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

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

2. A company hosts business-critical applications on Amazon EC2 instances in a VPC. The VPC uses default DHCP options sets. A security engineer needs to log all DNS queries that internal resources make in the VPC. The security engineer also must create a list of the most common DNS queries over time.

Which solution will meet these requirements?

- A. Install the Amazon CloudWatch agent on each EC2 instance in the VPC. Use the CloudWatch agent to stream the DNS query logs to an Amazon CloudWatch Logs log group. Use CloudWatch metric filters to automatically generate metrics that list the most common DNS queries.
- B. Install a BIND DNS server in the VPC. Create a bash script to list the DNS request number of common DNS queries from the BIND logs.
- C. Create VPC flow logs for all subnets in the VPStream the flow logs to an Amazon CloudWatch Logs log group. Use CloudWatch Logs Insights to list the most common DNS queries for the log group in a custom dashboard.
- D. Configure Amazon Route 53 Resolver query logging. Add an Amazon CloudWatch Logs log group as the destination. Use Amazon

CloudWatch Contributor Insights to analyze the data and create time series that display the most common DNS queries.

3. A company had one of its Amazon EC2 key pairs compromised. A Security Engineer must identify which current Linux EC2 instances were deployed and used the compromised key pair.
How can this task be accomplished?

- A. Obtain the list of instances by directly querying Amazon EC2 using: aws ec2 describe-instances --fi1ters "Name=key-name,Values=KEYNAMEHERE".
- B. Obtain the fingerprint for the key pair from the AWS Management Console, then search for the fingerprint in the Amazon Inspector logs.
- C. Obtain the output from the EC2 instance metadata using: curl http: //169.254.169.254/latest/meta-data/public- keys/0/.
- D. Obtain the fingerprint for the key pair from the AWS Management Console, then search for the fingerprint in Amazon CloudWatch Logs using: aws logs filter-log-events.

4. A security team is using Amazon EC2 Image Builder to build a hardened AMI with forensic capabilities. An AWS Key Management Service (AWS KMS) key will encrypt the forensic AMI. EC2 Image Builder successfully installs the required patches and packages in the security team’s AWS account. The security team uses a federated IAM role in the same AWS account to sign in to the AWS Management Console and attempts to launch the forensic AMI. The EC2 instance launches and immediately terminates.

What should the security team do to launch the EC2 instance successfully?

- A. Update the policy that is associated with the federated IAM role to allow the ec2:DescribeImages action for the forensic AML.
- B. Update the policy that is associated with the federated IAM role to allow the ec2:StartInstances action in the security team's AWS account.

- C. Update the policy that is associated with the KMS key that is used to encrypt the forensic AMI. Configure the policy to allow the kms:Encrypt and kms:Decrypt actions for the federated IAM role.

- D. Update the policy that is associated with the federated IAM role to allow the kms:DescribeKey action for the KMS key that is used to encrypt the forensic AMI.

5. A Security Administrator is restricting the capabilities of company root user accounts. The company uses AWS Organizations and has enabled it for all feature sets, including consolidated billing. The top-level account is used for billing and administrative purposes, not for operational AWS resource purposes.
How can the Administrator restrict usage of member root user accounts across the organization?

- A. Disable the use of the root user account at the organizational root. Enable multi-factor authentication of the root user account for each organizational member account.

- B. Configure IAM user policies to restrict root account capabilities for each Organizations member account.

- C. Create an organizational unit (OU) in Organizations with a service control policy that controls usage of the root user. Add all operational accounts to the new OU.

- D. Configure AWS CloudTrail to integrate with Amazon CloudWatch Logs and then create a metric filter for RootAccountUsage.

6. A company is designing a new application stack. The design includes web servers and backend servers that are hosted on Amazon EC2 instances. The design also includes an Amazon Aurora MySQL DB cluster.

The EC2 instances are in an Auto Scaling group that uses launch templates. The EC2 instances for the web layer and the backend layer are backed by Amazon Elastic Block Store (Amazon EBS) volumes. No layers are encrypted at rest. A security engineer needs to implement encryption at rest.

Which combination of steps will meet these requirements? (Choose two.)

- A. Modify EBS default encryption setting in the target AWS Region to enable encryption. Use an Auto Scaling group instance refresh.
- B. Modify the launch templates for the web layer and the backend layer to add AWS Certificate Manager (ACM) encryption for the attached EBS volumes. Use an Auto Scaling group instance refresh.
- C. Create a new AWS Key Management Service (AWS KMS) encrypted DB cluster from a snapshot of the existing DB cluster.
- D. Apply AWS Key Management Service (AWS KMS) encryption to the existing DB cluster.
- E. Apply AWS Certificate Manager (ACM) encryption to the existing DB cluster.

7. 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.

8. A company wants to remove all ssh keys permanently from a specific subset of its Amazon Linux 2 Amazon EC2 instances that are using the same IAM instance profile. However, three individuals who have ISM user accounts will need to access these instances by using an SSH session to perform critical duties.

How can a security engineer provide the access to meet these requirements?

C Assign an IAM policy to the instance profile to allow the EC2 instances to be managed by AWS System Manager. Provide the IAM user accounts with permission to use Systems Manager. Remove the SSH keys from the EC2 instances. Use Systems Manager Session Manger to select the EC2 instance and connect.

9. 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.

10. A security team is developing an application on an Amazon EC2 instance to get objects from an Amazon S3 bucket. All objects in the S3 bucket are encrypted with an AWS Key Management Service (AWS KMS) CMK. All network traffic for requests that are made within the VPC is restricted to the AWS infrastructure. This traffic does not traverse the public internet.

The security team is unable to get objects from the S3 bucket.

Which factors could cause this issue? (Choose three.)

- A. The IAM instance profile that is attached to the EC2 instance does not allow the s3:ListBucket action to the S3 bucket in the AWS accounts.

- B. The IAM instance profile that is attached to the EC2 instance does not allow the s3:ListParts action to the S3 bucket in the AWS accounts.
- C. The KMS key policy that encrypts the object in the S3 bucket does not allow the kms:ListKeys action to the EC2 instance profile ARN.
- D. The KMS key policy that encrypts the object in the S3 bucket does not allow the kms:Decrypt action to the EC2 instance profile ARN.
- E. The security group that is attached to the EC2 instance is missing an outbound rule to the S3 managed prefix list over port 443.
- F. The security group that is attached to the EC2 instance is missing an inbound rule from the S3 managed prefix list over port 443.

11. A company's security team is building a solution for logging and visualization. The solution will assist the company with the large variety and velocity of data that it receives from AWS across multiple accounts. The security team has enabled AWS CloudTrail and VPC Flow Logs in all of its accounts In addition, the company has an organization in AWS Organizations and has an AWS Security Hub master account.

The security team wants to use Amazon Detective However the security team cannot enable Detective and is unsure why

What must the security team do to enable Detective?

- A. Enable Amazon Macie so that Secunty H jb will allow Detective to process findings from Macie.
- B. Disable AWS Key Management Service (AWS KMS) encryption on CtoudTrail logs in every member account of the organization
- C. Enable Amazon GuardDuty on all member accounts Try to enable Detective in 48 hours
- D. Ensure that the principal that launches Detective has the organizations ListAccounts permission

12. 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? (Choose two.)

- A. Download a new copy of the SAML metadata file from the identity provider. Create a new IAM identity provider entity. Upload the new metadata file to the new IAM identity provider entity.
- B. During the next certificate rotation period and before the current certificate expires, add a new certificate as the secondary to the identity provider. Generate a new metadata file and upload it to the IAM identity provider entity. Perform automated or manual rotation of the certificate when required.
- C. 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.
- D. During the next certificate rotation period and before the current certificate expires, add a new certificate as the secondary to the identity provider. Generate a new copy of the metadata file and create a new IAM identity provider entity. Upload the metadata file to the new IAM identity provider entity. Perform automated or manual rotation of the certificate when required.
- E. Download a new copy of the SAML metadata file from the identity provider. Create a new IAM identity provider entity. Upload the new metadata file to the new IAM identity provider entity. Update the identity provider configurations to pass a new IAM identity provider entity name in the SAML assertion.

13. A security administrator is setting up a new AWS account. The security administrator wants to secure the data that a company stores in an Amazon S3 bucket. The security administrator also wants to reduce the chance of unintended data exposure and the potential for misconfiguration of objects that are in the S3 bucket.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Configure the S3 Block Public Access feature for the AWS account.
- B. Configure the S3 Block Public Access feature for all objects that are in the bucket.
- C. Deactivate ACLs for objects that are in the bucket.
  D. Use AWS PrivateLink for Amazon S3 to access the bucket.

14. A systems engineer must design and troubleshoot AWS services for a new project. The project deploys applications onto two Amazon EC2 instances that are named EC2A and EC2B. Both instances need to encrypt dozens of files by using an AWS Key Management Service (AWS KMS) customer managed key.

The key has the following key policy:

```
{
    "Id": "key-consolepolicy-1",
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
            "Principal": { "AWS": "arn:aws:iam::123456789012:root" },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Allow use of the key",
            "Effect": "Allow",
            "Principal": {
                "AWS":
                    ["arn:aws:iam::123456789012:role/EC2RoleA","arn:aws:iam::123456789012:role/EC2RoleB"]
            },
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        }
    ]
}
```

EC2RoleA is the role that EC2A uses. This role does not have any IAM policy that is related to AWS KMS. EC2RoleB is the role that EC2B uses. This role has the following IAM policy:



```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Deny",

            "Action": [
                "kms:Decrypt",
                "kms:Encrypt",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        }
    ]
}
```

Both IAM roles are within the same AWS account that contains the customer managed key.

What will happen when EC2Aand EC2B attempt to use the customer managed key?

- A. Both EC2A and EC2B can use the customer managed key properly for encryption.
- B. Neither EC2A nor EC2B will be able to use the customer managed key for encryption.
- C. EC2A cannot use the customer managed key for encryption. EC2B can use the customer managed key for encryption.
- D. EC2A can use the customer managed key for encryption. EC2B cannot use the customer managed key for encryption.

15. 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 ɹ€Account spend limitɹ€ 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 ɹ€consecutive periodsɹ€ value is equal to, or greater than 1.

16. A company uses AWS Organizations. The company has teams that use an AWS CloudHSM hardware security module (HSM) that is hosted in a central AWS account. One of the teams creates its own new dedicated AWS account and wants to use the HSM that is hosted in the central account.

How should a security engineer share the HSM that is hosted in the central account with the new dedicated account?

- A. Use AWS Resource Access Manager (AWS RAM) to share the VPC subnet ID of the HSM that is hosted in the central account with the new dedicated account. Configure the CloudHSM security group to accept inbound traffic from the private IP addresses of client instances in the new dedicated account.

- B. Use AWS Identity and Access Management (IAM) to create a cross-account role to access the CloudHSM cluster that is in the central account. Create a new IAM user in the new dedicated account. Assign the cross-account role the new IAM user.

- C. Use AWS Single Sign-On to create an AWS Security Token Service (AWS STS) token to authenticate from the new dedicated account to the central account. Use the cross-account permissions that are assigned to the STS token to invoke an operation on the HSM in the central account.

- D. Use AWS Resource Access Manager (AWS RAM) to share the ID of the HSM that is hosted in the central account with the new dedicated account. Configure the CloudHSM security group to accept inbound traffic from the private IP addresses of client instances in the new dedicated account.

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

and the EC2 instances and the traffic between the EC2 instances.
Which combination of activities must the company implement to meet its encryption requirements? (Choose two.)

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

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

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

19. An application team wants to use AWS Certificate Manager (ACM) to request public certificates to ensure that data is secured in transit. The domains that are being used are not currently hosted on Amazon Route 53

The application team wants to use an AWS managed distribution and caching solution to optimize requests to its systems and provide better points of presence to customers The distribution solution will use a primary domain name that is customized The distribution solution also will use several alternative domain names The certificates must renew automatically over an indefinite period of time.

Which combination of steps should the application team take to deploy this architecture? (Select THREE.)

A. Request a certificate (torn ACM in the us-west-2 Region Add the domain names that the certificate will secure

B. Send an email message to the domain administrators to request vacation of the domains for ACM

C. Request validation of the domains for ACM through DNS Insert CNAME records into each domain's DNS zone

D. Create an Application Load Balancer for me caching solution Select the newly requested certificate from ACM to be used for secure connections

E. Create an Amazon CloudFront distribution for the caching solution Enter the main CNAME record as the Origin Name Enter the subdomain names or alternate names in the Alternate Domain Names Distribution Settings Select the newly requested certificate from ACM to be used for secure connections

F. Request a certificate from ACM in the us-east-1 Region Add the domain names that the certificate wil secure

20. 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? (Choose 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.

21. A company's application uses standard tier secure string parameters from AWS Systems Manager Parameter Store. The application is receiving error messages when the company tries to update a parameter. The parameter uses an AWS Key Management Service (AWS KMS) customer managed key for encryption and decryption.

What are the reasons for the error messages? (Choose two.)

- A. The application does not have the kms:Encrypt permission for the customer managed key.
- B. The customer managed key is already being used to encrypt another secure string parameter.
- C. Standard tier secure string parameters cannot use a customer managed key for encryption.
- D. The customer managed key that is specified in the application has its key state set to Disabled.
- E. The customer managed key that is specified in the application is using a key alias instead of a key ID.

22. A security engineer is configuring AWS Config for an AWS account that uses a new 1AM entity. When the security engineer tries to configure AWS Config rules and automatic remediation options, errors occur. In the AWS CloudTrail logs, the security engineer sees the following error message: "Insufficient delivery policy to s3 bucket: DOC-EXAMPLE-BUCKET, unable to write to bucket, provided s3 key prefix is 'null'."

Which combination of steps should the security engineer take to remediate this issue? (Choose two.)

- A. Check the Amazon S3 bucket policy. Verify that the policy allows the config.amazonaws.com service to write to the target bucket.
- B. Verify that the IAM entity has the permissions necessary to perform the s3:GetBucketAcl and s3:PutObject* operations to write to the target bucket.
- C. Verify that the Amazon S3 bucket policy has the permissions necessary to perform the s3:GetBucketAcl and s3:PutObject* operations to write to the target bucket.
- D. Check the policy that is associated with the IAM entity. Verify that the policy allows the config.amazonaws.com service to write to the target bucket.
- E. Verify that the AWS Config service role has permissions to invoke the BatchGetResourceConfig action instead of the GetResourceConfigHistory action and s3:PutObject* operation.

23. A company is using AWS Organizations with all features enabled. The company has an AWS management account under an organization's root and a small number of AWS accounts under a child OU. The company expects to grow by more than 1,000 AWS accounts in the next year.

The company wants to enforce a policy that disallows any configuration changes to AWS Config settings in all AWS Organizations member accounts automatically when the company creates member accounts. The company will enforce this policy on all existing accounts and on any future AWS accounts that the company creates. The company also wants a centralized view of the compliance status of all accounts.

Which solution will meet these requirements?

- A. Configure AWS Config with trusted access in the Organizations management account.
- B. Configure AWS Control Tower to extend governance to the organization. Enroll Organizations member accounts.

- C. Use AWS Config to review the enforcement compliance of each AWS account.

- D. Create an SCP that denies access to all AWS Config API actions. Apply the SCP to the organization's root.

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

- A. Request KMS to provide the stored unencrypted data key and then use the retrieved data key to decrypt the data.

- B. Keep the plaintext data key stored in Amazon DynamoDB protected with IAM policies. Query DynamoDB to retrieve the data key to decrypt the data

- C. Use the Encrypt API to store an encrypted version of the data key with another customer managed key. Decrypt the data key and use it to decrypt the data when required.

- D. Store the encrypted data key alongside the encrypted data. Use the Decrypt API to retrieve the data key to decrypt the data when required.

25. A company has two VPCs in the same AWS Region and in the same AWS account. Each VPC uses a CIDR block that does not overlap with the CIDR block of the other VPC. One VPC contains AWS Lambda functions that run inside a subnet that accesses the internet through a NAT gateway. The Lambda functions require access to a publicly accessible Amazon Aurora MySQL database that is running in the other VPC.

A security engineer determines that the Aurora database uses a security group rule that allows connections from the NAT gateway IP address that the Lambda functions use. The company’s security policy states that no database should be publicly accessible.

What is the MOST secure way that the security engineer can provide the Lambda functions with access to the Aurora database?

- A. Move the Aurora database into a private subnet that has no internet access routes in the database's current VPC. Configure the Lambda functions to use the Aurora database’s new private IP address to access the database. Configure the Aurora database's security group to allow access from the private IP addresses of the Lambda functions.

- B. Establish a VPC endpoint between the two VPCs. In the Aurora database's VPC, configure a service VPC endpoint for Amazon RDS. In the Lambda functions’ VPC, configure an interface VPC endpoint that uses the service endpoint in the Aurora database's VPC. Configure the service endpoint to allow connections from the Lambda functions

- C. Establish an AWS Direct Connect interface between the VPCs. Configure the Lambda functions to use a new route table that accesses the Aurora database through the Direct Connect interface. Configure the Aurora database's security group to allow access from the Direct Connect interface IP address,

- D. Move the Lambda functions into a public subnet in their VPC. Move the Aurora database into a private subnet in its VPC. Configure the Lambda functions to use the Aurora database's new private IP address to access the database. Configure the Aurora database to allow access from the public IP addresses of the Lambda functions.

26. 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.

27. A developer is building a serverless application hosted on AWS that uses Amazon Redshift as a data store. The application has separate module for read/write and read-only functionality. The modules need their own database users for compliance reasons.
Which combination of steps should a security engineer implement to grant appropriate access? (Choose two.)

- A. Configure cluster security groups for each application module to control access to database users that are required for read-only and read-write.
- B. Configure a VPC endpoint for Amazon Redshift. Configure an endpoint policy that maps database users to each application module, and allow access to the tables that are required for read-only and read/write.
- C. Configure an IAM policy for each module. Specify the ARN of an Amazon Redshift database user that allows the GetClusterCredentials API call.
- D. Create local database users for each module.
- E. Configure an IAM policy for each module. Specify the ARN of an IAM user that allows the GetClusterCredentials API call.

28. A security engineer is designing an incident response plan to address the risk of a compromised Amazon EC2 instance. The plan must recommend a solution to meet the following requirements:
☞ A trusted forensic environment must be provisioned.
☞ Automated response processes must be orchestrated.
Which AWS services should be included in the plan? (Choose two.)

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

- D. Amazon Macie
- E. AWS Step Functions

29. A security engineer needs to implement a solution to create and control the keys that a company uses for cryptographic operations. The security engineer must create symmetric keys in which the key material is generated and used within a custom key store that is backed by an AWS CloudHSM cluster.

The security engineer will use symmetric and asymmetric data key pairs for local use within applications. The security engineer also must audit the use of the keys.

How can the security engineer meet these requirements?

- A. To create the keys, use AWS Key Management Service (AWS KMS) and the custom key stores with the CloudHSM cluster. For auditing, use Amazon Athena.
- B. To create the keys, use Amazon S3 and the custom key stores with the CloudHSM cluster. For auditing, use AWS CloudTrail.
- C. To create the keys, use AWS Key Management Service (AWS KMS) and the custom key stores with the CloudHSM cluster. For auditing, use Amazon GuardDuty.
- D. To create the keys, use AWS Key Management Service (AWS KMS) and the custom key stores with the CloudHSM cluster. For auditing, use AWS CloudTrail.

30. A company is implementing new compliance requirements to meet customer needs. According to the new requirements, the company must not use any Amazon RDS DB instances or DB clusters that lack encryption of the underlying storage. The company needs a solution that will generate an email alert when an unencrypted DB instance or DB cluster is created. The solution also must terminate the unencrypted DB instance or DB cluster.

Which solution will meet these requirements in the MOST operationally efficient manner?

- A. Create an AWS Config managed rule to detect unencrypted RDS storage. Configure an automatic remediation action to publish messages to an Amazon Simple Notification Service (Amazon SNS) topic that includes an AWS Lambda function and an email delivery target as subscribers. Configure the Lambda function to delete the unencrypted resource.
- B. Create an AWS Config managed rule to detect unencrypted RDS storage. Configure a manual remediation action to invoke an AWS Lambda function. Configure the Lambda function to publish messages to an Amazon Simple Notification Service (Amazon SNS) topic and to delete the unencrypted resource.
- C. Create an Amazon EventBridge rule that evaluates RDS event patterns and is initiated by the creation of DB instances or DB clusters. Configure the rule to publish messages to an Amazon Simple Notification Service (Amazon SNS) topic that includes an AWS Lambda function and an email delivery target as subscribers. Configure the Lambda function to delete the unencrypted resource.
- D. Create an Amazon EventBridge rule that evaluates RDS event patterns and is initiated by the creation of DB instances or DB clusters. Configure the rule to invoke an AWS Lambda function. Configure the Lambda function to publish messages to an Amazon Simple Notification Service (Amazon SNS) topic and to delete the unencrypted resource.

31. Which of the following are valid configurations for using SSL certificates with Amazon CloudFront? (Choose 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

32. A company is using AWS Organizations to create OUs for its accounts. The company has more than 20 accounts that are all part of the OUs. A

security engineer must implement a solution to ensure that no account can stop log file delivery to AWS CloudTrail.
Which solution will meet this requirement?

- A. Use the --is-multi-region-trail option while running the create-trail command to ensure that logs are configured across all AWS Regions.
- B. Create an SCP that includes a Deny rule for the cloudtrail:StopLogging action. Apply the SCP to all accounts in the OUs.
- C. Create an SCP that includes an Allow rule for the cloudtrail:StopLogging action. Apply the SCP to all accounts in the OUs.
- D. Use AWS Systems Manager to ensure that CloudTrail is always turned on.

33. A company's security information events management (SIEM) tool receives new AWS CloudTrail logs from an Amazon S3 bucket that is configured to send all object created event notifications to an Amazon SNS topic. An Amazon SQS queue is subscribed to this SNS topic. The company's SIEM tool then polls this SQS queue for new messages using an IAM role and fetches new log events from the S3 bucket based on the SQS messages. After a recent security review that resulted in restricted permissions, the SIEM tool has stopped receiving new CloudTrail logs.
Which of the following are possible causes of this issue? (Choose three.)

- A. The SQS queue does not allow the SQS:SendMessage action from the SNS topic.
- B. The SNS topic does not allow the SNS:Publish action from Amazon S3.
- C. The SNS topic is not delivering raw messages to the SQS queue.
- D. The S3 bucket policy does not allow CloudTrail to perform the PutObject action.
- E. The IAM role used by the SIEM tool does not have permission to subscribe to the SNS topic.
- F. The IAM role used by the SIEM tool does not allow the SQS:DeleteMessage action.

34. A company has an application that uses an Amazon RDS PostgreSQL database. The company is developing an application feature that will store sensitive information for an individual in the database.
During a security review of the environment, the company discovers that the RDS DB instance is not encrypting data at rest. The company needs a solution that will provide encryption at rest for all the existing data and for any new data that is entered for an individual.
Which combination of options can the company use to meet these requirements? (Choose two.)

- A. Create a snapshot of the DB instance. Copy the snapshot to a new snapshot, and enable encryption for the copy process. Use the new snapshot to restore the DB instance.
- B. Modify the configuration of the DB instance by enabling encryption. Create a snapshot of the DB instance. Use the snapshot to restore the DB instance.
- C. Use AWS Key Management Service (AWS KMS) to create a new default AWS managed aws/rds key. Select this key as the encryption key for operations with Amazon RDS.
- D. Use AWS Key Management Service (AWS KMS) to create a new CMK. Select this key as the encryption key for operations with Amazon RDS.
- E. Create a snapshot of the DB instance. Enable encryption on the snapshot. Use the snapshot to restore the DB instance.

35. A web application gives users the ability to log in, verify their membership’s validity, and browse artifacts that are stored in an Amazon S3 bucket. When a user attempts to download an object, the application must verify the permission to access the object and allow the user to download the object from a custom domain name such as example.com.

What is the MOST secure way for a security engineer to implement this functionality?

- A. Configure read-only access to the object by using a bucket ACL. Remove the access after a set time has elapsed.

- B. Implement an IAM policy to give the user read access to the S3 bucket.
- C. Create an S3 presigned URL. Provide the S3 presigned URL to the user through the application.
- D. Create an Amazon CloudFront signed URL. Provide the CloudFront signed URL to the user through the application.

36. An AWS Lambda function was misused to alter data, and a Security Engineer must identify who invoked the function and what output was produced. The Engineer cannot find any logs created by the Lambda function in Amazon CloudWatch Logs.
Which of the following explains why the logs are not available?

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

37. A security engineer receives an AWS abuse email message. According to the message, an Amazon EC2 instance that is running in the security engineer's AWS account is sending phishing email messages.
The EC2 instance is part of an application that is deployed in production. The application runs on many EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group across multiple subnets and multiple Availability Zones.
The instances normally communicate only over the HTTP, HTTPS, and MySQL protocols. Upon investigation, the security engineer discovers that email messages are being sent over port 587. All other traffic is normal.
The security engineer must create a solution that contains the compromised EC2 instance, preserves forensic evidence for analysis, and minimizes application downtime.

Which combination of steps must the security engineer take to meet these requirements? (Choose three.)

- A. Add an outbound rule to the security group that is attached to the compromised EC2 instance to deny traffic to 0.0.0.0/0 and port 587.
- B. Add an outbound rule to the network ACL for the subnet that contains the compromised EC2 instance to deny traffic to 0.0.0.0/0 and port 587.
- C. Gather volatile memory from the compromised EC2 instance. Suspend the compromised EC2 instance from the Auto Scaling group. Then take a snapshot of the compromised EC2 instance.
- D. Take a snapshot of the compromised EC2 instance. Suspend the compromised EC2 instance from the Auto Scaling group. Then gather volatile memory from the compromised EC2 instance.
- E. Move the compromised EC2 instance to an isolated subnet that has a network ACL that has no inbound rules or outbound rules.
- F. Replace the existing security group that is attached to the compromised EC2 instance with a new security group that has no inbound rules or outbound rules.

38. 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? (Choose 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.

39. 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? (Choose 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

40. A company is configuring three Amazon EC2 instances with each instance in a separate Availability Zone. The EC2 instances will be used as transparent proxies for outbound internet traffic for ports 80 and 443 so the proxies can block traffic to certain internet destinations as required by the company's security policies. A
Security Engineer completed the following:
Set up the proxy software on the EC2 instances.
▪

✑ Modified the route tables on the private subnets to use the proxy EC2 instances as the default route.
✑ Created a security group rule opening inbound port 80 and 443 TCP protocols on the proxy EC2 instance security group.
However, the proxy EC2 instances are not successfully forwarding traffic to the internet.
What should the Security Engineer do to make the proxy EC2 instances route traffic to the internet?

- A. Put all the proxy EC2 instances in a cluster placement group.

- B. Disable source and destination checks on the proxy EC2 instances.
- C. Open all inbound ports on the proxy EC2 instance security group.
- D. Change the VPC's DHCP domain-name-servers options set to the IP addresses of proxy EC2 instances.

41. A company hosts an end user application on AWS. Currently, the company deploys the application on Amazon EC2 instances behind an Elastic Load Balancer. The company wants to configure end-to-end encryption between the Elastic Load Balancer and the EC2 instances.

Which solution will meet this requirement with the LEAST operational effort?

- A. Use Amazon issued AWS Certificate Manager (ACM) certificates on the EC2 instances and the Elastic Load Balancer to configure end-to-end encryption.
- B. Import a third-party SSL certificate to AWS Certificate Manager (ACM). Install the third-party certificate on the EC2 instances. Associate the ACM imported third-party certificate with the Elastic Load Balancer.
- C. Deploy AWS CloudHSM. Import a third-party certificate. Configure the EC2 instances and the Elastic Load Balancer to use the CloudHSM imported certificate.
- D. Import a third-party certificate bundle to AWS Certificate Manager (ACM). Install the third-party certificate on the EC2 instances. Associate the ACM imported third-party certificate with the Elastic Load Balancer.

42. A company finds that one of its Amazon EC2 instances suddenly has a high CPU usage. The company does not know whether the EC2 instance is compromised or whether the operating system is performing background cleanup.

Which combination of steps should a security engineer take before investigating the issue? (Choose three.)

- A. Disable termination protection for the EC2 instance if termination protection has not been disabled.

- B. Enable termination protection for the EC2 instance if termination protection has not been enabled.
- C. Take snapshots of the Amazon Elastic Block Store (Amazon EBS) data volumes that are attached to the EC2 instance.
- D. Remove all snapshots of the Amazon Elastic Block Store (Amazon EBS) data volumes that are attached to the EC2 instance.
- E. Capture the EC2 instance metadata, and then tag the EC2 instance as under quarantine.
- F. Immediately remove any entries in the EC2 instance metadata that contain sensitive information.

43. A Security Engineer has created an Amazon CloudWatch event that invokes an AWS Lambda function daily. The Lambda function runs an Amazon Athena query that checks AWS CloudTrail logs in Amazon S3 to detect whether any IAM user accounts or credentials have been created in the past 30 days. The results of the
Athena query are created in the same S3 bucket. The Engineer runs a test execution of the Lambda function via the AWS Console, and the function runs successfully.
After several minutes, the Engineer finds that his Athena query has failed with the error message: `Insufficient Permissions`. The IAM permissions of the Security
Engineer and the Lambda function are shown below:

Security Engineer -

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

                ],
                "Resource": "*"
          }
     ]
}
```

Lambda function execution role -

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

What is causing the error?

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

- D. The Lambda function does not have permissions to access the CloudTrail S3 bucket.

44. A company is building a data processing application that uses AWS lambda functions. The applications Lambda functions need to communicate with an amazon RDS DB instance that is deployed within is CPS in the same AWS account.

What solution needs these requirements in the MOST secure way ?

A. Configure the DB instance to allow public access. Update the DB instance security group to allow access from the Lambda public address space for the AWS Region.4

B. Deploy the lambda functions inside the VPC. Attach a network ACL to the Lambda subnet. Provide outbound rule access to the VPC CIDR range only. Update the DB instance security group to allow traffic from 0.0.0.0/0.

C. Deploy the Lambda functions inside the VPC. Attach a security group to the Lambda functions. Provide outbound rule access to the VPC CIDR range only. Update the DB instance security group to allow traffic from the Lamgda security group.

D. Peer the Lambda default VPC with the VPC that hosts the DB instance to allow direct network access without the need for security groups.

45. A company wants to prevent SSH access through the use of SSH key pairs for any Amazon Linux 2 Amazon EC2 instances in its AWS account. However, a system administrator occasionally will need to access these EC2 instances through SSH in an emergency. For auditing purposes, the company needs to record any commands that a user runs in an EC2 instance.

What should a security engineer do to configure access to these EC2 instances to meet these requirements?

- A. Use the EC2 serial console. Configure the EC2 serial console to save all commands that are entered to an Amazon S3 bucket. Provide the EC2 instances with an IAM role that allows the EC2 serial console to access Amazon S3. Configure an IAM account for the system administrator. Provide an IAM policy that allows the IAM account to use the EC2 serial console,

- B. Use EC2 Instance Connect. Configure EC2 Instance Connect to save all commands that are entered to Amazon CloudWatch Logs. Provide the EC2 instances with an IAM role that allows the EC2 Instances to access CloudWatch Logs. Configure an IAM account for the system administrator. Provide an IAM policy that allows the IAM account to use EC2 Instance Connect.

- C. Use an EC2 key pair with an EC2 instance that needs SSH access. Access the EC2 instance with this key pair by using SSH. Configure the EC2 instance to save all commands that are entered to Amazon CloudWatch Logs. Provide the EC2 instance with an IAM role that allows the EC2 instance to access Amazon S3 and CloudWatch Logs.

- D. Use AWS Systems Manager Session Manager. Configure Session Manager to save all commands that are entered in a session to an Amazon S3 bucket. Provide the EC2 instances with an IAM role that allows Systems Manager to manage the EC2 instances. Configure an IAM account for the system administrator. Provide an IAM policy that allows the IAM account to use Session Manager.

46. A company uses Amazon EC2 Linux instances in the AWS Cloud. A member of the company's security team recently received a report about common vulnerability identifiers on the instances.

A security engineer needs to verify patching and perform remediation if the instances do not have the correct patches installed. The security engineer must determine which EC2 instances are at risk and must implement a solution to automatically update those instances with the applicable patches.

What should the security engineer do to meet these requirements?

- A. Use AWS Systems Manager Patch Manager to view vulnerability identifiers for missing patches on the instances. Use Patch Manager also to automate the patching process.

- B. Use AWS Shield Advanced to view vulnerability identifiers for missing patches on the instances. Use AWS Systems Manager Patch Manager to automate the patching process.

- C. Use Amazon GuardDuty to view vulnerability identifiers for missing patches on the instances. Use Amazon Inspector to automate the patching process.

- D. Use Amazon Inspector to view vulnerability identifiers for missing patches on the instances. Use Amazon Inspector also to automate the patching process.

47. A company has multiple accounts in the AWS Cloud. Users in the developer account need to have access to specific resources in the production account.

What is the MOST secure way to provide this access?

- A. Create one IAM user in the production account. Grant the appropriate permissions to the resources that are needed. Share the password only with the users that need access.
- B. Create cross-account access with an IAM role in the developer account. Grant the appropriate permissions to this role. Allow users in the developer account to assume this role to access the production resources.
- C. Create cross-account access with an IAM user account in the production account. Grant the appropriate permissions to this user account. Allow users in the developer account to use this user account to access the production resources.
- D. Create cross-account access with an IAM role in the production account. Grant the appropriate permissions to this role. Allow users in the developer account to assume this role to access the production resources.

48. A company is running its workloads in a single AWS Region and uses AWS Organizations. A security engineer must implement a solution to prevent users from launching resources in other Regions.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Create an IAM policy that has an aws:RequestedRegion condition that allows actions only in the designated Region. Attach the policy to all users.
- B. Create an IAM policy that has an aws:RequestedRegion condition that denies actions that are not in the designated Region. Attach the policy to the AWS account in AWS Organizations.

- C. Create an IAM policy that has an aws:RequestedRegion condition that allows the desired actions. Attach the policy only to the users who are in the designated Region.

- D. Create an SCP that has an aws:RequestedRegion condition that denies actions that are not in the designated Region. Attach the SCP to the AWS account in AWS Organizations.

49. 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 Security Engineer's solution must 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, then apply it to the ALB. Test to ensure the vulnerability has been mitigated, then redirect the Route 53 records to point to the ALB. Update security groups on the EC2 instances to prevent direct access from the internet.

- B. 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.

- C. 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.

- D. 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, then restore the security group to the original setting.

50. A company stores sensitive documents in Amazon S3 by using server-side encryption with an AWS Key Management Service (AWS KMS) CMK. A new requirement mandates that the CMK that is used for these documents can be used only for S3 actions.
Which statement should the company add to the key policy to meet this requirement?
A.

```
{
  "Effect": "Deny",
  "Principal": "*",
  "Action": "kms:*",
  "Resource": "*",
  "Condition": {
    "StringNotEquals": {
      "kms:CallerAccount": "s3.amazonaws.com"
    }
  }
}
```

B.

```
{
  "Effect": "Deny",
  "Principal": "*",
  "Action": "s3:*",
  "Resource": "*",
  "Condition": {
    "StringNotEquals": {
      "kms:ViaService": "kms.*amazonaws.com"
    }
  }
}
```

51. A systems engineer must design and troubleshoot AWS services for a new project. The project deploys applications onto two Amazon EC2 instances that are named EC2A and EC2B. Both instances need to encrypt dozens of files by using an AWS Key Management Service (AWS KMS) customer managed key.

The key has the following key policy:

```
{
    "Id": "key-consolepolicy-1",
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
            "Principal": { "AWS": "arn:aws:iam::123456789012:root" },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Allow use of the key",
            "Effect": "Allow",
            "Principal": {
                "AWS":
                    ["arn:aws:iam::123456789012:role/EC2RoleA","arn:aws:iam::123456789012:role/EC2RoleB"]
            },
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        }
    ]
}
```

EC2RoleA is the role that EC2A uses. This role does not have any IAM policy that is related to AWS KMS. EC2RoleB is the role that EC2B uses. This role has the following IAM policy:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Deny",

            "Action": [
                "kms:Decrypt",
                "kms:Encrypt",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        }
    ]
}
```

Both IAM roles are within the same AWS account that contains the customer managed key.

52. What will happen when EC2Aand EC2B attempt to use the customer managed key?

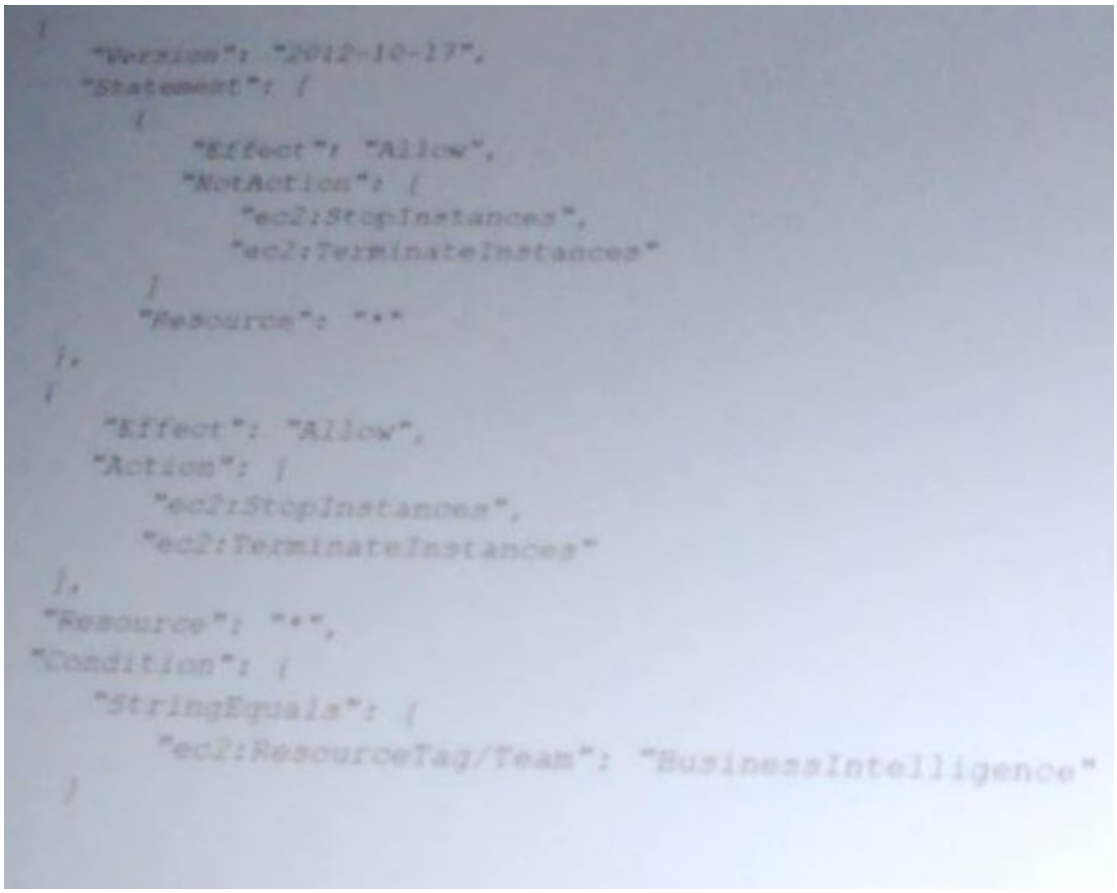
- A. Both EC2A and EC2B can use the customer managed key properly for encryption.
- B. Neither EC2A nor EC2B will be able to use the customer managed key for encryption.
- C. EC2A cannot use the customer managed key for encryption. EC2B can use the customer managed key for encryption.
- D. EC2A can use the customer managed key for encryption. EC2B cannot use the customer managed key for encryption.

53. A company created an AWS account for its developers to use for testing and learning purposes Because MM account will be shared among multiple teams of developers, the company wants to restrict the ability to stop and terminate Amazon EC2 instances so that a team can perform these actions only on the instances it owns.

Developers were Instructed to tag al their instances with a Team tag key and use the team name in the tag value One of the first teams to use this account is Business Intelligence A security engineer needs to develop a highly scalable solution for providing developers with access to the appropriate resources within the account The security engineer has already created individual 1AM roles for each team.

Which additional configuration steps should the security engineer take to complete the task?

A. For each team, create an AM policy similar to the one that fellows Populate the ec2: ResourceTag/Team condition key with a proper team name Attach resulting policies to the corresponding 1AM roles.



54. A company sends Amazon RDS snapshots to two accounts as part of its disaster recovery (DR) plan. The snapshots must be encrypted. However, each account needs to be able to decrypt the snapshots in case of a DR event.

Which solution will meet these requirements?

- A. Use the default AWS Key Management Service (AWS KMS) key to generate the snapshots. Create an AWS Lambda function that copies the KMS encryption key to the two accounts.
- B. Use an AWS Key Management Service (AWS KMS) customer managed key to generate the snapshots. Create an AWS Lambda function that imports the KMS key in the two accounts.
- C. Use the default AWS Key Management Service (AWS KMS) key to generate the snapshots. Share the KMS key with the two accounts by

using an IAM principal that has the proper KMS permissions in each account.

- D. Use an AWS Key Management Service (AWS KMS) customer managed key to generate the snapshots. Share the KMS key with the two accounts by using an IAM principal that has the proper KMS permissions in each account.

55. A company is using Amazon Elastic Container Service (Amazon ECS) to deploy an application that deals with sensitive data. During a recent security audit, the company identified a security issue in which Amazon RDS credentials were stored with the application code in the company's source code repository.
A security engineer needs to develop a solution to ensure that database credentials are stored securely and rotated periodically. The credentials should be accessible to the application only. The engineer also needs to prevent database administrators from sharing database credentials as plaintext with other teammates. The solution must also minimize administrative overhead.
Which solution meets these requirements?

- A. Use the AWS Systems Manager Parameter Store to generate database credentials. Use an IAM profile for ECS tasks to restrict access to database credentials to specific containers only.

- B. Use AWS Secrets Manager to store database credentials. Use an IAM inline policy for ECS tasks to restrict access to database credentials to specific containers only.

- C. Use the AWS Systems Manager Parameter Store to store database credentials. Use IAM roles for ECS tasks to restrict access to database credentials to specific containers only.

- D. Use AWS Secrets Manager to store database credentials. Use IAM roles for ECS tasks to restrict access to database credentials to specific containers only.

56. A company has a VPC that contains a publicly accessible subnet and a privately accessible subnet. Both subnets send network traffic that is destined for the company's data center through the public internet.

The public subnet uses Route Table A, which has a default route for network traffic to travel through the internet gateway of the VPC. The private subnet uses Route Table B, which has a default route for network traffic to travel through a NAT gateway within the VPC. Recently, the company created an AWS Site-to-Site VPN connection to the VPC from one of is data centers. The tunnel s active and is working property between the customer gateway and the virtual private gateway. The CIDR blocks of the VPC and the data center do not overlap.

According to a new security policy, all network traffic that originates from the VPC and travels to the data center must not travel across the public internet. A security engineer determines that resources in the public subnet and private subnet are still sending traffic across the public internet to the data center.

Which combination of steps will ensure that all network traffic that originates from the VPC will not use the public internet to communicate with the data cantor? (Choose two.)

- A. Adjust the route table for the public subnet to use the NAT gateway as its default route,
- B. Adjust the route table for the public subnet to use the customer gateway for the data center's CIDR block.
- C. Adjust the route table for the public subnet to use the virtual private gateway for the data cantor’s CIDR block
- D. Adjust the route table for the private subnet to use the customer gateway for the data center's CIDR block.
- E. Adjust the route table for the private subnet to use the virtual private gateway for the data centers CIDR block.

57. An Amazon API Gateway API invokes an AWS Lambda function that needs to interact with a software-as-a-service (SaaS) platform. A unique client token is generated in the SaaS platform to grant access to the Lambda function. A security engineer needs to design a solution to encrypt the access token at rest and pass the token to the Lambda function at runtime.

Which solution will meet these requirements MOST cost-effectively?

- A. Store the client token as a secret in AWS Secrets Manager. Use the AWS SDK to retrieve the secretin the Lambda function.
- B. Configure a token-based Lambda authorizer in API Gateway.
- C. Store the client token as a SecureString parameter in AWS Systems Manager Parameter Store. Use the AWS SDK to retrieve the value of the SecureString parameter in the Lambda function.
- D. Use AWS Key Management Service (AWS KMS) to encrypt the client token. Pass the token to the Lambda function at runtime through an environment variable.

58. An ecommerce website was down for 1 hour following a DDoS attack. Users were unable to connect to the website during the attack period. The ecommerce company's security team is worried about future potential attacks and wants to prepare for such events. The company needs to minimize downtime in its response to similar attacks in the future.
Which steps would help achieve this? (Choose two.)

- A. Enable Amazon GuardDuty to automatically monitor for malicious activity and block unauthorized access.
- B. Subscribe to AWS Shield Advanced and reach out to AWS Support in the event of an attack.
- C. Use VPC Flow Logs to monitor network traffic and an AWS Lambda function to automatically block an attacker's IP using security groups.
- D. Set up an Amazon CloudWatch Events rule to monitor the AWS CloudTrail events in real time, use AWS Config rules to audit the configuration, and use AWS Systems Manager for remediation.
- E. Use AWS WAF to create rules to respond to such attacks.

59. A company has developed a new Amazon RDS database application. The company must secure the RDS database credentials for encryption in transit and encryption at rest. The company also must rotate the credentials automatically on a regular basis.
Which solution meets these requirements?

- A. Use AWS Systems Manager Parameter Store to store the database credentials. Configure automatic rotation of the credentials.
- B. Use AWS Secrets Manager to store the database credentials. Configure automatic rotation of the credentials.
- C. Store the database credentials in an Amazon S3 bucket that is configured with server-side encryption with S3 managed encryption keys (SSE-S3). Rotate the credentials with IAM database authentication.
- D. Store the database credentials in Amazon S3 Glacier, and use S3 Glacier Vault Lock. Configure an AWS Lambda function to rotate credentials on a scheduled basis.

60. A company has retail stores. The company is designing a solution to store HTTPS, and traffic must be terminated before it reaches the instance. Communication to the instance must be over port 80. Company policy requires that workloads reside in private subnets.
Which solution meets these requirements?

- A. Create an Application Load Balancer. Add an HTTP listener for port 80 to redirect traffic to HTTPS on port 443. Add another listener with an AWS Certificate Manager (ACM) certificate for termination and a rule that forwards to the target instance through port 80.
- B. Allocate an Elastic IP address that has SSL termination activated. Associate the Elastic IP address with the instance on port 80.
- C. Create a Gateway Load Balancer. Add an HTTP listener for port 80 to redirect traffic to HTTPS on port 443. Add another listener with an AWS Certificate Manager (ACM) certificate for termination and a rule that forwards to the target instance through port 80.

61. A security team is developing an automated solution that uses an AWS Lambda function to provision an Amazon EC2 instance. The solution will provision the EC2 instance with an IAM role that has the permissions necessary to make API calls to other AWS services in the same AWS account. The security team can create the AMI for this EC2 instance. The team encrypts the AMI by using an AWS Key Management Service (AWS KMS) customer managed key.

When the team invokes the Lambda function to launch the EC2 instance, the team receives an access denied error message from the Lambda function’s execution role. The team analyzes the Lambda function execution role for missing permissions.

What is the MOST likely cause of this error message?

- A. The Lambda function’s execution role does not have kms:CreateGrant and kms:Decrypt KMS key permissions for the encrypted AMI.
- B. The Lambda function's execution role does not have iam:PassRole permission for the requested IAM instance profile.
- C. The company has reached the account's service quota for the EC2 instance type that the Lambda function is provisioning in the AWS Region.
- D. The Lambda function’s execution role does not have Amazon CloudWatch read and write permissions for the configured CloudWatch agent on the EC2 instance.

62. A company has decided to use encryption in its AWS account to secure the objects in Amazon S3 using server-side encryption. Object sizes range from 16,000 B to 5 MB. The requirements are as follows:
☞ The key material must be generated and stored in a certified Federal Information Processing Standard (FIPS) 140-2 Level 3 machine.
☞ The key material must be available in multiple Regions.
Which option meets these requirements?

- A. Use an AWS KMS customer managed key and store the key material in AWS with replication across Regions.
- B. Use an AWS customer managed key, import the key material into AWS KMS using in-house AWS CloudHSM, and store the key material securely in Amazon S3.
- C. Use an AWS KMS custom key store backed by AWS CloudHSM clusters, and copy backups across Regions.
- D. Use AWS CloudHSM to generate the key material and backup keys across Regions. Use the Java Cryptography Extension (JCE) and Public

Key Cryptography Standards #11 (PKCS #11) encryption libraries to encrypt and decrypt the data.

63. A DevOps team is planning to deploy a containerized application on Amazon Elastic Container Service (Amazon ECS). The team will use an Application Load Balancer (ALB) to distribute the incoming traffic for the ECS application. A security engineer needs to terminate the TLS traffic at the ALB to ensure security of data in transit.

Which solutions can the security engineer use to create a certificate and deploy the certificate at the ALB to meet these requirements? (Choose two.)

- A. Use TLS tools to create a certificate signing request (CSR). Get the CSR signed by a certificate authority (CA) to produce a certificate. Import the certificate into AWS Certificate Manager (ACM). Specify the certificate for the TLS listener on the ALB.

- B. Use AWS Certificate Manager (ACM) to request a certificate. Specify the certificate fort the TLS listener on the ALB.

- C. Use AWS Key Management Service (AWS KMS) tools to create a certificate signing request (CSR). Get the CSR signed by a certificate authority (CA) to produce a certificate. Import the certificate into AWS Certificate Manager (ACM). Specify the certificate for the TLS listener on the ALB.

- D. Configure automatic TLS support in the ECS cluster. Configure the ALB to pass the TLS connection to the containers in the cluster.

- E. Generate a certificate while creating the ECS cluster. Import the certificate into AWS Certificate Manager (ACM). Specify the certificate for the TLS listener on the ALB.

64. A Security Administrator is configuring an Amazon S3 bucket and must meet the following security requirements:
☞ Encryption in transit
☞ Encryption at rest
☞ Logging of all object retrievals in AWS CloudTrail
Which of the following meet these security requirements? (Choose three.)

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

65. 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 not bucket2

66. A company has decided to use AWS Key Management Service (AWS KMS) for all of its encryption keys. The company plans to create all of its keys as customer managed CMKs and will not import any encryption keys. The company must rotate its encryption keys once every 12 months.

Which solution will meet these requirements?

- A. Change the customer managed CMK key policy to enable automatic key rotation.
- B. Use AWS managed CMKs instead of customer managed CMKs so that AWS will rotate the keys automatically.
- C. Invoke an AWS Lambda function regularly to rotate the backing key of each customer managed CMK.
- D. Enable automatic key rotation for each customer managed CMK after it has been created in AWS KMS.

67. A company has an IAM group. All of the IAM users in the group have been assigned a multi-factor authentication (MFA) device and have full access to Amazon
S3.
The company needs to ensure that users in the group can perform S3 actions only after the users authenticate with MFA. A security engineer must design a solution that accomplishes this goal with the least maintenance overhead. Which combination of actions will meet these requirements? (Choose two.)

- A. Add a customer managed Deny policy to users in the group for s3:*actions.
- B. Add a customer managed Deny policy to the group for s3:*actions.
- C. Add a customer managed Allow policy to the group for s3:*actions.
- D. Add a condition to the policy: "Condition" : { "BoolIfExists": { "aws:MultiFactorAuthPresent": false } }
- E. Add a condition to the policy: ز€Condition": { "Bool" : { "aws:MultiFactorAuthPresent" : false } }

68. A company wants to establish separate AWS Key Management Service (AWS KMS) keys to use for different AWS services. The company's security engineer created the following key policy to allow the infrastructure deployment team to create encrypted Amazon Elastic Block Store (Amazon EBS) volumes by assuming the InfrastructueDeployment IAM role:

```
{
   "Version": "2012-10-17",
   "Id": "key-policy-ebs",
   "Statement": [
          {
               "Sid": "Enable IAM User Permissions",
               "Effect": "Allow",
               "Principal": {
                    "AWS": "arn:aws:iam::123456789012:root"
               },
               "Action": "kms:*",
               "Resource": "*"
          },
          {
               "Sid": "Allow use of the key",
               "Effect": "Allow",
               "Principal": {
                    "AWS": "arn:aws:iam::123456789012:role/aws-
reserved/sso.amazonaws.com/InfrastructureDeployment"
               },
               "Action": [
                    "kms:Encrypt",
                    "kms:Decrypt",
                    "kms:ReEncrypt*",
                    "kms:GenerateDataKey*",
                    "kms:DescribeKey",
                    "kms:CreateGrant",
                    "kms"ListGrants",
                    "kms:RevokeGrant"
   ],
   "Resource": "*",
   "Condition": {
        "StringEquals": {
             "kms:ViaService": "ec2.us-west-2.amazonaws.com"
        }
    }
  }
 ]
}
```

The security engineer recently discovered that IAM roles other than the InfrastructureDeployment role used this key for other services.
Which change to the policy should the security engineer make to resolve these issues?

- A. In the statement block that contains the Sid "Allow use of the key", under the "Condition" block, change StringEquals to StringLike.
- B. In the policy document, remove the statement block that contains the Sid "Enable IAM User Permissions". Add key management policies to the KMS policy.
- C. In the statement block that contains the Sid "Allow use of the key", under the "Condition" block, change the kms:ViaService value to ec2.us-east- 1.amazonaws.com.

- D. In the policy document, add a new statement block that grants the kms:Disable* permission to the security engineer's IAM role.

69. A company is designing the security architecture for 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. Point the ALB to an Auto Scaling group with Amazon EC2 instances in private subnets across multiple Availability Zones within the same Region. Create an Amazon CloudFront distribution that uses the ALB as its origin. Create appropriate AWS WAF ACLs and enable them on the CloudFront distribution.

- B. Create an Application Load Balancer (ALB) that uses private subnets across multiple Availability Zones within a single Region. Point the ALB to an Auto Scaling group with Amazon EC2 instances in private subnets across multiple Availability Zones within the same Region. Create an Amazon CloudFront distribution that uses the ALB as its origin. Create appropriate AWS WAF ACLs and enable them on the CloudFront distribution.

- C. Create an Application Load Balancer (ALB) that uses public subnets across multiple Availability Zones within a single Region. Point the ALB to an Auto Scaling group with Amazon EC2 instances in private subnets across multiple Availability Zones within the same Region. Create appropriate AWS WAF ACLs and enable them on the ALB.

- D. Create an Application Load Balancer (ALB) that uses private subnets across multiple Availability Zones within a single Region. Point the ALB to an Auto Scaling group with Amazon EC2 instances in private subnets across multiple Availability Zones within the same Region. Create appropriate AWS WAF ACLs and enable them on the ALB.

70. A company hosts several applications on amazon ec2 instances that run Amazon Linux 2. The company finds that some of the applications have

severe software vulnerabilities. A security engineer manually detected these vulnerabilities.

Which AWS solution should the company use to automatically and continually detect software vulnerabilities in the applications?

A. AWS Identity and Access Management (IAM)

B. Amazon Detective

C. Amazon Inspector

D. AWS System Manger Patch Manager

71. 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 regions. Specify a single Amazon S3 bucket as the storage location.
- D. Enable Amazon CloudWatch logging for all AWS services across all regions, and aggregate them to a single Amazon S3 bucket for later analysis.

72. A company has a new AWS account that does not have AWS CloudTrail configured. The account has an IAM access key that was issued by AWS Security Token
Service (AWS STS). A security engineer discovers that the IAM access key has been compromised within the last 24 hours.
The security engineer must stop the compromised IAM access key from

being used. The security engineer also must determine which activities the key has been used for so far.
What should the security engineer do to meet these requirements?

- A. In the CloudTrail console, under CloudTrail event history, search by access key for the compromised key, with the correlated events, and identify which IAM user the key belongs to. In the IAM console, revoke all active sessions for that IAM user.
- B. Create a new CloudTrail trail. In the CloudTrail console, under CloudTrail event history, search by access key for the compromised key, view the correlated events, and identify which IAM user the key belongs to. In the IAM console, revoke all active sessions for that IAM user.
- C. Create a new CloudTrail trail. In the CloudTrail console, under CloudTrail event history, search by access key for the compromised key, view the correlated events, and identify which IAM role the key belongs to. In the IAM console, delete that IAM role.
- D. In the CloudTrail console, under CloudTrail event history, search by access key for the compromised key, view the correlated events, and identify which IAM role the key belongs to. In the IAM console, revoke all active sessions for that IAM role.

73. A Security Engineer is working with the development team to design a supply chain application that stores sensitive inventory data in an Amazon S3 bucket. The application will use an AWS KMS customer master key (CMK) to encrypt the data on Amazon S3. The inventory data on Amazon S3 will be shared of vendors. All vendors will use AWS principals from their own AWS accounts to access the data on Amazon S3. The vendor list may change weekly, and the solution must support cross-account access.
What is the MOST efficient way to manage access control for the KMS CMK7?

- A. Use KMS grants to manage key access. Programmatically create and revoke grants to manage vendor access.
- B. Use an IAM role to manage key access. Programmatically update the IAM role policies to manage vendor access.
- C. Use KMS key policies to manage key access. Programmatically update the KMS key policies to manage vendor access.

- D. Use delegated access across AWS accounts by using IAM roles to manage key access. Programmatically update the IAM trust policy to manage cross- account vendor access.

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

75. A company is storing data in Amazon S3 Glacier. The security engineer implemented a new vault lock policy for 10TB of data and called initiate-vault-lock operation 12 hours ago. The audit team identified a typo in the policy that is allowing unintended access to the vault.
What is the MOST cost-effective way to correct this?

- A. Call the abort-vault-lock operation. Update the policy. Call the initiate-vault-lock operation again.
- B. Copy the vault data to a new S3 bucket. Delete the vault. Create a new vault with the data.
- C. Update the policy to keep the vault lock in place.
- D. Update the policy. Call initiate-vault-lock operation again to apply the new policy.

76. A company'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 to 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.

77. 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 KMS. Remove the scripts from the instance and clear the logs after the instance is configured.
- D. Block user access of the EC2 instance's metadata service using IAM policies. Remove all scripts and clear the logs after execution.

78. A company wants to gain better control of its large number of AWS accounts by establishing a centralized location where the accounts can be managed. The company also wants to prevent any users outside the company-owned AWS accounts from accessing a company Amazon S3 bucket.
Which solution meets these requirements with the LEAST amount of operational overhead?

- A. Implement an organization in AWS Organizations. Build a detective control by monitoring AWS CloudTrail logs for attempts to access the S3 bucket from IP addresses outside the company.
- B. Deploy an AWS Control Tower landing zone, and migrate the accounts. Create an S3 bucket policy that restricts access to only a principal list of accounts that have been manually entered.
- C. Create an organization in AWS Organizations. Invite the AWS accounts to join the organization. Create a resource policy that includes a PrincipalOrgID condition key for the S3 bucket.
- D. Invite all of the company's AWS accounts into AWS Control Tower. Use AWS Control Tower's automatic protection for the AWS accounts to deny access from external users.

79. A company has a large number of Amazon S3 buckets and a large number of objects in each S3 bucket. The company's security team wants to analyze the access patterns for the objects and buckets. These patterns include the most frequently accessed buckets and objects, the largest 100 objects downloaded, and the objects with the longest download time from public IP addresses.

The security team wants to view this information in a dashboard that is based on predetermined simple SQL queries.

Which combination of AWS services and features should a security engineer use to provide and display the information to the security team? (Choose three.)

- A. Amazon CloudWatch Logs Insights
- B. Amazon S3 server access logs

- C. Amazon CloudWatch Logs
- D. Amazon GuardDuty
- E. Amazon QuickSight
- F. Amazon Athena

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

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

81. A company recently deployed a new AWS account and wants to be notified immediately if a specific number of unauthorized AWS API requests are detected. A security engineer has turned on AWS CloudTrail for the

account and is sending CloudTrail logs to Amazon CloudWatch.
Which other action must the security engineer perform to receive automated alerts about unauthorized AWS API calls?

- A. Create a CloudWatch metric filter that looks for API call error codes. Configure an alarm that is based on that metric's rate to send an Amazon Simple Notification Service (Amazon SNS) notification when the threshold is exceeded.
- B. Configure CloudTrail to stream event data to Amazon Kinesis Data Streams. Configure an AWS Lambda function on the stream to initiate an alarm when the threshold is exceeded.
- C. Run an Amazon Athena SQL query against CloudTrail log files for unauthorized API requests. Use Amazon QuickSight to create an operational dashboard.
- D. Use the AWS Personal Health Dashboard to monitor the account's use of AWS services and to provide an alert if service error rates increase.

82. A company wants to deploy a continuous security threat-detection service at scale to automatically analyze all the company’s member accounts in AWS Organizations within the ap-east-1 Region. The company’s organization includes a management account, a security account, and many member accounts. When the company creates a new member account, the threat-detection service should automatically analyze the new account so that the company can review any findings from the security account.

Which solution uses AWS security best practices and meets these requirements with the LEAST effort?

- A. Activate Amazon GuardDuty in ap-east-1. Designate the security account as the GuardDuty delegated administrator by using the console.
- B. Activate Amazon GuardDuty in ap-east-1 with trusted access to AWS Organizations. Designate the management account as the GuardDuty organization administrator.
- C. Activate AWS Security Hub in ap-east-1. Designate the management account as the Security Hub delegated administrator by using the console.

- D. Activate AWS Control Tower in ap-east-1 with trusted access to AWS Organizations. Designate the security account as the organization administrator.

83. A company recently adopted new compliance standards that require all user actions in AWS to be logged. The user actions must be logged for all accounts that belong to an organization in AWS Organizations. The company needs to set alarms that respond when specified actions occur. The alarms must forward alerts to an email distribution list. The alerts must occur in as close to real time as possible.

Which solution will meet these requirements?

- A. Implement an AWS CloudTrail trail as an organizational trail. Configure the trail with Amazon CloudWatch Logs forwarding. In CloudWatch Logs, set a metric filter for any user action events that the company specifies. Create an Amazon CloudWatch alarm to provide alerts for occurrences within a reported period and to publish messages to an Amazon Simple Notification Service (Amazon SNS) topic.

- B. Implement an AWS CloudTrail trail. Configure the trail with Amazon CloudWatch Logs forwarding. In CloudWatch Logs, set a metric filter for any user action events that the company specifies. Create an Amazon CloudWatch alarm to provide alerts for occurrences within a reported period and to send messages to an Amazon Simple Queue Service (Amazon SQS) queue.

- C. Implement an AWS CloudTrail trail as an organizational trail. Configure the trail to store logs in an Amazon S3 bucket. Configure an Amazon EC2 instance to mount the S3 bucket as a file system to ingest new log files that are pushed to the S3 bucket. Configure the EC2 instance also to publish a message to an Amazon Simple Notification Service (Amazon SNS) topic when one of the specified actions is found in the logs.

- D. Implement an AWS CloudTrail trail. Configure the trail to store logs in an Amazon S3 bucket. Each hour, create an AWS Glue Data Catalog that references the S3 bucket. Configure Amazon Athena to initiate queries against the Data Catalog to identify the specified actions in the logs.

84. A company that builds document management systems recently performed a security review of its application on AWS. The review showed that uploads of documents through signed URLs into Amazon S3 could occur in the application without encryption in transit. A security engineer must implement a solution that prevents uploads that are not encrypted in transit.

Which solution will meet this requirement?

- A. Ensure that all client implementations are using HTTPS to upload documents into the application.
- B. Configure the s3-bucket-ssl-requests-only managed rule in AWS Config.
- C. Add an S3 bucket policy that denies all S3 actions for condition “aws:secureTransport”: “false”.
- D. Add an S3 bucket ACL with a grantee of AllUsers, a permission of WRITE, and a condition of secureTransport.

85. A company’s security engineer has configured a client account to capture AWS CloudTrail logs that are then sent to an Amazon S3 bucket. The S3 bucket that stores these CloudTrail logs has always been configured to use AWS Key Management Service (AWS KMS) with the default KMS key (aws/s3) for encryption. Recently, the company changed the key on the S3 bucket to a new KMS key.

Since the modification of the bucket key, the security engineer cannot retrieve new CloudTrail log files that are written to the S3 bucket. The security engineer receives the following error message: “An error occurred (AccessDenied) when calling the GetObject operation: Access Denied”.

Log files that were written to the S3 bucket before the bucket key was changed are still accessible. The company used the new KMS key to encrypt other S3 buckets, and the same error is occurring with those S3 buckets.

What is the MOST likely cause of this error?

- A. The security engineer’s IAM user does not have encrypt and decrypt permissions for the new KMS key.
- B. The security engineer’s IAM user does not have administrative permissions for the new KMS key.

- C. The S3 bucket policy needs modification to allow users to access objects that are encrypted with the new KMS key.

- D. The S3 bucket policy needs modification to allow the security engineer’s IAM user to access objects in the S3 bucket.

86. 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

87. A company is using AWS Organizations with all features enabled. The company has an AWS management account under an organization's root and a small number of AWS accounts under a child OU. The company expects to grow by more than 1,000 AWS accounts in the next year.

The company wants to enforce a policy that disallows any configuration changes to AWS Config settings in all AWS Organizations member accounts automatically when the company creates member accounts. The company will enforce this policy on all existing accounts and on any future AWS accounts that the company creates. The company also wants a centralized view of the compliance status of all accounts.

Which solution will meet these requirements?

- A. Configure AWS Config with trusted access in the Organizations management account.

- B. Configure AWS Control Tower to extend governance to the organization. Enroll Organizations member accounts.
- C. Use AWS Config to review the enforcement compliance of each AWS account.
- D. Create an SCP that denies access to all AWS Config API actions. Apply the SCP to the organization's root.

88. A company has an AWS WAF web ACL. According to a new compliance requirement, the company must configure comprehensive logging of all web ACL requests. The company has created an Amazon S3 bucket to store the logs.

Which combination of steps should the company take next to meet this requirement? (Choose two.)

- A. Enable logging for the web ACL. Associate the web ACL with the Amazon Kinesis data stream.
- B. Enable logging for the web ACL. Associate the web ACL with the Amazon Kinesis Data Firehose delivery stream.
- C. Configure log filtering for the web ACL. Associate the web ACL with the Amazon Kinesis Data Firehose delivery stream.
- D. Create an Amazon Kinesis data stream in any AWS Region. Specify the S3 bucket as the destination for the data stream.
- E. Create an Amazon Kinesis Data Firehose delivery stream in the same AWS Region as the web ACL. Specify the S3 bucket as the destination for the delivery stream.

89. 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.

90. A security engineer is attempting to troubleshoot a problem. An application that runs on an Amazon EC2 instance in a VPC cannot communicate with an Amazon RDS DB instance in another subnet of the same VPC. The connection request is timing out.

Which issues could be causing this problem? (Choose two.)

- A. The application instance's security group is not allowing outbound traffic.
- B. The network ACL of the application instance's subnet is not allowing traffic between the application and the DB instance.
- C. The VPC's route table is not configured correctly.
- D. There is no peering connection between the application and the database.
- E. The DB instance's security group is not allowing outbound traffic.

91. A company has an encrypted Amazon Aurora DB cluster in the us-east-1 Region. The DB cluster is encrypted with an AWS Key Management Service (AWS KMS) customer managed key. To meet compliance requirements, the company needs to copy a DB snapshot to the us-west-1 Region. However, when the company tries to copy the snapshot to us-west-1, the company cannot access the key that was used to encrypt the original database.

What should the company do to set up the snapshot in us-west-1 with proper encryption?

- A. Use AWS Secrets Manager to store the customer managed key in us-west-1 as a secret. Use this secret to encrypt the snapshot in us-west-1.
- B. Create a new customer managed key in us-west-1. Use this new key to encrypt the snapshot in us-west-1.
- C. Create an IAM policy that allows access to the customer managed key in us-east-1. Specify arn:aws:kms:us-west-1as the principal.
- D. Create an IAM policy that allows access to the customer managed key in us-east-1. Specify arn:aws:rds:us-west-1 :* as the principal.

92. A security engineer recently rotated all IAM access keys in an AWS account. The security engineer then configured AWS Config and enabled the following AWS
Config managed rules; mfa-enabled-for-iam-console-access, iam-user-mfa-enabled, access-key-rotated, and iam-user-unused-credentials-check.
The security engineer notices that all resources are displaying as noncompliant after the IAM GenerateCredentialReport API operation is invoked.
What could be the reason for the noncompliant status?

- A. The IAM credential report was generated within the past 4 hours.
- B. The security engineer does not have the GenerateCredentialReport permission.
- C. The security engineer does not have the GetCredentialReport permission.
- D. The AWS Config rules have a MaximumExecutionFrequency value of 24 hours.

93. A company has retail stores The company is designing a solution to store scanned copies of customer receipts on Amazon S3 Files will be between 100 KB and 5 MB in PDF format Each retail store must have a unique encryption key Each object must be encrypted with a unique key

Which solution will meet these requirements?

A. Create a dedicated AWS Key Management Service (AWS KMS) customer managed key for each retail store Use the S3 Put operation to upload the objects to Amazon S3 Specify server-side encryption with AWS KMS keys (SSE-KMS) and the key ID of the store's key

B. Create a new AWS Key Management Service (AWS KMS) customer managed key every day for each retail store Use the KMS Encrypt operation to encrypt objects Then upload the objects to Amazon S3

C. Run the AWS Key Management Service (AWS KMS) GenerateDataKey operation every day for each retail store Use the data key and client-side encryption to encrypt the objects Then upload the objects to Amazon S3

D. Use the AWS Key Management Service (AWS KMS) ImportKeyMaterial operation to import new key material to AWS KMS every day for each retail store Use a customer managed key and the KMS Encrypt operation to encrypt the objects Then upload the objects to Amazon S3

94. 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. Associate the web ACL with the ALB.
B. Configure an Amazon CloudFront distribution to use the ALB as an origin. Configure a web ACL rule for AWS WAF to block requests with a string match condition for the user agent of the IoT device Associate the web ACL with the ALB. Change the public DNS entry of the website to point to the CloudFront distribution.
C. Configure an Amazon CloudFront distribution to use a new ALB as an origin. Configure a web ACL rule for AWS WAF to block requests with a string match condition for the user agent of the IoT device. 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.

D. Activate AWS Shield Advanced to enable DDoS protection. Apply an AWS WAF ACL to the ALB and configure a listener rule on the ALB to block IoT devices based on the user agent.

95. A company has a legacy application that runs on a single Amazon EC2 instance. A security audit shows that the application has been using an IAM access key within its code to access an Amazon S3 bucket that is named DOC-EXAMPLE-BUCKET1 in the same AWS account. This access key pair has the s3:GetObject permission to all objects in only this S3 bucket. The company takes the application offline because the application is not compliant with the company's security policies for accessing other AWS resources from Amazon EC2.

A security engineer validates that AWS CloudTrail is turned on in all AWS Regions. CloudTrail is sending logs to an S3 bucket that is named DOC-EXAMPLE-BUCKET2. This S3 bucket is in the same AWS account as DOC-EXAMPLE-BUCKET1. However, CloudTrail has not been configured to send logs to Amazon CloudWatch Logs.

The company wants to know if any objects in DOC-EXAMPLE-BUCKET1 were accessed with the IAM access key in the past 60 days. If any objects were accessed, the company wants to know if any of the objects that are text files (.txt extension) contained personally identifiable information (PII).

Which combination of steps should the security engineer take to gather this information? (Choose two.)

- A. Configure Amazon Macie to identify any objects in DOC-EXAMPLE-BUCKET1 that contain PII and that were available to the access key.
- B. Use Amazon CloudWatch Logs Insights to identify any objects in DOC-EXAMPLE-BUCKET1 that contain PII and that were available to the access key.
- C. Use Amazon OpenSearch Service (Amazon Elasticsearch Service) to query the CloudTrail logs in DOC-EXAMPLE-BUCKET2 for API calls that used the access key to access an object that contained PII.
- D. Use Amazon Athena to query the CloudTrail logs in DOC-EXAMPLE-BUCKET2 for any API calls that used the access key to access an object that contained PII.

- E. Use AWS Identity and Access Management Access Analyzer to identify any API calls that used the access key to access objects that contained PII in DOC-EXAMPLE-BUCKET1.

96. A security engineer is trying to use Amazon EC2 Image Builder to create an image of an EC2 instance. The security engineer has configured the pipeline to send logs to an Amazon S3 bucket. When the security engineer runs the pipeline, the build fails with the following error: “AccessDenied: Access Denied status code: 403”.

The security engineer must resolve the error by implementing a solution that complies with best practices for least privilege access.

Which combination of steps will meet these requirements? (Choose two.)

- A. Ensure that the following policies are attached to the IAM role that the security engineer is using: EC2InstanceProfileForImageBuilder, EC2InstanceProfileForImageBuilderECRContainerBuilds, and AmazonSSMManagedInstanceCore.
- B. Ensure that the following policies are attached to the instance profile for the EC2 instance: EC2InstanceProfileForImageBuilder, EC2InstanceProfileForImageBuilderECRContainerBuilds, and AmazonSSMManagedInstanceCore.
- C. Ensure that the AWSImageBuilderFullAccess policy is attached to the instance profile for the EC2 instance.
- D. Ensure that the security engineer’s IAM role has the s3:PutObject permission for the S3 bucket.
- E. Ensure that the instance profile for the EC2 instance has the s3:PutObject permission for the S3 bucket.

97. A company wants to prevent public exposure of data that is stored in Amazon S3.

Which combination of steps should a security engineer take to meet this requirement? (Choose two.)

- A. Turn on S3 Block Public Access.

- B. Enforce S3 bucket encryption by using server-side encryption with AWS KMS managed keys (SSE-KMS).
- C. Enforce S3 bucket encryption by using server-side encryption with Amazon S3 managed encryption keys (SSE-S3).
- D. Use S3 Storage Lens.
- E. Use Amazon Macie.

98. An Amazon EC2 Auto Scaling group launches Amazon Linux EC2 instances and installs the Amazon CloudWatch agent to publish logs to Amazon CloudWatch Logs. The EC2 instances launch with an IAM role that has an IAM policy attached. The policy provides access to publish custom metrics to CloudWatch. The EC2 instances run in a private subnet inside a VPC. The VPC provides access to the internet for private subnets through a NAT gateway.

A security engineer notices that no logs are being published to CloudWatch Logs for the EC2 instances that the Auto Scaling group launches. The security engineer validates that the CloudWatch Logs agent is running and is configured properly on the EC2 instances. In addition, the security engineer validates that network communications are working properly to AWS services.

What can the security engineer do to ensure that the logs are published to CloudWatch Logs?

- A. Configure the IAM policy in use by the IAM role to have access to the required cloudwatch: API actions that will publish logs.
- B. Adjust the Amazon EC2 Auto Scaling service-linked role to have permissions to write to CloudWatch Logs.
- C. Configure the IAM policy in use by the IAM role to have access to the required AWS logs: API actions that will publish logs.
- D. Add an interface VPC endpoint to provide a route to CloudWatch Logs.

99. A company is running an Amazon RDS Multi-AZ DB instance inside a VPC. The DB instance is using two subnets that provide a default route to the internet through a NAT gateway.
The company also has application servers that run on Amazon EC2 instances that use the RDS database. The company has deployed these EC2 instances into two other private subnets within the same VPC. These EC2 instances use a default route to access the internet through the same NAT gateway. Each subnet in the VPC uses its own unique route table.
After a recent security audit, the company added a new security requirement. The DB instance must never be able to connect to the internet. A security engineer must make this change immediately without disrupting the application servers' network traffic.
How can the security engineer meet these requirements?

- A. Remove the existing NAT gateway. Create a new NAT gateway that only the application server subnets can use.
- B. Configure the DB instance's inbound network ACL to deny traffic from the security group ID of the NAT gateway.
- C. Modify the route tables of the DB instance subnets to remove the default route to the NAT gateway.
- D. Configure the route table of the NAT gateway to deny connections to the DB instance subnets.

100. A security engineer is working for a parent company that provides hosting and services to client companies. The parent company maintains an organization in AWS Organizations for all client company accounts. The parent company adds any new accounts to the organization when the new accounts are created. The parent company currently uses IAM users to administer the client company accounts. As more client accounts are added, the administration of the IAM accounts takes more time.

The security engineer must design a solution to reduce the amount of time that the parent company spends on administration and access provisioning for client accounts.

Which combination of steps should the security engineer take to meet these requirements? (Choose two.)

- A. Provision an external identity provider (IdP) for the parent company. Implement AWS Single Sign-On (AWS SSO) with the IdP as the identity source for AWS SSO.
- B. Provision an external identity provider (IdP) for each client company. Implement AWS Single Sign-On (AWS SSO) with the IdPs as the identity source for AWS SSO.
- C. Provision an external identity provider (IdP) for the parent company. Implement AWS Single Sign-On (AWS SSO) with employee IAM roles as the identity source for AWS SSO.
- D. In the AWS Single Sign-On console, select the users who require access to client accounts. Assign these users to the accounts.
- E. In the IAM console, select the users who require access to client accounts. Assign these users to the accounts.

101. A security engineer configures Amazon S3 Cross-Region Replication (CRR) for all objects that are in an S3 bucket in the us-east-1 Region. Some objects in this S3 bucket use server-side encryption with AWS KMS keys (SSE-KMS) for encryption at rest. The security engineer creates a destination S3 bucket in the us-west-2 Region. The destination S3 bucket is in the same AWS account as the source S3 bucket.

The security engineer also creates a customer managed key in us-west-2 to encrypt objects at rest in the destination S3 bucket. The replication configuration is set to use the key in us-west-2 to encrypt objects in the destination S3 bucket. The security engineer has provided the S3 replication configuration with an IAM role to perform the replication in Amazon S3.

After a day, the security engineer notices that no encrypted objects from the source S3 bucket are replicated to the destination S3 bucket. However, all the unencrypted objects are replicated.

Which combination of steps should the security engineer take to remediate this issue? (Choose three.)

- A. Change the replication configuration to use the key in us-east-1 to encrypt the objects that are in the destination S3 bucket.
- B. Grant the IAM role the kms:Encrypt permission for the key in us-east-1 that encrypts source objects.

- C. Grant the IAM role the s3:GetObjectVersionForReplication permission for objects that are in the source S3 bucket.
- D. Grant the IAM role the kms:Decrypt permission for the key in us-east-1 that encrypts source objects.
- E. Change the key policy of the key in us-east-1 to grant the kms:Decrypt permission to the security engineer's IAM account.
- F. Grant the IAM role the kms:Encrypt permission for the key in us-west-2 that encrypts objects that are in the destination S3 bucket.

102. A company is using Amazon Macie, AWS Firewall Manager, Amazon Inspector, and AWS Shield Advanced in its AWS account. The company wants to receive alerts if a DDoS attack occurs against the account.

Which solution will meet this requirement?

- A. Use Macie to detect an active DDoS event. Create Amazon CloudWatch alarms that respond to Macie findings.
- B. Use Amazon Inspector to review resources and to invoke Amazon CloudWatch alarms for any resources that are vulnerable to DDoS attacks.
- C. Create an Amazon CloudWatch alarm that monitors Firewall Manager metrics for an active DDoS event.
- D. Create an Amazon CloudWatch alarm that monitors Shield Advanced metrics for an active DDoS event.

103. A company has an external web application that runs on amazon EC2 instances behind an Application Load Balancer (ALB) within a VPC. The web application stores data in an Amazon RDS for MySQL DB instance. The company uses a Linux bastion host to apply schema updates to the database. Administrators connect to the bastion host through SSH from their corporate workstations. The following security groups are applied to the infrastructure:

sgLB associated with the ALB

sgWeb associated with the EC2 instances

sgDB associated with the DB instance

sgBastion associated with the bastion host

Which security group configuration will meet these requirements MOST securely ?

D.

- sgLB: Allow port 80 traffic and port 443 traffic from 0.0.0.0/0
- sgWeb: Allow port 80 traffic and port 443 traffic from 0.0.0.0/0
- sgDB: Allow port 3306 traffic from sgWeb and sgBastion
- sgBastion: Allow port 22 traffic from the corporate IP address range

104. 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.

105. A company is using AWS Organizations. The company wants to restrict AWS usage to the eu-west-1 Region for all accounts under an OU that is named "development." The solution must persist restrictions to existing and new AWS accounts under the development OU.

Which solution meets these requirements?

- A. Include the following SCP on the development OU:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyNonDefaultRegions",
            "Effect": "Deny",
            "NotAction": [
                <Desired Global Services> ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                        "eu-west-1"
                    ]
                },
                "ArnNotLike": {
                    "aws:PrincipalARN": "arn:aws:iam::*:role/CompanyAdminRole"
                }
            }
        }
```

106. A company's application uses Amazon DynamoDB to store data. The company's security policy requires all data to be encrypted at rest. The security policy also requires the company to use an on-premises hardware security module (HSM) to generate and manage the company's encryption keys.

A security engineer uses the on-premises HSM to generate an encryption key.

What should the security engineer do next to meet these requirements?

- A. Generate a new AWS Key Management Service (AWS KMS) customer managed key. Import the new key material. Grant DynamoDB access to use the key. Create a new DynamoDB table, and select the new key as the encryption key. Import the data into DynamoDB.

- B. Generate a new AWS Key Management Service (AWS KMS) customer managed key. Import the new key material. Create a new DynamoDB table, and select the new key as the encryption key. Disable the KMS key after table creation. Import the data into DynamoDB.

- C. Generate a new AWS Key Management Service (AWS KMS) AWS managed key. Import the new key material. Grant DynamoDB access to use the key. Create a new DynamoDB table, and select the new key as the encryption key. Import the data into DynamoDB.

- D. Generate a new AWS Key Management Service (AWS KMS) AWS managed key. Import the new key material. Use the AWS SDK integration with AWS KMS to encrypt the data locally by using the new KMS key. Create a new DynamoDB table, and select the new key as the encryption key. Disable the KMS key after table creation. Import the data into DynamoDB.

107. A company decides to use AWS Key Management Service (AWS KMS) for data encryption operations. The company must create a KMS key and automate the rotation of the key. The company also needs the ability to deactivate the key and schedule the key for deletion.

Which solution will meet these requirements?

- A. Create an asymmetric customer managed KMS key. Enable automatic key rotation.

- B. Create a symmetric customer managed KMS key. Disable the envelope encryption option.

- C. Create a symmetric customer managed KMS key. Enable automatic key rotation.

- D. Create an asymmetric customer managed KMS key. Disable the envelope encryption option.

108. A company wants to remove all ssh keys permanently from a specific subnet of its Amazon Linux 2 Amazon EC2 instances that are using the same IAM instance profile. However these individual who have IAM user accounts will need to access these instances by using an SSH session to perform critical duties.

How can a security engineer provide the access to meet these requirements?

A. Assign an IAM policy to the instance profile to allow the EC2 instances to be managed by AWS System Manager. Provide the

IAM use accounts with permission to use System Manger Remove all SSH keys from the EC2 instances. Use System Manger inventory to select the EC2 instance and connect.

B. Assign an IAM policy to the IAM user accounts to provide permission to use AWS System Manager Run Command. Remove the SSH keys from the EC2 instances. Use Run Command to open an SSH connection to the EC2 instance.

C. Assign an IAM policy to the instance profile to allow the EC2 instances to be managed by AWS System Manger. Provide the IAM user accounts with permission to use System Manager Remove the SSH keys from the EC2 instances. Use system Manager Session Manager to select the EC2 instance and connect.

D. Assign an IAM policy to the IAM user accounts to provide permission to use the EC2 service in the AWS Management Console. Remove the SSH keys from the EC2 intances. Connect to the EC2 instance as the ec2-user through the AWS Management Console's EC2 SSH client method.

109. A company is storing data in Amazon S3 Glacier. The security engineer implemented a new vault lock policy for 10TB of data and called initiate-vault-lock operation 12 hours ago. The audit team identified a typo in the policy that is allowing unintended access to the vault.
What is the MOST cost-effective way to correct this?

- A. Call the abort-vault-lock operation. Update the policy. Call the initiate-vault-lock operation again.
- B. Copy the vault data to a new S3 bucket. Delete the vault. Create a new vault with the data.
- C. Update the policy to keep the vault lock in place.
- D. Update the policy. Call initiate-vault-lock operation again to apply the new policy.

110. A company runs a cron job on an Amazon EC2 instance on a predefined schedule. The cron job calls a bash script that encrypts a 2 KB file. A security engineer creates an AWS Key Management Service (AWS KMS) CMK with a key policy. The key policy and the EC2 instance role have the necessary configuration for this job.

Which process should the bash script use to encrypt the file?

- A. Use the aws kms encrypt command to encrypt the file by using the existing CMK.
- B. Use the aws kms create-grant command to generate a grant for the existing CMK.
- C. Use the aws kms encrypt command to generate a data key. Use the plaintext data key to encrypt the file.
- D. Use the aws kms generate-data-key command to generate a data key. Use the encrypted data key to encrypt the file.

111. A security engineer receives an abuse report email message from the AWS Trust and Safety team. The abuse report identifies a resource that appears to be compromised. The abuse report indicates that the resource is an IAM access key that belongs to a DevOps engineer in the security engineer's company. The access key is used in a deployment system that uses AWS Lambda functions to launch AWS CloudFormation stacks.

The security engineer must address the abuse report, prevent any further use of the exposed access key, and implement security best practices.

Which solution will meet these requirements?

- A. Locate the compromised IAM access key and deactivate or delete the key. Generate new access keys for the Lambda deployment process. Apply the new keys to the deployment system. In the account that contained the compromised key, create a new support case in AWS Support to detail these remediation steps.
- B. Delete or deactivate the compromised IAM access key. Discontinue the use of IAM access keys. Create a new IAM role for the Lambda deployment process. Apply the IAM role to the deployment system Lambda functions. Respond directly to the abuse report message to detail these remediation steps.
- C. Locate the compromised IAM access key. Delete the IAM user that is associated with the access key. Generate a new access key. Store the new key as an AWS Secrets Manager secret. Encrypt the secret with an AWS Key Management Service (AWS KMS) customer managed key.

Update the Lambda functions to retrieve the access key from AWS Secrets Manager at runtime. In the account that contained the compromised key, create a new support case in AWS Support to detail these remediation steps.

- D. Delete or deactivate the compromised IAM access key. Generate and store a new access key as an environmental variable within the configuration of the deployment system's Lambda functions. Respond directly to the abuse report message to detail these remediation steps.

112. A company wants to store all objects that contain sensitive data in an Amazon S3 bucket. The company will use server-side encryption to encrypt the S3 bucket. The company's operations team manages access to the company's S3 buckets. The company's security team manages access to encryption keys.

The company wants to separate the duties of the two teams to ensure that configuration errors by only one of these teams will not compromise the data by granting unauthorized access to plaintext data.

Which solution will meet this requirement?

- A. Ensure that the operations team configures default bucket encryption on the S3 bucket to use server-side encryption with Amazon S3 managed encryption keys (SSE-S3). Ensure that the security team creates an IAM policy that controls access to use the encryption keys.

- B. Ensure that the operations team creates a bucket policy that requires requests to use server-side encryption with AWS KMS keys (SSE-KMS) that are customer managed. Ensure that the security team creates a key policy that controls access to the encryption keys.

- C. Ensure that the operations team creates a bucket policy that requires requests to use server-side encryption with Amazon S3 managed keys (SSE-S3). Ensure that the security team creates an IAM policy that controls access to the encryption keys.

- D. Ensure that the operations team creates a bucket policy that requires requests to use server-side encryption with customer-provided encryption keys (SSE-C). Ensure that the security team stores the customer-provided keys in AWS Key Management Service (AWS KMS). Ensure that the security team creates a key policy that controls access to the encryption keys.

113. A company is using an organization in AWS Organizations to manage its AWS accounts. The company runs its primary application on Amazon EC2 instances. A security engineer discovers unauthorized access in one of the company's developer AWS accounts. An investigation reveals that AWS access keys from the developer account were mistakenly added to public source code repository.

Which combination of actions should the security engineer take to secure the compromised account? (Choose two.)

- A. Rotate all the access key pairs in the compromised account.
- B. Create security group that denies traffic from the internet. Attach the security group to all EC2 instances in the compromised account
- C. Temporarily remove the compromised account from the organization.
- D. Delete all EC2 key pairs in the compromised account.
- E. Delete any potentially unauthorized IAM users in the compromised account. Change the password for all other IAM users.

114. A company is migrating its Amazon EC2 based applications to use Instance Metadata Service Version 2 (IMDSv2). A security engineer needs to determine whether any of the EC2 instances are still using Instance Metadata Service Version 1 (IMDSv1).

What should the security engineer do to confirm that the IMDSv1 endpoint is no longer being used?

- A. Configure logging on the Amazon CloudWatch agent for IMDSv1 as part of EC2 instance startup. Create a metric filter and a CloudWatch dashboard. Track the metric in the dashboard.
- B. Create an Amazon CloudWatch dashboard. Verify that the EC2:MetadataNoToken metric is zero across all EC2 instances. Monitor the dashboard.
- C. Create a security group that blocks access to HTTP for the IMDSv1 endpoint. Attach the security group to all EC2 instances.

- D. Configure user data scripts for all EC2 instances to send logging information to AWS CloudTrail when IMDSv1 is used. Create a metric filter and an Amazon CloudWatch dashboard. Track the metric in the dashboard.