. Install the Systems Manager Agent on all EC2 Linux instances that need interactive access.
- H. Configure a security group that allows SSH port 22 from all published IP addresses.
- I. Configure IAM user policies to allow development team access to the AWS Systems Manager Session Manager and attach to the team's IAM users.
- J. Enable AWS Systems Manager in the AWS Management Console and configure to access EC2 instances using the default AmazonEC2RoleforSSM role. Install the Systems Manager Agent on all EC2 Linux instances that need interactive access.
- K. Configure IAM policies to allow development team access to the EC2 console and attach to the team's IAM users.

**Answer: A**

#### NEW QUESTION 132

- (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 AWS WAF to block requests with a string match condition for the user agent of the IoT device.
- B. Associate the web ACL with the ALB.
- C. Configure an Amazon CloudFront distribution to use the ALB as its origin.
- D. Configure a web ACL rule for AWS 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 AWS 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 AWS Shield Advanced to enable DDoS protection
- J. Apply an AWS 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 134**

- (Exam Topic 1)

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

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

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

**Answer: AB**

#### **NEW QUESTION 139**

- (Exam Topic 1)

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

What is the likely cause of this access denial?

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

**Answer: D**

#### **NEW QUESTION 140**

- (Exam Topic 1)

A company is developing a new mobile app for social media sharing. The company's development team has decided to use Amazon S3 to store all media files generated by mobile app users The company wants to allow users to control whether their own files are public, private, or shared with other users in their social network what should the development team do to implement the type of access control with the LEAST administrative effort?

- A. Use individual ACLs on each S3 object.
- B. Use IAM groups for sharing files between application social network users
- C. Store each user's files in a separate S3 bucket and apply a bucket policy based on the user's sharing settings
- D. Generate presigned URLs for each file access

**Answer: A**

#### **NEW QUESTION 145**

- (Exam Topic 1)

A security engineer has noticed an unusually high amount of traffic coming from a single IP address. This was discovered by analyzing the Application Load Balancer's access logs. How can the security engineer limit the number of requests from a specific IP address without blocking the IP address?

- A. Add a rule to the Application Load Balancer to route the traffic originating from the IP address in question and show a static webpage.
- B. Implement a rate-based rule with AWS WAF
- C. Use AWS Shield to limit the originating traffic hit rate.
- D. Implement the GeoLocation feature in Amazon Route 53.

**Answer: C**

#### **NEW QUESTION 148**

- (Exam Topic 1)

A Security Administrator at a university is configuring a fleet of Amazon EC2 instances. The EC2 instances are shared among students, and non-root SSH access is allowed. The Administrator is concerned about students attacking other AWS account resources by using the EC2 instance metadata service.

What can the Administrator do to protect against this potential attack?

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

**Answer: A**

**Explanation:**

"To turn off access to instance metadata on an existing instance....." <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/configuring-instance-metadata-service.html> You can disable the service for existing (running or stopped) ec2 instances. <https://docs.aws.amazon.com/cli/latest/reference/ec2/modify-instance-metadata-options.html>

#### NEW QUESTION 152

- (Exam Topic 1)

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

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

**Answer: B**

#### NEW QUESTION 154

- (Exam Topic 1)

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

Which of the following actions could fix this issue?

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

**Answer: C**

#### NEW QUESTION 158

- (Exam Topic 1)

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

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

**Answer: C**

#### NEW QUESTION 161

- (Exam Topic 2)

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

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

**Answer: C**

#### Explanation:

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

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

A network access control list (ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC.

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

#### NEW QUESTION 164

- (Exam Topic 2)

A Software Engineer wrote a customized reporting service that will run on a fleet of Amazon EC2 instances. The company security policy states that application logs for the reporting service must be centrally collected. What is the MOST efficient way to meet these requirements?

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

**Answer: D**

**Explanation:**

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

**NEW QUESTION 168**

- (Exam Topic 2)

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

Which of the following actions would resolve this issue?

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

**Answer: C**

**NEW QUESTION 173**

- (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.
- > AWS 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 annual
- 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 annual
- 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 177**

- (Exam Topic 2)

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

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

When trying to download an object from the S3 bucket from 10.10.10.40, the IAM user receives an access denied message. What does the Administrator need to change to grant access to the user?

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

**Answer:** A

#### NEW QUESTION 182

- (Exam Topic 2)

A company has five AWS accounts and wants to use AWS 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 AWS 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 AWS 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 AWS Key Management Service

**Answer:** ACE

#### Explanation:

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

If you have created an organization in AWS Organizations, you can create a trail that will log all events for all AWS 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 AWS Organizations, see Organizations Terminology and Concepts. Note Reference: <https://docs.aws.amazon.com/awscloudtrail/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 186

- (Exam Topic 2)

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

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

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

**Answer: B**

**NEW QUESTION 190**

- (Exam Topic 2)

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

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

**Answer: BEF**

**NEW QUESTION 193**

- (Exam Topic 2)

An AWS 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 AWS 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 AWS 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://aws.amazon.com/blogs/security/iam-policies-and-bucket-policies-and-acls-oh-my-controlling-access-to-s>

#### NEW QUESTION 194

- (Exam Topic 2)

Which of the following is not a best practice for carrying out a security audit? Please select:

- A. Conduct an audit on a yearly basis
- B. Conduct an audit if application instances have been added to your account
- C. Conduct an audit if you ever suspect that an unauthorized person might have accessed your account
- D. Whenever there are changes in your organization

**Answer:** A

#### Explanation:

A year's time is generally too long a gap for conducting security audits. The AWS Documentation mentions the following:

You should audit your security configuration in the following situations: On a periodic basis.

If there are changes in your organization, such as people leaving.

If you have stopped using one or more individual AWS services. This is important for removing permissions that users in your account no longer need.

If you've added or removed software in your accounts, such as applications on Amazon EC2 instances, AWS OpsWorks stacks, AWS CloudFormation templates, etc.

If you ever suspect that an unauthorized person might have accessed your account.

Option B, C and D are all the right ways and recommended best practices when it comes to conducting audits. For more information on Security Audit guideline, please visit the below URL:

<https://docs.aws.amazon.com/eeneral/latest/gr/aws-security-audit-euide.html>

The correct answer is: Conduct an audit on a yearly basis. Submit your Feedback/Queries to our Experts.

#### NEW QUESTION 195

- (Exam Topic 2)

A Security Engineer is trying to determine whether the encryption keys used in an AWS service are in compliance with certain regulatory standards.

Which of the following actions should the Engineer perform to get further guidance?

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 200

- (Exam Topic 2)

A company wants to have a secure way of generating, storing and managing cryptographic exclusive access for the keys. Which of the following can be used for this purpose?

Please select:

- A. Use KMS and the normal KMS encryption keys
- B. Use KMS and use an external key material
- C. Use S3 Server Side encryption
- D. Use Cloud HSM

**Answer:** D

#### Explanation:

The AWS Documentation mentions the following:

The AWS CloudHSM service helps you meet corporate, contractual and regulatory compliance requirements for data security by using dedicated Hardware Security Module (HSM) instances within the AWS cloud. AWS and AWS Marketplace partners offer a variety of solutions for protecting sensitive data within the AWS platform, but for some applications and data subject to contractual or regulatory mandates for managing cryptographic keys, additional protection may be necessary. CloudHSM complements existing data protection solutions and allows you to protect your encryption keys within HSMs that are designed and validated to government standards for secure key management. CloudHSM allows you to securely generate, store and manage cryptographic keys used for data encryption in a way that keys are accessible only by you.

Option A, B and C are invalid because in all of these cases, the management of the key will be with AWS. Here the question specifically mentions that you want to have exclusive access over the keys. This can be achieved with Cloud HSM.

For more information on CloudHSM, please visit the following URL: <https://aws.amazon.com/cloudhsm/faq>

The correct answer is: Use Cloud HSM. Submit your Feedback/Queries to our Experts.

#### NEW QUESTION 204

- (Exam Topic 2)

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

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

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

**Answer:** ADF

**Explanation:**

[https://github.com/awslabs/aws-well-architected-labs/blob/master/Security/300\\_Incident\\_Response\\_with\\_AWS](https://github.com/awslabs/aws-well-architected-labs/blob/master/Security/300_Incident_Response_with_AWS)

**NEW QUESTION 205**

- (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.aws.amazon.com/elasticloadbalancing/latest/application/create-https-listener.html>

**NEW QUESTION 210**

- (Exam Topic 2)

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

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

The IAM user policy is as follows:

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

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

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

**Answer: CE**

**Explanation:**

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

**NEW QUESTION 215**

- (Exam Topic 2)

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

Please select:

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

**Answer: B**

**Explanation:**

The AWS Documentation gives an example on such a case

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

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

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

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

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

#### NEW QUESTION 217

- (Exam Topic 2)

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

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

**Answer:** B

#### Explanation:

[https://d1.awsstatic.com/whitepapers/aws\\_security\\_incident\\_response.pdf](https://d1.awsstatic.com/whitepapers/aws_security_incident_response.pdf)

#### NEW QUESTION 218

- (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 AWS Security Groups, please visit the following UR <https://docs.aws.amazon.com/AWSEC2/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 223

- (Exam Topic 2)

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

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

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

**Answer:** CE

#### NEW QUESTION 226

- (Exam Topic 2)

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

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

**Answer:** B

#### Explanation:

The AWS Documentation states the following

AWS KMS is integrated with CloudTrail, a service that captures API calls made by or on behalf of AWS KMS in your AWS account and delivers the log files to an Amazon S3 bucket that you specify. CloudTrail captures API calls from the AWS KMS console or from the AWS KMS API. Using the information collected by CloudTrail, you can determine what request was made, the source IP address from which the request was made, who made the request when it was made, and so on.

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

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

<https://docs.aws.amazon.com/kms/latest/developerguide/loeeing-usine-cloudtrail.html> The correct answer is: Enable a trail in Cloudtrail

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 228

- (Exam Topic 2)

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

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

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

**Answer:** BE

#### NEW QUESTION 230

- (Exam Topic 2)

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

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

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

**Answer:** D

#### Explanation:

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

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

#### NEW QUESTION 235

- (Exam Topic 2)

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

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

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

**Answer:** ACE

#### Explanation:

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

#### NEW QUESTION 236

- (Exam Topic 2)

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

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

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 240

- (Exam Topic 2)

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

How can the Security Engineer further protect currently running instances?

- A. Delete the key-pair key from the EC2 console, then create a new key pair.
- B. Use the modify-instance-attribute API to change the key on any EC2 instance that is using the key.

- C. Use the EC2 RunCommand to modify the authorized\_keys file on any EC2 instance that is using the key.
- D. Update the key pair in any AMI used to launch the EC2 instances, then restart the EC2 instances.

**Answer:** C

#### NEW QUESTION 241

- (Exam Topic 2)

A Software Engineer is trying to figure out why network connectivity to an Amazon EC2 instance does not appear to be working correctly. Its security group allows inbound HTTP traffic from 0.0.0.0/0, and the outbound rules have not been modified from the default. A custom network ACL associated with its subnet allows inbound HTTP traffic from 0.0.0.0/0 and has no outbound rules.

What would resolve the connectivity issue?

- A. The outbound rules on the security group do not allow the response to be sent to the client on the ephemeral port range.
- B. The outbound rules on the security group do not allow the response to be sent to the client on the HTTP port.
- C. An outbound rule must be added to the network ACL to allow the response to be sent to the client on the ephemeral port range.
- D. An outbound rule must be added to the network ACL to allow the response to be sent to the client on the HTTP port.

**Answer:** C

#### Explanation:

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html>

#### NEW QUESTION 244

- (Exam Topic 2)

Your IT Security team has advised to carry out a penetration test on the resources in their company's AWS 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 AWS Support
- D. Use a custom AWS Marketplace solution for conducting the penetration test

**Answer:** C

#### Explanation:

This concept is given in the AWS Documentation

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

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

Resolution

Before performing security testing on AWS resources, you must obtain approval from AWS. After you submit your request AWS will reply in about two business days.

AWS 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 AWS for penetration tests

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

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

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

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

#### NEW QUESTION 247

- (Exam Topic 2)

An application outputs logs to a text file. The logs must be continuously monitored for security incidents.

Which design will meet the requirements with MINIMUM effort?

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 250

- (Exam Topic 2)

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

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

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

**Answer: B**

#### NEW QUESTION 255

- (Exam Topic 2)

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

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

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

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

**Answer: B**

#### NEW QUESTION 259

- (Exam Topic 2)

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

- A. Enable AWS Guard Duty for the Instance
- B. Use AWS Trusted Advisor
- C. Use AWS inspector
- D. UseAWSMacie

**Answer: C**

#### Explanation:

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

Center for Internet security (CIS) Benchmarks

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

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

on the guidelines, please visit the below URL:

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

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 264

- (Exam Topic 2)

A Security Administrator is performing a log analysis as a result of a suspected AWS account compromise. The Administrator wants to analyze suspicious AWS CloudTrail log files but is overwhelmed by the volume of audit logs being generated.

What approach enables the Administrator to search through the logs MOST efficiently?

- A. Implement a "write-only" CloudTrail event filter to detect any modifications to the AWS account resources.
- B. Configure Amazon Macie to classify and discover sensitive data in the Amazon S3 bucket that contains the CloudTrail audit logs.
- C. Configure Amazon Athena to read from the CloudTrail S3 bucket and query the logs to examine account activities.
- D. Enable Amazon S3 event notifications to trigger an AWS Lambda function that sends an email alarm when there are new CloudTrail API entries.

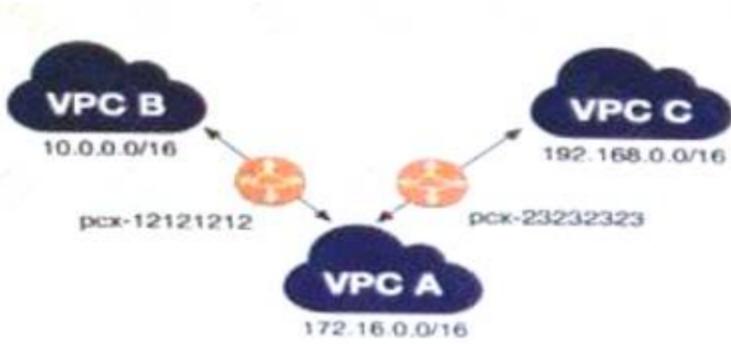
**Answer: C**

#### NEW QUESTION 265

- (Exam Topic 2)

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

How can this be accomplished? (Choose two.)



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

**Answer:** BD

**Explanation:**

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

**NEW QUESTION 269**

- (Exam Topic 2)

You are designing a custom IAM policy that would allow uses to list buckets in S3 only if they are MFA authenticated. Which of the following would best match this requirement?

- A. 

```
C:\Users\wk\Desktop\mudassar\Untitled.jpg "Version": "2012-10-17",
"Statement": {
  "Effect": "Allow",
  "Action": [
    "s3:ListAllMyBuckets",
    "s3:GetBucketLocation"
  ],
  "Resource": "Resource": "arn:aws:s3::*",
  "Condition": {
    "Bool": {"aws:MultiFactorAuthPresent": true}
  }
}
```
- B. 

```
C:\Users\wk\Desktop\mudassar\Untitled.jpg "Version": "2012-10-17",
"Statement": {
  "Effect": "Allow",
  "Action": [
    "s3:ListAllMyBuckets",
    "s3:GetBucketLocation"
  ],
  "Resource": "Resource": "arn:aws:s3::*",
  "Condition": {
    "Bool": {"aws:MultiFactorAuthPresent":false}
  }
}
```
- C. 

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

```

"Version": "2012-10-17",
"Statement": {
  "Effect": "Allow",
  "Action": [
    "s3:ListAllMyBuckets",
    "s3:GetBucketLocation"
  ],
  "Resource": "Resource": "arn:aws:s3:*:*:*",
  "Condition": {
    "aws:MultiFactorAuthPresent":false
  }
}
}
}

```

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

```

"Version": "2012-10-17",
"Statement": {
  "Effect": "Allow",
  "Action": [
    "s3:ListAllMyBuckets",
    "s3:GetBucketLocation"
  ],
  "Resource": "Resource": "arn:aws:s3:*:*:*",
  "Condition": {
    "aws:MultiFactorAuthPresent":true
  }
}
}
}

```

**Answer:** A

**Explanation:**

The Condition clause can be used to ensure users can only work with resources if they are MFA authenticated. Option B and C are wrong since the aws:MultiFactorAuthPresent clause should be marked as true. Here you are saying that onl if the user has been MFA activated, that means it is true, then allow access. Option D is invalid because the "boor clause is missing in the evaluation for the condition clause. Boolean conditions let you construct Condition elements that restrict access based on comparing a key to "true" or "false." Here in this scenario the boot attribute in the condition element will return a value True for option A which will ensure that access is allowed on S3 resources. For more information on an example on such a policy, please visit the following URL:

**NEW QUESTION 274**

- (Exam Topic 2)

An organization has three applications running on AWS, each accessing the same data on Amazon S3. The data on Amazon S3 is server-side encrypted by using an AWS 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 AWS 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 279**

- (Exam Topic 2)

You have an S3 bucket hosted in AWS. 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 AWS 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.aws.amazon.com/AmazonS3/latest/dev/ShareObjectPreSignedURL.html>  
The correct answer is: Use Pre-signed URL's Submit your Feedback/Queries to our Experts

#### NEW QUESTION 281

- (Exam Topic 2)

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

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

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 285

- (Exam Topic 2)

For compliance reasons, an organization limits the use of resources to three specific AWS regions. It wants to be alerted when any resources are launched in unapproved regions.

Which of the following approaches will provide alerts on any resources launched in an unapproved region?

- A. Develop an alerting mechanism based on processing AWS CloudTrail logs.
- B. Monitor Amazon S3 Event Notifications for objects stored in buckets in unapproved regions.
- C. Analyze Amazon CloudWatch Logs for activities in unapproved regions.
- D. Use AWS Trusted Advisor to alert on all resources being created.

**Answer: A**

#### Explanation:

<https://stackoverflow.com/questions/45449053/cloudwatch-alert-on-any-instance-creation>

#### NEW QUESTION 287

- (Exam Topic 2)

A company plans to migrate a sensitive dataset to Amazon S3. A Security Engineer must ensure that the data is encrypted at rest. The encryption solution must enable the company to generate its own keys without needing to manage key storage or the encryption process. What should the Security Engineer use to accomplish this?

- A. Server-side encryption with Amazon S3-managed keys (SSE-S3)
- B. Server-side encryption with AWS KMS-managed keys (SSE-KMS)
- C. Server-side encryption with customer-provided keys (SSE-C)
- D. Client-side encryption with an AWS KMS-managed CMK

**Answer: B**

#### Explanation:

Reference <https://aws.amazon.com/s3/faqs/>

#### NEW QUESTION 289

- (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 AWS Trusted Advisor to see what can be done.
- B. Use VPC Flow logs to diagnose the traffic
- C. Use AWS WAF to analyze the traffic
- D. Use AWS 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 AWS 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 AWS Security, please visit the following URL: <https://aws.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 294

- (Exam Topic 2)

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

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

**Answer:** B

#### Explanation:

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

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

#### NEW QUESTION 298

- (Exam Topic 2)

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

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

- A. Add the `aws:sourceVpce` condition to the AWS 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 AWS KMS with private DNS enabled.
- D. Use the KMS Import Key feature to securely transfer the AWS KMS key over a VPN.
- E. Add the following condition to the AWS KMS key policy: `"aws: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": {  
  "aws:sourceVpce": "vpce-0295a3caf8414c94a"  
}}
```

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

#### NEW QUESTION 303

- (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 it.
- B. Perform inspection within proxy software on the EC2 instance.
- C. Configure the host-based agent on each EC2 instance within the VPC.
- D. Perform inspection within the host-based agent.
- E. Enable VPC Flow Logs for all subnets in the VPC.
- 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 VPC.
- 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 AWS services and third party IDS/IPS solutions offered in AWS Marketplace to stay one step ahead of potential attackers."

#### NEW QUESTION 308

- (Exam Topic 2)

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

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

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

- F. Use VPC Flow Logs and AWS Lambda to restrict egress traffic to specific whitelisted URLs.
- G. Use AWS WAF to scan inbound traffic for web exploit
- H. Use a third-party AWS Marketplace solution to restrict egress traffic to specific whitelisted URLs.

**Answer: D**

**Explanation:**

AWS Shield is mainly for DDoS Attacks. AWS WAF is mainly for some other types of attacks like Injection and XSS etc. In this scenario, it seems it is WAF functionality that is needed. VPC logs do show the source and destination IP and Port, they never show any URL.. because URL are level 7 while VPC are concerned about lower network levels.  
<https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html>

**NEW QUESTION 312**

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

**Answer: B**

**Explanation:**

MetricFilter:

Type: 'AWS::Logs::MetricFilter' Properties:

LogGroupName: " FilterPattern: >

```
{ ($.eventName = AuthorizeSecurityGroupIngress) || ($.eventName = AuthorizeSecurityGroupEgress) || ($.eventName = RevokeSecurityGroupIngress) ||
 ($.eventName = RevokeSecurityGroupEgress)
 || ($.eventName = CreateSecurityGroup) || ($.eventName = DeleteSecurityGroup) }
```

MetricTransformations:

- MetricValue: '1'

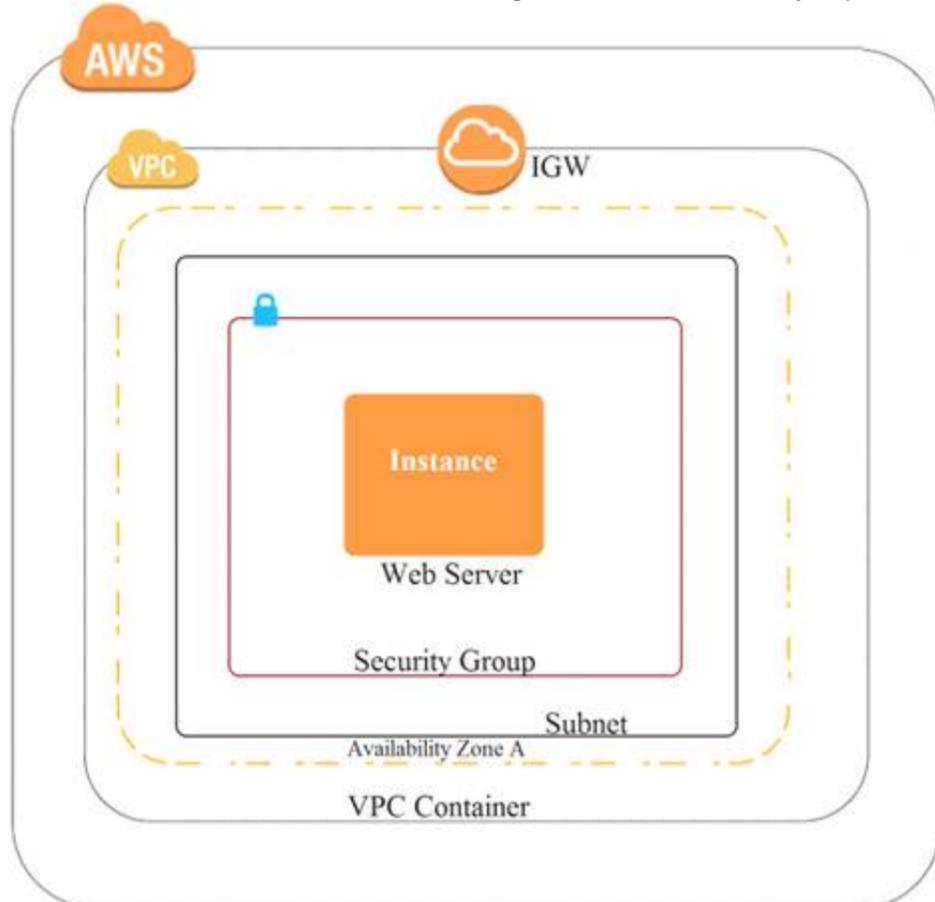
MetricNamespace: CloudTrailMetrics MetricName: SecurityGroupEventCount

**NEW QUESTION 313**

- (Exam Topic 2)

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

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



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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 318**

- (Exam Topic 2)

A Security Engineer must add additional protection to a legacy web application by adding the following HTTP security headers:

- Content Security-Policy
- X-Frame-Options
- X-XSS-Protection

The Engineer does not have access to the source code of the legacy web application. Which of the following approaches would meet this requirement?

- A. Configure an Amazon Route 53 routing policy to send all web traffic that does not include the required headers to a black hole.
- B. Implement an AWS Lambda@Edge origin response function that inserts the required headers.
- C. Migrate the legacy application to an Amazon S3 static website and front it with an Amazon CloudFront distribution.
- D. Construct an AWS WAF rule to replace existing HTTP headers with the required security headers by using regular expressions.

**Answer:** B

**NEW QUESTION 319**

- (Exam Topic 2)

Your company has defined privileged users for their AWS 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 AWS 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 AWS For more information on IAM best practices, please visit the below URL

<https://docs.aws.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 323**

- (Exam Topic 2)

A company plans to move most of its IT infrastructure to AWS. They want to leverage their existing on-premises Active Directory as an identity provider for AWS. Which combination of steps should a Security Engineer take to federate the company's on-premises Active Directory with AWS? (Choose two.)

- A. Create IAM roles with permissions corresponding to each Active Directory group.
- B. Create IAM groups with permissions corresponding to each Active Directory group.
- C. Configure Amazon Cloud Directory to support a SAML provider.
- D. Configure Active Directory to add relying party trust between Active Directory and AWS.
- E. Configure Amazon Cognito to add relying party trust between Active Directory and AWS.

**Answer:** AD

**Explanation:**

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

**NEW QUESTION 326**

- (Exam Topic 2)

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

Please select:

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

**Answer:** B

**Explanation:**

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

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

For more information on authorizing access to an instance, please visit the below URL: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/authorizing-access-to-an-instance.html>

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

**NEW QUESTION 329**

- (Exam Topic 2)

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

What is the SIMPLEST way to meet these requirements?

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

**Answer: C**

**NEW QUESTION 330**

.....

## **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

### **AWS-Certified-Security-Specialty Practice Exam Features:**

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

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The AWS-Certified-Security-Specialty Practice Test Here](#)**