Amazon

Clearcat.Net | FIRST ATTEMPT PASS | WWW.CLEARCATNET.COM

(SCS-C02)

AWS Certified Security - Specialty SCS-C02

Be AWS Security – Specialty Certified Now!
Clearcat.net
www.clearcatnet.com
SCS-C02
Dumps PDF
aws certified
Security
SPECIALTY
Latest Real Exam Q&A, FIRST ATTEMPT PASS
307 Q&A.
pdf
Full Premium Material PDF – Verified by Experts

Question:1 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company has an AWS Lambda function that creates image thumbnails from larger images. The Lambda function needs read and write access to an Amazon S3 bucket in the same AWS account.
Which solutions will provide the Lambda function this access? (Choose two.)

- A. Create an IAM user that has only programmatic access. Create a new access key pair. Add environmental variables to the Lambda function with the access key ID and secret access key. Modify the Lambda function to use the environmental variables at run time during communication with Amazon S3.
- B. Generate an Amazon EC2 key pair. Store the private key in AWS Secrets Manager. Modify the Lambda function to retrieve the private key from Secrets Manager and to use the private key during communication with Amazon S3.
- C. Create an IAM role for the Lambda function. Attach an IAM policy that allows access to the S3 bucket.
- D. Create an IAM role for the Lambda function. Attach a bucket policy to the S3 bucket to allow access. Specify the function's IAM role as the principal.
- E. Create a security group. Attach the security group to the Lambda function. Attach a bucket policy that allows access to the S3 bucket through the security group ID.

Correct Answer: *CD*
Explanation:
C. IAM role for Lambda with policy: This is the most common and recommended approach. You create an IAM role specifically for the Lambda function, then attach an IAM policy to the role that grants the necessary read and write permissions to the S3 bucket. Lambda functions assume this role when they are executed and can then interact with the S3 bucket.

D. IAM role for Lambda with a bucket policy: Another valid approach is to create an IAM role for the Lambda function and attach a bucket policy to the S3 bucket that allows access from the Lambda function's role. The bucket policy explicitly grants access to the function's role, so no IAM role-specific permissions are needed for the Lambda function itself, although this option is less common than the previous one.

Question:2 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A security engineer is configuring a new website that is named example.com. The security engineer wants to secure communications with the website by requiring users to connect to example.com through HTTPS.
Which of the following is a valid option for storing SSL/TLS certificates?

- A. Custom SSL certificate that is stored in AWS Key Management Service (AWS KMS)
- B. Default SSL certificate that is stored in Amazon CloudFront
- C. Custom SSL certificate that is stored in AWS Certificate Manager (ACM)
- D. Default SSL certificate that is stored in Amazon S3

Correct Answer: *C*

Question:3 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A security engineer needs to develop a process to investigate and respond to potential security events on a company's Amazon EC2 instances. All the EC2 instances are backed by Amazon Elastic Block Store (Amazon EBS). The company uses AWS Systems Manager to manage all the EC2 instances and has installed Systems Manager Agent (SSM Agent) on all the EC2 instances.
The process that the security engineer is developing must comply with AWS security best practices and must meet the following requirements:
A compromised EC2 instance's volatile memory and non-volatile memory must be preserved for forensic purposes.
A compromised EC2 instance's metadata must be updated with corresponding incident ticket information.
A compromised EC2 instance must remain online during the investigation but must be isolated to prevent the spread of malware.
Any investigative activity during the collection of volatile data must be captured as part of the process.
Which combination of steps should the security engineer take to meet these requirements with the LEAST operational overhead? (Choose three.)

- A. Gather any relevant metadata for the compromised EC2 instance. Enable termination protection. Isolate the instance by updating the instance's security groups to restrict access. Detach the instance from any Auto Scaling groups that the instance is a member of. Deregister the instance from any Elastic Load Balancing (ELB) resources.

- B. Gather any relevant metadata for the compromised EC2 instance. Enable termination protection. Move the instance to an isolation subnet that denies all source and destination traffic. Associate the instance with the subnet to restrict access. Detach the instance from any Auto Scaling groups that the instance is a member of. Deregister the instance from any Elastic Load Balancing (ELB) resources.
- C. Use Systems Manager Run Command to invoke scripts that collect volatile data.
- D. Establish a Linux SSH or Windows Remote Desktop Protocol (RDP) session to the compromised EC2 instance to invoke scripts that collect volatile data.
- E. Create a snapshot of the compromised EC2 instance's EBS volume for follow-up investigations. Tag the instance with any relevant metadata and incident ticket information.
- F. Create a Systems Manager State Manager association to generate an EBS volume snapshot of the compromised EC2 instance. Tag the instance with any relevant metadata and incident ticket information.

Correct Answer: *ACE*

Question:4

A company has an organization in AWS Organizations. The company wants to use AWS CloudFormation StackSets in the organization to deploy various AWS design patterns into environments. These patterns consist of Amazon EC2 instances, Elastic Load Balancing (ELB) load balancers, Amazon RDS databases, and Amazon Elastic Kubernetes Service (Amazon EKS) clusters or Amazon Elastic Container Service (Amazon ECS) clusters.
Currently, the company’s developers can create their own CloudFormation stacks to increase the overall speed of delivery. A centralized CI/CD pipeline in a shared services AWS account deploys each CloudFormation stack.
The company's security team has already provided requirements for each service in accordance with internal standards. If there are any resources that do not comply with the internal standards, the security team must receive notification to take appropriate action. The security team must implement a notification solution that gives developers the ability to maintain the same overall delivery speed that they currently have.
Which solution will meet these requirements in the MOST operationally efficient way?

- A. Create an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the security team's email addresses to the SNS topic. Create a custom AWS Lambda function that will run the aws cloudformation validate-template AWS CLI command on all CloudFormation templates before the build stage in the CI/CD pipeline. Configure the CI/CD pipeline to publish a notification to the SNS topic if any issues are found.
- B. Create an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the security team's email addresses to the SNS topic. Create custom rules in CloudFormation Guard for each resource configuration. In the CI/CD pipeline, before the build stage, configure a Docker image to run the cfn-guard command on the CloudFormation template. Configure the CI/CD pipeline to publish a notification to the SNS topic if any issues are found.
- C. Create an Amazon Simple Notification Service (Amazon SNS) topic and an Amazon Simple Queue Service (Amazon SQS) queue. Subscribe the security team's email addresses to the SNS topic. Create an Amazon S3 bucket in the shared services AWS account. Include an event notification to publish to the SQS queue when new objects are added to the S3 bucket. Require the developers to put their CloudFormation templates in the S3 bucket. Launch EC2 instances that automatically scale based on the SQS queue depth. Configure the EC2 instances to use CloudFormation Guard to scan the templates and deploy the templates if there are no issues. Configure the CI/CD pipeline to publish a notification to the SNS topic if any issues are found.
- D. Create a centralized CloudFormation stack set that includes a standard set of resources that the developers can deploy in each AWS account. Configure each CloudFormation template to meet the security requirements. For any new resources or configurations, update the CloudFormation template and send the template to the security team for review. When the review is completed, add the new CloudFormation stack to the repository for the developers to use.

Correct Answer: *B*
You may use a lambda function to validate the syntax and semantics of CloudFormation templates. But when it comes to validate to a compliance policy, CloudFormation Guard makes more sense.
Reference:
https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/best-practices.html#:~:text=Validate%20templates%20for,non%2Dcompliant%20resources

Question:5 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company is migrating one of its legacy systems from an on-premises data center to AWS. The application server will run on AWS, but the database must remain in the on-premises data center for compliance reasons. The database is sensitive to network latency. Additionally, the data that travels between the on-premises data center and AWS must have IPsec encryption.

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

- A. AWS Site-to-Site VPN
- B. AWS Direct Connect
- C. AWS VPN CloudHub
- D. VPC peering
- E. NAT gateway

Correct Answer: *AB*

Reference:

https://docs.aws.amazon.com/directconnect/latest/UserGuide/encryption-in-transit.html

Question:6 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company has an application that uses dozens of Amazon DynamoDB tables to store data. Auditors find that the tables do not comply with the company's data protection policy.

The company's retention policy states that all data must be backed up twice each month: once at midnight on the 15th day of the month and again at midnight on the 25th day of the month. The company must retain the backups for 3 months.

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

- A. Use the DynamoDB on-demand backup capability to create a backup plan. Configure a lifecycle policy to expire backups after 3 months.
- B. Use AWS DataSync to create a backup plan. Add a backup rule that includes a retention period of 3 months.
- C. Use AWS Backup to create a backup plan. Add a backup rule that includes a retention period of 3 months.
- D. Set the backup frequency by using a cron schedule expression. Assign each DynamoDB table to the backup plan.
- E. Set the backup frequency by using a rate schedule expression. Assign each DynamoDB table to the backup plan.

Correct Answer: *CD*

Reference:

https://aws.amazon.com/blogs/database/set-up-scheduled-backups-for-amazon-dynamodb-using-aws-backup/

Question:7 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company needs a security engineer to implement a scalable solution for multi-account authentication and authorization. The solution should not introduce additional user-managed architectural components. Native AWS features should be used as much as possible. The security engineer has set up AWS Organizations with all features activated and AWS IAM Identity Center (AWS Single Sign-On) enabled.

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

- A. Use AD Connector to create users and groups for all employees that require access to AWS accounts. Assign AD Connector groups to AWS accounts and link to the IAM roles in accordance with the employees' job functions and access requirements. Instruct employees to access AWS accounts by using the AWS Directory Service user portal.
- B. Use an IAM Identity Center default directory to create users and groups for all employees that require access to AWS accounts. Assign groups to AWS accounts and link to permission sets in accordance with the employees' job functions and access requirements. Instruct employees to access AWS accounts by using the IAM Identity Center user portal.
- C. Use an IAM Identity Center default directory to create users and groups for all employees that require access to AWS accounts. Link IAM Identity Center groups to the IAM users present in all accounts to inherit existing permissions. Instruct employees to access AWS accounts by using the IAM Identity Center user portal.
- D. Use AWS Directory Service for Microsoft Active Directory to create users and groups for all employees that require access to AWS accounts. Enable AWS Management Console access in the created directory and

specify IAM Identity Center as a source of information for integrated accounts and permission sets. Instruct employees to access AWS accounts by using the AWS Directory Service user portal.

Correct Answer: *B*
Reference:
https://aws.amazon.com/ko/iam/identity-center/faqs/

Question:8 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company has deployed Amazon GuardDuty and now wants to implement automation for potential threats. The company has decided to start with RDP brute force attacks that come from Amazon EC2 instances in the company's AWS environment. A security engineer needs to implement a solution that blocks the detected communication from a suspicious instance until investigation and potential remediation can occur.
Which solution will meet these requirements?

- A. Configure GuardDuty to send the event to an Amazon Kinesis data stream. Process the event with an Amazon Kinesis Data Analytics for Apache Flink application that sends a notification to the company through Amazon Simple Notification Service (Amazon SNS). Add rules to the network ACL to block traffic to and from the suspicious instance.
- B. Configure GuardDuty to send the event to Amazon EventBridge. Deploy an AWS WAF web ACL. Process the event with an AWS Lambda function that sends a notification to the company through Amazon Simple Notification Service (Amazon SNS) and adds a web ACL rule to block traffic to and from the suspicious instance.
- C. Enable AWS Security Hub to ingest GuardDuty findings and send the event to Amazon EventBridge. Deploy AWS Network Firewall. Process the event with an AWS Lambda function that adds a rule to a Network Firewall firewall policy to block traffic to and from the suspicious instance.
- D. Enable AWS Security Hub to ingest GuardDuty findings. Configure an Amazon Kinesis data stream as an event destination for Security Hub. Process the event with an AWS Lambda function that replaces the security group of the suspicious instance with a security group that does not allow any connections.

Correct Answer: *C*
Explanation:
Let Guardduty detections be sent to Security Hub as findings is a simple and elegant way.
https://docs.aws.amazon.com/guardduty/latest/ug/securityhub-integration.html

Use eventbridge to respond by invoke Lambda. Amazon Kinesis data stream not needed.
https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-cloudwatch-events.html

Suggest to only block specific port 389 against thse suspicious EC2 instance instead of isolate it in a security group, to minimize the impact while it has not been verified as a confirmed attack.

Question:9 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company has an AWS account that hosts a production application. The company receives an email notification that Amazon GuardDuty has detected an Impact:IAMUser/AnomalousBehavior finding in the account. A security engineer needs to run the investigation playbook for this security incident and must collect and analyze the information without affecting the application.
Which solution will meet these requirements MOST quickly?

- A. Log in to the AWS account by using read-only credentials. Review the GuardDuty finding for details about the IAM credentials that were used. Use the IAM console to add a DenyAll policy to the IAM principal.
- B. Log in to the AWS account by using read-only credentials. Review the GuardDuty finding to determine which API calls initiated the finding. Use Amazon Detective to review the API calls in context.
- C. Log in to the AWS account by using administrator credentials. Review the GuardDuty finding for details about the IAM credentials that were used. Use the IAM console to add a DenyAll policy to the IAM principal.
- D. Log in to the AWS account by using read-only credentials. Review the GuardDuty finding to determine which API calls initiated the finding. Use AWS CloudTrail Insights and AWS CloudTrail Lake to review the API calls in context.

Correct Answer: *B*
Explanation:

Using CloudTrail (Insights & Lake) is not entirely wrong for the the aforementioned case, however, since the ask is to analyze the events "QUICKLY", I think Detective provides a good integration with GuardDuty to correlate data and analyze them.
Reference:
https://aws.amazon.com/blogs/security/how-you-can-use-amazon-guardduty-to-detect-suspicious-activity-within-your-aws-account/#:~:text=Start%20an%20investigation%20with%20Amazon%20Detective

Question:10 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

Company A has an AWS account that is named Account A. Company A recently acquired Company B, which has an AWS account that is named Account B. Company B stores its files in an Amazon S3 bucket. The administrators need to give a user from Account A full access to the S3 bucket in Account B.
After the administrators adjust the IAM permissions for the user in Account A to access the S3 bucket in Account B, the user still cannot access any files in the S3 bucket.
Which solution will resolve this issue?

- A. In Account B, create a bucket ACL to allow the user from Account A to access the S3 bucket in Account B.
- B. In Account B, create an object ACL to allow the user from Account A to access all the objects in the S3 bucket in Account B.
- C. In Account B, create a bucket policy to allow the user from Account A to access the S3 bucket in Account B.
- D. In Account B, create a user policy to allow the user from Account A to access the S3 bucket in Account B.

Correct Answer: *C*
Explanation:
For cross-account access, got to update S3 bucket policy to allow principal from other account to access it.
Reference:
https://docs.aws.amazon.com/AmazonS3/latest/userguide/example-walkthroughs-managing-access-example2.html

Question:11 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company wants to receive an email notification about critical findings in AWS Security Hub. The company does not have an existing architecture that supports this functionality.
Which solution will meet the requirement?

- A. Create an AWS Lambda function to identify critical Security Hub findings. Create an Amazon Simple Notification Service (Amazon SNS) topic as the target of the Lambda function. Subscribe an email endpoint to the SNS topic to receive published messages.
- B. Create an Amazon Kinesis Data Firehose delivery stream. Integrate the delivery stream with Amazon EventBridge. Create an EventBridge rule that has a filter to detect critical Security Hub findings. Configure the delivery stream to send the findings to an email address.
- C. Create an Amazon EventBridge rule to detect critical Security Hub findings. Create an Amazon Simple Notification Service (Amazon SNS) topic as the target of the EventBridge rule. Subscribe an email endpoint to the SNS topic to receive published messages.
- D. Create an Amazon EventBridge rule to detect critical Security Hub findings. Create an Amazon Simple Email Service (Amazon SES) topic as the target of the EventBridge rule. Use the Amazon SES API to format the message. Choose an email address to be the recipient of the message.

Correct Answer: *C*
Reference:
https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-cwe-all-findings.html

Question:12 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

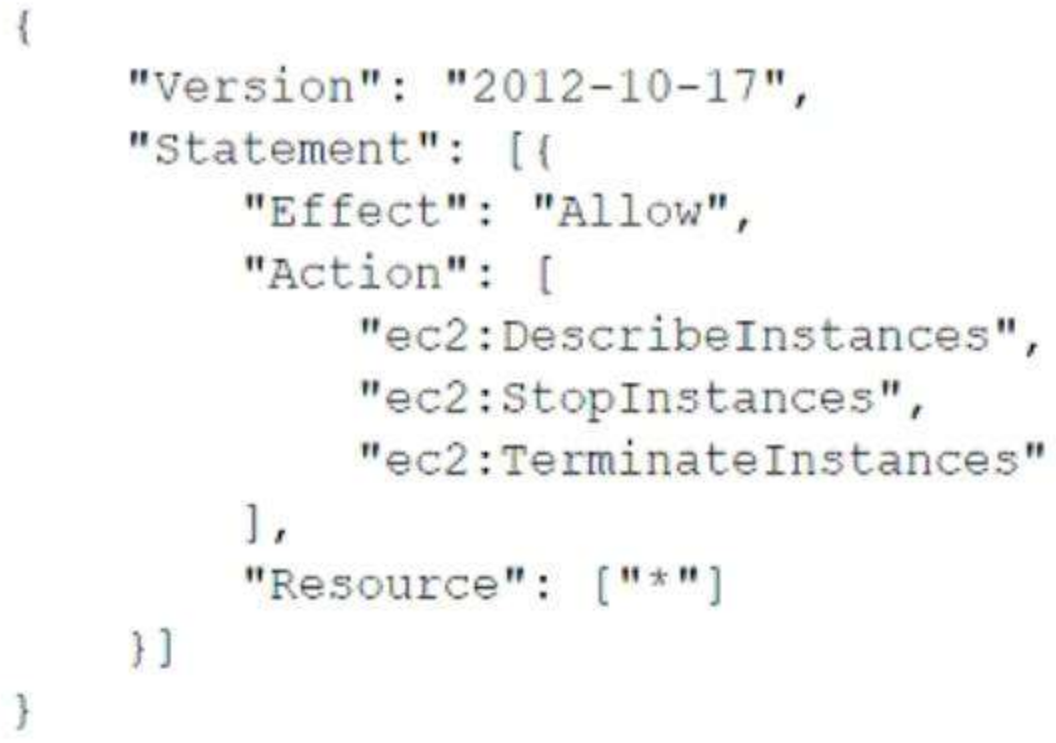
An international company has established a new business entity in South Korea. The company also has established a new AWS account to contain the workload for the South Korean region. The company has set up the workload in the new account in the ap-northeast-2 Region. The workload consists of three Auto Scaling groups of Amazon EC2 instances. All workloads that operate in this Region must keep system logs and application logs for 7 years.
A security engineer must implement a solution to ensure that no logging data is lost for each instance during scaling activities. The solution also must keep the logs for only the required period of 7 years.
Which combination of steps should the security engineer take to meet these requirements? (Choose three.)

- A. Ensure that the Amazon CloudWatch agent is installed on all the EC2 instances that the Auto Scaling groups launch. Generate a CloudWatch agent configuration file to forward the required logs to Amazon CloudWatch Logs.
- B. Set the log retention for desired log groups to 7 years.
- C. Attach an IAM role to the launch configuration or launch template that the Auto Scaling groups use. Configure the role to provide the necessary permissions to forward logs to Amazon CloudWatch Logs.
- D. Attach an IAM role to the launch configuration or launch template that the Auto Scaling groups use. Configure the role to provide the necessary permissions to forward logs to Amazon S3.
- E. Ensure that a log forwarding application is installed on all the EC2 instances that the Auto Scaling groups launch. Configure the log forwarding application to periodically bundle the logs and forward the logs to Amazon S3.
- F. Configure an Amazon S3 Lifecycle policy on the target S3 bucket to expire objects after 7 years.

Correct Answer: *ABC*
Explanation:
EC2 (with a role allowing sending events) >> CloudWatch agent >> CloudWatch Logs >> CloudWatch Logs retention period

Question:13 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A security engineer is designing an IAM policy to protect AWS API operations. The policy must enforce multi-factor authentication (MFA) for IAM users to access certain services in the AWS production account. Each session must remain valid for only 2 hours. The current version of the IAM policy is as follows:



```
{
        "Version": "2012-10-17",
        "Statement": [{
                "Effect": "Allow",
                "Action": [
                        "ec2:DescribeInstances",
                        "ec2:StopInstances",
                        "ec2:TerminateInstances"
                ],
                "Resource": ["*"]
        }]
}
```

Which combination of conditions must the security engineer add to the IAM policy to meet these requirements? (Choose two.)

- A. "Bool": {"aws:MultiFactorAuthPresent": "true"}
- B. "Bool": {"aws:MultiFactorAuthPresent": "false"}
- C. "NumericLessThan": {"aws:MultiFactorAuthAge": "7200"}
- D. "NumericGreaterThan": {"aws:MultiFactorAuthAge": "7200"}
- E. "NumericLessThan": {"MaxSessionDuration": "7200"}

Correct Answer: *AC*
Reference:
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_configure-api-require.html

Question:14 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company uses AWS Organizations and has production workloads across multiple AWS accounts. A security engineer needs to design a solution that will proactively monitor for suspicious behavior across all the accounts that contain production workloads.

The solution must automate remediation of incidents across the production accounts. The solution also must publish a notification to an Amazon Simple Notification Service (Amazon SNS) topic when a critical security finding is detected. In addition, the solution must send all security incident logs to a dedicated account.

Which solution will meet these requirements?

- A. Activate Amazon GuardDuty in each production account. In a dedicated logging account, aggregate all GuardDuty logs from each production account. Remediate incidents by configuring GuardDuty to directly invoke an AWS Lambda function. Configure the Lambda function to also publish notifications to the SNS topic.
- B. Activate AWS Security Hub in each production account. In a dedicated logging account, aggregate all Security Hub findings from each production account. Remediate incidents by using AWS Config and AWS Systems Manager. Configure Systems Manager to also publish notifications to the SNS topic.
- C. Activate Amazon GuardDuty in each production account. In a dedicated logging account, aggregate all GuardDuty logs from each production account. Remediate incidents by using Amazon EventBridge to invoke a custom AWS Lambda function from the GuardDuty findings. Configure the Lambda function to also publish notifications to the SNS topic.
- D. Activate AWS Security Hub in each production account. In a dedicated logging account, aggregate all Security Hub findings from each production account. Remediate incidents by using Amazon EventBridge to invoke a custom AWS Lambda function from the Security Hub findings. Configure the Lambda function to also publish notifications to the SNS topic.

Correct Answer: *C*

Explanation:

Security Hub by itself does not detect suspicious activity, but GuardDuty. Eventbridge rule is required to trigger remediation actions and SNS topic.

Question:15 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company is designing a multi-account structure for its development teams. The company is using AWS Organizations and AWS IAM Identity Center (AWS Single Sign-On). The company must implement a solution so that the development teams can use only specific AWS Regions and so that each AWS account allows access to only specific AWS services.

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

- A. Use IAM Identity Center to set up service-linked roles with IAM policy statements that include the Condition, Resource, and NotAction elements to allow access to only the Regions and services that are needed.
- B. Deactivate AWS Security Token Service (AWS STS) in Regions that the developers are not allowed to use.
- C. Create SCPs that include the Condition, Resource, and NotAction elements to allow access to only the Regions and services that are needed.
- D. For each AWS account, create tailored identity-based policies for IAM Identity Center. Use statements that include the Condition, Resource, and NotAction elements to allow access to only the Regions and services that are needed.

Correct Answer: *C*

Explanation:

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_examples_general.html#example-scp-deny-region

Question:16 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company is developing an ecommerce application. The application uses Amazon EC2 instances and an Amazon RDS MySQL database. For compliance reasons, data must be secured in transit and at rest. The company needs a solution that minimizes operational overhead and minimizes cost.

Which solution meets these requirements?

- A. Use TLS certificates from AWS Certificate Manager (ACM) with an Application Load Balancer. Deploy self-signed certificates on the EC2 instances. Ensure that the database client software uses a TLS connection to

Amazon RDS. Enable encryption of the RDS DB instance. Enable encryption on the Amazon Elastic Block Store (Amazon EBS) volumes that support the EC2 instances.

- B. Use TLS certificates from a third-party vendor with an Application Load Balancer. Install the same certificates on the EC2 instances. Ensure that the database client software uses a TLS connection to Amazon RDS. Use AWS Secrets Manager for client-side encryption of application data.
- C. Use AWS CloudHSM to generate TLS certificates for the EC2 instances. Install the TLS certificates on the EC2 instances. Ensure that the database client software uses a TLS connection to Amazon RDS. Use the encryption keys from CloudHSM for client-side encryption of application data.
- D. Use Amazon CloudFront with AWS WAF. Send HTTP connections to the origin EC2 instances. Ensure that the database client software uses a TLS connection to Amazon RDS. Use AWS Key Management Service (AWS KMS) for client-side encryption of application data before the data is stored in the RDS database.

Correct Answer: *A*
Explanation:
It addresses data encryption at rest at RDS and EBS and is the most cost-effective and efficient method. TLS certificates from a third-party vendor or generated by CloudHSM is unnecessarily increase cost and ops overhead. CloudFront with WAF is irrelevant to the requirement.

Question:17 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A security engineer is working with a company to design an ecommerce application. The application will run on Amazon EC2 instances that run in an Auto Scaling group behind an Application Load Balancer (ALB). The application will use an Amazon RDS DB instance for its database.
The only required connectivity from the internet is for HTTP and HTTPS traffic to the application. The application must communicate with an external payment provider that allows traffic only from a preconfigured allow list of IP addresses. The company must ensure that communications with the external payment provider are not interrupted as the environment scales.
Which combination of actions should the security engineer recommend to meet these requirements? (Choose three.)

- A. Deploy a NAT gateway in each private subnet for every Availability Zone that is in use.
- B. Place the DB instance in a public subnet.
- C. Place the DB instance in a private subnet.
- D. Configure the Auto Scaling group to place the EC2 instances in a public subnet.
- E. Configure the Auto Scaling group to place the EC2 instances in a private subnet.
- F. Deploy the ALB in a private subnet.

Correct Answer: *ACE*
Reference:
https://docs.aws.amazon.com/vpc/latest/userguide/nat-gateway-scenarios.html#private-nat-allowed-range

Question:18 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company uses several AWS CloudFormation stacks to handle the deployment of a suite of applications. The leader of the company's application development team notices that the stack deployments fail with permission errors when some team members try to deploy the stacks. However, other team members can deploy the stacks successfully.
The team members access the account by assuming a role that has a specific set of permissions that are necessary for the job responsibilities of the team members. All team members have permissions to perform operations on the stacks.
Which combination of steps will ensure consistent deployment of the stacks MOST securely? (Choose three.)

- A. Create a service role that has a composite principal that contains each service that needs the necessary permissions. Configure the role to allow the sts:AssumeRole action.
- B. Create a service role that has cloudformation.amazonaws.com as the service principal. Configure the role to allow the sts:AssumeRole action.
- C. For each required set of permissions, add a separate policy to the role to allow those permissions. Add the ARN of each CloudFormation stack in the resource field of each policy.
- D. For each required set of permissions, add a separate policy to the role to allow those permissions. Add the ARN of each service that needs the permissions in the resource field of the corresponding policy.
- E. Update each stack to use the service role.
  F Add a policy to each member role to allow the iam:PassRole action. Set the policy's resource field to the

ARN of the service role.

Correct Answer: *BDE*
Reference:
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-service.html
https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-iam-servicerole.html#using-iam-servicerole-add
https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-iam-servicerole.html

Question:19 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company used a lift-and-shift approach to migrate from its on-premises data centers to the AWS Cloud. The company migrated on-premises VMs to Amazon EC2 instances. Now the company wants to replace some of components that are running on the EC2 instances with managed AWS services that provide similar functionality. Initially, the company will transition from load balancer software that runs on EC2 instances to AWS Elastic Load Balancers. A security engineer must ensure that after this transition, all the load balancer logs are centralized and searchable for auditing. The security engineer must also ensure that metrics are generated to show which ciphers are in use.
Which solution will meet these requirements?

- A. Create an Amazon CloudWatch Logs log group. Configure the load balancers to send logs to the log group. Use the CloudWatch Logs console to search the logs. Create CloudWatch Logs filters on the logs for the required metrics.
- B. Create an Amazon S3 bucket. Configure the load balancers to send logs to the S3 bucket. Use Amazon Athena to search the logs that are in the S3 bucket. Create Amazon CloudWatch filters on the S3 log files for the required metrics.
- C. Create an Amazon S3 bucket. Configure the load balancers to send logs to the S3 bucket. Use Amazon Athena to search the logs that are in the S3 bucket. Create Athena queries for the required metrics. Publish the metrics to Amazon CloudWatch.
- D. Create an Amazon CloudWatch Logs log group. Configure the load balancers to send logs to the log group. Use the AWS Management Console to search the logs. Create Amazon Athena queries for the required metrics. Publish the metrics to Amazon CloudWatch.

Correct Answer: *C*
Explanation:
You can't send ELB access logs into CloudWatch Logs, but to S3 only:
https://docs.aws.amazon.com/elasticloadbalancing/latest/application/enable-access-logging.html
Regarding the alarm, natively there is no way to use query result as a metric.We could use a Lambda Function for this.

Question:20 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company uses AWS Organizations to manage a multi-account AWS environment in a single AWS Region. The organization's management account is named management-01. The company has turned on AWS Config in all accounts in the organization. The company has designated an account named security-01 as the delegated administrator for AWS Config.
All accounts report the compliance status of each account's rules to the AWS Config delegated administrator account by using an AWS Config aggregator. Each account administrator can configure and manage the account's own AWS Config rules to handle each account's unique compliance requirements.
A security engineer needs to implement a solution to automatically deploy a set of 10 AWS Config rules to all existing and future AWS accounts in the organization. The solution must turn on AWS Config automatically during account creation.
Which combination of steps will meet these requirements? (Choose two.)

- A. Create an AWS CloudFormation template that contains the 10 required AWS Config rules. Deploy the template by using CloudFormation StackSets in the security-01 account.
- B. Create a conformance pack that contains the 10 required AWS Config rules. Deploy the conformance pack from the security-01 account.
- C. Create a conformance pack that contains the 10 required AWS Config rules. Deploy the conformance pack from the management-01 account.
- D. Create an AWS CloudFormation template that will activate AWS Config. Deploy the template by using

CloudFormation StackSets in the security-01 account.

- E. Create an AWS CloudFormation template that will activate AWS Config. Deploy the template by using CloudFormation StackSets in the management-01 account.

Correct Answer: *BE*
Explanation:
Use management account to delegate accounts for auditing, security or compliance, then use delegated account to deploy conformance packs
Reference:
https://aws.amazon.com/blogs/mt/deploying-conformance-packs-across-an-organization-with-automatic-remediation/
Delegated administrator for AWS Organizations
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_delegate_policies.html

Question:21 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

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. Use Amazon CloudWatch Logs Insights to identify any objects in DOC-EXAMPLE-BUCKET1 that contain PII and that were available to the access key.
- B. Use Amazon OpenSearch 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.
- C. 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.
- D. 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.
- E. Configure Amazon Macie to identify any objects in DOC-EXAMPLE-BUCKET1 that contain PII and that were available to the access key.

Correct Answer: *CE*
Explanation:
Athena send the query results to s3 bucket > Macie can scan s3 bucket

Question:22 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

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

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

Correct Answer: *D*
Explanation:
Explicit deny statements cannot be overridden by allow statements "An explicit deny in any policy overrides any allows."
Reference:

https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_evaluation-logic.html#policy-eval-denyallow

Question:23 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

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.

Correct Answer: *D*
Reference:
https://docs.aws.amazon.com/waf/latest/developerguide/ddos-cloudwatch-metrics.html

Question:24 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

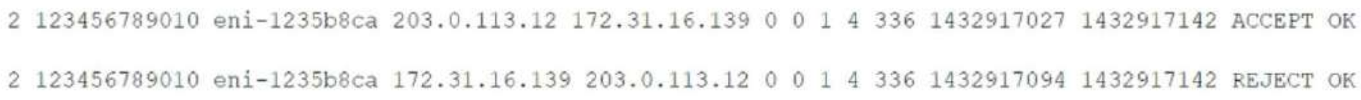
A company hosts a web application on an Apache web server. The application runs on Amazon EC2 instances that are in an Auto Scaling group. The company configured the EC2 instances to send the Apache web server logs to an Amazon CloudWatch Logs group that the company has configured to expire after 1 year.
Recently, the company discovered in the Apache web server logs that a specific IP address is sending suspicious requests to the web application. A security engineer wants to analyze the past week of Apache web server logs to determine how many requests that the IP address sent and the corresponding URLs that the IP address requested.
What should the security engineer do to meet these requirements with the LEAST effort?

- A. Export the CloudWatch Logs group data to Amazon S3. Use Amazon Macie to query the logs for the specific IP address and the requested URL.
- B. Configure a CloudWatch Logs subscription to stream the log group to an Amazon OpenSearch Service cluster. Use OpenSearch Service to analyze the logs for the specific IP address and the requested URLs.
- C. Use CloudWatch Logs Insights and a custom query syntax to analyze the CloudWatch logs for the specific IP address and the requested URLs.
- D. Export the CloudWatch Logs group data to Amazon S3. Use AWS Glue to crawl the S3 bucket for only the log entries that contain the specific IP address. Use AWS Glue to view the results.

Correct Answer: *C*
Reference:
https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CWL_QuerySyntax-examples.html

Question:25 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

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



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

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

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

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

Correct Answer: *D*
Explanation:
NACLs are stateless and do not track the state of a connection, while Security Groups are stateful and allow traffic based on the response to previous traffic. Default rule: NACLs have a default rule that denies all traffic, while

Security Groups have a default rule that allows all traffic.

Question:26 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company developed an application by using AWS Lambda, Amazon S3, Amazon Simple Notification Service (Amazon SNS), and Amazon DynamoDB. An external application puts objects into the company's S3 bucket and tags the objects with date and time. A Lambda function periodically pulls data from the company's S3 bucket based on date and time tags and inserts specific values into a DynamoDB table for further processing.

The data includes personally identifiable information (PII). The company must remove data that is older than 30 days from the S3 bucket and the DynamoDB table.

Which solution will meet this requirement with the MOST operational efficiency?

- A. Update the Lambda function to add a TTL S3 flag to S3 objects. Create an S3 Lifecycle policy to expire objects that are older than 30 days by using the TTL S3 flag.
- B. Create an S3 Lifecycle policy to expire objects that are older than 30 days. Update the Lambda function to add the TTL attribute in the DynamoDB table. Enable TTL on the DynamoDB table to expire entries that are older than 30 days based on the TTL attribute.
- C. Create an S3 Lifecycle policy to expire objects that are older than 30 days and to add all prefixes to the S3 bucket. Update the Lambda function to delete entries that are older than 30 days.
- D. Create an S3 Lifecycle policy to expire objects that are older than 30 days by using object tags. Update the Lambda function to delete entries that are older than 30 days.

Correct Answer: *B*

Explanation & Reference:

https://docs.aws.amazon.com/AmazonS3/latest/userguide/lifecycle-configuration-examples.html

Just need to set expiration days in the LifecycleConfiguration- add prefix, object tags are not needed.

https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/TTL.html

TTL is used for housekeeping data in DynamoDB by enabling TTL attribute by console or CLI, without the need for any lambda function/

Question:27 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

What are the MOST secure ways to protect the AWS account root user of a recently opened AWS account? (Choose two.)

- A. Use the AWS account root user access keys instead of the AWS Management Console.
- B. Enable multi-factor authentication for the AWS IAM users with the AdministratorAccess managed policy attached to them.
- C. Use AWS KMS to encrypt all AWS account root user and AWS IAM access keys and set automatic rotation to 30 days.
- D. Do not create access keys for the AWS account root user; instead, create AWS IAM users.
- E. Enable multi-factor authentication for the AWS account root user.

Correct Answer: *DE*

Question:28 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company is expanding its group of stores. On the day that each new store opens, the company wants to launch a customized web application for that store. Each store's application will have a non-production environment and a production environment. Each environment will be deployed in a separate AWS account. The company uses AWS Organizations and has an OU that is used only for these accounts.

The company distributes most of the development work to third-party development teams. A security engineer needs to ensure that each team follows the company's deployment plan for AWS resources. The security engineer also must limit access to the deployment plan to only the developers who need access. The security engineer already has created an AWS CloudFormation template that implements the deployment plan.

What should the security engineer do next to meet the requirements in the MOST secure way?

- A. Create an AWS Service Catalog portfolio in the organization's management account. Upload the CloudFormation template. Add the template to the portfolio's product list. Share the portfolio with the OU.
- B. Use the CloudFormation CLI to create a module from the CloudFormation template. Register the module as a private extension in the CloudFormation registry. Publish the extension. In the OU, create an SCP that allows access to the extension.
- C. Create an AWS Service Catalog portfolio in the organization's management account. Upload the

CloudFormation template. Add the template to the portfolio's product list. Create an IAM role that has a trust policy that allows cross-account access to the portfolio for users in the OU accounts. Attach the AWSServiceCatalogEndUserFullAccess managed policy to the role.
- D. Use the CloudFormation CLI to create a module from the CloudFormation template. Register the module as a private extension in the CloudFormation registry. Publish the extension. Share the extension with the OU.

Correct Answer: *A*
Explanation:
To use Service Catalog with multiple AWS accounts, you need to enable AWS Organizations with all features enabled. This allows you to centrally manage your accounts and apply policies across your organization. You can also use Service Catalog as a service principal for AWS Organizations, which lets you share your portfolios with organizational units (OUs) or accounts in your organization.

To create a Service Catalog portfolio, you need to use an administrator account, such as the organization's management account. You can upload your CloudFormation template as a product in your portfolio, and define constraints and tags for it. You can then share your portfolio with the OU that contains the accounts for the web applications. This will allow the developers in those accounts to launch products from the shared portfolio using the Service Catalog end user console.

Question:29 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A team is using AWS Secrets Manager to store an application database password. Only a limited number of IAM principals within the account can have access to the secret. The principals who require access to the secret change frequently. A security engineer must create a solution that maximizes flexibility and scalability.
Which solution will meet these requirements?

- A. Use a role-based approach by creating an IAM role with an inline permissions policy that allows access to the secret. Update the IAM principals in the role trust policy as required.
- B. Deploy a VPC endpoint for Secrets Manager. Create and attach an endpoint policy that specifies the IAM principals that are allowed to access the secret. Update the list of IAM principals as required.
- C. Use a tag-based approach by attaching a resource policy to the secret. Apply tags to the secret and the IAM principals. Use the aws:PrincipalTag and aws:ResourceTag IAM condition keys to control access.
- D. Use a deny-by-default approach by using IAM policies to deny access to the secret explicitly. Attach the policies to an IAM group. Add all IAM principals to the IAM group. Remove principals from the group when they need access. Add the principals to the group again when access is no longer allowed.

Correct Answer: *C*
Reference:
https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction_attribute-based-access-control.html
https://aws.amazon.com/blogs/security/simplify-granting-access-to-your-aws-resources-by-using-tags-on-aws-iam-users-and-roles/

Question:30 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company is hosting a web application on Amazon EC2 instances behind an Application Load Balancer (ALB). The application has become the target of a DoS attack. Application logging shows that requests are coming from a small number of client IP addresses, but the addresses change regularly.
The company needs to block the malicious traffic with a solution that requires the least amount of ongoing effort.
Which solution meets these requirements?

- A. Create an AWS WAF rate-based rule, and attach it to the ALB.
- B. Update the security group that is attached to the ALB to block the attacking IP addresses.
- C. Update the ALB subnet's network ACL to block the attacking client IP addresses.
- D. Create an AWS WAF rate-based rule, and attach it to the security group of the EC2 instances.

Correct Answer: *A*
Explanation:
AWS WAF can be deployed on Amazon CloudFront, the Application Load Balancer (ALB), Amazon API Gateway, and AWS AppSync.

Question:31 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company has hundreds of AWS accounts in an organization in AWS Organizations. The company operates out of a single AWS Region. The company has a dedicated security tooling AWS account in the organization. The security tooling account is configured as the organization's delegated administrator for Amazon GuardDuty and AWS Security Hub. The company has configured the environment to automatically enable GuardDuty and Security Hub for existing AWS accounts and new AWS accounts.

The company is performing control tests on specific GuardDuty findings to make sure that the company's security team can detect and respond to security events. The security team launched an Amazon EC2 instance and attempted to run DNS requests against a test domain, example.com, to generate a DNS finding. However, the GuardDuty finding was never created in the Security Hub delegated administrator account.

Why was the finding was not created in the Security Hub delegated administrator account?

- A. VPC flow logs were not turned on for the VPC where the EC2 instance was launched.
- B. The VPC where the EC2 instance was launched had the DHCP option configured for a custom OpenDNS resolver.
- C. The GuardDuty integration with Security Hub was never activated in the AWS account where the finding was generated.
- D. Cross-Region aggregation in Security Hub was not configured.

Correct Answer: *B*

Reference:

https://repost.aws/knowledge-center/guardduty-finding-types#:~:text=Note%3A%20GuardDuty%20only%20processes%20DNS%20logs%20if%20you%20use%20the%20default%20VPC%20DNS%20resolver.%20All%20other%20types%20of%20DNS%20resolvers%20won%27t%20generated%20DNS%20based%20findings.

Question:32 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

An ecommerce company has a web application architecture that runs primarily on containers. The application containers are deployed on Amazon Elastic Container Service (Amazon ECS). The container images for the application are stored in Amazon Elastic Container Registry (Amazon ECR).

The company's security team is performing an audit of components of the application architecture. The security team identifies issues with some container images that are stored in the container repositories.

The security team wants to address these issues by implementing continual scanning and on-push scanning of the container images. The security team needs to implement a solution that makes any findings from these scans visible in a centralized dashboard. The security team plans to use the dashboard to view these findings along with other security-related findings that they intend to generate in the future. There are specific repositories that the security team needs to exclude from the scanning process.

Which solution will meet these requirements?

- A. Use Amazon Inspector. Create inclusion rules in Amazon ECR to match repositories that need to be scanned. Push Amazon Inspector findings to AWS Security Hub.
- B. Use ECR basic scanning of container images. Create inclusion rules in Amazon ECR to match repositories that need to be scanned. Push findings to AWS Security Hub.
- C. Use ECR basic scanning of container images. Create inclusion rules in Amazon ECR to match repositories that need to be scanned. Push findings to Amazon Inspector.
- D. Use Amazon Inspector. Create inclusion rules in Amazon Inspector to match repositories that need to be scanned. Push Amazon Inspector findings to AWS Config.

Correct Answer: *A*

Question:33 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company has a single AWS account and uses an Amazon EC2 instance to test application code. The company recently discovered that the instance was compromised. The instance was serving up malware. The analysis of the instance showed that the instance was compromised 35 days ago.

A security engineer must implement a continuous monitoring solution that automatically notifies the company's security team about compromised instances through an email distribution list for high severity findings. The security engineer must implement the solution as soon as possible.

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

- A. Enable AWS Security Hub in the AWS account.

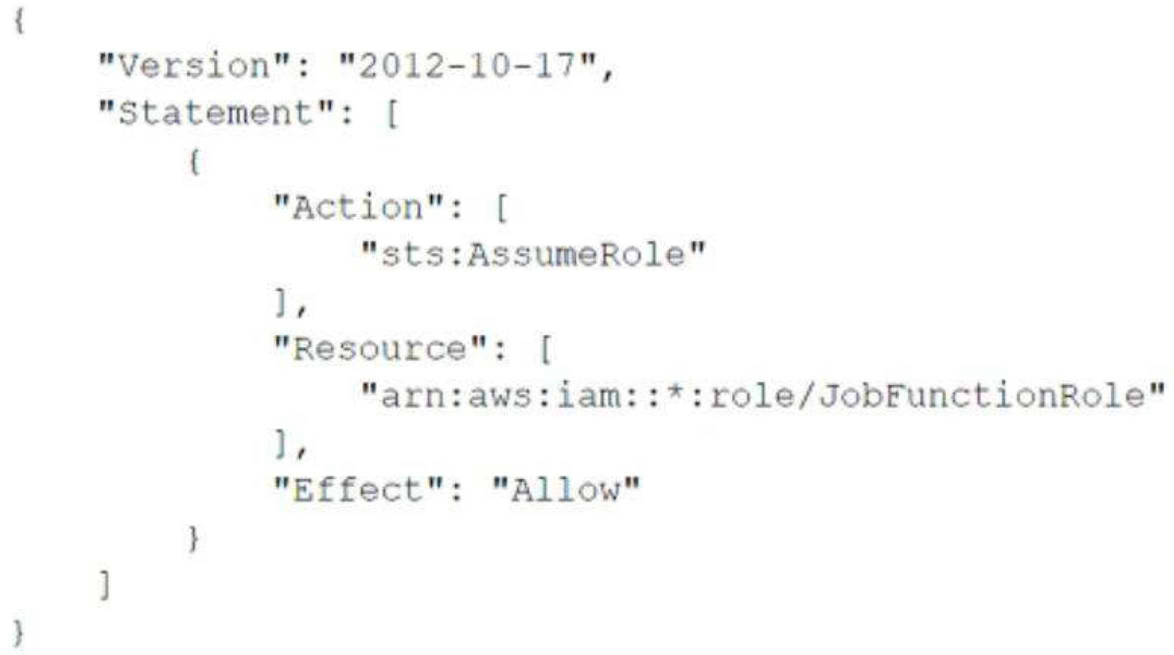
- B. Enable Amazon GuardDuty in the AWS account.
- C. Create an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the security team's email distribution list to the topic.
- D. Create an Amazon Simple Queue Service (Amazon SQS) queue. Subscribe the security team's email distribution list to the queue.
- E. Create an Amazon EventBridge rule for GuardDuty findings of high severity. Configure the rule to publish a message to the topic.
- F. Create an Amazon EventBridge rule for Security Hub findings of high severity. Configure the rule to publish a message to the queue.

Correct Answer: *BCE*

Question:34 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

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

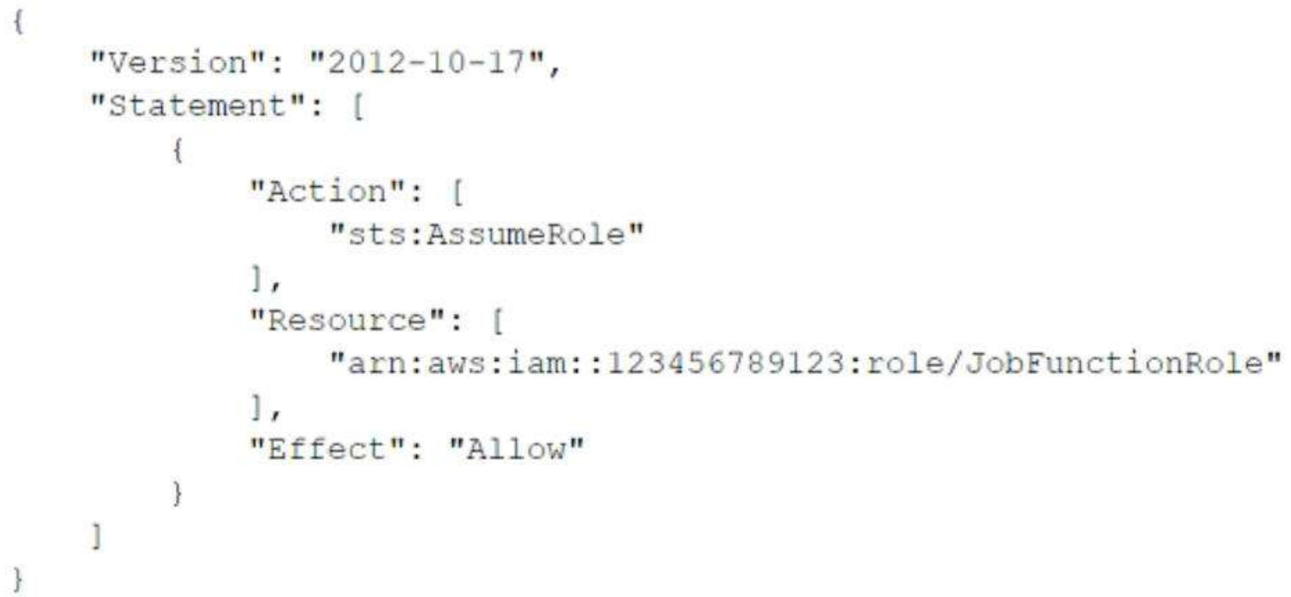
A user is unable to assume the IAM role in the target account. The policy attached to the role in the identity account is:



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

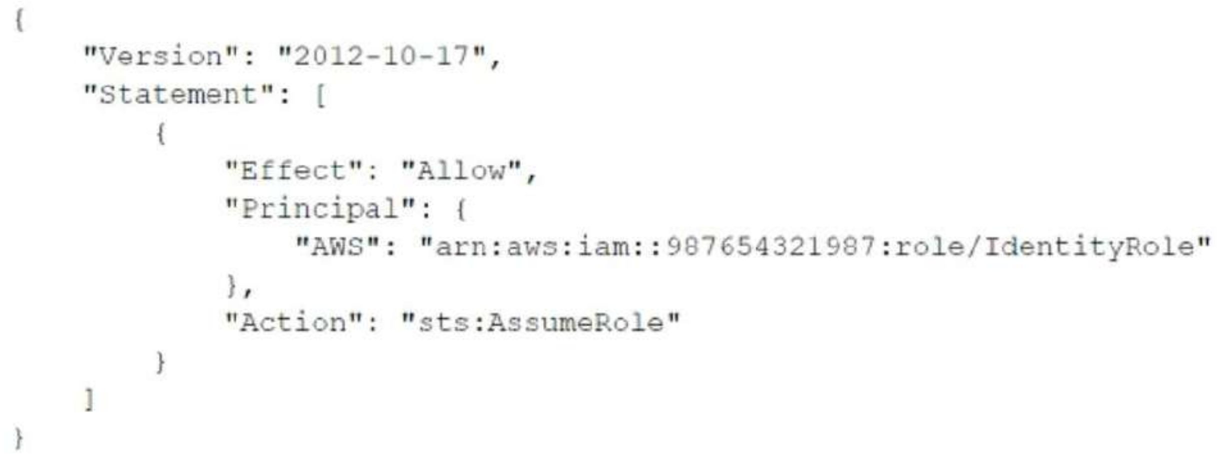
What should be done to enable the user to assume the appropriate role in the target account?

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



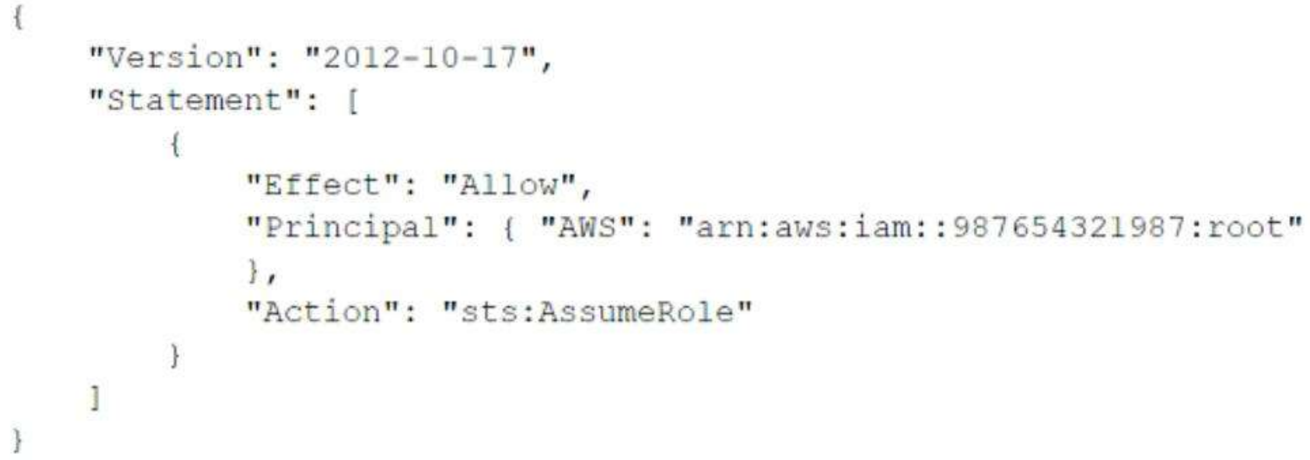
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": [
                "arn:aws:iam::123456789123:role/JobFunctionRole"
            ],
            "Effect": "Allow"
        }
    ]
}
```

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



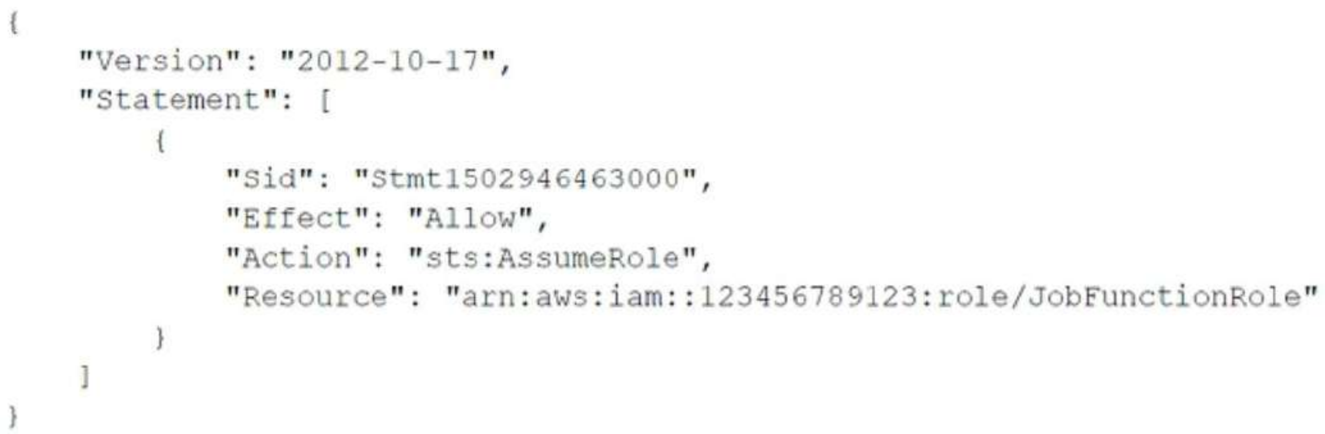
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::987654321987:role/IdentityRole"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

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



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

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



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

Correct Answer: *B*

Question:35 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company is using AWS Organizations to manage multiple AWS accounts for its human resources, finance, software development, and production departments. All the company's developers are part of the software development AWS account.

The company discovers that developers have launched Amazon EC2 instances that were preconfigured with software that the company has not approved for use. The company wants to implement a solution to ensure that developers can launch EC2 instances with only approved software applications and only in the software development AWS account.

Which solution will meet these requirements?

- A. In the software development account, create AMIs of preconfigured instances that include only approved software. Include the AMI IDs in the condition section of an AWS CloudFormation template to launch the appropriate AMI based on the AWS Region. Provide the developers with the CloudFormation template to launch EC2 instances in the software development account.
- B. Create an Amazon EventBridge rule that runs when any EC2 RunInstances API event occurs in the software development account. Specify AWS Systems Manager Run Command as a target of the rule. Configure Run Command to run a script that will install all approved software onto the instances that the developers launch.
- C. Use an AWS Service Catalog portfolio that contains EC2 products with appropriate AMIs that include only approved software. Grant the developers permission to access only the Service Catalog portfolio to launch a product in the software development account.
- D. In the management account, create AMIs of preconfigured instances that include only approved software. Use AWS CloudFormation StackSets to launch the AMIs across any AWS account in the organization. Grant the developers permission to launch the stack sets within the management account.

Correct Answer: *C*

Question:36 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company has enabled Amazon GuardDuty in all AWS Regions as part of its security monitoring strategy. In one of its VPCs, the company hosts an Amazon EC2 instance that works as an FTP server. A high number of clients from multiple locations contact the FTP server. GuardDuty identifies this activity as a brute force attack because of the high number of connections that happen every hour.

The company has flagged the finding as a false positive, but GuardDuty continues to raise the issue. A security engineer must improve the signal-to-noise ratio without compromising the company's visibility of potential anomalous behavior.

Which solution will meet these requirements?

- A. Disable the FTP rule in GuardDuty in the Region where the FTP server is deployed.
- B. Add the FTP server to a trusted IP list. Deploy the list to GuardDuty to stop receiving the notifications.
- C. Create a suppression rule in GuardDuty to filter findings by automatically archiving new findings that match the specified criteria.
- D. Create an AWS Lambda function that has the appropriate permissions to delete the finding whenever a

new occurrence is reported.

Correct Answer: *C*

Question:37

A company is running internal microservices on Amazon Elastic Container Service (Amazon ECS) with the Amazon EC2 launch type. The company is using Amazon Elastic Container Registry (Amazon ECR) private repositories.
A security engineer needs to encrypt the private repositories by using AWS Key Management Service (AWS KMS). The security engineer also needs to analyze the container images for any common vulnerabilities and exposures (CVEs).
Which solution will meet these requirements?

- A. Enable KMS encryption on the existing ECR repositories. Install Amazon Inspector Agent from the ECS container instances' user data. Run an assessment with the CVE rules.
- B. Recreate the ECR repositories with KMS encryption and ECR scanning enabled. Analyze the scan report after the next push of images.
- C. Recreate the ECR repositories with KMS encryption and ECR scanning enabled. Install AWS Systems Manager Agent on the ECS container instances. Run an inventory report.
- D. Enable KMS encryption on the existing ECR repositories. Use AWS Trusted Advisor to check the ECS container instances and to verify the findings against a list of current CVEs.

Correct Answer: *B*

Question:38

A company's security engineer has been tasked with restricting a contractor's IAM account access to the company's Amazon EC2 console without providing access to any other AWS services. The contractor's IAM account must not be able to gain access to any other AWS service, even if the IAM account is assigned additional permissions based on IAM group membership.
What should the security engineer do to meet these requirements?

- A. Create an inline IAM user policy that allows for Amazon EC2 access for the contractor's IAM user.
- B. Create an IAM permissions boundary policy that allows Amazon EC2 access. Associate the contractor's IAM account with the IAM permissions boundary policy.
- C. Create an IAM group with an attached policy that allows for Amazon EC2 access. Associate the contractor's IAM account with the IAM group.
- D. Create a IAM role that allows for EC2 and explicitly denies all other services. Instruct the contractor to always assume this role.

Correct Answer: *B*

Question:39

A company manages multiple AWS accounts using AWS Organizations. The company's security team notices that some member accounts are not sending AWS CloudTrail logs to a centralized Amazon S3 logging bucket. The security team wants to ensure there is at least one trail configured for all existing accounts and for any account that is created in the future.
Which set of actions should the security team implement to accomplish this?

- A. Create a new trail and configure it to send CloudTrail logs to Amazon S3. Use Amazon EventBridge to send notification if a trail is deleted or stopped.
- B. Deploy an AWS Lambda function in every account to check if there is an existing trail and create a new trail, if needed.
- C. Edit the existing trail in the Organizations management account and apply it to the organization.
- D. Create an SCP to deny the cloudtrail:Delete* and cloudtrail:Stop* actions. Apply the SCP to all accounts.

Correct Answer: *C*

Question:40

A company recently had a security audit in which the auditors identified multiple potential threats. These potential threats can cause usage pattern changes such as DNS access peak, abnormal instance traffic, abnormal network interface traffic, and unusual Amazon S3 API calls. The threats can come from different sources and can occur at any

time. The company needs to implement a solution to continuously monitor its system and identify all these incoming threats in near-real time.
Which solution will meet these requirements?

- A. Enable AWS CloudTrail logs, VPC flow logs, and DNS logs. Use Amazon CloudWatch Logs to manage these logs from a centralized account.
- B. Enable AWS CloudTrail logs, VPC flow logs, and DNS logs. Use Amazon Macie to monitor these logs from a centralized account.
- C. Enable Amazon GuardDuty from a centralized account. Use GuardDuty to manage AWS CloudTrail logs, VPC flow logs, and DNS logs.
- D. Enable Amazon Inspector from a centralized account. Use Amazon Inspector to manage AWS CloudTrail logs, VPC flow logs, and DNS logs.

Correct Answer: *C*

Question:41 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company that uses AWS Organizations is using AWS IAM Identity Center (AWS Single Sign-On) to administer access to AWS accounts. A security engineer is creating a custom permission set in IAM Identity Center. The company will use the permission set across multiple accounts. An AWS managed policy and a customer managed policy are attached to the permission set. The security engineer has full administrative permissions and is operating in the management account.
When the security engineer attempts to assign the permission set to an IAM Identity Center user who has access to multiple accounts, the assignment fails.
What should the security engineer do to resolve this failure?

- A. Create the customer managed policy in every account where the permission set is assigned. Give the customer managed policy the same name and same permissions in each account.
- B. Remove either the AWS managed policy or the customer managed policy from the permission set. Create a second permission set that includes the removed policy. Apply the permission sets separately to the user.
- C. Evaluate the logic of the AWS managed policy and the customer managed policy. Resolve any policy conflicts in the permission set before deployment.
- D. Do not add the new permission set to the user. Instead, edit the user's existing permission set to include the AWS managed policy and the customer managed policy.

Correct Answer: *A*

Question:42 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company has thousands of AWS Lambda functions. While reviewing the Lambda functions, a security engineer discovers that sensitive information is being stored in environment variables and is viewable as plaintext in the Lambda console. The values of the sensitive information are only a few characters long.
What is the MOST cost-effective way to address this security issue?

- A. Set up IAM policies from the Lambda console to hide access to the environment variables.
- B. Use AWS Step Functions to store the environment variables. Access the environment variables at runtime. Use IAM permissions to restrict access to the environment variables to only the Lambda functions that require access.
- C. Store the environment variables in AWS Secrets Manager, and access them at runtime. Use IAM permissions to restrict access to the secrets to only the Lambda functions that require access.
- D. Store the environment variables in AWS Systems Manager Parameter Store as secure string parameters, and access them at runtime. Use IAM permissions to restrict access to the parameters to only the Lambda functions that require access.

Correct Answer: *D*

Question:43 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A security engineer is using AWS Organizations and wants to optimize SCPs. The security engineer needs to ensure that the SCPs conform to best practices.
Which approach should the security engineer take to meet this requirement?

- A. Use AWS IAM Access Analyzer to analyze the polices. View the findings from policy validation checks.
- B. Review AWS Trusted Advisor checks for all accounts in the organization.

- C. Set up AWS Audit Manager. Run an assessment for all AWS Regions for all accounts.
- D. Ensure that Amazon Inspector agents are installed on all Amazon EC2 instances in all accounts.

Correct Answer: *A*

Question:44 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company uses Amazon RDS for MySQL as a database engine for its applications. A recent security audit revealed an RDS instance that is not compliant with company policy for encrypting data at rest. A security engineer at the company needs to ensure that all existing RDS databases are encrypted using server-side encryption and that any future deviations from the policy are detected.

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

- A. Create an AWS Config rule to detect the creation of unencrypted RDS databases. Create an Amazon EventBridge rule to trigger on the AWS Config rules compliance state change and use Amazon Simple Notification Service (Amazon SNS) to notify the security operations team.
- B. Use AWS System Manager State Manager to detect RDS database encryption configuration drift. Create an Amazon EventBridge rule to track state changes and use Amazon Simple Notification Service (Amazon SNS) to notify the security operations team.
- C. Create a read replica for the existing unencrypted RDS database and enable replica encryption in the process. Once the replica becomes active, promote it into a standalone database instance and terminate the unencrypted database instance.
- D. Take a snapshot of the unencrypted RDS database. Copy the snapshot and enable snapshot encryption in the process. Restore the database instance from the newly created encrypted snapshot. Terminate the unencrypted database instance.
- E. Enable encryption for the identified unencrypted RDS instance by changing the configurations of the existing database.

Correct Answer: *AD*

Question:45 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company has recently recovered from a security incident that required the restoration of Amazon EC2 instances from snapshots. The company uses an AWS Key Management Service (AWS KMS) customer managed key to encrypt all Amazon Elastic Block Store (Amazon EBS) snapshots.

The company performs a gap analysis of its disaster recovery procedures and backup strategies. A security engineer needs to implement a solution so that the company can recover the EC2 instances if the AWS account is compromised and the EBS snapshots are deleted.

Which solution will meet this requirement?

- A. Create a new Amazon S3 bucket. Use EBS lifecycle policies to move EBS snapshots to the new S3 bucket. Use lifecycle policies to move snapshots to the S3 Glacier Instant Retrieval storage class. Use S3 Object Lock to prevent deletion of the snapshots.
- B. Use AWS Systems Manager to distribute a configuration that backs up all attached disks to Amazon S3.
- C. Create a new AWS account that has limited privileges. Allow the new account to access the KMS key that encrypts the EBS snapshots. Copy the encrypted snapshots to the new account on a recurring basis.
- D. Use AWS Backup to copy EBS snapshots to Amazon S3. Use S3 Object Lock to prevent deletion of the snapshots.

Correct Answer: *C*

Question:46 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company's security engineer is designing an isolation procedure for Amazon EC2 instances as part of an incident response plan. The security engineer needs to isolate a target instance to block any traffic to and from the target instance, except for traffic from the company's forensics team. Each of the company's EC2 instances has its own dedicated security group. The EC2 instances are deployed in subnets of a VPC. A subnet can contain multiple instances.

The security engineer is testing the procedure for EC2 isolation and opens an SSH session to the target instance. The procedure starts to simulate access to the target instance by an attacker. The security engineer removes the existing security group rules and adds security group rules to give the forensics team access to the target instance on port 22. After these changes, the security engineer notices that the SSH connection is still active and usable. When the

security engineer runs a ping command to the public IP address of the target instance, the ping command is blocked.
What should the security engineer do to isolate the target instance?

- A. Add an inbound rule to the security group to allow traffic from 0.0.0.0/0 for all ports. Add an outbound rule to the security group to allow traffic to 0.0.0.0/0 for all ports. Then immediately delete these rules.
- B. Remove the port 22 security group rule. Attach an instance role policy that allows AWS Systems Manager Session Manager connections so that the forensics team can access the target instance.
- C. Create a network ACL that is associated with the target instance's subnet. Add a rule at the top of the inbound rule set to deny all traffic from 0.0.0.0/0. Add a rule at the top of the outbound rule set to deny all traffic to 0.0.0.0/0.
- D. Create an AWS Systems Manager document that adds a host-level firewall rule to block all inbound traffic and outbound traffic. Run the document on the target instance.

Correct Answer: *B*

Question:47 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A startup company is using a single AWS account that has resources in a single AWS Region. A security engineer configures an AWS CloudTrail trail in the same Region to deliver log files to an Amazon S3 bucket by using the AWS CLI.
Because of expansion, the company adds resources in multiple Regions. The security engineer notices that the logs from the new Regions are not reaching the S3 bucket.
What should the security engineer do to fix this issue with the LEAST amount of operational overhead?

- A. Create a new CloudTrail trail. Select the new Regions where the company added resources.
- B. Change the S3 bucket to receive notifications to track all actions from all Regions.
- C. Create a new CloudTrail trail that applies to all Regions.
- D. Change the existing CloudTrail trail so that it applies to all Regions.

Correct Answer: *D*

Question:48 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company's public Application Load Balancer (ALB) recently experienced a DDoS attack. To mitigate this issue, the company deployed Amazon CloudFront in front of the ALB so that users would not directly access the Amazon EC2 instances behind the ALB.
The company discovers that some traffic is still coming directly into the ALB and is still being handled by the EC2 instances.
Which combination of steps should the company take to ensure that the EC2 instances will receive traffic only from CloudFront? (Choose two.)

- A. Configure CloudFront to add a cache key policy to allow a custom HTTP header that CloudFront sends to the ALB.
- B. Configure CloudFront to add a custom HTTP header to requests that CloudFront sends to the ALB.
- C. Configure the ALB to forward only requests that contain the custom HTTP header.
- D. Configure the ALB and CloudFront to use the X-Forwarded-For header to check client IP addresses.
- E. Configure the ALB and CloudFront to use the same X.509 certificate that is generated by AWS Certificate Manager (ACM).

Correct Answer: *BC*

Question:49 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company discovers a billing anomaly in its AWS account. A security consultant investigates the anomaly and discovers that an employee who left the company 30 days ago still has access to the account. The company has not monitored account activity in the past.
The security consultant needs to determine which resources have been deployed or reconfigured by the employee as quickly as possible.
Which solution will meet these requirements?

- A. In AWS Cost Explorer, filter chart data to display results from the past 30 days. Export the results to a data table. Group the data table by resource.
- B. Use AWS Cost Anomaly Detection to create a cost monitor. Access the detection history. Set the time frame to Last 30 days. In the search area, choose the service category.

- C. In AWS CloudTrail, filter the event history to display results from the past 30 days. Create an Amazon Athena table that contains the data. Partition the table by event source.
- D. Use AWS Audit Manager to create an assessment for the past 30 days. Apply a usage-based framework to the assessment. Configure the assessment to assess by resource.

Correct Answer: *C*

Question:50

A security engineer is checking an AWS CloudFormation template for vulnerabilities. The security engineer finds a parameter that has a default value that exposes an application's API key in plaintext. The parameter is referenced several times throughout the template. The security engineer must replace the parameter while maintaining the ability to reference the value in the template.

Which solution will meet these requirements in the MOST secure way?

- A. Store the API key value as a SecureString parameter in AWS Systems Manager Parameter Store. In the template, replace all references to the value with {{resolve:ssm:MySSMParameterName:1}}.
- B. Store the API key value in AWS Secrets Manager. In the template, replace all references to the value with {{resolve:secretsmanager:MySecretId:SecretString}}.
- C. Store the API key value in Amazon DynamoDB. In the template, replace all references to the value with {{resolve:dynamodb:MyTableName:MyPrimaryKey}}.
- D. Store the API key value in a new Amazon S3 bucket. In the template, replace all references to the value with {{resolve:s3:MyBucketName:MyObjectName}}.

Correct Answer: *B*

Question:51

A company's AWS CloudTrail logs are all centrally stored in an Amazon S3 bucket. The security team controls the company's AWS account. The security team must prevent unauthorized access and tampering of the CloudTrail logs.

Which combination of steps should the security team take? (Choose three.)

- A. Configure server-side encryption with AWS KMS managed encryption keys (SSE-KMS).
- B. Compress log files with secure gzip.
- C. Create an Amazon EventBridge rule to notify the security team of any modifications on CloudTrail log files.
- D. Implement least privilege access to the S3 bucket by configuring a bucket policy.
- E. Configure CloudTrail log file integrity validation.
- F. Configure Access Analyzer for S3.

Correct Answer: *ADE*

Question:52

A company has several petabytes of data. The company must preserve this data for 7 years to comply with regulatory requirements. The company's compliance team asks a security officer to develop a strategy that will prevent anyone from changing or deleting the data.

Which solution will meet this requirement MOST cost-effectively?

- A. Create an Amazon S3 bucket. Configure the bucket to use S3 Object Lock in compliance mode. Upload the data to the bucket. Create a resource-based bucket policy that meets all the regulatory requirements.
- B. Create an Amazon S3 bucket. Configure the bucket to use S3 Object Lock in governance mode. Upload the data to the bucket. Create a user-based IAM policy that meets all the regulatory requirements.
- C. Create a vault in Amazon S3 Glacier. Create a Vault Lock policy in S3 Glacier that meets all the regulatory requirements. Upload the data to the vault.
- D. Create an Amazon S3 bucket. Upload the data to the bucket. Use a lifecycle rule to transition the data to a vault in S3 Glacier. Create a Vault Lock policy that meets all the regulatory requirements.

Correct Answer: *C*

Question:53

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

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

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

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

Correct Answer: *C*

Question:54 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company has several workloads running on AWS. Employees are required to authenticate using on-premises ADFS and SSO to access the AWS Management Console. Developers migrated an existing legacy web application to an Amazon EC2 instance. Employees need to access this application from anywhere on the internet, but currently, there is no authentication system built into the application.
How should the security engineer implement employee-only access to this system without changing the application?

- A. Place the application behind an Application Load Balancer (ALB). Use Amazon Cognito as authentication for the ALB. Define a SAML-based Amazon Cognito user pool and connect it to ADFS.
- B. Implement AWS IAM Identity Center (AWS Single Sign-On) in the management account and link it to ADFS as an identity provider. Define the EC2 instance as a managed resource, then apply an IAM policy on the resource.
- C. Define an Amazon Cognito identity pool, then install the connector on the Active Directory server. Use the Amazon Cognito SDK on the application instance to authenticate the employees using their Active Directory user names and passwords.
- D. Create an AWS Lambda custom authorizer as the authenticator for a reverse proxy on Amazon EC2. Ensure the security group on Amazon EC2 only allows access from the Lambda function.

Correct Answer: *A*

Question:55 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company is using AWS to run a long-running analysis process on data that is stored in Amazon S3 buckets. The process runs on a fleet of Amazon EC2 instances that are in an Auto Scaling group. The EC2 instances are deployed in a private subnet of a VPC that does not have internet access. The EC2 instances and the S3 buckets are in the same AWS account.
The EC2 instances access the S3 buckets through an S3 gateway endpoint that has the default access policy. Each EC2 instance is associated with an instance profile role that has a policy that explicitly allows the s3:GetObject action and the s3:PutObject action for only the required S3 buckets.
The company learns that one or more of the EC2 instances are compromised and are exfiltrating data to an S3 bucket that is outside the company's organization in AWS Organizations. A security engineer must implement a solution to stop this exfiltration of data and to keep the EC2 processing job functional.
Which solution will meet these requirements?

- A. Update the policy on the S3 gateway endpoint to allow the S3 actions only if the values of the aws:ResourceOrgID and aws:PrincipalOrgID condition keys match the company's values.
- B. Update the policy on the instance profile role to allow the S3 actions only if the value of the aws:ResourceOrgID condition key matches the company's value.
- C. Add a network ACL rule to the subnet of the EC2 instances to block outgoing connections on port 443.
- D. Apply an SCP on the AWS account to allow the S3 actions only if the values of the aws:ResourceOrgID and aws:PrincipalOrgID condition keys match the company's values.

Correct Answer: *A*

Question:56 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company that operates in a hybrid cloud environment must meet strict compliance requirements. The company

wants to create a report that includes evidence from on-premises workloads alongside evidence from AWS resources. A security engineer must implement a solution to collect, review, and manage the evidence to demonstrate compliance with company policy.
Which solution will meet these requirements?

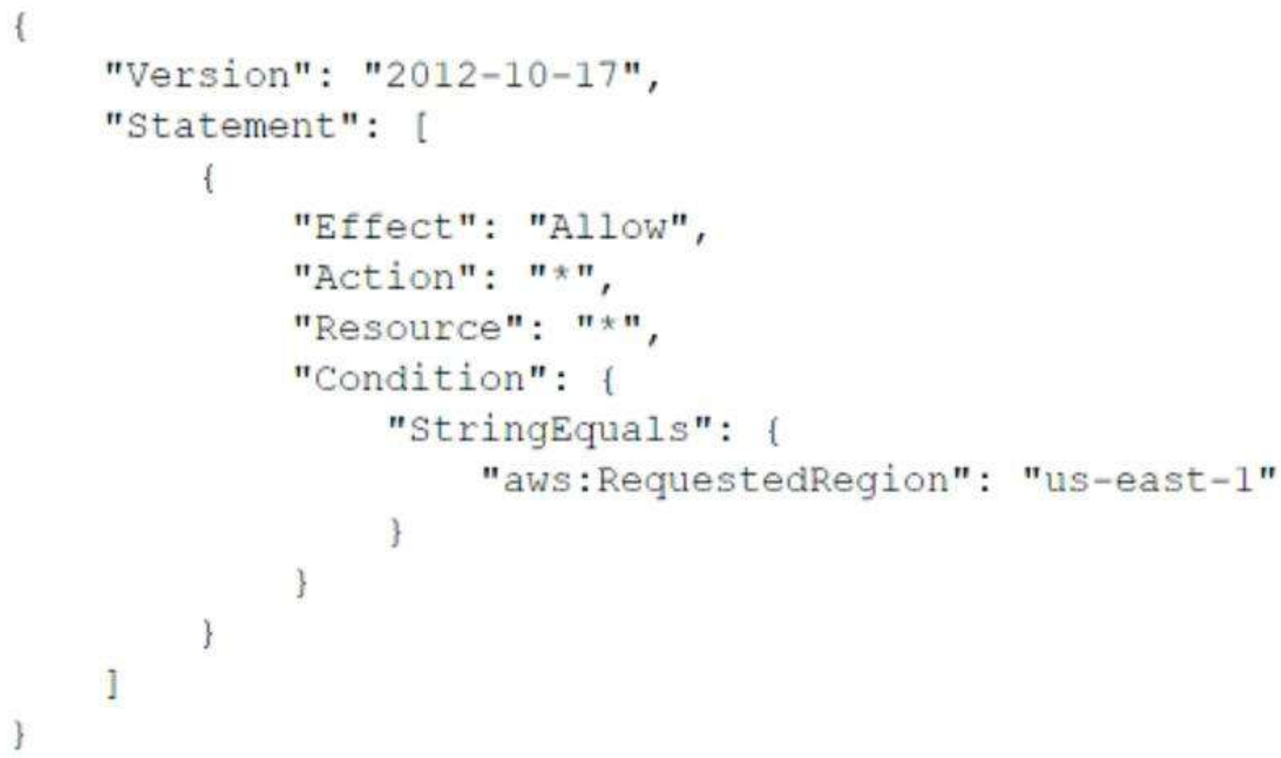
- A. Create an assessment in AWS Audit Manager from a prebuilt framework or a custom framework. Upload manual evidence from the on-premises workloads. Add the evidence to the assessment. Generate an assessment report after Audit Manager collects the necessary evidence from the AWS resources.
- B. Install the Amazon CloudWatch agent on the on-premises workloads. Use AWS Config to deploy a conformance pack from a sample conformance pack template or a custom YAML template. Generate an assessment report after AWS Config identifies noncompliant workloads and resources.
- C. Set up the appropriate security standard in AWS Security Hub. Upload manual evidence from the on-premises workloads. Wait for Security Hub to collect the evidence from the AWS resources. Download the list of controls as a .csv file.
- D. Install the Amazon CloudWatch agent on the on-premises workloads. Create a CloudWatch dashboard to monitor the on-premises workloads and the AWS resources. Run a query on the workloads and resources. Download the results.

Correct Answer: *A*

Question:57 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

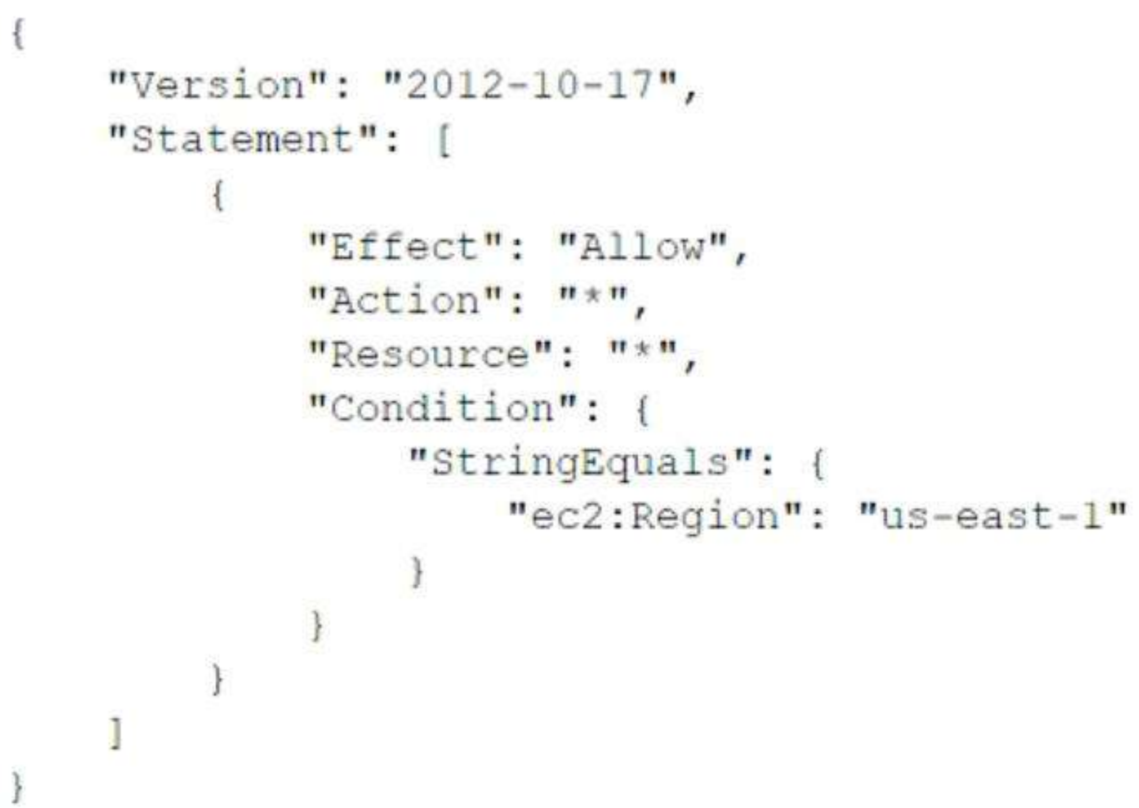
To meet regulatory requirements, a security engineer needs to implement an IAM policy that restricts the use of AWS services to the us-east-1 Region.
What policy should the engineer implement?

- A.



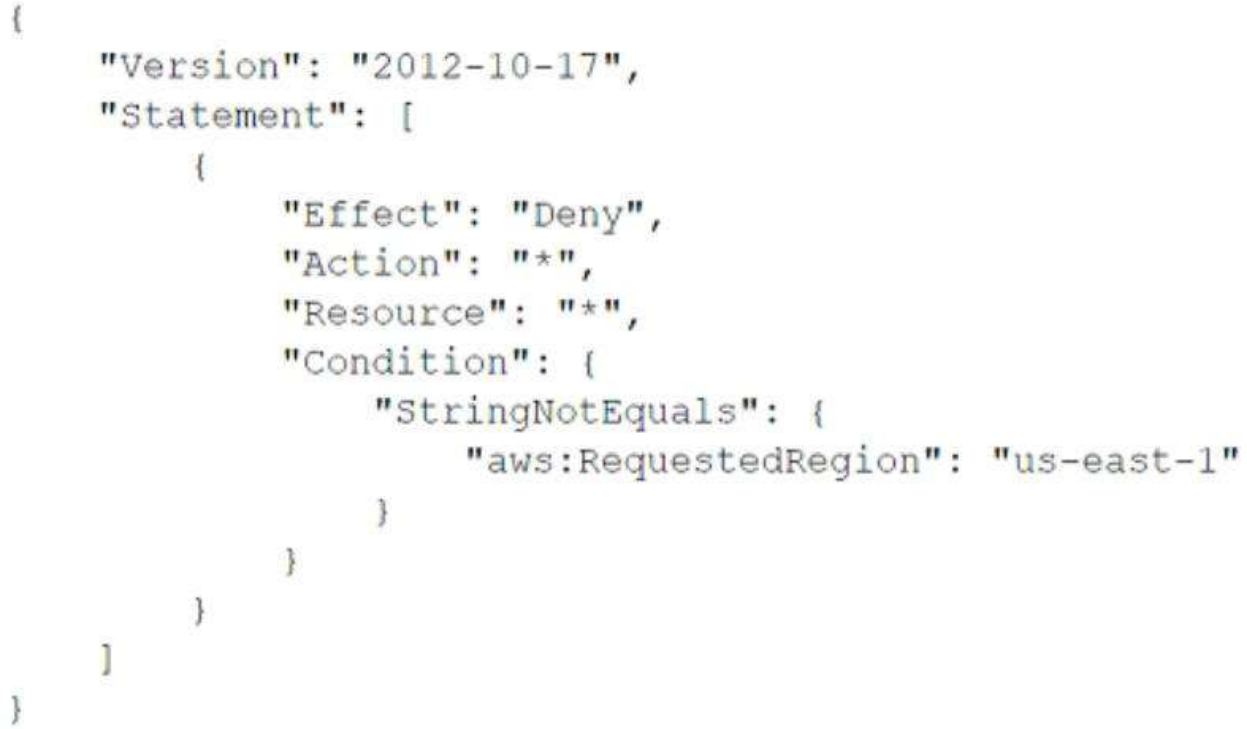
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestedRegion": "us-east-1"
                }
            }
 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

- B.



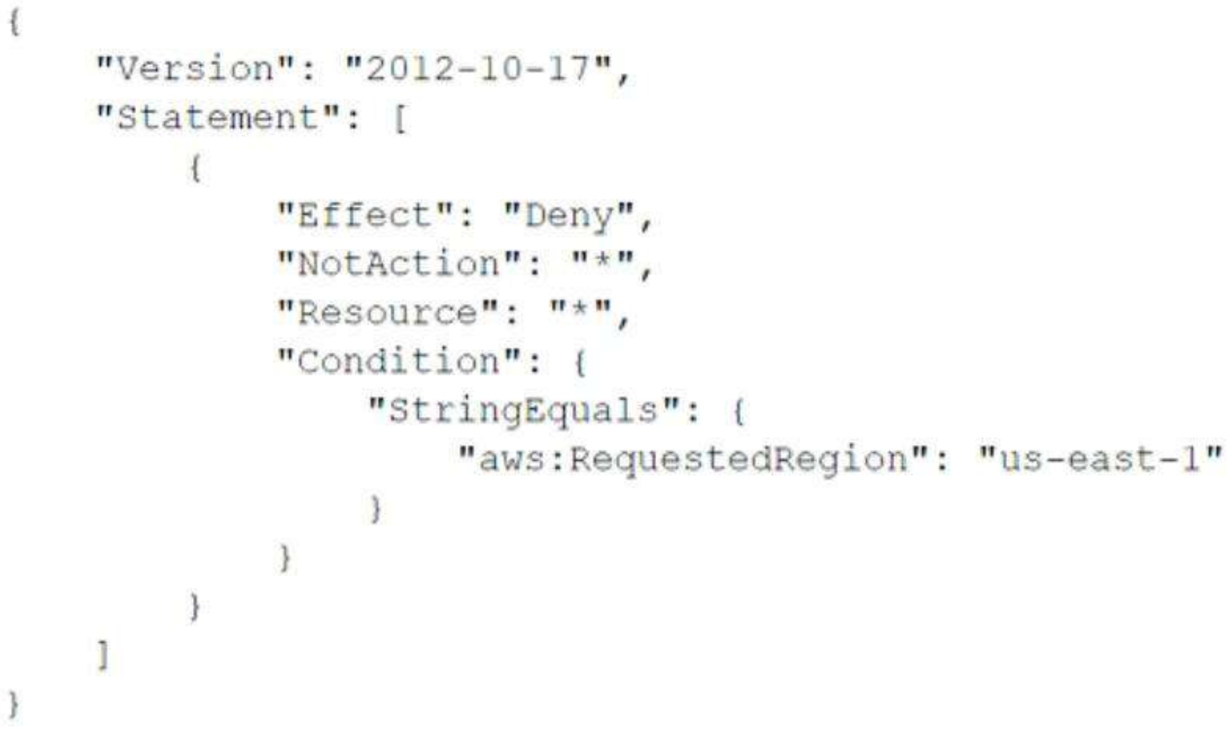
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:Region": "us-east-1"
                }
            }
        }
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

- C.



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

- D.



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

Correct Answer: *C*

Question:58 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

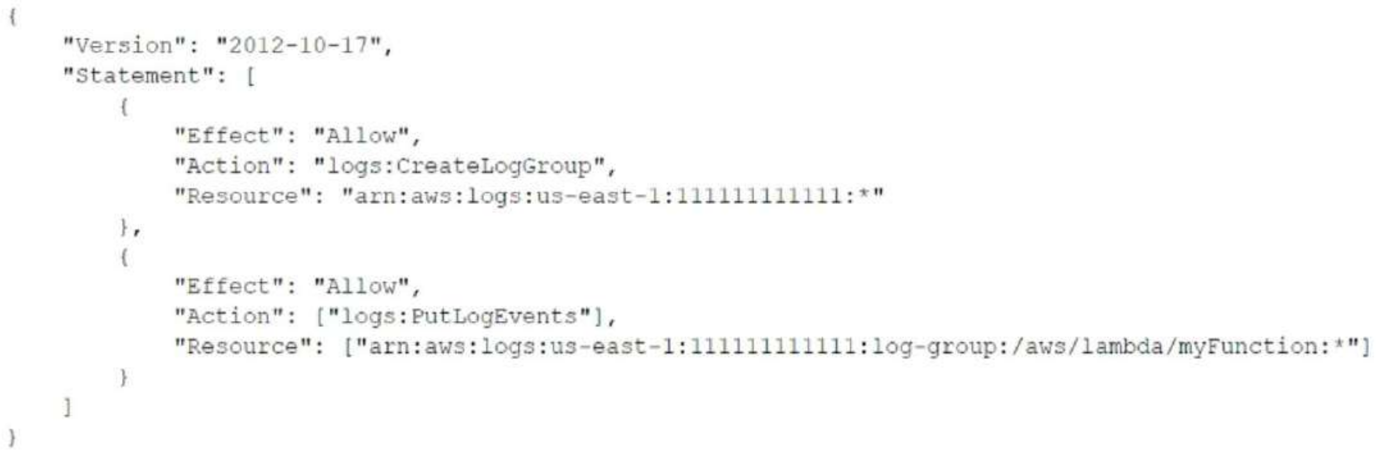
A company has a web server in the AWS Cloud. The company will store the content for the web server in an Amazon S3 bucket. A security engineer must use an Amazon CloudFront distribution to speed up delivery of the content. None of the files can be publicly accessible from the S3 bucket directly.
Which solution will meet these requirements?

- A. Configure the permissions on the individual files in the S3 bucket so that only the CloudFront distribution has access to them.
- B. Create an origin access control (OAC). Associate the OAC with the CloudFront distribution. Configure the S3 bucket permissions so that only the OAC can access the files in the S3 bucket.
- C. Create an S3 role in AWS Identity and Access Management (IAM). Allow only the CloudFront distribution to assume the role to access the files in the S3 bucket.
- D. Create an S3 bucket policy that uses only the CloudFront distribution ID as the principal and the Amazon Resource Name (ARN) as the target.

Correct Answer: *B*

Question:59 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A security engineer logs in to the AWS Lambda console with administrator permissions. The security engineer is trying to view logs in Amazon CloudWatch for a Lambda function that is named myFunction. When the security engineer chooses the option in the Lambda console to view logs in CloudWatch, an "error loading Log Streams" message appears.
The IAM policy for the Lambda function's execution role contains the following:



```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "logs:CreateLogGroup",
            "Resource": "arn:aws:logs:us-east-1:111111111111:*"
        },
        {
            "Effect": "Allow",
            "Action": ["logs:PutLogEvents"],
            "Resource": ["arn:aws:logs:us-east-1:111111111111:log-group:/aws/lambda/myFunction:*"]
        }
    ]
}
```

How should the security engineer correct the error?

- A. Move the logs:CreateLogGroup action to the second Allow statement.
- B. Add the logs:PutDestination action to the second Allow statement.
- C. Add the logs:GetLogEvents action to the second Allow statement.
- D. Add the logs:CreateLogStream action to the second Allow statement.

Correct Answer: *D*

Question:60 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company has a new partnership with a vendor. The vendor will process data from the company's customers. The company will upload data files as objects into an Amazon S3 bucket. The vendor will download the objects to perform data processing. The objects will contain sensitive data.

A security engineer must implement a solution that prevents objects from residing in the S3 bucket for longer than 72 hours.

Which solution will meet these requirements?

- A. Use Amazon Macie to scan the S3 bucket for sensitive data every 72 hours. Configure Macie to delete the objects that contain sensitive data when they are discovered.
- B. Configure an S3 Lifecycle rule on the S3 bucket to expire objects that have been in the S3 bucket for 72 hours.
- C. Create an Amazon EventBridge scheduled rule that invokes an AWS Lambda function every day. Program the Lambda function to remove any objects that have been in the S3 bucket for 72 hours.
- D. Use the S3 Intelligent-Tiering storage class for all objects that are uploaded to the S3 bucket. Use S3 Intelligent-Tiering to expire objects that have been in the $3 bucket for 72 hours.

Correct Answer: *B*

Question:61 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company accidentally deleted the private key for an Amazon Elastic Block Store (Amazon EBS)-backed Amazon EC2 instance. A security engineer needs to regain access to the instance.

Which combination of steps will meet this requirement? (Choose two.)

- A. Stop the instance. Detach the root volume. Generate a new key pair.
- B. Keep the instance running. Detach the root volume. Generate a new key pair.
- C. When the volume is detached from the original instance, attach the volume to another instance as a data volume. Modify the authorized_keys file with a new public key. Move the volume back to the original instance. Start the instance.
- D. When the volume is detached from the original instance, attach the volume to another instance as a data volume. Modify the authorized_keys file with a new private key. Move the volume back to the original instance. Start the instance.
- E. When the volume is detached from the original instance, attach the volume to another instance as a data volume. Modify the authorized_keys file with a new public key. Move the volume back to the original instance that is running.

Correct Answer: *AC*

Question:62 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company purchased a subscription to a third-party cloud security scanning solution that integrates with AWS Security Hub. A security engineer needs to implement a solution that will remediate the findings from the third-party scanning solution automatically.

Which solution will meet this requirement?

- A. Set up an Amazon EventBridge rule that reacts to new Security Hub findings. Configure an AWS Lambda function as the target for the rule to remediate the findings.
- B. Set up a custom action in Security Hub. Configure the custom action to call AWS Systems Manager Automation runbooks to remediate the findings.
- C. Set up a custom action in Security Hub. Configure an AWS Lambda function as the target for the custom action to remediate the findings.
- D. Set up AWS Config rules to use AWS Systems Manager Automation runbooks to remediate the findings.

Correct Answer: *A*

Question:63 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

An application is running on an Amazon EC2 instance that has an IAM role attached. The IAM role provides access to an AWS Key Management Service (AWS KMS) customer managed key and an Amazon S3 bucket. The key is used to access 2 TB of sensitive data that is stored in the S3 bucket.

A security engineer discovers a potential vulnerability on the EC2 instance that could result in the compromise of the sensitive data. Due to other critical operations, the security engineer cannot immediately shut down the EC2 instance for vulnerability patching.

What is the FASTEST way to prevent the sensitive data from being exposed?

- A. Download the data from the existing S3 bucket to a new EC2 instance. Then delete the data from the S3 bucket. Re-encrypt the data with a client-based key. Upload the data to a new S3 bucket.
- B. Block access to the public range of S3 endpoint IP addresses by using a host-based firewall. Ensure that internet-bound traffic from the affected EC2 instance is routed through the host-based firewall.
- C. Revoke the IAM role's active session permissions. Update the S3 bucket policy to deny access to the IAM role. Remove the IAM role from the EC2 instance profile.
- D. Disable the current key. Create a new KMS key that the IAM role does not have access to, and re-encrypt all the data with the new key. Schedule the compromised key for deletion.

Correct Answer: *C*

Question:64 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company is building an application on AWS that will store sensitive information. The company has a support team with access to the IT infrastructure, including databases. The company's security engineer must introduce measures to protect the sensitive data against any data breach while minimizing management overhead. The credentials must be regularly rotated.

What should the security engineer recommend?

- A. Enable Amazon RDS encryption to encrypt the database and snapshots. Enable Amazon Elastic Block Store (Amazon EBS) encryption on Amazon EC2 instances. Include the database credential in the EC2 user data field. Use an AWS Lambda function to rotate database credentials. Set up TLS for the connection to the database.
- B. Install a database on an Amazon EC2 instance. Enable third-party disk encryption to encrypt the Amazon Elastic Block Store (Amazon EBS) volume. Store the database credentials in AWS CloudHSM with automatic rotation. Set up TLS for the connection to the database.
- C. Enable Amazon RDS encryption to encrypt the database and snapshots. Enable Amazon Elastic Black Store (Amazon EBS) encryption on Amazon EC2 instances. Store the database credentials in AWS Secrets Manager with automatic rotation. Set up TLS for the connection to the RDS hosted database.
- D. Set up an AWS CloudHSM cluster with AWS Key Management Service (AWS KMS) to store KMS keys. Set up Amazon RDS encryption using AWS KMS to encrypt the database. Store database credentials in the AWS Systems Manager Parameter Store with automatic rotation. Set up TLS for the connection to the RDS hosted database.

Correct Answer: *C*

Question:65 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company is using Amazon Route 53 Resolver for its hybrid DNS infrastructure. The company has set up Route 53 Resolver forwarding rules for authoritative domains that are hosted on on-premises DNS servers.

A new security mandate requires the company to implement a solution to log and query DNS traffic that goes to the on-premises DNS servers. The logs must show details of the source IP address of the instance from which the query originated. The logs also must show the DNS name that was requested in Route 53 Resolver.

Which solution will meet these requirements?

- A. Use VPC Traffic Mirroring. Configure all relevant elastic network interfaces as the traffic source, include amazon-dns in the mirror filter, and set Amazon CloudWatch Logs as the mirror target. Use CloudWatch Insights on the mirror session logs to run queries on the source IP address and DNS name.
- B. Configure VPC flow logs on all relevant VPCs. Send the logs to an Amazon S3 bucket. Use Amazon Athena to run SQL queries on the source IP address and DNS name.
- C. Configure Route 53 Resolver query logging on all relevant VPCs. Send the logs to Amazon CloudWatch Logs. Use CloudWatch Insights to run queries on the source IP address and DNS name.
- D. Modify the Route 53 Resolver rules on the authoritative domains that forward to the on-premises DNS servers. Send the logs to an Amazon S3 bucket. Use Amazon Athena to run SQL queries on the source IP address and DNS name.

Correct Answer: *C*

Question:66 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A security engineer is configuring account-based access control (ABAC) to allow only specific principals to put objects into an Amazon S3 bucket. The principals already have access to Amazon S3.

The security engineer needs to configure a bucket policy that allows principals to put objects into the S3 bucket only if the value of the Team tag on the object matches the value of the Team tag that is associated with the principal. During testing, the security engineer notices that a principal can still put objects into the S3 bucket when the tag values do not match.

Which combination of factors are causing the PutObject operation to succeed when the tag values are different? (Choose two.)

- A. The principal's identity-based policy grants access to put objects into the S3 bucket with no conditions.
- B. The principal's identity-based policy overrides the condition because the identity-based policy contains an explicit allow.
- C. The S3 bucket's resource policy does not deny access to put objects.
- D. The S3 bucket's resource policy cannot allow actions to the principal.
- E. The bucket policy does not apply to principals in the same zone of trust.

Correct Answer: *AC*

Question:67 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company is hosting multiple applications within a single VPC in its AWS account. The applications are running behind an Application Load Balancer that is associated with an AWS WAF web ACL. The company's security team has identified that multiple port scans are originating from a specific range of IP addresses on the internet.

A security engineer needs to deny access from the offending IP addresses.

Which solution will meet these requirements?

- A. Modify the AWS WAF web ACL with an IP set match rule statement to deny incoming requests from the IP address range.
- B. Add a rule to all security groups to deny the incoming requests from the IP address range.
- C. Modify the AWS WAF web ACL with a rate-based rule statement to deny the incoming requests from the IP address range.

- D. Configure the AWS WAF web ACL with regex match conditions. Specify a pattern set to deny the incoming requests based on the match condition.

Correct Answer: *A*

Question:68 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company has contracted with a third party to audit several AWS accounts. To enable the audit, cross-account IAM roles have been created in each account targeted for audit. The auditor is having trouble accessing some of the accounts.

Which of the following may be causing this problem? (Choose three.)

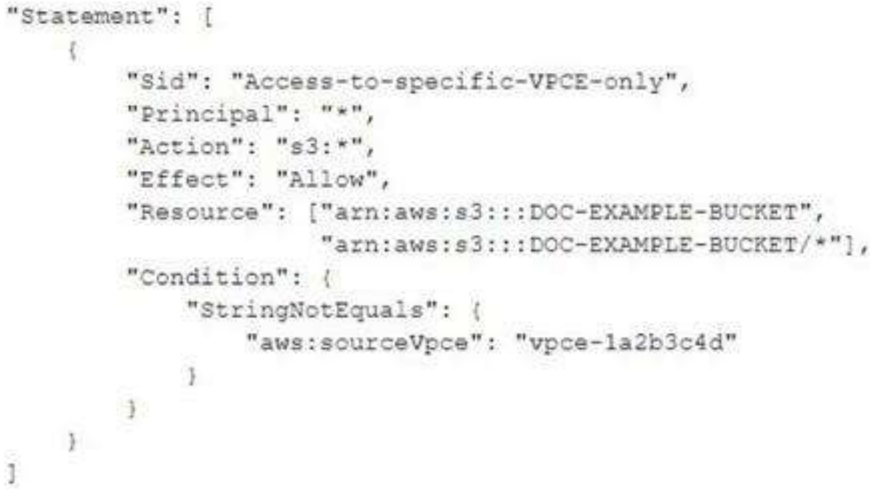
- A. The external ID used by the auditor is missing or incorrect.
- B. The auditor is using the incorrect password.
- C. The auditor has not been granted sts:AssumeRole for the role in the destination account.
- D. The Amazon EC2 role used by the auditor must be set to the destination account role.
- E. The secret key used by the auditor is missing or incorrect.
- F. The role ARN used by the auditor is missing or incorrect.

Correct Answer: *ACF*

Question:69 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

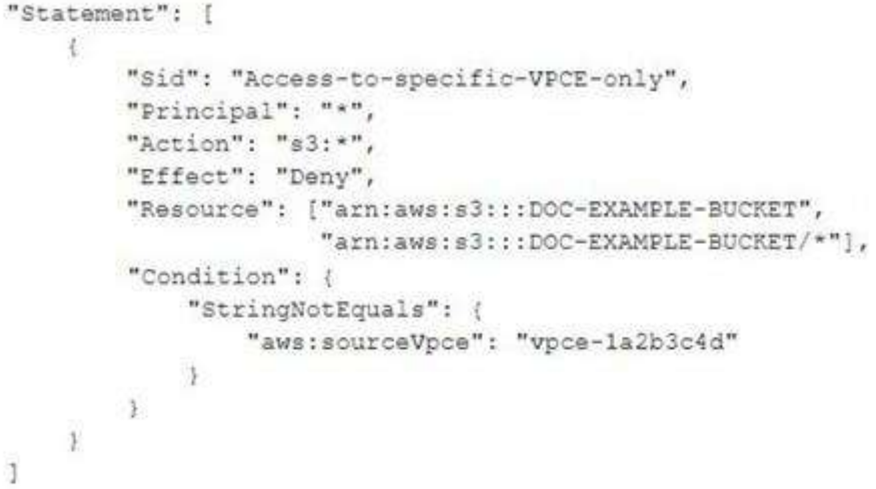
A security engineer needs to configure an Amazon S3 bucket policy to restrict access to an S3 bucket that is named DOC-EXAMPLE-BUCKET. The policy must allow access to only DOC-EXAMPLE-BUCKET from only the following endpoint: vpce-1a2b3c4d. The policy must deny all access to DOC-EXAMPLE-BUCKET if the specified endpoint is not used.

Which bucket policy statement meets these requirements?



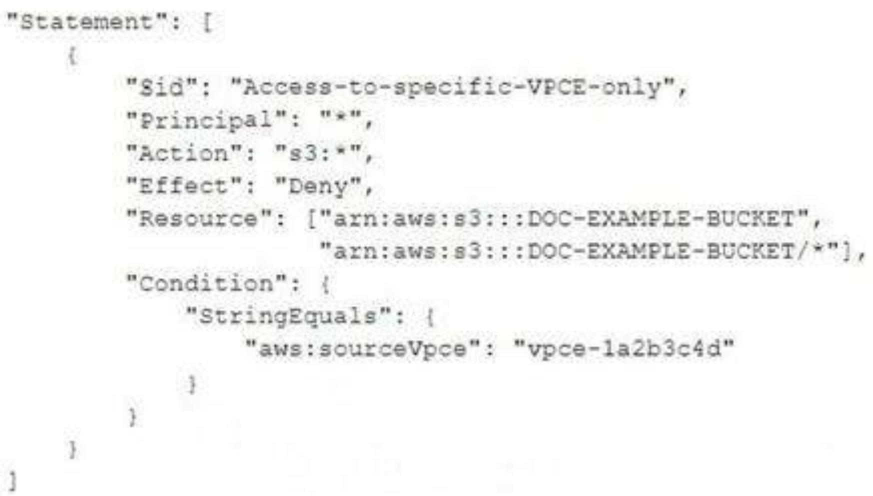
```
"Statement": [
    {
        "Sid": "Access-to-specific-VPCE-only",
        "Principal": "*",
        "Action": "s3:*",
        "Effect": "Allow",
        "Resource": ["arn:aws:s3:::DOC-EXAMPLE-BUCKET",
                     "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"],
        "Condition": {
            "StringNotEquals": {
                "aws:sourceVpce": "vpce-1a2b3c4d"
            }
        }
    }
]
```

- A.



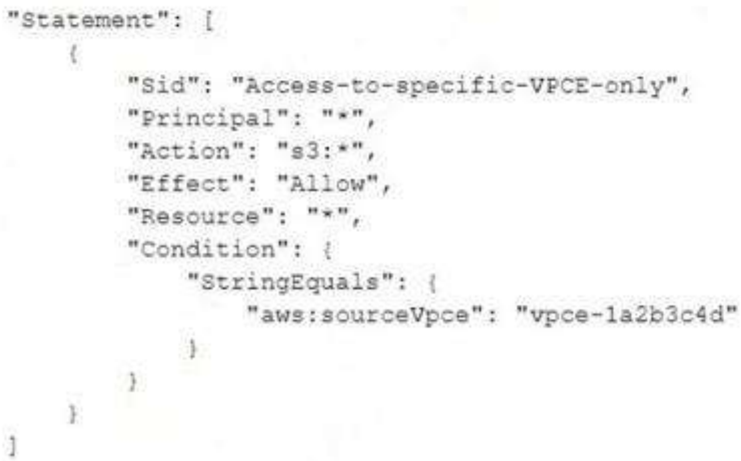
```
"Statement": [
    {
        "Sid": "Access-to-specific-VPCE-only",
        "Principal": "*",
        "Action": "s3:*",
        "Effect": "Deny",
        "Resource": ["arn:aws:s3:::DOC-EXAMPLE-BUCKET",
                     "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"],
        "Condition": {
            "StringNotEquals": {
                "aws:sourceVpce": "vpce-1a2b3c4d"
            }
        }
    }
]
```

- B.



```
"Statement": [
    {
        "Sid": "Access-to-specific-VPCE-only",
        "Principal": "*",
        "Action": "s3:*",
        "Effect": "Deny",
        "Resource": ["arn:aws:s3:::DOC-EXAMPLE-BUCKET",
                     "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"],
        "Condition": {
            "StringEquals": {
                "aws:sourceVpce": "vpce-1a2b3c4d"
            }
        }
    }
]
```

- C.



```
"Statement": [
    {
        "Sid": "Access-to-specific-VPCE-only",
        "Principal": "*",
        "Action": "s3:*",
        "Effect": "Allow",
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "aws:sourceVpce": "vpce-1a2b3c4d"
            }
        }
    }
]
```

- D.

Correct Answer: *B*

Question:70 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company has a group of Amazon EC2 instances in a single private subnet of a VPC with no internet gateway attached. A security engineer has installed the Amazon CloudWatch agent on all instances in that subnet to capture logs from a specific application. To ensure that the logs flow securely, the company's networking team has created VPC endpoints for CloudWatch monitoring and CloudWatch logs. The networking team has attached the endpoints to the VPC.

The application is generating logs However, when the security engineer queries CloudWatch, the logs do not appear.

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

- A. Ensure that the EC2 instance profile that is attached to the EC2 instances has permissions to create log streams and write logs.
- B. Create a metric filter on the logs so that they can be viewed in the AWS Management Console.
- C. Check the CloudWatch agent configuration file on each EC2 instance to make sure that the CloudWatch agent is collecting the proper log files.
- D. Check the VPC endpoint policies of both VPC endpoints to ensure that the EC2 instances have permissions to use them.
- E. Create a NAT gateway in the subnet so that the EC2 instances can communicate with CloudWatch.
- F. Ensure that the security groups allow all the EC2 instances to communicate with each other to aggregate logs before sending.

Correct Answer: *ACD*

Question:71 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company uses AWS Signer with all of the company's AWS Lambda functions. A developer recently stopped working for the company. The company wants to ensure that all the code that the developer wrote can no longer be deployed to the Lambda functions.

Which solution will meet this requirement?

- A. Revoke all versions of the signing profile assigned to the developer.
- B. Examine the developer's IAM roles. Remove all permissions that grant access to Signer.
- C. Re-encrypt all source code with a new AWS Key Management Service (AWS KMS) key.
- D. Use Amazon CodeGuru to profile all the code that the Lambda functions use.

Correct Answer: *A*

Question:72 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company plans to use AWS Key Management Service (AWS KMS) to implement an encryption strategy to protect data at rest. The company requires client-side encryption for company projects. The company is currently conducting multiple projects to test the company's use of AWS KMS. These tests have led to a sudden increase in the company's AWS resource consumption. The test projects include applications that issue multiple requests each second to KMS endpoints for encryption activities.

The company needs to develop a solution that does not throttle the company's ability to use AWS KMS. The solution must improve key usage for client-side encryption and must be cost optimized.

Which solution will meet these requirements?

- A. Use keyrings with the AWS Encryption SDK. Use each keyring individually or combine keyrings into a multi-keyring. Decrypt the data by using a keyring that has the primary key in the multi-keyring.
- B. Use data key caching. Use the local cache that the AWS Encryption SDK provides with a caching cryptographic materials manager.
- C. Use KMS key rotation. Use a local cache in the AWS Encryption SDK with a caching cryptographic materials manager.
- D. Use keyrings with the AWS Encryption SDK. Use each keyring individually or combine keyrings into a multi-keyring. Use any of the wrapping keys in the multi-keyring to decrypt the data.

Correct Answer: *B*

Question:73 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A security team is working on a solution that will use Amazon EventBridge to monitor new Amazon S3 objects. The solution will monitor for public access and for changes to any S3 bucket policy or setting that result in public access. The security team configures EventBridge to watch for specific API calls that are logged from AWS CloudTrail. EventBridge has an action to send an email notification through Amazon Simple Notification Service (Amazon SNS) to the security team immediately with details of the API call.

Specifically, the security team wants EventBridge to watch for the s3:PutObjectAcl, s3:DeleteBucketPolicy, and s3:PutBucketPolicy API invocation logs from CloudTrail. While developing the solution in a single account, the security team discovers that the s3:PutObjectAcl API call does not invoke an EventBridge event However, the s3:DeleteBucketPolicy API call and the s3:PutBucketPolicy API call do invoke an event.

The security team has enabled CloudTrail for AWS management events with a basic configuration in the AWS Region in which EventBridge is being tested. Verification of the EventBridge event pattern indicates that the pattern is set up correctly. The security team must implement a solution so that the s3:PutObjectAcl API call will invoke an EventBridge event. The solution must not generate false notifications.

Which solution will meet these requirements?

- A. Modify the EventBridge event pattern by selecting Amazon S3. Select All Events as the event type.
- B. Modify the EventBridge event pattern by selecting Amazon S3. Select Bucket Level Operations as the event type.
- C. Enable CloudTrail Insights to identify unusual API activity.
- D. Enable CloudTrail to monitor data events for read and write operations to S3 buckets.

Correct Answer: *D*

Question:74 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company uses Amazon GuardDuty. The company's security team wants all High severity findings to automatically generate a ticket in a third-party ticketing system through email integration.

Which solution will meet this requirement?

- A. Create a verified identity for the third-party ticketing email system in Amazon Simple Email Service (Amazon SES). Create an Amazon EventBridge rule that includes an event pattern that matches High severity GuardDuty findings. Specify the SES identity as the target for the EventBridge rule.
- B. Create an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the third-party ticketing email system to the SNS topic. Create an Amazon EventBridge rule that includes an event pattern that matches High severity GuardDuty findings. Specify the SNS topic as the target for the EventBridge rule.
- C. Use the GuardDuty CreateFilter API operation to build a filter in GuardDuty to monitor for High severity findings. Export the results of the filter to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the third-party ticketing email system to the SNS topic.
- D. Use the GuardDuty CreateFilter API operation to build a filter in GuardDuty to monitor for High severity findings. Create an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the third-party ticketing email system to the SNS topic. Create an Amazon EventBridge rule that includes an event pattern that matches GuardDuty findings that are selected by the filter. Specify the SNS topic as the target for the EventBridge rule.

Correct Answer: *B*

Question:75 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company is using AWS Organizations to implement a multi-account strategy. The company does not have on-premises infrastructure. All workloads run on AWS. The company currently has eight member accounts. The company anticipates that it will have no more than 20 AWS accounts total at any time.

The company issues a new security policy that contains the following requirements:

• No AWS account should use a VPC within the AWS account for workloads.
• The company should use a centrally managed VPC that all AWS accounts can access to launch workloads in subnets.
• No AWS account should be able to modify another AWS account's application resources within the centrally managed VPC.
• The centrally managed VPC should reside in an existing AWS account that is named Ac-count-A within an organization.

The company uses an AWS CloudFormation template to create a VPC that contains multiple subnets in Account-A. This template exports the subnet IDs through the CloudFormation Outputs section.

Which solution will complete the security setup to meet these requirements?

- A. Use a CloudFormation template in the member accounts to launch workloads. Configure the template to use the Fn::ImportValue function to obtain the subnet ID values.
- B. Use a transit gateway in the VPC within Account-A. Configure the member accounts to use the transit gateway to access the subnets in Account-A to launch workloads.
- C. Use AWS Resource Access Manager (AWS RAM) to share Account-A's VPC subnets with the remaining member accounts. Configure the member accounts to use the shared subnets to launch workloads.
- D. Create a peering connection between Account-A and the remaining member accounts. Configure the member accounts to use the subnets in Account-A through the VPC peering connection to launch workloads.

Correct Answer: *C*

Question:76 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company's security team needs to receive a notification whenever an AWS access key has not been rotated in 90 or more days. A security engineer must develop a solution that provides these notifications automatically.

Which solution will meet these requirements with the LEAST amount of effort?

- A. Deploy an AWS Config managed rule to run on a periodic basis of 24 hours. Select the access-keys-rotated managed rule, and set the maxAccessKeyAge parameter to 90 days. Create an Amazon EventBridge rule with an event pattern that matches the compliance type of NON_ COMPLIANT from AWS Config for the managed rule. Configure EventBridge to send an Amazon Simple Notification Service (Amazon SNS) notification to the security team.
- B. Create a script to export a .csv file from the AWS Trusted Advisor check for IAM access key rotation. Load the script into an AWS Lambda function that will upload the .csv file to an Amazon S3 bucket. Create an Amazon Athena table query that runs when the .csv file is uploaded to the S3 bucket. Publish the results for any keys older than 90 days by using an invocation of an Amazon Simple Notification Service (Amazon SNS) notification to the security team.
- C. Create a script to download the IAM credentials report on a periodic basis. Load the script into an AWS Lambda function that will run on a schedule through Amazon EventBridge. Configure the Lambda script to load the report into memory and to filter the report for records in which the key was last rotated at least 90 days ago. If any records are detected, send an Amazon Simple Notification Service (Amazon SNS) notification to the security team.
- D. Create an AWS Lambda function that queries the IAM API to list all the users. Iterate through the users by using the ListAccessKeys operation. Verify that the value in the CreateDate field is not at least 90 days old. Send an Amazon Simple Notification Service (Amazon SNS) notification to the security team if the value is at least 90 days old. Create an Amazon EventBridge rule to schedule the Lambda function to run each day.

Correct Answer: *A*

Question:77 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company maintains an open-source application that is hosted on a public GitHub repository. While creating a new commit to the repository, an engineer uploaded their AWS access key and secret access key. The engineer reported the mistake to a manager, and the manager immediately disabled the access key.

The company needs to assess the impact of the exposed access key. A security engineer must recommend a solution that requires the least possible managerial overhead.

Which solution meets these requirements?

- A. Analyze an AWS Identity and Access Management (IAM) use report from AWS Trusted Advisor to see when the access key was last used.
- B. Analyze Amazon CloudWatch Logs for activity by searching for the access key.
- C. Analyze VPC flow logs for activity by searching for the access key.
- D. Analyze a credential report in AWS Identity and Access Management (IAM) to see when the access key was last used.

Correct Answer: *D*

Question:78 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company plans to create individual child accounts within an existing organization in AWS Organizations for each of its DevOps teams. AWS CloudTrail has been enabled and configured on all accounts to write audit logs to an Amazon S3 bucket in a centralized AWS account. A security engineer needs to ensure that DevOps team members are unable to modify or disable this configuration.

How can the security engineer meet these requirements?

- A. Create an IAM policy that prohibits changes to the specific CloudTrail trail and apply the policy to the AWS account root user.
- B. Create an S3 bucket policy in the specified destination account for the CloudTrail trail that prohibits configuration changes from the AWS account root user in the source account.
- C. Create an SCP that prohibits changes to the specific CloudTrail trail and apply the SCP to the appropriate organizational unit or account in Organizations.

- D. Create an IAM policy that prohibits changes to the specific CloudTrail trail and apply the policy to a new IAM group. Have team members use individual IAM accounts that are members of the new IAM group.

Correct Answer: *C*

Question:79 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company's policy requires that all API keys be encrypted and stored separately from source code in a centralized security account. This security account is managed by the company's security team. However, an audit revealed that an API key is stored with the source code of an AWS Lambda function in an AWS CodeCommit repository in the DevOps account.

How should the security team securely store the API key?

- A. Create a CodeCommit repository in the security account using AWS Key Management Service (AWS KMS) for encryption. Require the development team to migrate the Lambda source code to this repository.
- B. Store the API key in an Amazon S3 bucket in the security account using server-side encryption with Amazon S3 managed encryption keys (SSE-S3) to encrypt the key. Create a presigned URL for the S3 key, and specify the URL in a Lambda environmental variable in the AWS CloudFormation template. Update the Lambda function code to retrieve the key using the URL and call the API.
- C. Create a secret in AWS Secrets Manager in the security account to store the API key using AWS Key Management Service (AWS KMS) for encryption. Grant access to the IAM role used by the Lambda function so that the function can retrieve the key from Secrets Manager and call the API.
- D. Create an encrypted environment variable for the Lambda function to store the API key using AWS Key Management Service (AWS KMS) for encryption. Grant access to the IAM role used by the Lambda function so that the function can decrypt the key at runtime.

Correct Answer: *C*

Question:80 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

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

What will enable the security engineer to save the change?

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

Correct Answer: *C*

Question:81 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company uses AWS Organizations. The company wants to implement short-term credentials for third-party AWS accounts to use to access accounts within the company's organization. Access is for the AWS Management Console and third-party software-as-a-service (SaaS) applications. Trust must be enhanced to prevent two external accounts from using the same credentials. The solution must require the least possible operational effort.

Which solution will meet these requirements?

- A. Use a bearer token authentication with OAuth or SAML to manage and share a central Amazon Cognito user pool across multiple Amazon API Gateway APIs.
- B. Implement AWS IAM Identity Center (AWS Single Sign-On), and use an identity source of choice. Grant access to users and groups from other accounts by using permission sets that are assigned by account.
- C. Create a unique IAM role for each external account. Create a trust policy Use AWS Secrets Manager to

create a random external key.
- D. Create a unique IAM role for each external account. Create a trust policy that includes a condition that uses the sts:ExternalId condition key.

Correct Answer: *D*

Question:82 ***SCS-C02: Actual Exam Q&A*** **|** ***CLEARCATNET***

A company is evaluating its security posture. In the past, the company has observed issues with specific hosts and host header combinations that affected the company's business. The company has configured AWS WAF web ACLs as an initial step to mitigate these issues.

The company must create a log analysis solution for the AWS WAF web ACLs to monitor problematic activity. The company wants to process all the AWS WAF logs in a central location. The company must have the ability to filter out requests based on specific hosts.

A security engineer starts to enable access logging for the AWS WAF web ACLs.

What should the security engineer do next to meet these requirements with the MOST operational efficiency?

- A. Specify Amazon Redshift as the destination for the access logs. Deploy the Amazon Athena Redshift connector. Use Athena to query the data from Amazon Redshift and to filter the logs by host.
- B. Specify Amazon CloudWatch as the destination for the access logs. Use Amazon CloudWatch Logs Insights to design a query to filter the logs by host.
- C. Specify Amazon CloudWatch as the destination for the access logs. Export the CloudWatch logs to an Amazon S3 bucket. Use Amazon Athena to query the logs and to filter the logs by host.
- D. Specify Amazon CloudWatch as the destination for the access logs. Use Amazon Redshift Spectrum to query the logs and to filter the logs by host.

Correct Answer: *B*

Question:83 ***SCS-C02: Actual Exam Q&A*** **|** ***CLEARCATNET***

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.

Correct Answer: *BE*

Question:84 ***SCS-C02: Actual Exam Q&A*** **|** ***CLEARCATNET***

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

Which solution meets these criteria?

- A. A customer managed key that uses customer provided key material

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

Correct Answer: *A*

Question:85 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

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

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

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

Correct Answer: *CE*

Question:86 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company uses SAML federation to grant users access to AWS accounts. A company workload that is in an isolated AWS account runs on immutable infrastructure with no human access to Amazon EC2. The company requires a specialized user known as a break glass user to have access to the workload AWS account and instances in the case of SAML errors. A recent audit discovered that the company did not create the break glass user for the AWS account that contains the workload.

The company must create the break glass user. The company must log any activities of the break glass user and send the logs to a security team.

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

- A. Create a local individual break glass IAM user for the security team. Create a trail in AWS CloudTrail that has Amazon CloudWatch Logs turned on. Use Amazon EventBridge to monitor local user activities.
- B. Create a break glass EC2 key pair for the AWS account. Provide the key pair to the security team. Use AWS CloudTrail to monitor key pair activity. Send notifications to the security team by using Amazon Simple Notification Service (Amazon SNS).
- C. Create a break glass IAM role for the account. Allow security team members to perform the AssumeRoleWithSAML operation. Create an AWS CloudTrail trail that has Amazon CloudWatch Logs turned on. Use Amazon EventBridge to monitor security team activities.
- D. Create a local individual break glass IAM user on the operating system level of each workload instance. Configure unrestricted security groups on the instances to grant access to the break glass IAM users.
- E. Configure AWS Systems Manager Session Manager for Amazon EC2. Configure an AWS CloudTrail filter based on Session Manager. Send the results to an Amazon Simple Notification Service (Amazon SNS) topic.

Correct Answer: *AE*

Question:87 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

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

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

- A. Create a custom authorization service using AWS Lambda.
- B. Configure a SAML identity provider in Amazon Cognito to map attributes to the Amazon Cognito user pool attributes.
- C. Configure the SAML identity provider to add the Amazon Cognito user pool as a relying party.
- D. Configure an Amazon Cognito identity pool to integrate with social login providers.
- E. Update DynamoDB to store the user email addresses and passwords.
- F. Update API Gateway to use a COGNITO_USER_POOLS authorizer.

Correct Answer: *BCF*

Question:88 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company needs to improve its ability to identify and prevent IAM policies that grant public access or cross-account access to resources. The company has implemented AWS Organizations and has started using AWS Identity and Access Management Access Analyzer to refine overly broad access to accounts in the organization.

A security engineer must automate a response in the company's organization for any newly created policies that are overly permissive. The automation must remediate external access and must notify the company's security team.

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

- A. Create an AWS Step Functions state machine that checks the resource type in the finding and adds an explicit Deny statement in the trust policy for the IAM role. Configure the state machine to publish a notification to an Amazon Simple Notification Service (Amazon SNS) topic.
- B. Create an AWS Batch job that forwards any resource type findings to an AWS Lambda function. Configure the Lambda function to add an explicit Deny statement in the trust policy for the IAM role. Configure the AWS Batch job to publish a notification to an Amazon Simple Notification Service (Amazon SNS) topic.
- C. In Amazon EventBridge, create an event rule that matches active IAM Access Analyzer findings and invokes AWS Step Functions for resolution.
- D. In Amazon CloudWatch, create a metric filter that matches active IAM Access Analyzer findings and invokes AWS Batch for resolution.
- E. Create an Amazon Simple Queue Service (Amazon SQS) queue. Configure the queue to forward a notification to the security team that an external principal has been granted access to the specific IAM role and has been blocked.
- F. Create an Amazon Simple Notification Service (Amazon SNS) topic for external or cross-account access notices. Subscribe the security team's email addresses to the topic.

Correct Answer: *ACF*

Question:89 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A security engineer is configuring a mechanism to send an alert when three or more failed sign-in attempts to the AWS Management Console occur during a 5-minute period. The security engineer creates a trail in AWS CloudTrail to assist in this work.

Which solution will meet these requirements?

- A. In CloudTrail, turn on Insights events on the trail. Configure an alarm on the insight with eventName matching ConsoleLogin and errorMessage matching "Failed authentication''. Configure a threshold of 3 and a period of 5 minutes.
- B. Configure CloudTrail to send events to Amazon CloudWatch Logs. Create a metric filter for the relevant log group. Create a filter pattern with eventName matching ConsoleLogin and errorMessage matching "Failed authentication". Create a CloudWatch alarm with a threshold of 3 and a period of 5 minutes.
- C. Create an Amazon Athena table from the CloudTrail events. Run a query for eventName matching ConsoleLogin and for errorMessage matching "Failed authentication". Create a notification action from the query to send an Amazon Simple Notification Service (Amazon SNS) notification when the count equals 3 within a period of 5 minutes.
- D. In AWS Identity and Access Management Access Analyzer, create a new analyzer. Configure the analyzer

to send an Amazon Simple Notification Service (Amazon SNS) notification when a failed sign-in event occurs 3 times for any IAM user within a period of 5 minutes.

Correct Answer: *B*

Question:90 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company's security engineer is developing an incident response plan to detect suspicious activity in an AWS account for VPC hosted resources. The security engineer needs to provide visibility for as many AWS Regions as possible.

Which combination of steps will meet these requirements MOST cost-effectively? (Choose two.)

- A. Turn on VPC Flow Logs for all VPCs in the account.
- B. Activate Amazon GuardDuty across all AWS Regions.
- C. Activate Amazon Detective across all AWS Regions.
- D. Create an Amazon Simple Notification Service (Amazon SNS) topic. Create an Amazon EventBridge rule that responds to findings and publishes the findings to the SNS topic.
- E. Create an AWS Lambda function. Create an Amazon EventBridge rule that invokes the Lambda function to publish findings to Amazon Simple Email Service (Amazon SES).

Correct Answer: *BD*

Question:91 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company stores images for a website in an Amazon S3 bucket. The company is using Amazon CloudFront to serve the images to end users. The company recently discovered that the images are being accessed from countries where the company does not have a distribution license.

Which actions should the company take to secure the images to limit their distribution? (Choose two.)

- A. Update the S3 bucket policy to restrict access to a CloudFront origin access control (OAC).
- B. Update the website DNS record to use an Amazon Route 53 geolocation record deny list of countries where the company lacks a license.
- C. Add a CloudFront geo restriction deny list of countries where the company lacks a license.
- D. Update the S3 bucket policy with a deny list of countries where the company lacks a license.
- E. Enable the Restrict Viewer Access option in CloudFront to create a deny list of countries where the company lacks a license.

Correct Answer: *AC*

Question:92 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company has deployed servers on Amazon EC2 instances in a VPC. External vendors access these servers over the internet. Recently, the company deployed a new application on EC2 instances in a new CIDR range. The company needs to make the application available to the vendors.

A security engineer verified that the associated security groups and network ACLs are allowing the required ports in the inbound direction. However, the vendors cannot connect to the application.

Which solution will provide the vendors access to the application?

- A. Modify the security group that is associated with the EC2 instances to have the same outbound rules as inbound rules.
- B. Modify the network ACL that is associated with the CIDR range to allow outbound traffic to ephemeral ports.
- C. Modify the inbound rules on the internet gateway to allow the required ports.
- D. Modify the network ACL that is associated with the CIDR range to have the same outbound rules as inbound rules.

Correct Answer: *B*

Question:93 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company uses infrastructure as code (IaC) to create AWS infrastructure. The company writes the code as AWS CloudFormation templates to deploy the infrastructure. The company has an existing CI/CD pipeline that the company can use to deploy these templates.

After a recent security audit, the company decides to adopt a policy-as-code approach to improve the company's security posture on AWS. The company must prevent the deployment of any infrastructure that would violate a security policy, such as an unencrypted Amazon Elastic Block Store (Amazon EBS) volume.

Which solution will meet these requirements?

- A. Turn on AWS Trusted Advisor. Configure security notifications as webhooks in the preferences section of the CI/CD pipeline.
- B. Turn on AWS Config. Use the prebuilt rules or customized rules. Subscribe tile CI/CD pipeline to an Amazon Simple Notification Service (Amazon SNS) topic that receives notifications from AWS Config.
- C. Create rule sets in AWS CloudFormation Guard. Run validation checks for CloudFormation templates as a phase of the CI/CD process.
- D. Create rule sets as SCPs. Integrate the SCPs as a part of validation control in a phase of the CI/CD process.

Correct Answer: *C*

Question:94 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company is running an Amazon RDS for MySQL DB instance in a VPC. The VPC must not send or receive network traffic through the internet.

A security engineer wants to use AWS Secrets Manager to rotate the DB instance credentials automatically. Because of a security policy, the security engineer cannot use the standard AWS Lambda function that Secrets Manager provides to rotate the credentials.

The security engineer deploys a custom Lambda function in the VPC. The custom Lambda function will be responsible for rotating the secret in Secrets Manager. The security engineer edits the DB instance's security group to allow connections from this function. When the function is invoked, the function cannot communicate with Secrets Manager to rotate the secret properly.

What should the security engineer do so that the function can rotate the secret?

- A. Add an egress-only internet gateway to the VPC. Allow only the Lambda function's subnet to route traffic through the egress-only internet gateway.
- B. Add a NAT gateway to the VPC. Configure only the Lambda function's subnet with a default route through the NAT gateway.
- C. Configure a VPC peering connection to the default VPC for Secrets Manager. Configure the Lambda function's subnet to use the peering connection for routes.
- D. Configure a Secrets Manager interface VPC endpoint. Include the Lambda function's private subnet during the configuration process.

6

Correct Answer: *D*

Question:95 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

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

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

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

Correct Answer: *BD*

Question:96 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company is using Amazon Elastic Container Service (Amazon ECS) to run its container-based application on AWS. The company needs to ensure that the container images contain no severe vulnerabilities. The company also must ensure that only specific IAM roles and specific AWS accounts can access the container images.

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

- A. Pull images from the public container registry. Publish the images to Amazon Elastic Container Registry (Amazon ECR) repositories with scan on push configured in a centralized AWS account. Use a CI/CD pipeline to deploy the images to different AWS accounts. Use identity-based policies to restrict access to which IAM principals can access the images.
- B. Pull images from the public container registry. Publish the images to a private container registry that is hosted on Amazon EC2 instances in a centralized AWS account. Deploy host-based container scanning tools to EC2 instances that run Amazon ECS. Restrict access to the container images by using basic authentication over HTTPS.
- C. Pull images from the public container registry. Publish the images to Amazon Elastic Container Registry (Amazon ECR) repositories with scan on push configured in a centralized AWS account. Use a CI/CD pipeline to deploy the images to different AWS accounts. Use repository policies and identity-based policies to restrict access to which IAM principals and accounts can access the images.
- D. Pull images from the public container registry. Publish the images to AWS CodeArtifact repositories in a centralized AWS account. Use a CI/CD pipeline to deploy the images to different AWS accounts. Use repository policies and identity-based policies to restrict access to which IAM principals and accounts can access the images.

Correct Answer: *C*

Question:97 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company's data scientists want to create artificial intelligence and machine learning (AI/ML) training models by using Amazon SageMaker. The training models will use large datasets in an Amazon S3 bucket. The datasets contain sensitive information.

On average, the data scientists need 30 days to train models. The S3 bucket has been secured appropriately. The company's data retention policy states that all data that is older than 45 days must be removed from the S3 bucket.

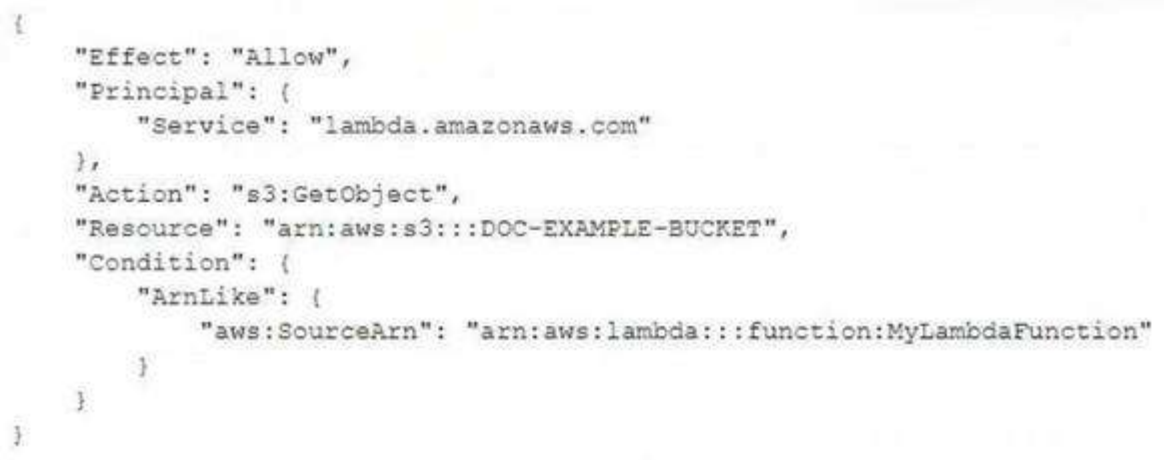
Which action should a security engineer take to enforce this data retention policy?

- A. Configure an S3 Lifecycle rule on the S3 bucket to delete objects after 45 days.
- B. Create an AWS Lambda function to check the last-modified date of the S3 objects and delete objects that are older than 45 days. Create an S3 event notification to invoke the Lambda function for each PutObject operation.
- C. Create an AWS Lambda function to check the last-modified date of the S3 objects and delete objects that are older than 45 days. Create an Amazon EventBridge rule to invoke the Lambda function each month.
- D. Configure S3 Intelligent-Tiering on the S3 bucket to automatically transition objects to another storage class.

Correct Answer: *A*

Question:98 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

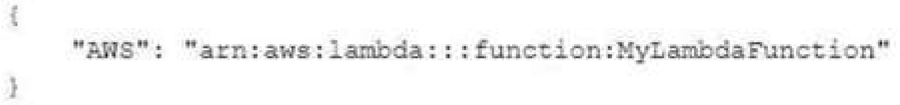
A security engineer is troubleshooting an AWS Lambda function that is named MyLambdaFunction. The function is encountering an error when the function attempts to read the objects in an Amazon S3 bucket that is named DOC-EXAMPLE-BUCKET. The S3 bucket has the following bucket policy:



```
{
    "Effect": "Allow",
    "Principal": {
        "Service": "lambda.amazonaws.com"
    },
    "Action": "s3:GetObject",
    "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
    "Condition": {
        "ArnLike": {
            "aws:SourceArn": "arn:aws:lambda:::function:MyLambdaFunction"
        }
    }
}
```

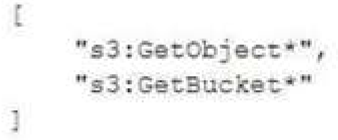
Which change should the security engineer make to the policy to ensure that the Lambda function can read the bucket objects?

- A. Remove the Condition element. Change the Principal element to the following:



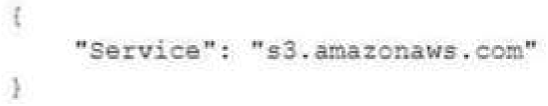
```
{
    "AWS": "arn:aws:lambda:::function:MyLambdaFunction"
}
```

- B. Change the Action element to the following:



```
[
    "s3:GetObject*",
    "s3:GetBucket*"
]
```

- C. Change the Resource element to "arn:aws:s3:::DOC-EXAMPLE- BUCKET/*''.
- D. Change the Resource element to "arn:aws:lambda:::function:MyLambdaFunction". Change the Principal element to the following:



```
{
    "Service": "s3.amazonaws.com"
}
```

Correct Answer: *C*

Question:99 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

An IAM user receives an Access Denied message when the user attempts to access objects in an Amazon S3 bucket. The user and the S3 bucket are in the same AWS account. The S3 bucket is configured to use server-side encryption with AWS KMS keys (SSE-KMS) to encrypt all of its objects at rest by using a customer managed key from the same AWS account. The S3 bucket has no bucket policy defined. The IAM user has been granted permissions through an IAM policy that allows the kms:Decrypt permission to the customer managed key. The IAM policy also allows the s3:List* and s3:Get* permissions for the S3 bucket and its objects.

Which of the following is a possible reason that the IAM user cannot access the objects in the S3 bucket?

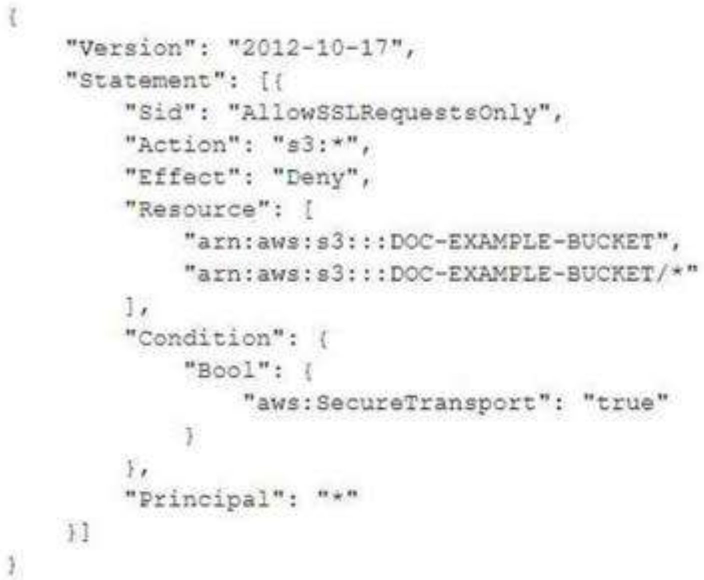
- A. The IAM policy needs to allow the kms:DescribeKey permission.
- B. The S3 bucket has been changed to use the AWS managed key to encrypt objects at rest.
- C. An S3 bucket policy needs to be added to allow the IAM user to access the objects.
- D. The KMS key policy has been edited to remove the ability for the AWS account to have full access to the key.

Correct Answer: *D*

Question:100 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

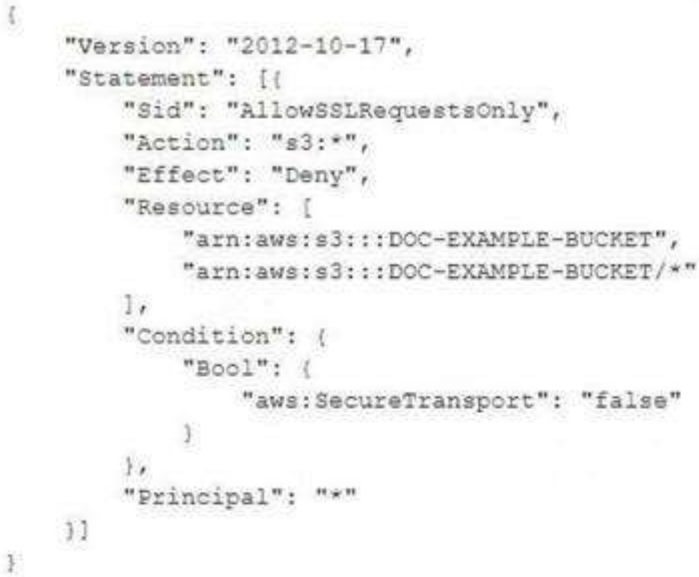
A company has a guideline that mandates the encryption of all Amazon S3 bucket data in transit. A security engineer must implement an S3 bucket policy that denies any S3 operations if data is not encrypted.

Which S3 bucket policy will meet this requirement?



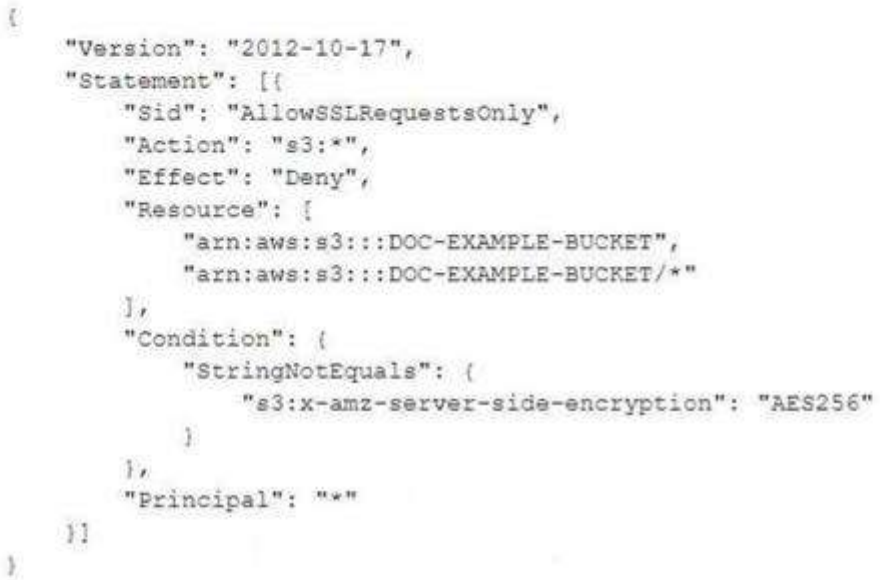
```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "AllowSSLRequestsOnly",
        "Action": "s3:*",
        "Effect": "Deny",
        "Resource": [
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
        ],
        "Condition": {
            "Bool": {
                "aws:SecureTransport": "true"
            }
        },
        "Principal": "*"
    }]
}
```

- A.



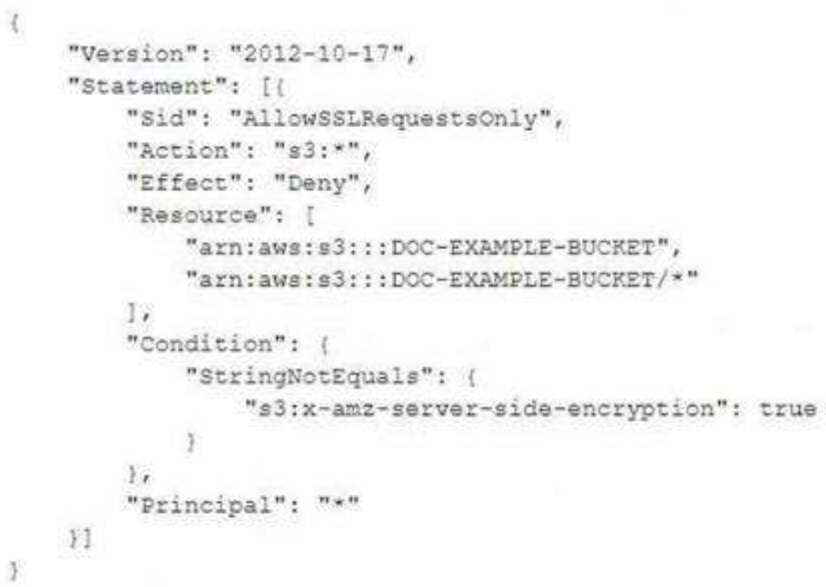
```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "AllowSSLRequestsOnly",
        "Action": "s3:*",
        "Effect": "Deny",
        "Resource": [
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
        ],
        "Condition": {
            "Bool": {
                "aws:SecureTransport": "false"
            }
        },
        "Principal": "*"
    }]
}
```

- B.



```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "AllowSSLRequestsOnly",
        "Action": "s3:*",
        "Effect": "Deny",
        "Resource": [
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
        ],
        "Condition": {
            "StringNotEquals": {
                "s3:x-amz-server-side-encryption": "AES256"
            }
        },
        "Principal": "*"
    }]
}
```

- C.



```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "AllowSSLRequestsOnly",
        "Action": "s3:*",
        "Effect": "Deny",
        "Resource": [
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
        ],
        "Condition": {
            "StringNotEquals": {
                "s3:x-amz-server-side-encryption": true
            }
        },
        "Principal": "*"
    }]
}
```

- D.

Correct Answer: *B*

Question:101 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A security engineer wants to use Amazon Simple Notification Service (Amazon SNS) to send email alerts to a company's security team for Amazon GuardDuty findings that have a High severity level. The security engineer also wants to deliver these findings to a visualization tool for further examination.

Which solution will meet these requirements?

- A. Set up GuardDuty to send notifications to an Amazon CloudWatch alarm with two targets in CloudWatch. From CloudWatch, stream the findings through Amazon Kinesis Data Streams into an Amazon Open Search Service domain as the first target for delivery. Use Amazon QuickSight to visualize the findings. Use OpenSearch queries for further analysis. Deliver email alerts to the security team by configuring an SNS topic as a second target for the CloudWatch alarm. Use event pattern matching with an Amazon EventBridge event rule to send only High severity findings in the alerts.
- B. Set up GuardDuty to send notifications to AWS CloudTrail with two targets in CloudTrail. From CloudTrail, stream the findings through Amazon Kinesis Data Firehose into an Amazon OpenSearch Service domain as the first target for delivery. Use OpenSearch Dashboards to visualize the findings. Use OpenSearch queries for further analysis. Deliver email alerts to the security team by configuring an SNS topic as a second target for CloudTrail. Use event pattern matching with a CloudTrail event rule to send only High severity findings in the alerts.
- C. Set up GuardDuty to send notifications to Amazon EventBridge with two targets. From EventBridge, stream the findings through Amazon Kinesis Data Firehose into an Amazon OpenSearch Service domain as the first target for delivery. Use OpenSearch Dashboards to visualize the findings. Use OpenSearch queries for further analysis. Deliver email alerts to the security team by configuring an SNS topic as a second target for EventBridge. Use event pattern matching with an EventBridge event rule to send only High severity findings in the alerts.
- D. Set up GuardDuty to send notifications to Amazon EventBridge with two targets. From EventBridge, stream the findings through Amazon Kinesis Data Streams into an Amazon OpenSearch Service domain as the first target for delivery. Use Amazon QuickSight to visualize the findings. Use OpenSearch queries for further analysis. Deliver email alerts to the security team by configuring an SNS topic as a second target for EventBridge. Use event pattern matching with an EventBridge event rule to send only High severity findings in the alerts.

Correct Answer: *C*
Explanation:
According to this AWS article, it is GuardDuty -> EventBrdige -> Firehouse -> OpenSearch -> OpenSearch visualization.
Reference:

https://aws.amazon.com/blogs/security/visualizing-amazon-guardduty-findings/

Question:102 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A security engineer needs to implement a write-once-read-many (WORM) model for data that a company will store in Amazon S3 buckets. The company uses the S3 Standard storage class for all of its S3 buckets. The security engineer must ensure that objects cannot be overwritten or deleted by any user, including the AWS account root user.

Which solution will meet these requirements?

- A. Create new S3 buckets with S3 Object Lock enabled in compliance mode. Place objects in the S3 buckets.
- B. Use S3 Glacier Vault Lock to attach a Vault Lock policy to new S3 buckets. Wait 24 hours to complete the Vault Lock process. Place objects in the S3 buckets.
- C. Create new S3 buckets with S3 Object Lock enabled in governance mode. Place objects in the S3 buckets.
- D. Create new S3 buckets with S3 Object Lock enabled in governance mode. Add a legal hold to the S3 buckets. Place objects in the S3 buckets.

Correct Answer: *A*
Explanation:
In compliance mode, a protected object version can't be overwritten or deleted by any user, including the root user in your AWS account. When an object is locked in compliance mode, its retention mode can't be changed, and its retention period can't be shortened. Compliance mode helps ensure that an object version can't be overwritten or deleted for the duration of the retention period. In governance mode, users can't overwrite or delete an object version or alter its lock settings unless they have special permissions. With governance mode, you protect objects against being deleted by most users, but you can still grant some users permission to alter the retention settings or delete the objects if necessary. You can also use governance mode to test retention-period settings before creating a compliance-mode retention period.

Question:103 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company needs complete encryption of the traffic between external users and an application. The company hosts the application on a fleet of Amazon EC2 instances that run in an Auto Scaling group behind an Application Load Balancer (ALB).

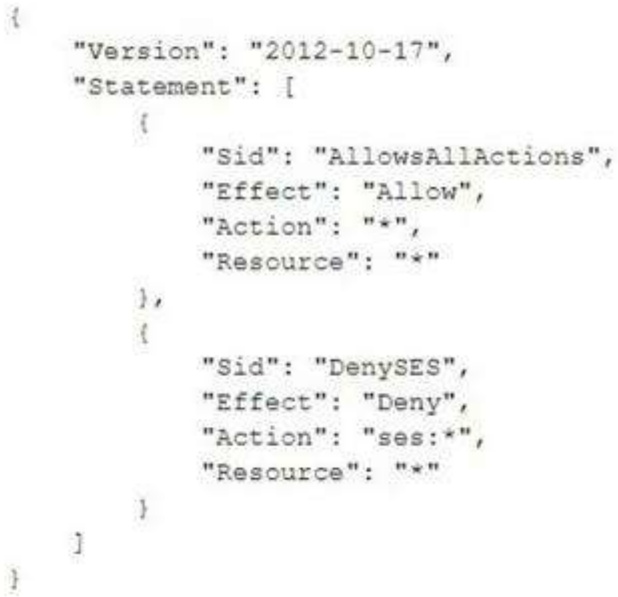
How can a security engineer meet these requirements?

- A. Create a new Amazon-issued certificate in AWS Secrets Manager. Export the certificate from Secrets Manager. Import the certificate into the ALB and the EC2 instances.
- B. Create a new Amazon-issued certificate in AWS Certificate Manager (ACM). Associate the certificate with the ALExport the certificate from ACM. Install the certificate on the EC2 instances.
- C. Import a new third-party certificate into AWS Identity and Access Management (IAM). Export the certificate from IAM. Associate the certificate with the ALB and the EC2 instances.
- D. Import a new third-party certificate into AWS Certificate Manager (ACM). Associate the certificate with the ALB. Install the certificate on the EC2 instances.

Correct Answer: *D*
Explanation:
To encrypt traffic between external users and the application behind the Application Load Balancer (ALB), a certificate should be imported into AWS Certificate Manager (ACM) and associated with the ALB. The same certificate should also be installed on the EC2 instances.

Question:104 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company has an organization with SCPs in AWS Organizations. The root SCP for the organization is as follows:



```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsAllActions",
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*"
        },
        {
            "Sid": "DenySES",
            "Effect": "Deny",
            "Action": "ses:*",
            "Resource": "*"
        }
    ]
}
```

The company's developers are members of a group that has an IAM policy that allows access to Amazon Simple Email Service (Amazon SES) by allowing ses:* actions. The account is a child to an OU that has an SCP that allows Amazon SES. The developers are receiving a not-authorized error when they try to access Amazon SES through the AWS Management Console.

Which change must a security engineer implement so that the developers can access Amazon SES?

- A. Add a resource policy that allows each member of the group to access Amazon SES.
- B. Add a resource policy that allows "Principal": {"AWS": "arn:aws:iam::account-number:group/Dev"}.
- C. Remove the AWS Control Tower control (guardrail) that restricts access to Amazon SES.
- D. Remove Amazon SES from the root SCP.

Correct Answer: *D*
Explanation:
A SCP identifies the maximum level of access that IAM entity within that OU can have. Since SES is denied in the SCP, it does not matter if you allow it in other policies. It will simply not be allowed because the SCP does not allow it.

Question:105 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company hosts a public website on an Amazon EC2 instance. HTTPS traffic must be able to access the website. The company uses SSH for management of the web server.

The website is on the subnet 10.0.1.0/24. The management subnet is 192.168.100.0/24. A security engineer must create a security group for the EC2 instance.

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

- A. Allow port 22 from source 0.0.0.0/0.
- B. Allow port 443 from source 0.0 0 0/0.
- C. Allow port 22 from 192.168.100.0/24.
- D. Allow port 22 from 10.0.1.0/24.
- E. Allow port 443 from 10.0.1.0/24.

Correct Answer: *BC*

Question:106 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A security engineer wants to forward custom application-security logs from an Amazon EC2 instance to Amazon CloudWatch. The security engineer installs the CloudWatch agent on the EC2 instance and adds the path of the logs to the CloudWatch configuration file.

However, CloudWatch does not receive the logs. The security engineer verifies that the awslogs service is running on the EC2 instance.

What should the security engineer do next to resolve the issue?

- A. Add AWS CloudTrail to the trust policy of the EC2 in stance. Send the custom logs to CloudTrail instead of CloudWatch.
- B. Add Amazon S3 to the trust policy of the EC2 instance. Configure the application to write the custom logs to an S3 bucket that CloudWatch can use to ingest the logs.
- C. Add Amazon Inspector to the trust policy of the EC2 instance. Use Amazon Inspector instead of the CloudWatch agent to collect the custom logs.
- D. Attach the CloudWatchAgentServerPolicy AWS managed policy to the EC2 instance role.

Correct Answer: *D*
Explanation:
Uses of CloudWatchAgentServerPolicy ;
It allows the CloudWatch agent to publish metrics and logs to CloudWatch on behalf of the IAM role or user the policy is attached to.
It provides permissions for the agent to access and manage its own configuration files stored in S3.
The policy grants permissions across multiple AWS services like CloudWatch, S3, KMS etc. to allow end-to-end functionality of the monitoring agent.

Question:107 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***
A systems engineer is troubleshooting the connectivity of a test environment that includes a virtual security appliance deployed inline. In addition to using the virtual security appliance, the development team wants to use security groups and network ACLs to accomplish various security requirements in the environment.

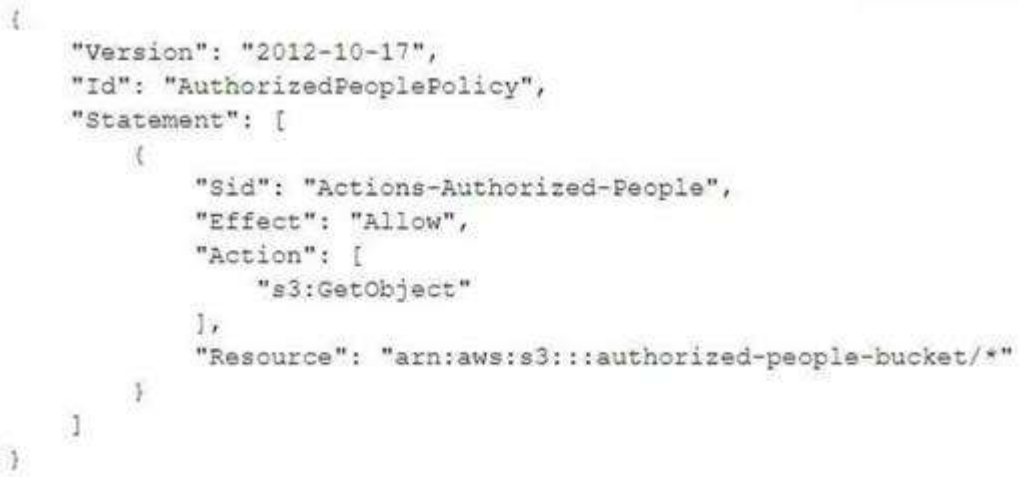
What configuration is necessary to allow the virtual security appliance to route the traffic?

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

Correct Answer: *C*
Explanation:
When you deploy a virtual security appliance inline in a subnet, you need to ensure that it can effectively route traffic between different subnets. The "Network Source/Destination check" is a feature in Amazon EC2 that controls whether source/destination checking is enabled or disabled on a network interface.

In this context, the virtual security appliance acts as a router, and the "Network Source/Destination check" should be disabled on its elastic network interface. When this check is disabled, the network interface can handle traffic that is not specifically destined for the instance it is attached to, allowing it to route traffic between different subnets.

Question:108 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***
A security engineer needs to create an Amazon S3 bucket policy to grant least privilege read access to IAM user accounts that are named User1, User2, and User3. These IAM user accounts are members of the AuthorizedPeople IAM group. The security engineer drafts the following S3 bucket policy:



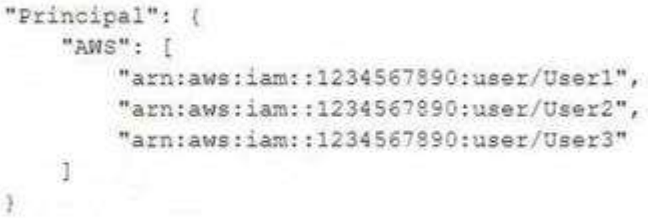
```
{
    "Version": "2012-10-17",
    "Id": "AuthorizedPeoplePolicy",
    "Statement": [
        {
            "Sid": "Actions-Authorized-People",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": "arn:aws:s3:::authorized-people-bucket/*"
        }
    ]
}
```

When the security engineer tries to add the policy to the S3 bucket, the following error message appears: "Missing required field Principal."

The security engineer is adding a Principal element to the policy. The addition must provide read access to only User1, User2, and User3.

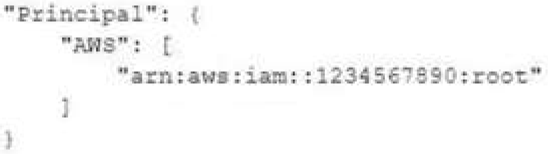
Which solution meets these requirements?

- A.



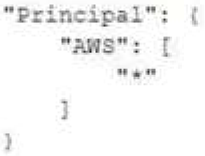
```
"Principal": {
    "AWS": [
        "arn:aws:iam::1234567890:user/User1",
        "arn:aws:iam::1234567890:user/User2",
        "arn:aws:iam::1234567890:user/User3"
    ]
}
```

- B.



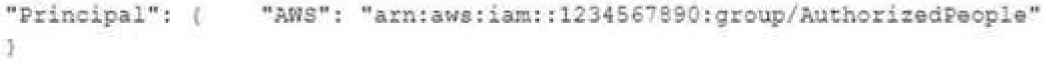
```
"Principal": {
    "AWS": [
        "arn:aws:iam::1234567890:root"
    ]
}
```

- C.



```
"Principal": {
    "AWS": [
        "*"
    ]
}
```

- D.



```
"Principal": {    "AWS": "arn:aws:iam::1234567890:group/AuthorizedPeople"
}
```

Correct Answer: *A*
Explanation:
You can specify any of the following principals in a policy:
AWS account and root user
IAM roles
Role sessions
IAM users
Federated user sessions
AWS services
All principals

You cannot identify a user group as a principal in a policy (such as a resource-based policy) because groups relate to permissions, not authentication, and principals are authenticated IAM entities.

Reference:
https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_principal.html#Principal_specifying

Question:109 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

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-keys-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 GetCredenlialReport permission.
- D. The AWS Config rules have a MaximumExecutionFrequency value of 24 hours.

Correct Answer: *A*
Explanation:
AWS Config rules such as mfa-enabled-for-iam-console-access, iam-user-mfa-enabled, access-keys-rotated, and iam-user-unused-credentials-check rely on data from the IAM credential report. The IAM credential report is updated automatically every four hours, and changes in IAM (such as rotating access keys) may not be reflected in the report immediately. If the IAM credential report was generated within the past 4 hours, AWS Config might not yet have the updated information, causing the resources to display as noncompliant.

Question:110 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company is using AWS WAF to protect a customized public API service that is based on Amazon EC instances. The API uses an Application Load Balancer.

The AWS WAF web ACL is configured with an AWS Managed Rules rule group. After a software upgrade to the API and the client application, some types of requests are no longer working and are causing application stability issues. A security engineer discovers that AWS WAF logging is not turned on for the web ACL.

The security engineer needs to immediately return the application to service, resolve the issue, and ensure that logging is not turned off in the future. The security engineer turns on logging for the web ACL and specifies Amazon CloudWatch Logs as the destination.

Which additional set of steps should the security engineer take to meet the requirements?

- A. Edit the rules in the web ACL to include rules with Count actions. Review the logs to determine which rule is blocking the request. Modify the IAM policy of all AWS WAF administrators so that they cannot remove the logging configuration for any AWS WAF web ACLs.
- B. Edit the rules in the web ACL to include rules with Count actions. Review the logs to determine which rule is blocking the request. Modify the AWS WAF resource policy so that AWS WAF administrators cannot remove the logging configuration for any AWS WAF web ACLs.
- C. Edit the rules in the web ACL to include rules with Count and Challenge actions. Review the logs to determine which rule is blocking the request. Modify the AWS WAF resource policy so that AWS WAF administrators cannot remove the logging configuration for any AWS WAF web ACLs.
- D. Edit the rules in the web ACL to include rules with Count and Challenge actions. Review the logs to determine which rule is blocking the request. Modify the IAM policy of all AWS WAF administrators so that they cannot remove the logging configuration for any AWS WAF web ACLs.

Correct Answer: *A*
Explanation:
AWS documentation recommends applying least privilege permissions through IAM policies when managing access to resources across multiple accounts. This helps ensure permissions are restricted at the identity level rather than at the individual resource level.

Question:111 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A security engineer is creating an AWS Lambda function. The Lambda function needs to use a role that is named LambdaAuditRole to assume a role that is named AcmeAuditFactoryRole in a different AWS account.

When the code is processed, the following error message appears: "An error occurred (AccessDenied) when calling the AssumeRole operation."

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

- A. Ensure that LambdaAuditRole has the sts:AssumeRole permission for AcmeAuditFactoryRole.
- B. Ensure that LambdaAuditRole has the AWSLambdaBasicExecutionRole managed policy attached.
- C. Ensure that the trust policy for AcmeAuditFactoryRole allows the sts:AssumeRole action from LambdaAuditRole.
- D. Ensure that the trust policy for LambdaAuditRole allows the sts:AssumeRole action from the lambda.amazonaws.com service.
- E. Ensure that the sts:AssumeRole API call is being issued to the us-east-1 Region endpoint.

Correct Answer: *AC*
Reference:
https://repost.aws/knowledge-center/lambda-function-assume-iam-role

Question:112 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company has AWS accounts in an organization in AWS Organizations. The organization includes a dedicated security account.

All AWS account activity across all member accounts must be logged and reported to the dedicated security account. The company must retain all the activity logs in a secure storage location within the dedicated security account for 2 years. No changes or deletions of the logs are allowed.

Which combination of steps will meet these requirements with the LEAST operational overhead? (Choose two.)

- A. In the dedicated security account, create an Amazon S3 bucket. Configure S3 Object Lock in compliance mode and a retention period of 2 years on the S3 bucket. Set the bucket policy to allow the organization's management account to write to the S3 bucket.
- B. In the dedicated security account, create an Amazon S3 bucket. Configure S3 Object Lock in compliance mode and a retention period of 2 years on the S3 bucket. Set the bucket policy to allow the organization's member accounts to write to the S3 bucket.
- C. In the dedicated security account, create an Amazon S3 bucket that has an S3 Lifecycle configuration that expires objects after 2 years. Set the bucket policy to allow the organization's member accounts to write to the S3 bucket.
- D. Create an AWS CloudTrail trail for the organization. Configure logs to be delivered to the logging Amazon S3 bucket in the dedicated security account.
- E. Turn on AWS CloudTrail in each account. Configure logs to be delivered to an Amazon S3 bucket that is created in the organization's management account. Forward the logs to the S3 bucket in the dedicated security account by using AWS Lambda and Amazon Kinesis Data Firehose.

Correct Answer: *BD*
Explanation:
Each Member Account has to write into the security Account S3 bucket, not only the Organization Management Account.
Reference:
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-set-bucket-policy-for-multiple-accounts.html

Question:113 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company is testing its incident response plan for compromised credentials. The company runs a database on an Amazon EC2 instance and stores the sensitive database credentials as a secret in AWS Secrets Manager. The secret has rotation configured with an AWS Lambda function that uses the generic rotation function template. The EC2 instance and the Lambda function are deployed in the same private subnet. The VPC has a Secrets Manager VPC endpoint.

A security engineer discovers that the secret cannot rotate. The security engineer determines that the VPC endpoint is working as intended. The Amazon CloudWatch logs contain the following error: "setSecret: Unable to log into database".

Which solution will resolve this error?

- A. Use the AWS Management Console to edit the JSON structure of the secret in Secrets Manager so that the secret automatically conforms with the structure that the database requires.
- B. Ensure that the security group that is attached to the Lambda function allows outbound connections to the EC2 instance. Ensure that the security group that is attached to the EC2 instance allows inbound connections from the security group that is attached to the Lambda function.
- C. Use the Secrets Manager list-secrets command in the AWS CLI to list the secret. Identify the database credentials. Use the Secrets Manager rotate-secret command in the AWS CLI to force the immediate rotation of the secret.
- D. Add an internet gateway to the VPC. Create a NAT gateway in a public subnet. Update the VPC route tables so that traffic from the Lambda function and traffic from the EC2 instance can reach the Secrets Manager public endpoint.

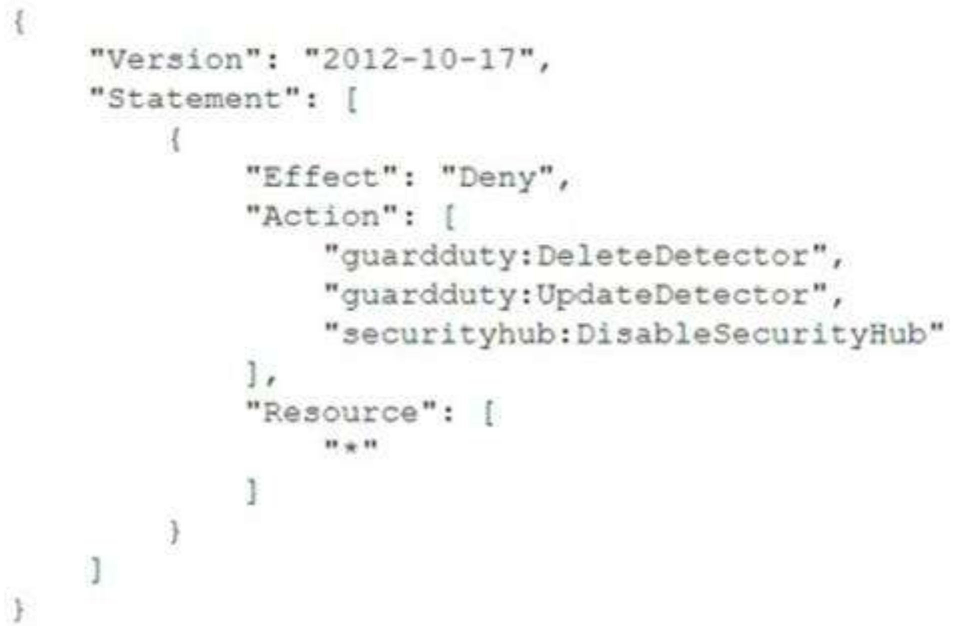
Correct Answer: *B*
Explanation:
When a Lambda function needs to access resources inside a Virtual Private Cloud (VPC), it does so using ENI which resides in a subnet of the VPC and can have a security group associated with it. The security group acts as a virtual firewall for the ENI.

Question:114

A company deploys a set of standard IAM roles in AWS accounts. The IAM roles are based on job functions within the company. To balance operational efficiency and security, a security engineer implemented AWS Organizations SCPs to restrict access to critical security services in all company accounts.

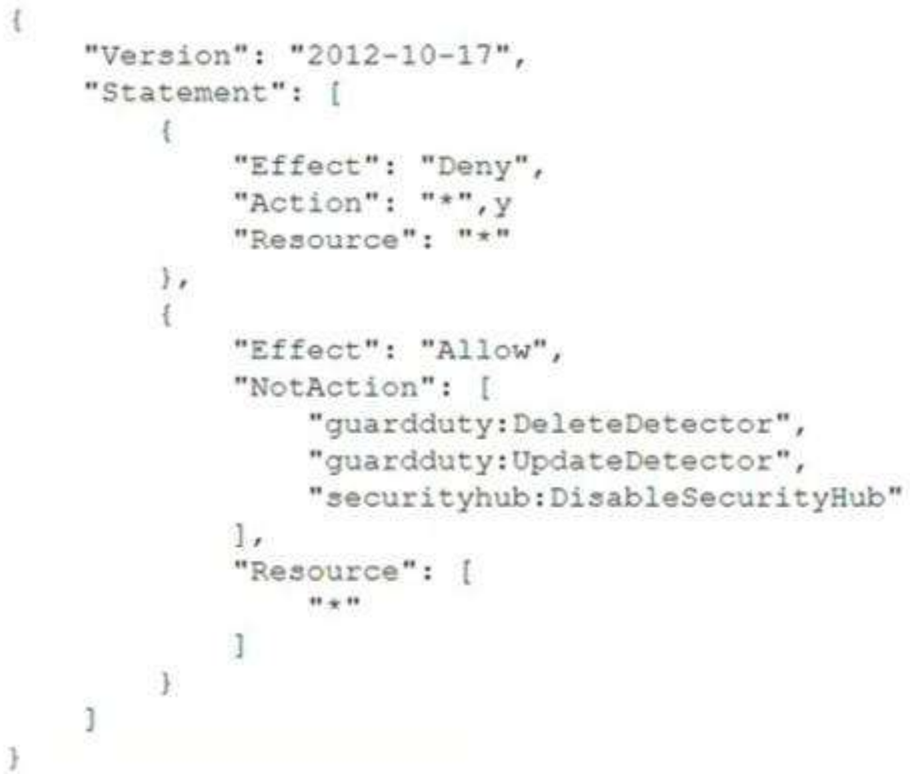
All of the company's accounts and OUs within AWS Organizations have a default FullAWSAccess SCP that is attached. The security engineer needs to ensure that no one can disable Amazon GuardDuty and AWS Security Hub. The security engineer also must not override other permissions that are granted by IAM policies that are defined in the accounts.

Which SCP should the security engineer attach to the root of the organization to meet these requirements?



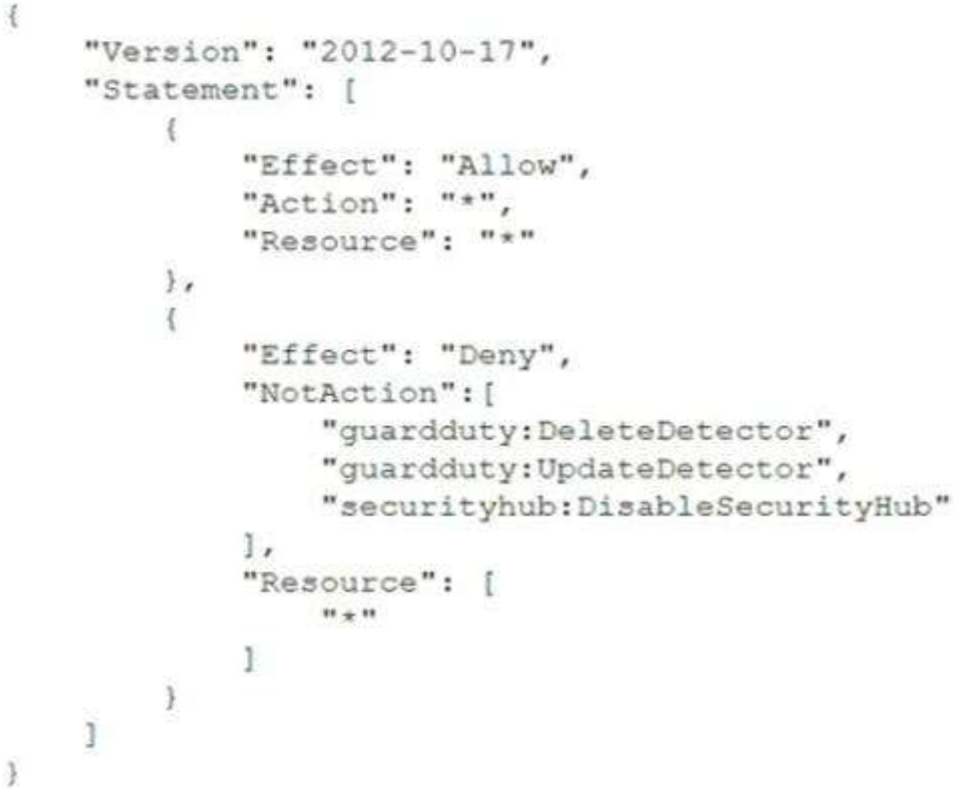
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "guardduty:DeleteDetector",
                "guardduty:UpdateDetector",
                "securityhub:DisableSecurityHub"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

- A.



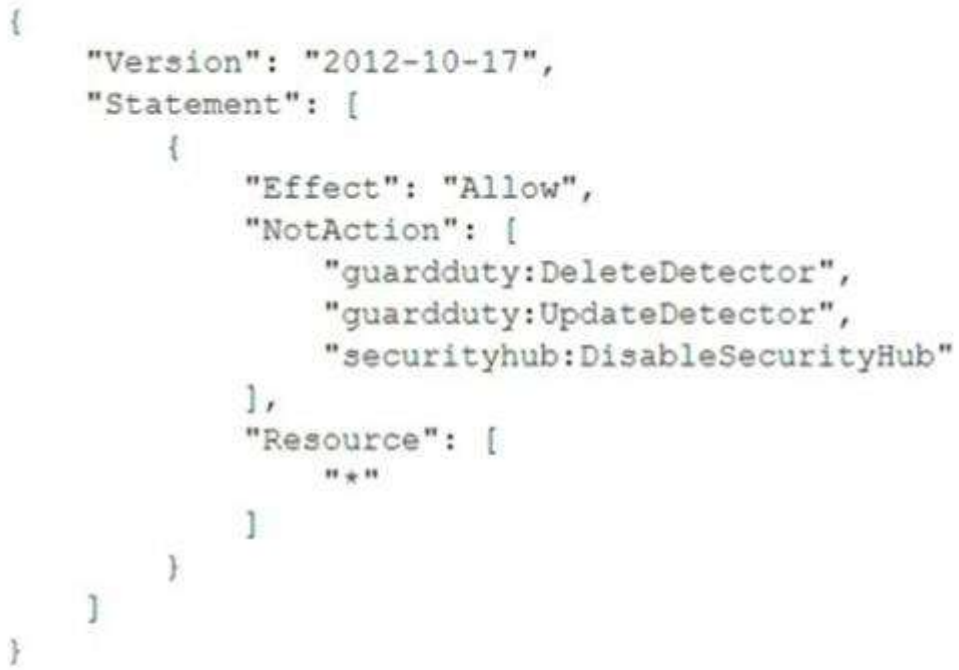
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "*",y
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "NotAction": [
                "guardduty:DeleteDetector",
                "guardduty:UpdateDetector",
                "securityhub:DisableSecurityHub"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

- B.



```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "NotAction":[
                "guardduty:DeleteDetector",
                "guardduty:UpdateDetector",
                "securityhub:DisableSecurityHub"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

- C.



```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "NotAction": [
                "guardduty:DeleteDetector",
                "guardduty:UpdateDetector",
                "securityhub:DisableSecurityHub"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

- D.

Correct Answer: *A*

Question:115 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company needs to follow security best practices to deploy resources from an AWS CloudFormation template. The CloudFormation template must be able to configure sensitive database credentials.

The company already uses AWS Key Management Service (AWS KMS) and AWS Secrets Manager.

Which solution will meet the requirements?

- A. Use a dynamic reference in the CloudFormation template to reference the database credentials in Secrets Manager.
- B. Use a parameter in the CloudFormation template to reference the database credentials. Encrypt the CloudFormation template by using AWS KMS.
- C. Use a SecureString parameter in the CloudFormation template to reference the database credentials in Secrets Manager.
- D. Use a SecureString parameter in the CloudFormation template to reference an encrypted value in AWS KMS.

Correct Answer: *A*
Explanation:
"Updating a secret in Secrets Manager doesn't automatically update the secret in CloudFormation. In order for CloudFormation to update a secretsmanager dynamic reference, you must perform a stack update that updates the resource containing the dynamic reference, either by updating the resource property that contains the secretsmanager dynamic reference, or updating another of the resource's properties."

Question:116 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

An international company wants to combine AWS Security Hub findings across all the company's AWS Regions and from multiple accounts. In addition, the company wants to create a centralized custom dashboard to correlate these findings with operational data for deeper analysis and insights. The company needs an analytics tool to search and visualize Security Hub findings.

Which combination of steps will meet these requirements? (Chose three.)

- A. Designate an AWS account as a delegated administrator for Security Hub. Publish events to Amazon CloudWatch from the delegated administrator account, all member accounts, and required Regions that are enabled for Security Hub findings.
- B. Designate an AWS account in an organization in AWS Organizations as a delegated administrator for

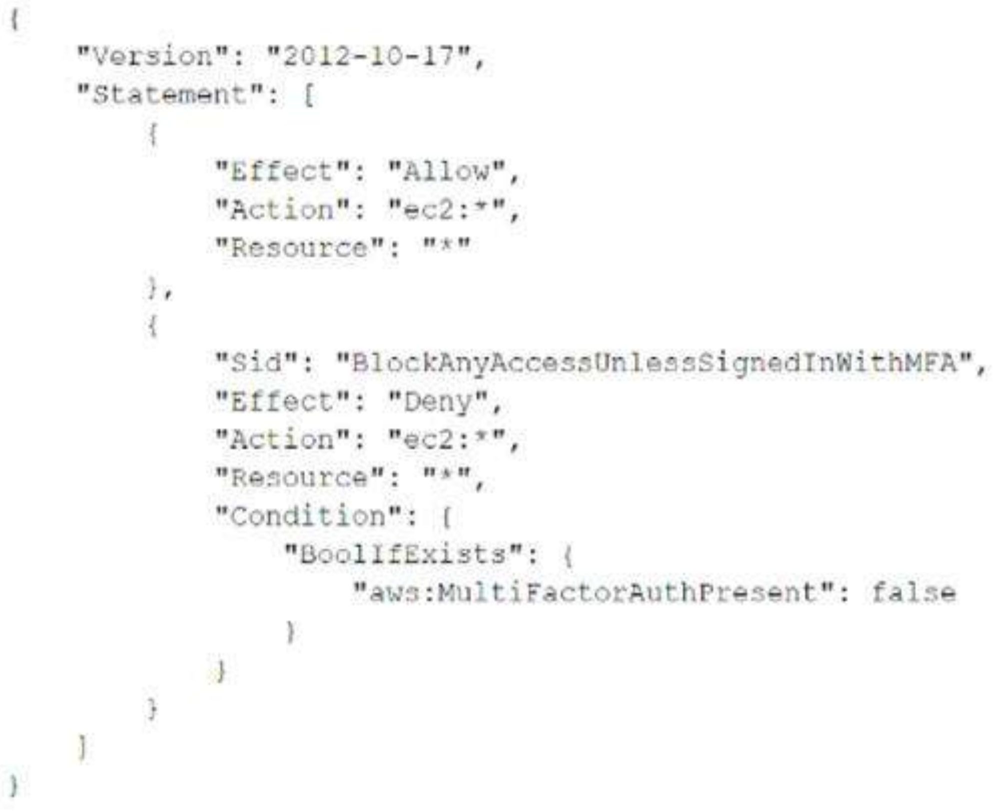
Security Hub. Publish events to Amazon EventBridge from the delegated administrator account, all member accounts, and required Regions that are enabled for Security Hub findings.

- C. In each Region, create an Amazon EventBridge rule to deliver findings to an Amazon Kinesis data stream. Configure the Kinesis data streams to output the logs to a single Amazon S3 bucket.
- D. In each Region, create an Amazon EventBridge rule to deliver findings to an Amazon Kinesis Data Firehose delivery stream. Configure the Kinesis Data Firehose delivery streams to deliver the logs to a single Amazon S3 bucket.
- E. Use AWS Glue DataBrew to crawl the Amazon S3 bucket and build the schema. Use AWS Glue Data Catalog to query the data and create views to flatten nested attributes. Build Amazon QuickSight dashboards by using Amazon Athena.
- F. Partition the Amazon S3 data. Use AWS Glue to crawl the S3 bucket and build the schema. Use Amazon Athena to query the data and create views to flatten nested attributes. Build Amazon QuickSight dashboards that use the Athena views.

Correct Answer: *BDF*
Reference:
https://aws.amazon.com/blogs/architecture/visualize-aws-security-hub-findings-using-analytics-and-business-intelligence-tools/

Question:117 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

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



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

After implementing the policy, the administrator receives reports that users are unable to perform Amazon EC2 commands using the AWS CLI.

What should the administrator do to resolve this problem while still enforcing multi-factor authentication?

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

assume-role CLI command and pass --serial-number and --token-code parameters. Store the resulting values in environment variables. Add sts:AssumeRole to NotAction in the policy.

Correct Answer: *B*

Question:118

A company is developing a mechanism that will help data scientists use Amazon SageMaker to read, process, and output data to an Amazon S3 bucket. Data scientists will have access to a dedicated S3 prefix for each of their projects. The company will implement bucket policies that use the dedicated S3 prefixes to restrict access to the S3 objects. The projects can last up to 60 days.

The company's security team mandates that data cannot remain in the S3 bucket after the end of the projects that use the data.

Which solution will meet these requirements MOST cost-effectively?

- A. Create an AWS Lambda function to identify and delete objects in the S3 bucket that have not been accessed for 60 days. Create an Amazon EventBridge scheduled rule that runs every day to invoke the Lambda function.
- B. Create a new S3 bucket. Configure the new S3 bucket to use S3 Intelligent-Tiering. Copy the objects to the new S3 bucket.
- C. Create an S3 Lifecycle configuration for each S3 bucket prefix for each project. Set the S3 Lifecycle configurations to expire objects after 60 days.
- D. Create an AWS Lambda function to delete objects that have not been accessed for 60 days. Create an S3 event notification for S3 Intelligent-Tiering automatic archival events to invoke the Lambda function.

Correct Answer: *C*
Reference:
https://docs.aws.amazon.com/AmazonS3/latest/userguide/lifecycle-configuration-examples.html#lifecycle-config-conceptual-ex3

Question:119

A company has AWS accounts that are in an organization in AWS Organizations. An Amazon S3 bucket in one of the accounts is publicly accessible.

A security engineer must change the configuration so that the S3 bucket is no longer publicly accessible. The security engineer also must ensure that the S3 bucket cannot be made publicly accessible in the future.

Which solution will meet these requirements?

- A. Configure the S3 bucket to use an AWS Key Management Service (AWS KMS) key. Encrypt all objects in the S3 bucket by creating a bucket policy that enforces encryption. Configure an SCP to deny the s3:GetObject action for the OU that contains the AWS account.
- B. Enable the PublicAccessBlock configuration on the S3 bucket. Configure an SCP to deny the s3:GetObject action for the OU that contains the AWS account.
- C. Enable the PublicAccessBlock configuration on the S3 bucket. Configure an SCP to deny the s3:PutPublicAccessBlock action for the OU that contains the AWS account.
- D. Configure the S3 bucket to use S3 Object Lock in governance mode. Configure an SCP to deny the s3:PutPublicAccessBlock action for the OU that contains the AWS account.

Correct Answer: *C*
Enable PublicAccessBlock Configuration:
https://aws.amazon.com/s3/features/block-public-access/?nc1=h_ls
Explanation:
Configure an SCP (Service Control Policy):
An SCP is a policy that you can attach to an AWS Organization, organizational unit (OU), or an account. It acts as a guardrail to control permissions across accounts. In your case, you want to deny the s3:PutPublicAccessBlock action for the OU containing your AWS account.
Go to the AWS Organizations console.

Navigate to the OU that contains your account.
Create a new SCP or edit an existing one.
Add a statement that denies the s3:PutPublicAccessBlock action for the relevant S3 buckets.
Attach the SCP to the OU.
Ensure that your AWS account is part of the OU.

Question:120 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

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 settings 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.

Correct Answer: *AC*

Question:121 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

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.

Correct Answer: *BC*
Reference:
Download the updated SAML metadata file from your identity service provider, then update it in AWS.
https://docs.aws.amazon.com/IAM/latest/UserGuide/troubleshoot_saml.html#troubleshoot_saml_invalid-metadata

Question:122 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company is implementing a new application in a new AWS account. A VPC and subnets have been created for the application. The application has been peered to an existing VPC in another account in the same AWS Region for database access Amazon EC2 instances will regularly be created and terminated in the application VPC, but only some of them will need access to the databases in the peered VPC over TCP port 1521. A security engineer must ensure that only the EC2 instances that need access to the databases can access them through the network.

How can the security engineer implement this solution?

- A. Create a new security group in the database VPC and create an inbound rule that allows all traffic from the IP address range of the application VPC. Add a new network ACL rule on the database subnets. Configure the rule to TCP port 1521 from the IP address range of the application VPC. Attach the new security group to the database instances that the application instances need to access.
- B. Create a new security group in the application VPC with an inbound rule that allows the IP address range of the database VPC over TCP port 1521. Create a new security group in the database VPC with an inbound rule that allows the IP address range of the application VPC over port 1521. Attach the new security group to the database instances and the application instances that need database access.
- C. Create a new security group in the application VPC with no inbound rules. Create a new security group in the database VPC with an inbound rule that allows TCP port 1521 from the new application security group in the application VPAttach the application security group to the application instances that need database access and attach the database security group to the database instances.
- D. Create a new security group in the application VPC with an inbound rule that allows the IP address range of the database VPC over TCP port 1521. Add a new network ACL rule on the database subnets. Configure the rule to allow all traffic from the IP address range of the application VPC. Attach the new security group to the application instances that need database access.

Correct Answer: *C*
Explanation:
The VPCs are peered, so you can reference security groups in other VPCs:
https://docs.aws.amazon.com/vpc/latest/peering/vpc-peering-security-groups.html

Question:123

A company needs a forensic-logging solution for hundreds of applications running in Docker on Amazon EC2. The solution must perform real-time analytics on the logs, must support the replay of messages, and must persist the logs.

Which AWS services should be used to meet these requirements? (Choose two.)

- A. Amazon Athena
- B. Amazon Kinesis
- C. Amazon SQS
- D. Amazon OpenSearch Service
- E. Amazon EMR

Correct Answer: *BD*
Reference:
Kinesis for forensic analysis and OpenSearch for discovery and processing
https://docs.aws.amazon.com/opensearch-service/latest/developerguide/what-is.html

Question:124

A company has many member accounts in an organization in AWS Organizations. The company is concerned about the potential for misuse of the AWS account root user credentials for member accounts in the organization. To address this potential misuse, the company wants to ensure that even if the account root user credentials are compromised the account is still protected.

Which solution will meet this requirement?

- A. Block service access by using SCPs for the root user
- B. Remove the password for the root user
- C. Delete access keys for the root user
- D. Create an Amazon EventBridge rule to detect any AWS account root user API events

Correct Answer: *A*
Reference:
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_examples_general.html#example-scp-root-user

Question:125 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

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.

Correct Answer: *A*
Explanation:
The problem is with the ec2 instance not being able to publish logs from the cloudwatch agent running on the instance and not really to do with the autoscaling service role. The auto scaling service role will instead require the following Create, describe, modify, and delete CloudWatch alarms for scaling policies and retrieve metrics used for predictive scaling.
Reference:
https://docs.aws.amazon.com/autoscaling/ec2/userguide/autoscaling-service-linked-role.html#service-linked-role-permissions

Question:126 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company uses Amazon Elastic Container Service (Amazon ECS) containers that have the Fargate launch type. The containers run web and mobile applications that are written in Java and Node.js. To meet network segmentation requirements, each of the company's business units deploys applications in its own dedicated AWS account. Each business unit stores container images in an Amazon Elastic Container Registry (Amazon ECR) private registry in its own account.

A security engineer must recommend a solution to scan ECS containers and ECR registries for vulnerabilities in operating systems and programming language libraries. The company's audit team must be able to identify potential vulnerabilities that exist in any of the accounts where applications are deployed.

Which solution will meet these requirements?

- A. In each account, update the ECR registry to use Amazon Inspector instead of the default scanning service. Configure Amazon Inspector to forward vulnerability findings to AWS Security Hub in a central security account. Provide access for the audit team to use Security Hub to review the findings.
- B. In each account, configure AWS Config to monitor the configuration of the ECS containers and the ECR registry. Configure AWS Config conformance packs for vulnerability scanning. Create an AWS Config aggregator in a central account to collect configuration and compliance details from all accounts. Provide the audit team with access to AWS Config in the account where the aggregator is configured.
- C. In each account, configure AWS Audit Manager to scan the ECS containers and the ECR registry. Configure Audit Manager to forward vulnerability findings to AWS Security Hub in a central security account. Provide access for the audit team to use Security Hub to review the findings.

- D. In each account, configure Amazon GuardDuty to scan the ECS containers and the ECR registry. Configure GuardDuty to forward vulnerability findings to AWS Security Hub in a central security account. Provide access for the audit team to use Security Hub to review the findings.

Correct Answer: *A*
Explanation:
Amazon Inspector: Amazon Inspector is a tool specifically designed to scan containers and registries for vulnerabilities in operating systems and programming language libraries.

Integration with AWS Security Hub: Configuring Amazon Inspector to send vulnerability findings to AWS Security Hub in a central security account allows for centralized visibility and facilitates access for the audit team to review the findings.

Account configuration: Updating each ECR registry in each account to use Amazon Inspector ensures that all registries and containers are properly scanned in each business account.

Question:127 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***
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.

Correct Answer: *A*

Question:128 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***
A company hosts an application on Amazon EC2 that is subject to specific rules for regulatory compliance. One rule states that traffic to and from the workload must be inspected for network-level attacks. This involves inspecting the whole packet.

To comply with this regulatory rule, a security engineer must install intrusion detection software on a c5n.4xlarge EC2 instance. The engineer must then configure the software to monitor traffic to and from the application instances.

What should the security engineer do next?
- A. Place the network interface in promiscuous mode to capture the traffic
- B. Configure VPC Flow Logs to send traffic to the monitoring EC2 instance using a Network Load Balancer.
- C. Configure VPC traffic mirroring to send traffic to the monitoring EC2 instance using a Network Load Balancer.
- D. Use Amazon Inspector to detect network-level attacks and trigger an AWS Lambda function to send the suspicious packets to the EC2 instance.

Correct Answer: *C*
Reference:
https://aws.amazon.com/blogs/aws/new-vpc-traffic-mirroring/

Question:129 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company deploys a distributed web application on a fleet of Amazon EC2 instances. The fleet is behind an Application Load Balancer (ALB) that will be configured to terminate the TLS connection. All TLS traffic to the ALB must stay secure, even if the certificate private key is compromised.

How can a security engineer meet this requirement?

- A. Create an HTTPS listener that uses a certificate that is managed by AWS Certificate Manager (ACM).
- B. Create an HTTPS listener that uses a security policy that uses a cipher suite with perfect forward secrecy (PFS).
- C. Create an HTTPS listener that uses the Server Order Preference security feature.
- D. Create a TCP listener that uses a custom security policy that allows only cipher suites with perfect forward secrecy (PFS).

Correct Answer: *B*
Explanation:
Perfect Forward Secrecy (PFS): This is the key feature that addresses the security requirement. PFS ensures that even if the private key is compromised in the future, past communications cannot be decrypted. This meets the requirement that "All TLS traffic to the ALB must stay secure, even if the certificate private key is compromised."
Reference:
https://aws.amazon.com/blogs/aws/elastic-load-balancing-perfect-forward-secrecy-and-other-security-enhancements/

Question:130 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

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.

Correct Answer: *A*
Reference:
https://aws.amazon.com/blogs/mt/monitor-changes-and-auto-enable-logging-in-aws-cloudtrail/

Question:131 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company wants to create a log analytics solution for logs generated from its on-premises devices. The logs are collected from the devices onto a server on premises. The company wants to use AWS services to perform near real-time log analysis. The company also wants to store these logs for 365 days for pattern matching and substring search capabilities later.

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

- A. Install Amazon Kinesis Agent on the on-premises server to send the logs to Amazon DynamoDB. Configure an AWS Lambda trigger on DynamoDB streams to perform near real-time log analysis. Export the DynamoDB data to Amazon S3 periodically. Run Amazon Athena queries for pattern matching and substring search. Set up S3 Lifecycle policies to delete the log data after 365 days.

- B. Install Amazon Managed Streaming for Apache Kafka (Amazon MSK) on the on-premises server. Create an MSK cluster to collect the streaming data and analyze the data in real time. Set the data retention period to 365 days to store the logs persistently for pattern matching and substring search.
- C. Install Amazon Kinesis Agent on the on-premises server to send the logs to Amazon Kinesis Data Firehose. Configure Amazon Managed Service for Apache Flink (previously known as Amazon Kinesis Data Analytics) as the destination for real-time processing. Store the logs in Amazon OpenSearch Service for pattern matching and substring search. Configure an OpenSearch Service Index State Management (ISM) policy to delete the data after 365 days.
- D. Use Amazon API Gateway and AWS Lambda to write the logs from the on-premises server to Amazon DynamoDB. Configure a Lambda trigger on DynamoDB streams to perform near real-time log analysis. Run Amazon Athena federated queries on DynamoDB data for pattern matching and substring search. Set up TTL to delete data after 365 days.

Correct Answer: *C*
Explanation:
Pre-built tools: Leverages pre-built tools like Kinesis Agent for data collection and Firehose for delivery. Flink provides real-time processing capabilities without needing to build custom logic.

Managed Services: Utilizes managed services like OpenSearch Service which eliminates the need for manual provisioning and maintenance of an Elasticsearch cluster.

Automated Lifecycle Management: OpenSearch Service ISM policy automates data deletion after 365 days, reducing manual intervention.

Question:132 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company has a large fleet of Linux Amazon EC2 instances and Windows EC2 instances that run in private subnets. The company wants all remote administration to be performed as securely as possible in the AWS Cloud.

Which solution will meet these requirements?

- A. Do not use SSH-RSA private keys during the launch of new instances Implement AWS Systems Manager Session Manager
- B. Generate new SSH-RSA private keys for existing instances Implement AWS Systems Manager Session Manager
- C. Do not use SSH-RSA private keys during the launch of new instances Configure EC2 Instance Connect
- D. Generate new SSH-RSA private keys for existing instances Configure EC2 Instance Connect

Correct Answer: *A*
Explanation:
AWS SSM is for private entry in ec2 that doesnt require SSH keys
Reference:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/connect-linux-inst-eic.html

Question:133 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company has decided to move its fleet of Linux-based web server instances to an Amazon EC2 Auto Scaling group. Currently, the instances are static and are launched manually. When an administrator needs to view log files, the administrator uses SSH to establish a connection to the instances and retrieves the logs manually.

The company often needs to query the logs to produce results about application sessions and user issues. The company does not want its new automatically scaling architecture to result in the loss of any log files when instances are scaled in.

Which combination of steps should a security engineer take to meet these requirements MOST cost-effectively? (Choose two.)

- A. Configure a cron job on the instances to forward the log files to Amazon S3 periodically.

- B. Configure AWS Glue and Amazon Athena to query the log files.
- C. Configure the Amazon CloudWatch agent on the instances to forward the logs to Amazon CloudWatch Logs.
- D. Configure Amazon CloudWatch Logs Insights to query the log files.
- E. Configure the instances to write the logs to an Amazon Elastic File System (Amazon EFS) volume.

Correct Answer: *CD*
Explanation:
Configure the Amazon CloudWatch agent on the instances to forward the logs to Amazon CloudWatch Logs:
This approach ensures that log files are automatically collected and stored in Amazon CloudWatch Logs, which can be queried using CloudWatch Logs Insights. This method is cost-effective because it leverages Amazon CloudWatch, which is included in the cost of running EC2 instances.

Configure CloudWatch Logs Insights to query the log files:
CloudWatch Logs Insights is a fully managed service that allows you to query and analyze log data in real-time. It is integrated with Amazon CloudWatch Logs, making it a natural choice for querying log files.

Question:134 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company uses an external identity provider to allow federation into different AWS accounts. A security engineer for the company needs to identify the federated user that terminated a production Amazon EC2 instance a week ago.

What is the FASTEST way for the security engineer to identify the federated user?

- A. Review the AWS CloudTrail event history logs in an Amazon S3 bucket and look for the TerminateInstances event to identify the federated user from the role session name.
- B. Filter the AWS CloudTrail event history for the TerminateInstances event and identify the assumed IAM role. Review the AssumeRoleWithSAML event call in CloudTrail to identify the corresponding username.
- C. Search the AWS CloudTrail logs for the TerminateInstances event and note the event time. Review the IAM Access Advisor tab for all federated roles. The last accessed time should match the time when the instance was terminated.
- D. Use Amazon Athena to run a SQL query on the AWS CloudTrail logs stored in an Amazon S3 bucket and filter on the TerminateInstances event. Identify the corresponding role and run another query to filter the AssumeRoleWithWebIdentity event for the user name.

Correct Answer: *B*
Reference:
https://aws.amazon.com/blogs/security/how-to-easily-identify-your-federated-users-by-using-aws-cloudtrail/

Question:135 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

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

Which of the following troubleshooting steps should be performed?

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

Correct Answer: *B*

Question:136 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company has an application that needs to get objects from an Amazon S3 bucket. The application runs on Amazon EC2 instances.

All the objects in the S3 bucket are encrypted with an AWS Key Management Service (AWS KMS) customer managed key. The resources in the VPC do not have access to the internet and use a gateway VPC endpoint to access Amazon

S3.

The company discovers that the application 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 instances does not allow the s3:ListBucket action for the S3 bucket.
- B. The IAM instance profile that is attached to the EC2 instances does not allow the s3:ListParts action for the S3 bucket.
- C. The KMS key policy that encrypts the objects 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 objects in the S3 bucket does not allow the kms:Decrypt action to the EC2 instance profile ARN.
- E. The S3 bucket policy does not allow access from the gateway VPC endpoint.
- F. The security group that is attached to the EC2 instances is missing an inbound rule from the S3 managed prefix list over port 443.

Correct Answer: *ADE*

Question:137 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company runs workloads in the us-east-1 Region. The company has never deployed resources to other AWS Regions and does not have any multi-Region resources. The company needs to replicate its workloads and infrastructure to the us-west-1 Region.

A security engineer must implement a solution that uses AWS Secrets Manager to store secrets in both Regions. The solution must use AWS Key Management Service (AWS KMS) to encrypt the secrets. The solution must minimize latency and must be able to work if only one Region is available.

The security engineer uses Secrets Manager to create the secrets in us-east-1.

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

- A. Encrypt the secrets in us-east-1 by using an AWS managed KMS key. Replicate the secrets to us-west-1. Encrypt the secrets in us-west-1 by using a new AWS managed KMS key in us-west-1.
- B. Encrypt the secrets in us-east-1 by using an AWS managed KMS key. Configure resources in us-west-1 to call the Secrets Manager endpoint in us-east-1.
- C. Encrypt the secrets in us-east-1 by using a customer managed KMS key. Configure resources in us-west-1 to call the Secrets Manager endpoint in us-east-1.
- D. Encrypt the secrets in us-east-1 by using a customer managed KMS key. Replicate the secrets to us-west-1. Encrypt the secrets in us-west-1 by using the customer managed KMS key from us-east-1.

Correct Answer: *D*

Explanation:

Customer Managed KMS Key:

Encrypting secrets in us-east-1 with a customer managed KMS key allows greater control over key rotation policies and permissions, ensuring higher security and compliance.

Replication of secrets to us-west-1:

Replicating the secrets to us-west-1 ensures that the secrets are available in both regions, meeting the requirement to function even if only one region is available.

Using the same customer managed KMS key in us-west-1:

Encrypting the secrets in us-west-1 using the KMS key from us-east-1 ensures consistency in encryption and secret management across regions. Additionally, this can help minimize latency, as the same key is used for both regions, making the replication process more efficient.

Question:138 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company is using an AWS Key Management Service (AWS KMS) AWS owned key in its application to encrypt files in an AWS account. The company's security team wants the ability to change to new key material for new files whenever a potential key breach occurs. A security engineer must implement a solution that gives the security team the ability to change the key whenever the team wants to do so.

Which solution will meet these requirements?

- A. Create a new customer managed key. Add a key rotation schedule to the key. Invoke the key rotation schedule every time the security team requests a key change.
- B. Create a new AWS managed key. Add a key rotation schedule to the key. Invoke the key rotation schedule every time the security team requests a key change.
- C. Create a key alias. Create a new customer managed key every time the security team requests a key change. Associate the alias with the new key.
- D. Create a key alias. Create a new AWS managed key every time the security team requests a key change. Associate the alias with the new key.

Correct Answer: *C*

Explanation:

According to AWS documentation:

Customer managed keys provide full control over the lifecycle, including the ability to rotate and change the key material. Key aliases allow you to abstract the underlying key from the application, making it easier to switch to a new key without changing the application code. AWS owned keys and AWS managed keys do not provide the same level of control for key rotation and material changes as customer managed keys. By creating a key alias and associating it with a new customer managed key each time the security team requests a key change, you ensure that the encryption uses fresh key material while maintaining seamless integration with your application.

Question:139 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A security engineer needs to set up an Amazon CloudFront distribution for an Amazon S3 bucket that hosts a static website. The security engineer must allow only specified IP addresses to access the website. The security engineer also must prevent users from accessing the website directly by using S3 URLs.

Which solution will meet these requirements?

- A. Generate an S3 bucket policy. Specify cloudfront.amazonaws.com as the principal. Use the aws:SourceIp condition key to allow access only if the request comes from the specified IP addresses.
- B. Create a CloudFront origin access control (OAC). Create the S3 bucket policy so that only the OAC has access. Create an AWS WAF web ACL, and add an IP set rule. Associate the web ACL with the CloudFront distribution.
- C. Implement security groups to allow only the specified IP addresses access and to restrict S3 bucket access by using the CloudFront distribution.
- D. Create an S3 bucket access point to allow access from only the CloudFront distribution. Create an AWS WAF web ACL and add an IP set rule. Associate the web ACL with the CloudFront distribution.

Correct Answer: *B*

Question:140 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

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 the scripts have completed.

Correct Answer: ***B***

Explanation:
Using AWS Systems Manager Parameter Store with encrypted string parameters and IAM roles ensures that sensitive information is securely stored, managed, and accessed only by authorized instances. This approach minimizes the risk of exposure and simplifies the management of sensitive data.

Question:141 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company has a VPC that has no internet access and has the private DNS hostnames option enabled. An Amazon Aurora database is running inside the VPC. A security engineer wants to use AWS Secrets Manager to automatically rotate the credentials for the Aurora database. The security engineer configures the Secrets Manager default AWS Lambda rotation function to run inside the same VPC that the Aurora database uses. However, the security engineer determines that the password cannot be rotated properly because the Lambda function cannot communicate with the Secrets Manager endpoint.

What is the MOST secure way that the security engineer can give the Lambda function the ability to communicate with the Secrets Manager endpoint?

- A. Add a NAT gateway to the VPC to allow access to the Secrets Manager endpoint.
- B. Add a gateway VPC endpoint to the VPC to allow access to the Secrets Manager endpoint.
- C. Add an interface VPC endpoint to the VPC to allow access to the Secrets Manager endpoint.
- D. Add an internet gateway for the VPC to allow access to the Secrets Manager endpoint.

Correct Answer: *C*
Reference:
"You can establish a private connection between your VPC and Secrets Manager by creating an interface VPC endpoint."
https://docs.aws.amazon.com/secretsmanager/latest/userguide/vpc-endpoint-overview.html

Question:142 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company has two AWS accounts: Account A and Account B. Each account has a VPC. An application that runs in the VPC in Account A needs to write to an Amazon S3 bucket in Account B. The application in Account A already has permission to write to the S3 bucket in Account B.

The application and the S3 bucket are in the same AWS Region. The company cannot send network traffic over the public internet.

Which solution will meet these requirements?

- A. In both accounts, create a transit gateway and VPC attachments in a subnet in each Availability Zone. Update the VPC route tables.
- B. Deploy a software VPN appliance in Account A. Create a VPN connection between the software VPN appliance and a virtual private gateway in Account B.
- C. Create a VPC peering connection between the VPC in Account A and the VPC in Account B. Update the VPC route tables, network ACLs, and security groups to allow network traffic between the peered IP ranges
- D. In Account A, create a gateway VPC endpoint for Amazon S3. Update the VPC route table in Account A.

Correct Answer: *D*
Explanation:
However, gateway endpoints do not allow access from on-premises networks, from peered VPCs in other AWS Regions, or through a transit gateway. For those scenarios, you must use an interface endpoint, which is available for an additional cost.
Reference:
https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints-s3.html

Question:143 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A security engineer receives a notice about suspicious activity from a Linux-based Amazon EC2 instance that uses Amazon Elastic Block Store (Amazon EBS)-based storage. The instance is making connections to known malicious addresses.

The instance is in a development account within a VPC that is in the us-east-1 Region. The VPC contains an internet gateway and has a subnet in us-east-1a and us-east-1b. Each subnet is associate with a route table that uses the internet gateway as a default route. Each subnet also uses the default network ACL. The suspicious EC2 instance runs within the us-east-1b subnet. During an initial investigation, a security engineer discovers that the suspicious instance is the only instance that runs in the subnet.

Which response will immediately mitigate the attack and help investigate the root cause?

- A. Log in to the suspicious instance and use the netstat command to identify remote connections. Use the IP addresses from these remote connections to create deny rules in the security group of the instance. Install diagnostic tools on the instance for investigation. Update the outbound network ACL for the subnet in us-east-1b to explicitly deny all connections as the first rule during the investigation of the instance.
- B. Update the outbound network ACL for the subnet in us-east-1 b to explicitly deny all connections as the first rule. Replace the security group with a new security group that allows connections only from a diagnostics security group. Update the outbound network ACL for the us-east-1 b subnet to remove the deny all rule. Launch a new EC2 instance that has diagnostic tools. Assign the new security group to the new EC2 instance. Use the new EC2 instance to investigate the suspicious instance.
- C. Ensure that the Amazon Elastic Block Store (Amazon EBS) volumes that are attached to the suspicious EC2 instance will not delete upon termination. Terminate the instance. Launch a new EC2 instance in us-east-1a that has diagnostic tools. Mount the EBS volumes from the terminated instance for investigation.
- D. Create an AWS WAF web ACL that denies traffic to and from the suspicious instance. Attach the AWS WAF web ACL to the instance to mitigate the attack. Log in to the instance and install diagnostic tools to investigate the instance.

Correct Answer: *B*

Question:144 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

An online media company has an application that customers use to watch events around the world. The application is hosted on a fleet of Amazon EC2 instances that run Amazon Linux 2. The company uses AWS Systems Manager to manage the EC2 instances. The company applies patches and application updates by using the AWS-AmazonLinux2DefaultPatchBaseline patching baseline in Systems Manager Patch Manager.

The company is concerned about potential attacks on the application during the week of an upcoming event. The company needs a solution that can immediately deploy patches to all the EC2 instances in response to a security incident or vulnerability. The solution also must provide centralized evidence that the patches were applied successfully.

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

- A. Create a new patching baseline in Patch Manager. Specify Amazon Linux 2 as the product. Specify Security as the classification. Set the automatic approval for patches to 0 days. Ensure that the new patching baseline is the designated default for Amazon Linux 2.
- B. Use the Patch Now option with the scan and install operation in the Patch Manager console to apply patches against the baseline to all nodes. Specify an Amazon S3 bucket as the patching log storage option.
- C. Use the Clone function of Patch Manager to create a copy of the AWS-AmazonLmux2DefaultPatchBaseline built-in baseline. Set the automatic approval for patches to 1 day.
- D. Create a patch policy that patches all managed nodes and sends a patch operation log output to an Amazon S3 bucket. Use a custom scan schedule to set Patch Manager to check every hour for new patches. Assign the baseline to the patch policy.
- E. Use Systems Manager Application Manager to inspect the package versions that were installed on the EC2 instances. Additionally use Application Manager to validate that the patches were correctly installed.

Correct Answer: *AB*

Explanation:

A: Creating a new patching baseline with the specific settings ensures that security patches are automatically approved without delay (0 days). This immediate approval is crucial during a security incident when rapid patch deployment is necessary. Making this baseline the designated default for Amazon Linux 2 ensures that it is applied consistently across all instances.

B: Using the Patch Now option with the scan and install operation ensures that patches are deployed immediately to all EC2 instances. By specifying an Amazon S3 bucket for log storage, the company can centrally store and review logs to provide evidence that the patches were applied successfully. This meets the requirement for centralized evidence of successful patch application.

Question:145 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A developer operations team uses AWS Identity and Access Management (IAM) to manage user permissions. The team created an Amazon EC2 instance profile role that uses an AWS managed ReadOnlyAccess policy. When an application that is running on Amazon EC2 tries to read a file from an encrypted Amazon S3 bucket, the application receives an AccessDenied error.

The team administrator has verified that the S3 bucket policy allows everyone in the account to access the S3 bucket. There is no object ACL that is attached to the file.

What should the administrator do to fix the IAM access issue?

- A. Edit the ReadOnlyAccess policy to add kms:Decrypt actions
- B. Add the EC2 IAM role as the authorized Principal to the S3 bucket policy
- C. Attach an inline policy with kms:Decrypt permissions to the IAM role
- D. Attach an inline policy with S3:* permissions to the IAM role

Correct Answer: *C*

Question:146 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company uses AWS Organizations and has Amazon Elastic Kubernetes Service (Amazon EKS) clusters in many AWS accounts. A security engineer integrates Amazon EKS with AWS CloudTrail. The CloudTrail trails are stored in an Amazon S3 bucket in each account to monitor API calls. The security engineer observes that CloudTrail logs are not displaying Kubernetes pod creation events.

What should the security engineer do to view the Kubernetes events from Amazon CloudWatch?

- A. Configure the EKS clusters to use private S3 VPC endpoints. Configure the S3 buckets for logging.
- B. Enable Kubernetes API server component logs for each cluster.
- C. Enable cross-origin resource sharing (CORS) in the S3 bucket that is used for logging.
- D. Configure CloudWatch. View the events in the CloudWatch console.

Correct Answer: *B*

Explanation:

The security engineer should enable Kubernetes API server component logs for each cluster. This is because the API server component logs contain details about the Kubernetes events such as pod creation, which are not included in the AWS CloudTrail logs. Once these logs are enabled, they can be viewed from Amazon CloudWatch.

Question:147 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A security engineer needs to build a solution to turn AWS CloudTrail back on in multiple AWS Regions in case it is ever turned off.

What is the MOST efficient way to implement this solution?

- A. Use AWS Config with a managed rule to initiate the AWS-EnableCloudTrail remediation.
- B. Create an Amazon EventBridge event with a cloudtrail.amazonaws.com event source and a StartLogging event name to invoke an AWS Lambda function to call the StartLogging
  API.
- C. Create an Amazon CloudWatch alarm with a cloudtrail.amazonaws.com event source and a StopLoggmg event name to invoke an AWS Lambda function to call the StartLogging API.
- D. Monitor AWS Trusted Advisor to ensure CloudTrail logging is enabled.

Correct Answer: *A*

Explanation:

The most efficient way to implement this solution is to use AWS Config with a managed rule to initiate the AWS-EnableCloudTrail remediation. This will automatically turn AWS CloudTrail back on if it is ever turned off.

Reference:

https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/automatically-re-enable-aws-cloudtrail-by-using-a-custom-remediation-rule-in-aws-config.html

Question:148 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

An ecommerce company is developing new architecture for an application release. The company needs to implement TLS for incoming traffic to the application. Traffic for the application will originate from the internet. TLS does not have to be implemented in an end-to-end configuration because the company is concerned about impacts on performance The incoming traffic types will be HTTP and HTTPS The application uses ports 80 and 443.

What should a security engineer do to meet these requirements?

- A. Create a public Application Load Balancer. Create two listeners: one listener on port 80 and one listener on port 443. Create one target group. Create a rule to forward traffic from port 80 to the listener on port 443. Provision a public TLS certificate in AWS Certificate Manager (ACM). Attach the certificate to the listener on port 443.
- B. Create a public Application Load Balancer. Create two listeners one listener on port 80 and one listener on port 443. Create one target group. Create a rule to forward traffic from port 80 to the listener on port 443. Provision a public TLS certificate in AWS Certificate Manager (ACM). Attach the certificate to the listener on port 80.
- C. Create a public Network Load Balancer. Create two listeners one listener on port 80 and one listener on port 443. Create one target group. Create a rule to forward traffic from port 80 to the listener on port 443. Set the protocol for the listener on port 443 to TLS.
- D. Create a public Network Load Balancer. Create a listener on port 443. Create one target group. Create a rule to forward traffic from port 443 to the target group. Set the protocol for the listener on port 443 to TLS.

Correct Answer: *A*

Explanation:

The security engineer should create a public Application Load Balancer, create two listeners (one on port 80 and one on port 443), create one target group, and create a rule to forward traffic from port 80 to the listener on port 443. Then, they should provision a public TLS certificate in AWS Certificate Manager (ACM) and attach the certificate to the listener on port 443. This setup will implement TLS for incoming traffic to the application, without requiring an end-to-end configuration.

Question:149 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company needs a solution to protect critical data from being permanently deleted. The data is stored in Amazon S3 buckets.

The company needs to replicate the S3 objects from the company's primary AWS Region to a secondary Region to meet disaster recovery requirements. The company must also ensure that users who have administrator access cannot permanently delete the data in the secondary Region.

Which solution will meet these requirements?

- A. Configure AWS Backup to perform cross-Region S3 backups. Select a backup vault in the secondary Region. Enable AWS Backup Vault Lock in governance mode for the backups in the secondary Region.
- B. Implement S3 Object Lock in compliance mode in the primary Region. Configure S3 replication to replicate the objects to an S3 bucket in the secondary Region.
- C. Configure S3 replication to replicate the objects to an S3 bucket in the secondary Region. Create an S3 bucket policy to deny the s3:ReplicateDelete action on the S3 bucket in the secondary Region.
- D. Configure S3 replication to replicate the objects to an S3 bucket in the secondary Region. Configure S3 object versioning on the S3 bucket in the secondary Region.

Correct Answer: *B*

Explanation:

S3 Object Lock in compliance mode prevents objects from being deleted or overwritten, even by administrators. This would ensure that once the data is replicated to the secondary Region, it cannot be permanently deleted. Object Lock is a perfect fit for protecting critical data against accidental or malicious deletion.

Reference:

https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock-managing.html#object-lock-managing-replication

Question:150 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company in France uses Amazon Cognito with the Cognito Hosted UI as an identity broker for sign-in and sign-up processes. The company is marketing an application and expects that all the application’s users will come from France.

When the company launches the application, the company’s security team observes fraudulent sign-ups for the application. Most of the fraudulent registrations are from users outside of France.

The security team needs a solution to perform custom validation at sign-up. Based on the results of the validation, the solution must accept or deny the registration request.

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

- A. Create a pre sign-up AWS Lambda trigger. Associate the Amazon Cognito function with the Amazon Cognito user pool.
- B. Use a geographic match rule statement to configure an AWS WAF web ACL Associate the web ACL with the Amazon Cognito user pool.
- C. Configure an app client for the application's Amazon Cognito user pool. Use the app client ID to validate the requests in the hosted UI.
- D. Update the application’s Amazon Cognito user pool to configure a geographic restriction setting.
- E. Use Amazon Cognito to configure a social identity provider (IdP) to validate the requests on the hosted UI.

Correct Answer: *AB*
Explanation:
A. Create a pre sign-up AWS Lambda trigger. Associate the Amazon Cognito function with the Amazon Cognito user pool.

This allows the team to perform custom validation during the sign-up process. The Lambda function can include logic to check the geographic location of the sign-up request and accept or deny it based on whether it originates from France.

B. Use a geographic match rule statement to configure an AWS WAF web ACL. Associate the web ACL with the Amazon Cognito user pool.

This adds an additional layer of security by using AWS WAF to block sign-up requests from outside France before they reach the Cognito user pool.

Question:151 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A security engineer is configuring AWS Config for an AWS account that uses a new IAM 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.

Correct Answer: *AB*

Question:152 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company is undergoing a layer 3 and layer 4 DDoS attack on its web servers running on AWS.

Which combination of AWS services and features will provide protection in this scenario? (Choose three.)

- A. Amazon Route 53
- B. AWS Certificate Manager (ACM)
- C. Amazon S3
- D. AWS Shield
- E. Network Load Balancer
- F. Amazon GuardDuty

Correct Answer: *ADE*

Question:153 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company wants to implement host-based security for Amazon EC2 instances and containers in Amazon Elastic Container Registry (Amazon ECR). The company has deployed AWS Systems Manager Agent (SSM Agent) on the EC2 instances. All the company's AWS accounts are in one organization in AWS Organizations. The company will analyze the workloads for software vulnerabilities and unintended network exposure. The company will push any findings to AWS Security Hub, which the company has configured for the organization.

The company must deploy the solution to all member accounts, including new accounts, automatically. When new workloads come online, the solution must scan the workloads.

Which solution will meet these requirements?

- A. Use SCPs to configure scanning of EC2 instances and ECR containers for all accounts in the organization.
- B. Configure a delegated administrator for Amazon GuardDuty for the organization. Create an Amazon EventBridge rule to initiate analysis of ECR containers
- C. Configure a delegated administrator for Amazon Inspector for the organization. Configure automatic scanning for new member accounts.
- D. Configure a delegated administrator for Amazon Inspector for the organization. Create an AWS Config rule to initiate analysis of ECR containers.

Correct Answer: *C*

Question:154 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company uses AWS Organizations to manage several AWS accounts. The company processes a large volume of sensitive data. The company uses a serverless approach to microservices. The company stores all the data in either Amazon S3 or Amazon DynamoDB. The company reads the data by using either AWS Lambda functions or container-based services that the company hosts on Amazon Elastic Kubernetes Service (Amazon EKS) on AWS Fargate.

The company must implement a solution to encrypt all the data at rest and enforce least privilege data access controls. The company creates an AWS Key Management Service (AWS KMS) customer managed key.

What should the company do next to meet these requirements?

- A. Create a key policy that allows the kms:Decrypt action only for Amazon S3 and DynamoDB. Create an SCP that denies the creation of S3 buckets and DynamoDB tables that are not encrypted with the key.
- B. Create an IAM policy that denies the kms:Decrypt action for the key. Create a Lambda function than runs on a schedule to attach the policy to any new roles. Create an AWS Config rule to send alerts for resources that are not encrypted with the key.
- C. Create a key policy that allows the kms:Decrypt action only for Amazon S3, DynamoDB, Lambda, and Amazon EKS. Create an SCP that denies the creation of S3 buckets and DynamoDB tables that are not encrypted with the key.
- D. Create a key policy that allows the kms:Decrypt action only for Amazon S3, DynamoDB, Lambda, and Amazon EKS. Create an AWS Config rule to send alerts for resources that are not encrypted with the key.

Correct Answer: *C*

Question:155 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

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 invoked 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 invoked was not current.

Correct Answer: *A*

Question:156 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company is worried about potential DDoS attacks. The company has a web application that runs on Amazon EC2 instances. The application uses Amazon S3 to serve static content such as images and videos.

A security engineer must create a resilient architecture that can withstand DDoS attacks.

Which solution will meet these requirements MOST cost-effectively?

- A. Create an Amazon CloudWatch alarm that invokes an AWS Lambda function when an EC2 instance’s CPU utilization reaches 90%. Program the Lambda function to update security groups that are attached to the EC2 instance to deny inbound ports 80 and 443.
- B. Put the EC2 instances into an Auto Scaling group behind an Elastic Load Balancing (ELB) load balancer. Use Amazon CioudFront with Amazon S3 as an origin.
- C. Set up a warm standby disaster recovery (DR) environment. Fail over to the warm standby DR environment if a DDoS attack is detected on the application.
- D. Subscribe to AWS Shield Advanced. Configure permissions to allow the Shield Response Team to manage resources on the company's behalf during a DDoS event.

Correct Answer: *B*

Question:157 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company uses an organization in AWS Organizations to manage hundreds of AWS accounts. Some of the accounts provide access to external AWS principals through cross-account IAM roles and Amazon S3 bucket policies.

The company needs to identify which external principals have access to which accounts.

Which solution will provide this information?

- A. Enable AWS Identity and Access Management Access Analyzer for the organization. Configure the organization as a zone of trust. Filter findings by AWS account ID.
- B. Create a custom AWS Config rule to monitor IAM roles in each account. Deploy an AWS Config aggregator to a central account. Filter findings by AWS account ID.
- C. Activate Amazon Inspector. Integrate Amazon Inspector with AWS Security Hub. Filter findings by AWS account ID for the IAM role resource type and the S3 bucket policy resource type.
- D. Configure the organization to use Amazon GuardDuty. Filter findings by AWS account ID for the Discovery:IAMUser/AnomalousBehavior finding type.

Correct Answer: *A*

Question:158 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company has AWS accounts in an organization in AWS Organizations. The company needs to install a corporate software package on all Amazon EC2 instances for all the accounts in the organization.

A central account provides base AMIs for the EC2 instances. The company uses AWS Systems Manager for software inventory and patching operations.

A security engineer must implement a solution that detects EC2 instances that do not have the required software. The solution also must automatically install the software if the software is not present.

Which solution will meet these requirements?

- A. Provide new AMIs that have the required software pre-installed. Apply a tag to the AMIs to indicate that the AMIs have the required software. Configure an SCP that allows new EC2 instances to be launched only if the instances have the tagged AMIs. Tag all existing EC2 instances.
- B. Configure a custom patch baseline in Systems Manager Patch Manager. Add the package name for the required software to the approved packages list. Associate the new patch baseline with all EC2 instances. Set up a maintenance window for software deployment.
- C. Centrally enable AWS Config. Set up the ec2-managedinstance-applications-required AWS Config rule for all accounts. Create an Amazon EventBridge rule that reacts to AWS Config events. Configure the EventBridge rule to invoke an AWS Lambda function that uses Systems Manager Run Command to install the required software.
- D. Create a new Systems Manager Distributor package for the required software. Specify the download location. Select all EC2 instances in the different accounts. Install the software by using Systems Manager Run Command.

Correct Answer: *C*

Question:159 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A development team is creating an open source toolset to manage a company's software as a service (SaaS) application. The company stores the code in a public repository so that anyone can view and download the toolset's code.

The company discovers that the code contains an IAM access key and secret key that provide access to internal resources in the company's AWS environment

A security engineer must implement a solution to identify whether unauthorized usage of the exposed credentials has occurred. The solution also must prevent any additional usage of the exposed credentials.

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

- A. Use AWS Identity and Access Management Access Analyzer to determine which resources the exposed credentials accessed and who used them.
- B. Deactivate the exposed IAM access key from the user's IAM account.
- C. Create a rule in Amazon GuardDuty to block the access key in the source code from being used.
- D. Create a new IAM access key and secret key for the user whose credentials were exposed.
- E. Generate an IAM credential report. Check the report to determine when the user that owns the access key last logged in.

Correct Answer: *AB*

Question:160 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company needs to create a centralized solution to analyze log files. The company uses an organization in AWS Organizations to manage its AWS accounts.

The solution must aggregate and normalize events from the following sources:

• The entire organization in Organizations
• All AWS Marketplace offerings that run in the company's AWS accounts
• The company's on-premises systems

Which solution will meet these requirements?

- A. Configure a centralized Amazon S3 bucket for the logs. Enable VPC Flow Logs, AWS CloudTrail. and Amazon Route 53 logs in all accounts. Configure all accounts to use the centralized S3 bucket. Configure AWS Glue crawlers to parse the log files. Use Amazon Athena to query the log data.
- B. Configure log streams in Amazon CloudWatch Logs for the sources that need monitoring Create log subscription filters for each log stream. Forward the messages to Amazon OpenSearch Service for analysis.
- C. Set up a delegated Amazon Security Lake administrator account in Organizations. Enable and configure Security Lake for the organization. Add the accounts that need monitoring. Use Amazon Athena to query the log data.
- D. Apply an SCP to configure all member accounts and services to deliver log files to a centralized Amazon S3 bucket. Use Amazon OpenSearch Service to query the centralized S3 bucket for log entries.

Correct Answer: *C*

Question:161 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company uses AWS Organizations. The company has more than 100 AWS accounts and will increase the number of accounts. The company also uses an external corporate identity provider (IdP).

The company needs to provide users with role-based access to the accounts. The solution must maximize scalability and operational efficiency.

Which solution will meet these requirements?

- A. In each account, create a set of dedicated IAM users. Ensure that all users assume these IAM users through federation with the existing IdP.
- B. Deploy an IAM role in a central identity account. Allow users to assume the role through federation with the existing IdP. In each account, deploy a set of IAM roles that match the desired access patterns. Include a trust policy that allows access from the central identity account. Edit the permissions policy for the role in each account to match user access requirements.
- C. Enable AWS IAM Identity Center. Integrate IAM Identity Center with the company's existing IdP. Create permission sets that match the desired access patterns. Assign permissions to match user access requirements.
- D. In each account, deploy a set of IAM roles that match the desired access patterns. Create a trust policy with the existing IdP. Update each role's permissions policy to use SAML-based IAM condition keys that are based on user access requirements.

Correct Answer: *C*

Question:162 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company has a web-based application that runs behind an Application Load Balancer (ALB). The application is experiencing a credential stuffing attack that is producing many failed login attempts. The attack is coming from many IP addresses. The login attempts are using a user agent string of a known mobile device emulator.

A security engineer needs to implement a solution to mitigate the credential stuffing attack. The solution must still allow legitimate logins to the application.

Which solution will meet these requirements?

- A. Create an Amazon CloudWatch alarm that reacts to login attempts that contain the specified user agent string Add an Amazon Simple Notification Service (Amazon SNS) topic to the alarm.
- B. Modify the inbound security group on the ALB to deny traffic from the IP addresses that are involved in the attack.
- C. Create an AWS WAF web ACL for the ALB Create a custom rule that blocks requests that contain the user agent string of the device emulator.
- D. Create an AWS WAF web ACL for the ALB. Create a custom rule that allows requests from legitimate user agent strings.

Correct Answer: *C*

Question:163 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company is investigating controls to protect sensitive data. The company uses Amazon Simple Notification Service (Amazon SNS) topics to publish messages from application components to custom logging services.

The company is concerned that an application component might publish sensitive data that will be accidentally exposed in transaction logs and debug logs.

Which solution will protect the sensitive data in these messages from accidental exposure?

- A. Use Amazon Made to scan the SNS topics for sensitive data elements in the SNS messages. Create an AWS Lambda function that masks sensitive data inside the messages when Macie records a new finding.
- B. Configure an inbound message data protection policy. In the policy, include the De-identify operation to mask the sensitive data inside the messages. Apply the policy to the SNS topics.
- C. Configure the SNS topics with an AWS Key Management Service (AWS KMS) customer managed key to encrypt the data elements inside the messages. Grant permissions to all message publisher IAM roles to allow access to the key to encrypt data.
- D. Create an Amazon GuardDuty finding for sensitive data that is transmitted to the SNS topics. Create an AWS Security Hub custom remediation action to block messages that contain sensitive data from being delivered to subscribers of the SNS topics.

Correct Answer: *B*

Question:164 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company has created a set of AWS Lambda functions to automate incident response steps for incidents that occur on Amazon EC2 instances. The Lambda functions need to collect relevant artifacts, such as instance ID and security group configuration. The Lambda functions must then write a summary to an Amazon S3 bucket.

The company runs its workloads in a VPC that uses public subnets and private subnets. The public subnets use an internet gateway to access the internet. The private subnets use a NAT gateway to access the internet.

All network traffic to Amazon S3 that is related to the incident response process must use the AWS network. This traffic must not travel across the internet.

Which solution will meet these requirements?

- A. Deploy the Lambda functions to a private subnet in the VPC. Configure the Lambda functions to access the S3 service through the NAT gateway.
- B. Deploy the Lambda functions to a private subnet in the VPC. Create an S3 gateway endpoint to access the S3 service.
- C. Deploy the S3 bucket and the Lambda functions in the same private subnet. Configure the Lambda functions to use the default endpoint for the S3 service.
- D. Deploy an Amazon Simple Queue Service (Amazon SQS) queue and the Lambda functions in the same private subnet. Configure the Lambda functions to send data to the SQS queue. Configure the SQS queue to send data to the S3 bucket.

Correct Answer: *B*

Question:165 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company uses an organization in AWS Organizations to manage its AWS accounts. The company has implemented an SCP in the root account to prevent resources from being shared with external accounts.

The company now needs to allow applications in its marketing team's AWS account to share resources with external accounts. The company must continue to prevent all the other accounts in the organization from sharing resources with external accounts. All the accounts in the organization are members of the same OU.

Which solution will meet these requirements?

- A. Create a new SCP in the marketing team's account Configure the SCP to explicitly allow resource sharing.
- B. Edit the existing SCP to add a Condition statement that excludes the marketing team's account.
- C. Edit the existing SCP to include an Allow statement that specifies the marketing team's account.

- D. Create an IAM permissions boundary policy to explicitly allow resource sharing Attach the policy to IAM users in the marketing team's account.

Correct Answer: *B*

Question:166 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A security administrator has enabled AWS Security Hub for all the AWS accounts in an organization in AWS Organizations. The security team wants near-real-time response and remediation for deployed AWS resources that do not meet security standards. All changes must be centrally logged for auditing purposes.

The organization has reached the quotas for the number of SCPs attached to an OU and SCP document size. The team wants to avoid making any changes to any of the SCPs. The solution must maximize scalability and cost-effectiveness.

Which combination of actions should the security administrator take to meet these requirements? (Choose three.)

- A. Create an AWS Config custom rule to detect configuration changes to AWS resources. Create an AWS Lambda function to remediate the AWS resources in the delegated administrator AWS account.
- B. Use AWS Systems Manager Change Manager to track configuration changes to AWS resources. Create a Systems Manager document to remediate the AWS resources in the delegated administrator AWS account.
- C. Create a Security Hub custom action to reference in an Amazon EventBridge event rule in the delegated administrator AWS account.
- D. Create an Amazon EventBridge event rule to Invoke an AWS Lambda function that will take action on AWS resources.
- E. Create an Amazon EventBridge event rule to invoke an AWS Lambda function that will evaluate AWS resource configuration for a set of API requests and create a finding for noncompllant AWS resources.
- F. Create an Amazon EventBridge event rule to invoke an AWS Lambda function on a schedule to assess specific AWS Config rules.

Correct Answer: *ACD*

Question:167 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A security engineer must Implement monitoring of a company's Amazon Aurora MySQL DB instances. The company wants to receive email notifications when unknown users try to log in to the database endpoint.

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

- A. Enable Amazon GuardDuty. Enable the Amazon RDS Protection feature in GuardDuty to detect login attempts by unknown users. Create an Amazon EventBridge rule to filter GuardDuty findings. Send email notifications by using Amazon Simple Notification Service (Amazon SNS).
- B. Enable the server_audit_loggIng parameter on the Aurora MySQL DB instances. Use AWS Lambda to periodically scan the delivered log files for login attempts by unknown users. Send email notifications by using Amazon Simple Notification Service (Amazon SNS).
- C. Create an Amazon RDS Custom AMI. Include a third-party security agent in the AMI to detect login attempts by unknown users. Deploy RDS Custom DB instances. Migrate data from the existing installation to the RDS Custom DB instances. Configure email notifications from the third-party agent.
- D. Write a stored procedure to detect login attempts by unknown users. Schedule a recurring job inside the database engine. Configure Aurora MySQL to use Amazon Simple Notification Service (Amazon SNS) to send email notifications.

Correct Answer: *A*

Question:168 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company runs a global ecommerce website that is hosted on AWS. The company uses Amazon CloudFront to serve content to its user base. The company wants to block inbound traffic from a specific set of countries to comply with recent data regulation policies.

Which solution will meet these requirements MOST cost-effectively?

- A. Create an AWS WAF web ACL with an IP match condition to deny the countries' IP ranges. Associate the

- web ACL with the CloudFront distribution.
- B. Create an AWS WAF web ACL with a geo match condition to deny the specific countries. Associate the web ACL with the CloudFront distribution.
- C. Use the geo restriction feature in CloudFront to deny the specific countries.
- D. Use geolocation headers in CloudFront to deny the specific countries.

Correct Answer: *C*

Question:169 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company deploys its application as a service on an Amazon Elastic Container Service (Amazon ECS) cluster with theAWS Fargate launch type. A security engineer suspects that some incoming requests are malicious. The security engineer needs to inspect the running container by retrieving log files and memory dump flies.

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

- A. Migrate the application to an ECS cluster with the Amazon EC2 launch type. Configure the EC2 instances with proper remote access. Log in and inspect the container.
- B. Update the application to dump the required data to STDOUT. Use the awslogs log driver to pass the logs to Amazon CloudWatch Logs. Examine the log files in CloudWatch Logs.
- C. Turn on Amazon CloudWatch Container Insights for the ECS cluster. Send the log data to Amazon CloudWatch Logs by using AWS Distro for OpenTelemetry. Examine the log data in CloudWatch Logs.
- D. Update the ECS task role with AWS Systems Manager permissions. Enable the ECS Exec feature for the ECS service. Use ECS Exec to inspect the container.

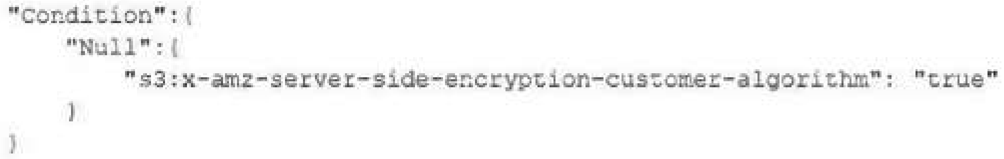
Correct Answer: *D*

Question:170 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

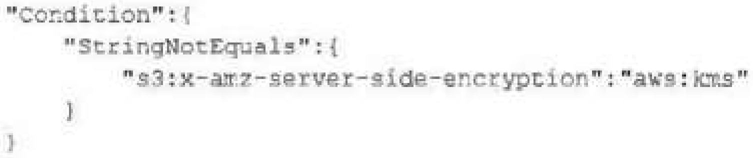
A company uses AWS Organizations and has many AWS accounts. The company has a new requirement to use server-side encryption with customer-provided keys (SSE-C) on all new object uploads to Amazon S3 buckets.

A security engineer is creating an SCP that includes a Deny effect for the s3:PutObject action.

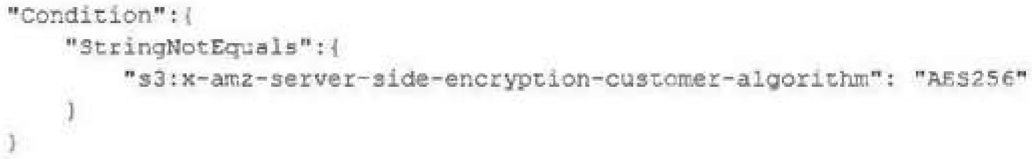
Which condition must the security engineer add to the SCP to enforce the new SSE-C requirement?

- A. 

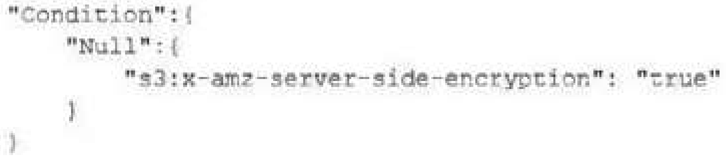
```
"Condition":{
    "Null":{
        "s3:x-amz-server-side-encryption-customer-algorithm": "true"
    }
}
```

- B. 

```
"Condition":{
    "StringNotEquals":{
        "s3:x-amz-server-side-encryption":"aws:kms"
    }
}
```

- C. 

```
"Condition":{
    "StringNotEquals":{
        "s3:x-amz-server-side-encryption-customer-algorithm": "AES256"
    }
}
```

- D. 

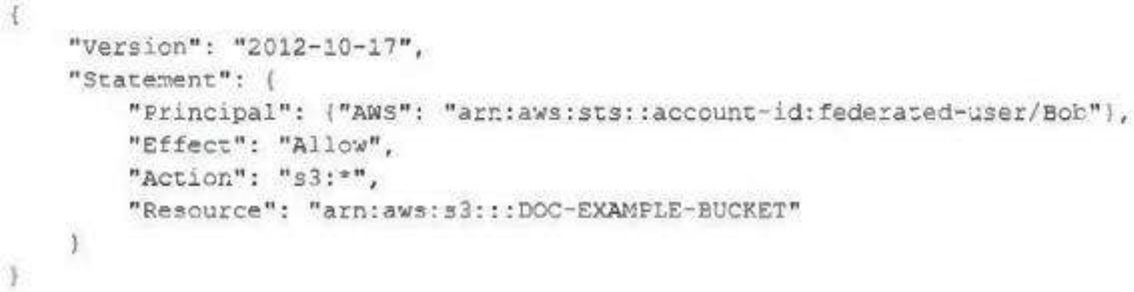
```
"Condition":{
    "Null":{
        "s3:x-amz-server-side-encryption": "true"
    }
}
```

Correct Answer: *A*

Question:171 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

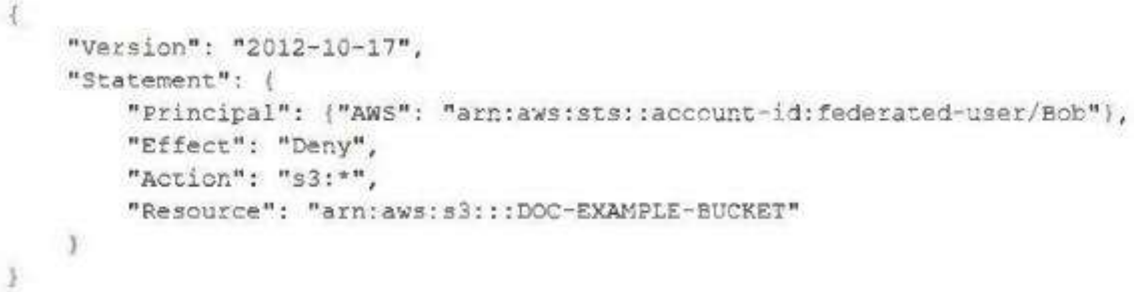
A company wants to deny a specific federated user named Bob access to an Amazon S3 bucket named DOC-EXAMPLE-BUCKET. The company wants to meet this requirement by using a bucket policy. The company also needs to ensure that this bucket policy affects Bob's S3 permissions only. Any other permissions that Bob has must remain intact.

Which policy should the company use to meet these requirements?



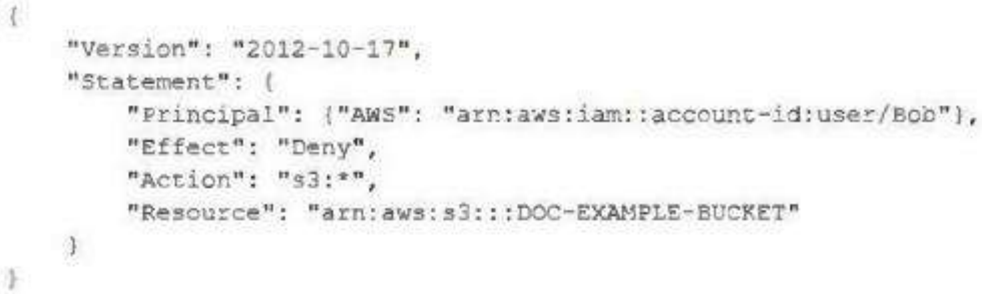
```
{
    "Version": "2012-10-17",
    "Statement": {
        "Principal": {"AWS": "arn:aws:sts::account-id:federated-user/Bob"},
        "Effect": "Allow",
        "Action": "s3:*",
        "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET"
    }
}
```

- A.



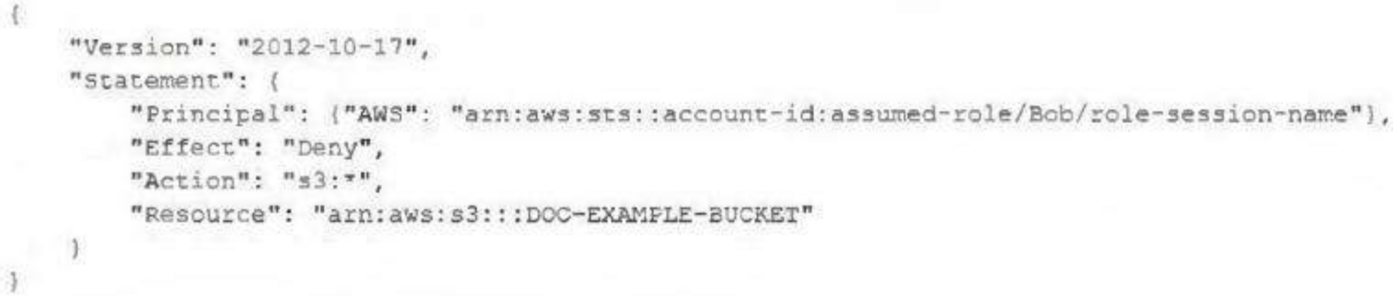
```
{
    "Version": "2012-10-17",
    "Statement": {
        "Principal": {"AWS": "arn:aws:sts::account-id:federated-user/Bob"},
        "Effect": "Deny",
        "Action": "s3:*",
        "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET"
    }
}
```

- B.



```
{
    "Version": "2012-10-17",
    "Statement": {
        "Principal": {"AWS": "arn:aws:iam::account-id:user/Bob"},
        "Effect": "Deny",
        "Action": "s3:*",
        "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET"
    }
}
```

- C.
- D.



```
{
    "Version": "2012-10-17",
    "Statement": {
        "Principal": {"AWS": "arn:aws:sts::account-id:assumed-role/Bob/role-session-name"},
        "Effect": "Deny",
        "Action": "s3:*",
        "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET"
    }
}
```

Correct Answer: *B*

Question:172 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company runs an online game on AWS. When players sign up for the game, their username and password credentials are stored in an Amazon Aurora database.

The number of users has grown to hundreds of thousands of players. The number of requests for password resets and login assistance has become a burden for the company's customer service team.

The company needs to implement a solution to give players another way to log in to the game. The solution must remove the burden of password resets and login assistance while securely protecting each player's credentials.

Which solution will meet these requirements?

- A. When a new player signs up, use an AWS Lambda function to automatically create an IAM access key and a secret access key. Program the Lambda function to store the credentials on the player's device. Create IAM keys for existing players.
- B. Migrate the player credentials from the Aurora database to AWS Secrets Manager. When a new player signs up, create a key-value pair in Secrets Manager for the player's user ID and password.
- C. Configure Amazon Cognito user pools to federate access to the game with third-party identity providers (IdPs), such as social IdPs. Migrate the game's authentication mechanism to Cognito.
- D. Instead of using usernames and passwords for authentication, issue API keys to new and existing players. Create an Amazon API Gateway API to give the game client access to the game's functionality.

Correct Answer: *C*

Question:173 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company suspects that an attacker has exploited an overly permissive role to export credentials from Amazon EC2 instance metadata. The company uses Amazon GuardDuty and AWS Audit Manager. The company has enabled AWS CloudTrail logging and Amazon CloudWatch logging for all of its AWS accounts.

A security engineer must determine if the credentials were used to access the company's resources from an external account.

Which solution will provide this information?

- A. Review GuardDuty findings to find InstanceCredentialExfiltration events.
- B. Review assessment reports in the Audit Manager console to find InstanceCredentialExfiltration events.
- C. Review CloudTrail logs for GetSessionToken API calls to AWS Security Token Service (AWS STS) that come from an account ID from outside the company.
- D. Review CloudWatch logs for GetSessionToken API calls to AWS Security Token Service (AWS STS) that come from an account ID from outside the company.

Correct Answer: *A*

Question:174 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A security engineer needs to run an AWS CloudFormation script. The CloudFormation script builds AWS infrastructure to support a stack that includes web servers and a MySQL database. The stack has been deployed in pre-production environments and is ready for production.

The production script must comply with the principle of least privilege. Additionally, separation of duties must exist between the security engineer's IAM account and CloudFormation.

Which solution will meet these requirements?

- A. Use IAM Access Analyzer policy generation to generate a policy that allows the CloudFormation script to run and manage the stack. Attach the policy to a new IAM role. Modify the security engineer's IAM permissions to be able to pass the new role to CloudFormation.
- B. Create an IAM policy that allows ec2:* and rds:* permissions. Attach the policy to a new IAM role. Modify the security engineer's IAM permissions to be able to assume the new role.
- C. Use IAM Access Analyzer policy generation to generate a policy that allows the CloudFormation script to run and manage the stack. Modify the security engineer's IAM permissions to be able to run the CloudFormation script.
- D. Create an IAM policy that allows ec2:* and rds:* permissions. Attach the policy to a new IAM role. Use the IAM policy simulator to confirm that the policy allows the AWS API calls that are necessary to build the stack. Modify the security engineer's IAM permissions to be able to pass the new role to CloudFormation.

Correct Answer: *A*

Question:175 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company that uses AWS Organizations is migrating workloads to AWS. The company's application team determines that the workloads will use Amazon EC2 instances, Amazon S3 buckets, Amazon DynamoDB tables, and Application

Load Balancers. For each resource type, the company mandates that deployments must comply with the following requirements:

• All EC2 instances must be launched from approved AWS accounts.
• All DynamoDB tables must be provisioned with a standardized naming convention.
• All infrastructure that is provisioned in any accounts in the organization must be deployed by AWS CloudFormation templates.

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

- A. Create CloudFormation templates in an administrator AWS account. Share the stack sets with an application AWS account. Restrict the template to be used specifically by the application AWS account.
- B. Create CloudFormation templates in an application AWS account. Share the output with an administrator AWS account ta review compliant resources. Restrict output to only the administrator AWS account.
- C. Use permissions boundaries to prevent the application AWS account from provisioning specific resources unless conditions for the internal compliance requirements are met.
- D. Use SCPs to prevent the application AWS account from provisioning specific resources unless conditions for the internal compliance requirements are met.
- E. Activate AWS Config managed rules for each service in the application AWS account.

Correct Answer: *AD*

Question:176 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company has a batch-processing system that uses Amazon S3, Amazon EC2, and AWS Key Management Service (AWS KMS). The system uses two AWS accounts: Account A and Account B.

Account A hosts an S3 bucket that stores the objects that will be processed. The S3 bucket also stores the results of the processing. All the S3 bucket objects are encrypted by a KMS key that is managed in Account A.

Account B hosts a VPC that has a fleet of EC2 instances that access the S3 bucket in Account A by using statements in the bucket policy. The VPC was created with DNS hostnames enabled and DNS resolution enabled.

A security engineer needs to update the design of the system without changing any of the system's code. No AWS API calls from the batch-processing EC2 instances can travel over the internet.

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

- A. In the Account B VPC, create a gateway VPC endpoint for Amazon S3. For the gateway VPC endpoint, create a resource policy that allows the s3:GetObject, s3:ListBucket, s3:PutObject, and s3:PutObjectAcl actions for the S3 bucket.
- B. In the Account B VPC, create an interface VPC endpoint for Amazon S3. For the interface VPC endpoint, create a resource policy that allows the s3:GetObject, s3:ListBucket, s3:PutObject, and s3:PutObjectAcl actions for the S3 bucket.
- C. In the Account B VPC, create an interface VPC endpoint for AWS KMS. For the interface VPC endpoint, create a resource policy that allows the kms:Encrypt, kms:Decrypt, and kms:GenerateDataKey actions for the KMS key. Ensure that private DNS is turned on for the endpoint.
- D. In the Account B VPC, create an interface VPC endpoint for AWS KMS. For the interface VPC endpoint, create a resource policy that allows the kms:Encrypt, kms:Decrypt, and kms:GenerateDataKey actions for the KMS key. Ensure that private DNS is turned off for the endpoint.
- E. In the Account B VPC, verify that the S3 bucket policy allows the s3:PutObjectAcl action for cross-account use. In the Account B VPC, create a gateway VPC endpoint for Amazon S3. For the gateway VPC endpoint, create a resource policy that allows the s3:GetObject, s3:ListBucket, and s3:PutObject actions for the S3 bucket.

Correct Answer: *AC*

Question:177 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A security engineer is designing an IAM policy for a script that will use the AWS CLI. The script currently assumes an IAM role that is attached to three AWS managed IAM policies: AmazonEC2FullAccess, AmazonDynamoDBFullAccess, and AmazonVPCFullAccess.

The security engineer needs to construct a least privilege IAM policy that will replace the AWS managed IAM policies that are attached to this role.

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

- A. In AWS CloudTrail, create a trail for management events. Run the script with the existing AWS managed IAM policies. Use IAM Access Analyzer to generate a new IAM policy that is based on access activity in the trail. Replace the existing AWS managed IAM policies with the generated IAM policy for the role.
- B. Remove the existing AWS managed IAM policies from the role. Attach the IAM Access Analyzer Role Policy Generator to the role. Run the script. Return to IAM Access Analyzer and generate a least privilege IAM policy. Attach the new IAM policy to the role.
- C. Create an account analyzer in IAM Access Analyzer. Create an archive rule that has a filter that checks whether the PrincipalArn value matches the ARN of the role. Run the script. Remove the existing AWS managed IAM policies from the role.
- D. In AWS CloudTrail, create a trail for management events. Remove the existing AWS managed IAM policies from the role. Run the script. Find the authorization failure in the trail event that is associated with the script. Create a new IAM policy that includes the action and resource that caused the authorization failure. Repeat the process until the script succeeds. Attach the new IAM policy to the role.

Correct Answer: *A*

Question:178 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A security engineer is designing a cloud architecture to support an application. The application runs on Amazon EC2 instances and processes sensitive information, including credit card numbers.

The application will send the credit card numbers to a component that is running in an isolated environment. The component will encrypt, store, and decrypt the numbers. The component then will issue tokens to replace the numbers in other parts of the application.

The component of the application that manages the tokenization process will be deployed on a separate set of EC2 instances. Other components of the application must not be able to store or access the credit card numbers.

Which solution will meet these requirements?

- A. Use EC2 Dedicated Instances for the tokenization component of the application.
- B. Place the EC2 instances that manage the tokenization process into a partition placement group.
- C. Create a separate VPDeploy new EC2 instances into the separate VPC to support the data tokenization.
- D. Deploy the tokenization code onto AWS Nitro Enclaves that are hosted on EC2 instances.

Correct Answer: *D*

Question:179 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company has two AWS accounts: Account A and Account B. Account A has an IAM role that IAM users in Account B assume when they need to upload sensitive documents to Amazon S3 buckets in Account A.

A new requirement mandates that users can assume the role only if they are authenticated with multi-factor authentication (MFA). A security engineer must recommend a solution that meets this requirement with minimum risk and effort.

Which solution should the security engineer recommend?

- A. Add an aws:MultiFactorAuthPresent condition to the role's permissions policy.
- B. Add an aws MultiFactorAuthPresent condition to the role’s trust policy.
- C. Add an aws:MultiFactorAuthPresent condition to the session policy.
- D. Add an aws:MultiFactorAuthPresent condition to the S3 bucket policies.

Correct Answer: *B*

Question:180 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company wants to receive automated email notifications when AWS access keys from developer AWS accounts are detected on code repository sites.

Which solution will provide the required email notifications?

- A. Create an Amazon EventBridge rule to send Amazon Simple Notification Service (Amazon SNS) email notifications for Amazon GuardDuty UnauthorizedAccess:IAMUser/lnstanceCredentialExfiltration.OutsideAWS findings.
- B. Change the AWS account contact information for the Operations type to a separate email address. Periodically poll this email address for notifications.
- C. Create an Amazon EventBridge rule that reacts to AWS Health events that have a value of Risk for the service category. Configure email notifications by using Amazon Simple Notification Service (Amazon SNS).
- D. Implement new anomaly detection software. Ingest AWS CloudTrail logs. Configure monitoring for ConsoleLogin events in the AWS Management Console. Configure email notifications from the anomaly detection software.

Correct Answer: *A*

Question:181 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company deployed an Amazon EC2 instance to a VPC on AWS. A recent alert indicates that the EC2 instance is receiving a suspicious number of requests over an open TCP port from an external source. The TCP port remains open for long periods of time.

The company's security team needs to stop all activity to this port from the external source to ensure that the EC2 instance is not being compromised. The application must remain available to other users.

Which solution will meet these requirements?

- A. Update the network ACL that is attached to the subnet that is associated with the EC2 instance. Add a Deny statement for the port and the source IP addresses.
- B. Update the elastic network interface security group that is attached to the EC2 instance to remove the port from the inbound rule list.
- C. Update the elastic network interface security group that is attached to the EC2 instance by adding a Deny entry in the inbound list for the port and the source IP addresses.
- D. Create a new network ACL for the subnet. Deny all traffic from the EC2 instance to prevent data from being removed.

Correct Answer: *A*

Question:182 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company has secured the AWS account root user for its AWS account by following AWS best practices. The company also has enabled AWS CloudTrail, which is sending its logs to Amazon S3. A security engineer wants to receive notification in near-real time if a user uses the AWS account root user credentials to sign in to the AWS Management Console

Which solutions will provide this notification? (Choose two.)

- A. Use AWS Trusted Advisor and its security evaluations for the root account. Configure an Amazon EventBridge event rule that is invoked by the Trusted Advisor API. Configure the rule to target an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe any required endpoints to the SNS topic so that these endpoints can receive notification.
- B. Use AWS IAM Access Analyzer. Create an Amazon Cloud Watch Logs metric filter to evaluate log entries from Access Analyzer that detect a successful root account login. Create an Amazon CloudWatch alarm that monitors whether a root login has occurred. Configure the CloudWatch alarm to notify an Amazon Simple Notification Service (Amazon SNS) topic when the alarm enters the ALARM state. Subscribe any required endpoints to this SNS topic so that these endpoints can receive notification.
- C. Configure AWS CloudTrail to send its logs to Amazon CloudWatch Logs. Configure a metric filter on the CloudWatch Logs log group used by CloudTrail to evaluate log entries for successful root account logins. Create an Amazon CloudWatch alarm that monitors whether a root login has occurred. Configure the

CloudWatch alarm to notify an Amazon Simple Notification Service (Amazon SNS) topic when the alarm enters the ALARM state. Subscribe any required endpoints to this SNS topic so that these endpoints can receive notification.

- D. Configure AWS CloudTrail to send log notifications to an Amazon Simple Notification Service (Amazon SNS) topic. Create an AWS Lambda function that parses the CloudTrail notification for root login activity and notifies a separate SNS topic that contains the endpoints that should receive notification. Subscribe the Lambda function to the SNS topic that is receiving log notifications from CloudTrail.
- E. Configure an Amazon EventBridge event rule that runs when Amazon CloudWatch API calls are recorded for a successful root login. Configure the rule to target an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe any required endpoints to the SNS topic so that these endpoints can receive notification.

Correct Answer: *CE*

Question:183 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company has AWS accounts that are in an organization in AWS Organizations. A security engineer needs to set up AWS Security Hub in a dedicated account for security monitoring.

The security engineer must ensure that Security Hub automatically manages all existing accounts and all new accounts that are added to the organization. Security Hub also must receive findings from all AWS Regions.

Which combination of actions will meet these requirements with the LEAST operational overhead? (Choose two.)

- A. Configure a finding aggregation Region for Security Hub. Link the other Regions to the aggregation Region.
- B. Create an AWS Lambda function that routes events from other Regions to the dedicated Security Hub account. Create an Amazon EventBridge rule to invoke the Lambda function.
- C. Turn on the option to automatically enable accounts for Security Hub.
- D. Create an SCP that denies the securityhub:DisableSecurityHub permission. Attach the SCP to the organization's root account.
- E. Configure services in other Regions to write events to an AWS CloudTrail organization trail. Configure Security Hub to read events from the trail.

Correct Answer: *AC*

Question:184 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

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

Which solution meets these requirements?

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

Correct Answer: *B*

Question:185 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company needs to implement DNS Security Extensions (DNSSEC) for a specific subdomain. The subdomain is already registered with Amazon Route 53. A security engineer has enabled DNSSEC signing and has created a key-signing key (KSK). When the security engineer tries to test the configuration, the security engineer receives an error for a broken trust chain.

What should the security engineer do to resolve this error?

- A. Replace the KSK with a zone-signing key (ZSK).
- B. Deactivate and then activate the KSK.
- C. Create a Delegation Signer (DS) record in the parent hosted zone.
- D. Create a Delegation Signer (DS) record in the subdomain.

Correct Answer: *C*

Question:186 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company used AWS Organizations to set up an environment with multiple AWS accounts. The company's organization currently has two AWS accounts, and the company expects to add more than 50 AWS accounts during the next 12 months. The company will require all existing and future AWS accounts to use Amazon GuardDuty. Each existing AWS account has GuardDuty active. The company reviews GuardDuty findings by logging into each AWS account individually.

The company wants a centralized view of the GuardDuty findings for the existing AWS accounts and any future AWS accounts. The company also must ensure that any new AWS account has GuardDuty automatically turned on.

Which solution will meet these requirements?

- A. Enable AWS Security Hub in the organization's management account. Configure GuardDuty within the management account to send all GuardDuty findings to Security Hub.
- B. Create a new AWS account in the organization. Enable GuardDuty in the new account. Designate the new account as the delegated administrator account for GuardDuty. Configure GuardDuty to add existing accounts as member accounts. Select the option to automatically add new AWS accounts to the organization.
- C. Create a new AWS account in the organization. Enable GuardDuty in the new account. Enable AWS Security Hub in each account. Select the option to automatically add new AWS accounts to the organization.
- D. Enable AWS Security Hub in the organization's management account. Designate the management account as the delegated administrator account for Security Hub. Add existing accounts as member accounts. Select the option to automatically add new AWS accounts to the organization. Send all Security Hub findings to the organization's GuardDuty account.

Correct Answer: *B*

Question:187 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

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 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 Systems Manager. Provide the IAM user accounts with permission to use Systems Manager. Remove the SSH keys from the EC2 instances. Use Systems Manager Inventory to select the EC2 instance and connect.
- B. Assign an IAM policy to the IAM user accounts to provide permission to use AWS Systems 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 Systems Manager. Provide the IAM user accounts with permission to use Systems Manager. Remove the SSH keys from the EC2 instances. Use Systems 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 instances. Connect to the EC2 instance as the ec2-user through the AWS Management Console's EC2 SSH client method.

Correct Answer: *C*

Question:188 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company is storing data in Amazon S3 Glacier. A security engineer implemented a new vault lock policy for 10 TB of data and called the 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 error?

- 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 the initiate-vault-lock operation again to apply the new policy.

Correct Answer: *A*

Question:189 SCS-C02: Actual Exam Q&A | CLEARCATNET

A company uses HTTP Live Streaming (HLS) to stream live video content to paying subscribers by using Amazon CloudFront. HLS splits the video content into chunks so that the user can request the right chunk based on different conditions. Because the video events last for several hours, the total video is made up of thousands of chunks.

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

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

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

Correct Answer: *B*

Question:190 SCS-C02: Actual Exam Q&A | CLEARCATNET

A company runs workloads in the us-east-1 Region. The company has never deployed resources to other AWS Regions and does not have any multi-Region resources. The company needs to replicate its workloads and infrastructure to the us-west-1 Region.

A security engineer must implement a solution that uses AWS Secrets Manager to store secrets in both Regions. The solution must use AWS Key Management Service (AWS KMS) to encrypt the secrets. The solution must minimize latency and must be able to work if only one Region is available.

The security engineer uses Secrets Manager to create the secrets in us-east-1.

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

- A. Encrypt the secrets in us-east-1 by using an AWS managed KMS key. Replicate the secrets to us-west-1. Encrypt the secrets in us-west-1 by using a new AWS managed KMS key in us-west-1.
- B. Encrypt the secrets in us-east-1 by using an AWS managed KMS key. Configure resources in us-west-1 to call the Secrets Manager endpoint in us-east-1.
- C. Encrypt the secrets in us-east-1 by using a customer managed KMS key. Configure resources in us-west-1 to call the Secrets Manager endpoint in us-east-1.
- D. Encrypt the secrets in us-east-1 by using a customer managed KMS key. Replicate the secrets to us-west-1. Encrypt the secrets in us-west-1 by using the customer managed KMS key from us-east-1.

Correct Answer: *D*

Question:191 SCS-C02: Actual Exam Q&A | CLEARCATNET

A company operates a web application that runs on Amazon EC2 instances. The application listens on port 80 and port 443. The company uses an Application Load Balancer (ALB) with AWS WAF to terminate SSL and to forward traffic to the application instances only on port 80.

The ALB is in public subnets that are associated with a network ACL that is named NACL1. The application instances are in dedicated private subnets that are associated with a network ACL that is named NACL2. An Amazon RDS for PostgreSQL DB instance that uses port 5432 is in a dedicated private subnet that is associated with a network ACL that is named NACL3. All the network ACLs currently allow all inbound and outbound traffic.

Which set of network ACL changes will increase the security of the application while ensuring functionality?

- A. Make the following changes to NACL3:
  • Add a rule that allows inbound traffic on port 5432 from NACL2.
  • Add a rule that allows outbound traffic on ports 1024-65536 to NACL2.
  • Remove the default rules that allow all inbound and outbound traffic.
- B. Make the following changes to NACL3:
  • Add a rule that allows inbound traffic on port 5432 from the Cl DR blocks of the application instance subnets.
  • Add a rule that allows outbound traffic on ports 1024-65536 to the application instance subnets.
  • Remove the default rules that allow all inbound and outbound traffic.
- C. Make the following changes to NACL2:
  • Add a rule that allows outbound traffic on port 5432 to the CIDR blocks of the RDS subnets.
  • Remove the default rules that allow all inbound and outbound traffic.
- D. Make the following changes to NACL2:
  • Add a rule that allows inbound traffic on port 5432 from the CIDR blocks of the RDS subnets.
  • Add a rule that allows outbound traffic on port 5432 to the RDS subnets.

Correct Answer: *B*

Question:192 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

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? (Choose two.)

- A. Verify that the S3 bucket policy allows 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 S3 Glacier Flexible Retrieval.
- 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.

Correct Answer: *AD*

Question:193 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company has public certificates that are managed by AWS Certificate Manager (ACM). The certificates are either imported certificates or managed certificates from ACM with mixed validation methods. A security engineer needs to design a monitoring solution to provide alerts by email when a certificate is approaching its expiration date.

What is the MOST operationally efficient way to meet this requirement?

- A. Create an AWS Lambda function to list all certificates and to go through each certificate to describe the certificate by using the AWS SDK. Filter on the NotAfter attribute and send an email notification. Use an Amazon EventBridge rate expression to schedule the Lambda function to run daily.
- B. Create an Amazon CloudWatch alarm. Add all the certificate ARNs in the AWS/CertificateManager namespace to the DaysToExpiry metric. Configure the alarm to publish a notification to an Amazon Simple Notification Service (Amazon SNS) topic when the value for the DaysToExpiry metric is less than or equal to 31.
- C. Set up AWS Security Hub. Turn on the AWS Foundational Security Best Practices standard with integrated ACM to send findings. Configure and use a custom action by creating a rule to match the pattern from the ACM findings on the NotBefore attribute as the event source. Create an Amazon Simple Notification Service (Amazon SNS) topic as the target.
- D. Create an Amazon EventBridge rule by using a predefined pattern for ACM Choose the metric in the ACM

Certificate Approaching Expiration event as the event pattern. Create an Amazon Simple Notification Service (Amazon SNS) topic as the target.

Correct Answer: *D*

Question:194 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

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.

Correct Answer: *C*

Question:195 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

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

What should the security engineer recommend?

- A. Within the Auto Scaling lifecycle, add a hook to create and attach an Amazon Elastic Block Store (Amazon EBS) log volume each time an EC2 instance is created. 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. Add an 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.

Correct Answer: *C*

Question:196 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company uses Amazon EC2 instances to host frontend services behind an Application Load Balancer. Amazon Elastic Block Store (Amazon EBS) volumes are attached to the EC2 instances. The company uses Amazon S3 buckets to store large files for images and music.

The company has implemented a security architecture on AWS to prevent, identify, and isolate potential ransomware attacks. The company now wants to further reduce risk.

A security engineer must develop a disaster recovery solution that can recover to normal operations if an attacker bypasses preventive and detective controls. The solution must meet an RPO of 1 hour.

Which solution will meet these requirements?

- A. Use AWS Backup to create backups of the EC2 instances and S3 buckets every hour. Create AWS

CloudFormation templates that replicate existing architecture components. Use AWS CodeCommit to store the CloudFormation templates alongside application configuration code.
- B. Use AWS Backup to create backups of the EBS volumes and S3 objects every day. Use Amazon Security Lake to create a centralized data lake for AWS CloudTrail logs and VPC flow logs. Use the logs for automated response.
- C. Use Amazon Security Lake to create a centralized data lake for AWS CloudTrail logs and VPC flow logs. Use the logs for automated response. Enable AWS Security Hub to establish a single location for recovery procedures. Create AWS CloudFormation templates that replicate existing architecture components. Use AWS CodeCommit to store the CloudFormation templates alongside application configuration code.
- D. Create EBS snapshots every 4 hours. Enable Amazon GuardDuty Malware Protection. Create automation to immediately restore the most recent snapshot for any EC2 instances that produce an Execution:EC2/MaliciousFile finding in GuardDuty.

Correct Answer: *A*

Question:197 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company has an application that runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances are in an Amazon EC2 Auto Scaling group and are attached to Amazon Elastic Block Store (Amazon EBS) volumes.

A security engineer needs to preserve all forensic evidence from one of the instances.

Which order of steps should the security engineer use to meet this requirement?
- A. Take an EBS volume snapshot of the instance and store the snapshot in an Amazon S3 bucket. Take a memory snapshot of the instance and store the snapshot in an S3 bucket Detach the instance from the Auto Scaling group. Deregister the instance from the ALB. Stop the instance.
- B. Take a memory snapshot of the instance and store the snapshot in an Amazon S3 bucket. Stop the instance. Take an EBS volume snapshot of the instance and store the snapshot in an S3 bucket. Detach the instance from the Auto Scaling group. Deregister the instance from the ALB.
- C. Detach the instance from the Auto Scaling group. Deregister the instance from the ALB. Take an EBS volume snapshot of the instance and store the snapshot in an Amazon S3 bucket. Take a memory snapshot of the instance and store the snapshot in an S3 bucket. Stop the instance.
- D. Detach the instance from the Auto Scaling group. Deregister the instance from the ALB Stop the instance. Take a memory snapshot of the instance and store the snapshot in an Amazon S3 bucket. Take an EBS volume snapshot of the instance and store the snapshot in an S3 bucket.

Correct Answer: *C*

Question:198 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

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? (Choose three.)
- A. Request a certificate from 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 validation 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 the 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 will secure.

Correct Answer: *CEF*

Question:199 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company's security engineer wants to receive an email alert whenever Amazon GuardDuty, AWS Identity and Access Management Access Analyzer, or Amazon Macie generate a high-severity security finding. The company uses AWS Control Tower to govern all of its accounts. The company also uses AWS Security Hub with all of the AWS service integrations turned on.

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

- A. Set up separate AWS Lambda functions for GuardDuty, IAM Access Analyzer, and Macie to call each service's public API to retrieve high-severity findings. Use Amazon Simple Notification Service (Amazon SNS) to send the email alerts. Create an Amazon EventBridge rule to invoke the functions on a schedule.
- B. Create an Amazon EventBridge rule with a pattern that matches Security Hub findings events with high severity. Configure the rule to send the findings to a target Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the desired email addresses to the SNS topic.
- C. Create an Amazon EventBridge rule with a pattern that matches AWS Control Tower events with high severity. Configure the rule to send the findings to a target Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the desired email addresses to the SNS topic.
- D. Host an application on Amazon EC2 to call the GuardDuty. IAM Access Analyzer, and Macie APIs. Within the application, use the Amazon Simple Notification Service (Amazon SNS) API to retrieve high-severity findings and to send the findings to an SNS topic. Subscribe the desired email addresses to the SNS topic.

Correct Answer: *B*

Question:200 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company hosts an application on Amazon EC2 instances. The application also uses Amazon S3 and Amazon Simple Queue Service (Amazon SQS). The application is behind an Application Load Balancer (ALB) and scales with AWS Auto Scaling.

The company's security policy requires the use of least privilege access, which has been applied to all existing AWS resources. A security engineer needs to implement private connectivity to AWS services.

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

- A. Use an interface VPC endpoint for Amazon SQS.
- B. Configure a connection to Amazon S3 through AWS Transit Gateway.
- C. Use a gateway VPC endpoint for Amazon S3.
- D. Modify the IAM role applied to the EC2 instances in the Auto Scaling group to allow outbound traffic to the interface endpoints.
- E. Modify the endpoint policies on all VPC endpoints. Specify the SQS and S3 resources that the application uses.
- F. Configure a connection to Amazon S3 through AWS Firewall Manager.

Correct Answer: *ACE*
Explanation:
These steps ensure that the application can securely access Amazon S3 and Amazon SQS without traversing the public internet, while also maintaining fine-grained control over which resources can be accessed

Question:201 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

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.

Correct Answer: *B*
Explanation:
For the CloudWatch alarm to trigger on security group changes, the following must be correctly configured:
Metric Filter:
A CloudWatch Logs metric filter must exist to detect security group API calls (e.g., AuthorizeSecurityGroupIngress, DeleteSecurityGroup) in CloudTrail logs. If the filter is missing or has an incorrect pattern, the metric will not be generated.
Alarm Setup:
The alarm must reference the metric created by the filter and have an associated action (e.g., SNS topic) to send notifications. If the alarm lacks an action or references an invalid metric, alerts will not be delivered.

Question:202 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

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 secret in 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.

Correct Answer: *C*

Question:203 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company is using an Amazon CloudFront distribution to deliver content from two origins. One origin is a dynamic application that is hosted on Amazon EC2 instances. The other origin is an Amazon S3 bucket for static assets.

A security analysis shows that HTTPS responses from the application do not comply with a security requirement to provide an X-Frame-Options HTTP header to prevent frame-related cross-site scripting attacks. A security engineer must make the full stack compliant by adding the missing HTTP header to the responses.

Which solution will meet these requirements?

- A. Create a Lambda@Edge function. Include code to add the X-Frame-Options header to the response. Configure the function to run in response to the CloudFront origin response event.
- B. Create a Lambda@Edge function. Include code to add the X-Frame-Options header to the response. Configure the function to run in response to the CloudFront viewer request event.
- C. Update the CloudFront distribution by adding X-Frame-Options to custom headers in the origin settings.
- D. Customize the EC2 hosted application to add the X-Frame-Options header to the responses that are returned to CloudFront.

Correct Answer: *A*
Explanation:
This approach ensures that the header is added to all responses, regardless of the origin (EC2 or S3), and it does not require changes to the application code or the CloudFront distribution settings

Question:204 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

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? (Choose 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.

Correct Answer: *BE*

Question:205 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company has an AWS Key Management Service (AWS KMS) customer managed key with imported key material. Company policy requires all encryption keys to be rotated every year.

What should a security engineer do to meet this requirement for this customer managed key?

- A. Enable automatic key rotation annually for the existing customer managed key.
- B. Use the AWS CLI to create an AWS Lambda function to rotate the existing customer managed key annually.
- C. Import new key material to the existing customer managed key. Manually rotate the key.
- D. Create a new customer managed key. Import new key material to the new key. Point the key alias to the new key.

Correct Answer: *D*

Explanation:

To comply with the policy of rotating encryption keys annually, the recommended approach is to create a new customer managed key, import new key material to this new key, and then update the key alias to point to the new key. This ensures that the key rotation is handled correctly and securely.

Question:206 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A healthcare company has multiple AWS accounts in an organization in AWS Organizations. The company uses Amazon S3 buckets to store sensitive information of patients. The company needs to restrict users from deleting any S3 bucket across the organization.

What is the MOST scalable solution that meets these requirements?

- A. Permissions boundaries in AWS Identity and Access Management (IAM)
- B. S3 bucket policies
- C. Tag policies
- D. SCPs

Correct Answer: *D*

Question:207 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company needs to detect unauthenticated access to its Amazon Elastic Kubernetes Service (Amazon EKS) clusters. The company needs a solution that requires no additional configuration of the existing EKS deployment.

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

- A. Install an Amazon EKS add-on from a security vendor.
- B. Enable AWS Security Hub. Monitor the Kubernetes findings.
- C. Monitor Amazon CloudWatch Container Insights metrics for Amazon EKS.
- D. Enable Amazon GuardDuty. Use EKS Audit Log Monitoring.

Correct Answer: *D*

Explanation:

Amazon GuardDuty provides comprehensive security monitoring for EKS clusters, including the ability to detect unauthenticated access attempts. It requires minimal configuration and integrates seamlessly with existing EKS deployments.

Reference:

https://aws.amazon.com/blogs/security/how-to-detect-security-issues-in-amazon-eks-clusters-using-amazon-guardduty-part-1/

Question:208

A security engineer is investigating a malware infection that has spread across a set of Amazon EC2 instances. A key indicator of the compromise is outbound traffic on TCP port 2905 to a set of command and control hosts on the internet.

The security engineer creates a network ACL rule that denies the identified outbound traffic. The security engineer applies the network ACL rule to the subnet of the EC2 instances. The security engineer must identify any EC2 instances that are trying to communicate on TCP port 2905.

Which solution will identify the affected EC2 instances with the LEAST operational effort?

- A. Create a Network Access Scope in Amazon VPC Network Access Analyzer. Use the Network Access Scope to identify EC2 instances that try to send traffic to TCP port 2905.
- B. Enable VPC flow logs for the VPC where the affected EC2 instances are located. Configure the flow logs to capture rejected traffic. In the flow logs, search for REJECT records that have a destination TCP port of 2905.
- C. Enable Amazon GuardDuty. Create a custom GuardDuty IP list to create a finding when an EC2 instance tries to communicate with one of the command and control hosts. Use Amazon Detective to identify the EC2 instances that initiate the communication.
- D. Create a firewall in AWS Network Firewall. Attach the firewall to the subnet of the EC2 instances. Create a custom rule to identify and log traffic from the firewall on TCP port 2905. Create an Amazon CloudWatch Logs metric filter to identify firewall logs that reference traffic on TCP port 2905.

Correct Answer: *B*

Explanation:

Enabling flow logs and filtering for records with REJECT on TCP port 2905, the security engineer can quickly identify which EC2 instances are attempting to communicate with command and control hosts.

Question:209

A security engineer uses Amazon Macie to scan a company's Amazon S3 buckets for sensitive data. The company has many S3 buckets and many objects stored in the S3 buckets. The security engineer must identify S3 buckets that contain sensitive data and must perform additional scanning on those S3 buckets.

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

- A. Configure S3 Cross-Region Replication (CRR) on the S3 buckets to replicate the objects to a second AWS Region. Configure Macie in the second Region to scan the replicated objects daily.
- B. Create an AWS Lambda function as an S3 event destination for the S3 buckets. Configure the Lambda function to start a Macie scan of an object when the object is uploaded to an S3 bucket.
- C. Configure Macie automated discovery to continuously sample data from the S3 buckets. Perform full scans of the S3 buckets where Macie discovers sensitive data.
- D. Configure Macie scans to run on the S3 buckets. Aggregate the results of the scans in an Amazon DynamoDB table. Use the DynamoDB table for queries.

Correct Answer: *C*

Explanation:

This approach leverages Macie's automated discovery feature, which continuously samples data to identify sensitive information. It minimizes manual intervention and administrative tasks, allowing you to focus full scans only on buckets where sensitive data is detected.

Question:210

A security engineer for a large company is managing a data processing application used by 1,500 subsidiary companies. The parent and subsidiary companies all use AWS. The application uses TCP port 443 and runs on Amazon C2 behind a Network Load Balancer (NLB). For compliance reasons, the application should only be accessible to the subsidiaries and should not be available on the public internet. To meet the compliance requirements for restricted access, the engineer has received the public and private CIDR block ranges for each subsidiary.

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

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

Correct Answer: *C*
Reference:
https://docs.aws.amazon.com/elasticloadbalancing/latest/network/load-balancer-access-logs.html

Question:211 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company runs workloads on Amazon EC2 instances. The company needs to continually scan the EC2 instances for software vulnerabilities and unintended network exposure.

Which solution will meet these requirements?

- A. Use Amazon Inspector. Set the scan mode to hybrid scanning.
- B. Use Amazon GuardDuty. Enable the Malware Protection feature.
- C. Use Amazon Inspector. Enable the Malware Protection feature.
- D. Use Amazon GuardDuty. Enable the Runtime Monitoring feature.

Correct Answer: *A*
Explanation:
Amazon Inspector is specifically designed for this purpose. It automatically discovers and scans EC2 instances for software vulnerabilities and unintended network exposure, providing detailed findings and remediation recommendations

Question:212 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company has a requirement that no Amazon EC2 security group can allow SSH access from the CIDR block 0.0.0.0/0. The company wants to monitor compliance with this requirement at all times and wants to receive a near-real-time notification if any security group is noncompliant.

A security engineer has configured AWS Config and will use the restricted-ssh managed rule to monitor the security groups.

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

- A. Configure AWS Config to send its configuration snapshots to an Amazon S3 bucket. Create an AWS Lambda function to run on a PutEvent to the S3 bucket. Configure the Lambda function to parse the snapshot for a compliance change to the restricted-ssh managed rule. Configure the Lambda function to send a notification to an Amazon Simple Notification Service (Amazon SNS) topic if a change is discovered.
- B. Configure an Amazon EventBridge event rule that is invoked by a compliance change event from AWS Config for the restricted-ssh managed rule. Configure the event rule to target an Amazon Simple Notification Service (Amazon SNS) topic that will provide a notification.
- C. Configure AWS Config to push all its compliance notifications to Amazon CloudWatch Logs. Configure a CloudWatch Logs metric filter on the AWS Config log group to look for a compliance notification change on the restricted-ssh managed rule. Create an Amazon CloudWatch alarm on the metric filter to send a notification to an Amazon Simple Notification Service (Amazon SNS) topic if the alarm is in the ALARM state.

- D. Configure an Amazon CloudWatch alarm on the CloudWatch metric for the restricted-ssh managed rule. Configure the CloudWatch alarm to send a notification to an Amazon Simple Notification Service (Amazon SNS) topic if the alarm is in the ALARM state.

Correct Answer: *B*
Reference:
https://docs.aws.amazon.com/config/latest/developerguide/restricted-ssh.html

Question:213 *SCS-C02: Actual Exam Q&A | CLEARCATNET*
A security engineer discovers that a company's user passwords have no required minimum length. The company is using the following two identity providers (IdPs):
• AWS Identity and Access Management (IAM) federated with on-premises Active Directory
• Amazon Cognito user pools that contain the user database for an AWS Cloud application that the company developed

Which combination of actions should the security engineer take to implement a required minimum length for the passwords? (Choose two.)

- A. Update the password length policy in the IAM configuration.
- B. Update the password length policy in the Cognito configuration.
- C. Update the password length policy in the on-premises Active Directory configuration
- D. Create an SCP in AWS Organizations. Configure the SCP to enforce a minimum password length for IAM and Cognito.
- E. Create an IAM policy that includes a condition for minimum password length. Enforce the policy for IAM and Cognito.

Correct Answer: *BC*
Explanation:
For Amazon Cognito:
You can configure password length requirements directly in Cognito user pools5
The minimum password length can be set between 6 and 99 characters, though users can set passwords up to 256 characters long5
This is configured through the Password Policy settings in the Cognito user pool5
For Active Directory (federated with IAM):
Since IAM is federated with on-premises Active Directory, the password policies are managed at the Active Directory level13
Password length requirements can be configured in Active Directory through Group Policy settings13
Changes must be made in Active Directory, not IAM, since AD is the authoritative source for authentication

Question:214 *SCS-C02: Actual Exam Q&A | CLEARCATNET*
A company uses AWS Key Management Service (AWS KMS). During an attempt to attach an encrypted Amazon Elastic Block Store (Amazon EBS) volume to an Amazon EC2 instance, the attachment fails. The company discovers that a customer managed key has become unusable because the key material for the key was deleted. The company needs the data that is on the EBS volume.

A security engineer must recommend a solution to decrypt the EBS volume's encrypted data key. The solution must also attach the volume to the EC2 instance.

Which solution will meet these requirements?

- A. Import new key material into the key. Attach the EBS volume.
- B. Restore the EBS volume from a snapshot that was taken before the deletion of the key material.
- C. Reimport the same key material that originally was imported into the key. Attach the EBS volume.
- D. Create a new key. Import new key material. Attach the EBS volume.

Correct Answer: *C*
Explanation:
The snapshot will be encrypted with the same key that was deleted so decryption of the snapshot will be impossible. Importing the same key material as the deleted key will restore the ability to decrypt the volume.

Question:215 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company needs to analyze access logs for an Application Load Balancer (ALB). The ALB directs traffic to the company’s online login portal. The company needs to use visualizations to identify login attempts by bots from a list of known IP sources.

Which solution will meet these requirements?

- A. Configure the ALB to send logs directly to Amazon CloudWatch Logs. Analyze and visualize the logs by using CloudWatch Logs Insights.
- B. Configure the ALB to send logs directly to Amazon Redshift. Analyze the logs by using SQL queries. Visualize the logs by using custom reports.
- C. Configure the ALB to send logs directly to Amazon OpenSearch Service. Analyze the logs by using OpenSearch dashboards. Visualize the logs by using custom OpenSearch dashboards.
- D. Configure the ALB to send logs directly to an Amazon S3 bucket. Analyze the logs by using Amazon Athena. Visualize the logs by using Amazon QuickSight.

Correct Answer: *D*

Explanation:

Amazon S3: Storing logs in S3 is cost-effective and scalable. Amazon Athena: Allows you to run SQL queries on the log data stored in S3, making it easy to filter and analyze specific login attempts, including those from known bot IPs

Question:216 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

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) customer managed key 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 KMS key.
- B. Use the aws kms create-grant command to generate a grant for the existing KMS key.
- 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.

Correct Answer: *A*

Question:217 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A security engineer needs to analyze Apache web server access logs that are stored in an Amazon S3 bucket. Amazon EC2 instance web servers generated the logs. The EC2 instances have the Amazon CloudWatch agent installed and configured to report their access logs.

The security engineer needs to use a query in Amazon Athena to analyze the logs. The query must identify IP addresses that have attempted and failed to access restricted web server content held at the /admin URL path. The query also must identify the URLs that the IP addresses attempted to access.

Which query will meet these requirements?

- A. SELECT client_ip, client_request FROM logs WHERE client_request LIKE '%/admin%!’ AND server_status = '403’
- B. SELECT client_ip FROM logs WHERE client_request CONTAINS '%/admin%’ AND server_status = '401' GROUP BY client_ip
- C. SELECT DISTINCT (client_ip), client_request, client_id FROM logs WHERE server status = ‘403’ LIMIT 1000
- D. SELECT DISTINCT (client_ip), client_request FROM logs WHERE user_id <> ‘admin’ AND server_status = ‘401!’

Correct Answer: *A*

Question:218 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company uses Amazon Cognito as an OAuth 2.0 identity platform for its web and mobile applications. The company needs to capture successful and unsuccessful login attempts. The company also needs to query the data about the login attempts.

Which solution will meet these requirements?

- A. Configure Cognito to send logs of user activity to Amazon CloudWatch. Configure Amazon EventBridge to invoke an AWS Lambda function to export the logs to an Amazon S3 bucket. Use Amazon Athena to query the logs for event names of SignUp with event sources of cognito-idp.amazonaws.com.
- B. Enable AWS CloudTrail to deliver logs to an Amazon S3 bucket. Use Amazon Athena to query the logs for event names of InitiateAuth with event sources of cognito-idp.amazonaws.com.
- C. Configure AWS CloudTrail to send Cognito CloudTrail events to Amazon CloudWatch for monitoring. Query the event logs for event names of SignUp with event sources of cognito-idp.amazonaws.com.
- D. Configure Amazon CloudWatch metrics to monitor and report Cognito events. Create a CloudWatch dashboard for the provided metrics. Display the Cognito user pools for event names of InitiateAuth with event sources of cognito-idp.amazonaws.com.

Correct Answer: *B*
Explanation:
AWS CloudTrail provides detailed logs of all API calls made to Amazon Cognito, including login attempts. Amazon S3 is used to store these logs, ensuring they are easily accessible and durable. Amazon Athena allows you to run SQL queries on the logs stored in S3, making it straightforward to filter and analyze the data for specific events, such as InitiateAuth, which corresponds to login attempts. This setup ensures that you can capture both successful and unsuccessful login attempts and query the data efficiently.

Question:219 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

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.

Correct Answer: *B*
Explanation:
KMS Key Policy Permissions: If the KMS key policy does not explicitly grant the necessary decrypt permissions to the security engineer's IAM user or role, they will not be able to read the encrypted log files. This is a common issue when dealing with SSE-KMS encryption. Digest Files: These files are not encrypted with the KMS key, which is why they are readable even if the log files are not. To resolve this, the security engineer should ensure that the KMS key policy includes the appropriate permissions for their IAM user or role to decrypt the log files.

Question:220 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company needs to securely deploy resources and workloads across AWS accounts. The accounts are in an organization in AWS Organizations.

The company needs to use AWS CloudFormation for infrastructure as code (IaC) management of approved architectural patterns. The company also must enforce tagging requirements and specific guidelines for resource and workload configuration and creation.

Which solution will meet these requirements?

- A. Use CloudFormation stack policies to prevent the creation of resources that do not meet the tagging or configuration requirements. Use Amazon EventBridge rules to detect API calls that attempt to create resources outside of CloudFormation.

- B. Use an AWS CodePipeline pipeline to test and deploy IaC defined workloads through CloudFormation into the accounts. Use AWS Config rules to enforce the tagging requirements. Apply an SCP to prevent the creation of misconfigured resources in all OUs.
- C. Create an IAM permissions boundary to prevent the creation of misconfigured resources through CloudFormation and to enforce the tagging requirements. Apply the permissions boundary to all account roles. Use AWS Config rules to identify existing resources that are in a misconfigured state.
- D. Use AWS Service Catalog with CloudFormation to manage access to approved architecture configurations. Provision Service Catalog portfolios to the accounts across the organization. Use AWS Config rules to enforce the tagging requirements and other resource configuration policies across accounts.

Correct Answer: *D*
Explanation:
AWS Service Catalog: This service allows you to create and manage catalogs of approved products that can be deployed using CloudFormation. This ensures that only approved architectural patterns are used. Provisioning Portfolios: By provisioning Service Catalog portfolios to the accounts across the organization, you can control which resources and configurations are available for deployment. AWS Config Rules: These rules can be used to enforce tagging requirements and other configuration policies, ensuring compliance across all accounts. This approach provides a comprehensive solution for managing and enforcing infrastructure standards and compliance across multiple AWS accounts.

Question:221
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.

Correct Answer: *B*
Explanation:
EC2:MetadataNoToken Metric: This metric indicates the number of requests to the instance metadata service that do not use a token, which is a characteristic of IMDSv1. If this metric is zero, it means that no requests are being made to the IMDSv1 endpoint. Amazon CloudWatch Dashboard: By creating a dashboard, the security engineer can easily monitor this metric across all EC2 instances in real-time. This method provides a straightforward and effective way to ensure that all instances have transitioned to using IMDSv2.

Question:222
A company is planning to create an organization by using AWS Organizations. The company needs to integrate user management with the company’s external identity provider (IdP). The company also needs to centrally manage access to all of its AWS accounts and applications from the organization’s management account.

Which solution will meet these requirements?

- A. Configure AWS Directory Service with the external IdP. Create IAM policies and associate them with users from the external IdP.
- B. Enable AWS IAM Identity Center and use the external IdP as the identity source. Create permission sets and account assignments by using IAM Identity Center.
- C. Configure AWS Identity and Access Management (IAM) to use the external IdP as an IdP. Create IAM policies and associate them with users from the external IdP.
- D. Enable Amazon Cognito in the organization’s management account. Create an identity pool and associate

it with the external IdP. Create IAM roles and associate them with the identity pool.

Correct Answer: *B*

Explanation:

The best solution for integrating user management with an external identity provider (IdP) and centrally managing access to all AWS accounts and applications is B. Enable AWS IAM Identity Center and use the external IdP as the identity source. Create permission sets and account assignments by using IAM Identity Center. AWS IAM Identity Center (formerly AWS Single Sign-On) allows you to connect your external IdP, such as Okta or Microsoft Entra ID, using SAML 2.0 or SCIM protocols1. This setup enables centralized management of user access across all AWS accounts and applications within your organization

Question:223

A company uses Amazon Elastic Container Registry (Amazon ECR) as the repository for its production applications. A security engineer must implement an automated solution to report any vulnerabilities that ECR enhanced scanning detects. The solution must provide notification of vulnerability findings in an instant message to the company's Slack account

Which solution will meet these requirements with the MOST operational efficiency?

- A. Activate Amazon Inspector scans for the ECR repository. Create an Amazon Simple Notification Service (Amazon SNS) topic. Configure an AWS Chatbot client for Slack that consumes the SNS topic. Create an Amazon EventBridge rule for Amazon Inspector findings. Specify the SNS topic as the target for the rule.
- B. Activate Amazon Inspector scans for the ECR repository. Write a script to use AWS CLI commands to retrieve image scan findings from Amazon Inspector. Configure the script to send the findings to a Slack endpoint. Launch an Amazon EC2 instance to run the script.
- C. Activate Amazon Inspector scans for the ECR repository. Create an AWS Step Functions state machine. Set a first step in the state machine to call the Amazon Inspector ListFindings API operation. Create an Amazon Simple Notification Service (Amazon SNS) topic with Slack as the target. Add a second step in the state machine to call the Amazon SNS Publish API operation.
- D. Activate AWS Security Hub scans for the ECR repository. Create a custom action in Security Hub for findings. Define an Amazon EventBridge rule for the custom action. Configure the EventBridge rule to redirect the findings to a Slack channel.

Correct Answer: *A*

Question:224

A company uses AWS Config rules to identify Amazon S3 buckets that are not compliant with the company's data protection policy. The S3 buckets are hosted in several AWS Regions and several AWS accounts. The accounts are in an organization in AWS Organizations.

The company needs a solution to remediate the organization's existing noncompliant S3 buckets and any noncompliant S3 buckets that are created in the future.

Which solution will meet these requirements?

- A. Deploy an AWS Config aggregator with organization-wide resource data aggregation. Create an AWS Lambda function that responds to AWS Config findings of noncompliant S3 buckets by deleting or reconfiguring the S3 buckets.
- B. Deploy an AWS Config aggregator with organization-wide resource data aggregation. Create an SCP that contains a Deny statement that prevents the creation of new noncompliant S3 buckets. Apply the SCP to all OUs in the organization.
- C. Deploy an AWS Config aggregator that scopes only the accounts and Regions that the company currently uses. Create an AWS Lambda function that responds to AWS Config findings of noncompliant S3 buckets by deleting or reconfiguring the S3 buckets.
- D. Deploy an AWS Config aggregator that scopes only the accounts and Regions that the company currently uses. Create an SCP that contains a Deny statement that prevents the creation of new noncompliant S3 buckets. Apply the SCP to all OUs in the organization.

Correct Answer: *A*

Explanation:
AWS Config Aggregator: This allows you to aggregate AWS Config data from multiple accounts and Regions into a single account, providing a comprehensive view of compliance status across the organization. AWS Lambda Function: By creating a Lambda function that responds to noncompliant findings, you can automate the remediation process. This function can be configured to either delete or reconfigure noncompliant S3 buckets, ensuring they meet the company's data protection policy. This approach ensures that both existing and future noncompliant S3 buckets are addressed automatically, maintaining compliance across the organization.

Question:225 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company’s engineering team is developing a new application that creates AWS Key Management Service (AWS KMS) customer managed key grants for users. Immediately after a grant is created, users must be able to use the KMS key to encrypt a 512-byte payload. During load testing, AccessDeniedException errors occur occasionally when a user first attempts to use the key to encrypt.

Which solution should the company’s security specialist recommend to eliminate these AccessDeniedException errors?

- A. Instruct users to implement a retry mechanism every 2 minutes until the call succeeds.
- B. Instruct the engineering team to consume a random grant token from users and to call the CreateGrant operation by passing the grant token to the operation. Instruct users to use that grant token in their call to encrypt.
- C. Instruct the engineering team to create a random name for the grant when calling the CreateGrant operation. Return the name to the users and instruct them to provide the name as the grant token in the call to encrypt.
- D. Instruct the engineering team to pass the grant token returned in the CreateGrant response to users. Instruct users to use that grant token in their call to encrypt.

Correct Answer: *D*
Explanation:
The AWS KMS API follows an eventual consistency model. When you create a grant, the grant might not be effective immediately. To use the permissions in a new grant immediately, use the grant token for the grant.
Reference:
https://docs.aws.amazon.com/kms/latest/developerguide/using-grant-token.html

Question:226 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company hosts its public website on Amazon EC2 instances behind an Application Load Balancer (ALB). The website is experiencing a global DDoS attack by a specific IoT device brand that has a unique user agent.

A security engineer is creating an AWS WAF web ACL and will associate the web ACL with the ALB. The security engineer must implement a rule statement as part of the web ACL to block the requests. The rule statement must mitigate the current attack and future attacks from these IoT devices without blocking requests from customers.

Which rule statement will meet these requirements?

- A. Use an IP set match rule statement that includes the IP address for IoT devices from the user agent.
- B. Use a geographic match rule statement. Configure the statement to block countries that the IoT devices are located in.
- C. Use a rate-based rule statement. Set a rate limit that is equal to the number of requests that are coming from the IoT devices.
- D. Use a string match rule statement that includes details of the IoT device brand from the user agent.

Correct Answer: *D*
Explanation:
This approach targets the unique user agent string of the IoT devices involved in the DDoS attack, effectively blocking malicious traffic while allowing legitimate requests from customers to pass through.

Question:227 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company has configured a gateway VPC endpoint in a VPC. Only Amazon EC2 instances that reside in a single subnet in the VPC can use the endpoint.

The company has modified the route table for this single subnet to route traffic to Amazon S3 through the gateway VPC endpoint. The VPC provides internet access through an internet gateway.

A security engineer attempts to use instance profile credentials from an EC2 instance to retrieve an object from the S3 bucket, but the attempt fails. The security engineer verifies that the EC2 instance has an IAM instance profile with the correct permissions to access the S3 bucket and to retrieve objects. The security engineer also verifies that the S3 bucket policy is allowing access properly. Additionally, the security engineer verifies that the EC2 instance's security group and the subnet's network ACLs allow the communication.

What else should the security engineer check to determine why the request from the EC2 instance is failing?

- A. Verify that the EC2 instance's security group does not have an implicit inbound deny rule for Amazon S3.
- B. Verify that the VPC endpoint's security group does not have an explicit inbound deny rule for the EC2 instance.
- C. Verify that the internet gateway is allowing traffic to Amazon S3.
- D. Verify that the VPC endpoint policy is allowing access to Amazon S3.

Correct Answer: *D*
Explanation:
Even if the IAM instance profile, S3 bucket policy, security group, and network ACLs are correctly configured, the VPC endpoint policy must also allow access to the S3 bucket. If the endpoint policy is too restrictive, it could prevent the EC2 instance from accessing S3, causing the request to fail.
Reference:
https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints-s3.html

Question:228 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***
A security administrator is restricting the capabilities of company root user accounts. The company uses AWS Organizations and has all features enabled.
The management account is used for billing and administrative purposes, but it is not used for operational AWS resource purposes.

How can the security 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 (MFA) of the root user account for each organization member account.
- B. Configure IAM user policies to restrict root account capabilities for each organization member account.
- C. Create an OU in Organizations, and attach an SCP that controls usage of the root user. Add all member accounts to the new OU.
- D. Configure AWS CloudTrail to integrate with Amazon CloudWatch Logs. Create a metric filter for RootAccountUsage.

Correct Answer: *C*
Explanation:
SCP Enforcement: SCPs act as guardrails, preventing root users in member accounts from performing any AWS actions. Centralized Management: The SCP is managed by the organization's management account, ensuring member root users cannot bypass it.

Question:229 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***
A company wants to start processing sensitive data on Amazon EC2 instances. The company will use Amazon CloudWatch Logs to monitor, store, and access log files from the EC2 instances.

The company's developers use CloudWatch Logs for troubleshooting. A security engineer must implement a solution that prevents the developers from viewing the sensitive data. The solution must automatically apply to any new log groups that are created in the account in the future.

Which solution will meet these requirements?

- A. Create a CloudWatch Logs account-wide data protection policy. Specify the appropriate data identifiers for the policy. Ensure that the developers do not have the logs:Unmask IAM permission.
- B. Export the CloudWatch Logs data to an Amazon S3 bucket. Set up automated discovery by using Amazon

Macie on the S3 bucket. Create a custom data identifier for the sensitive data. Remove the developers' access to CloudWatch Logs. Grant permissions for the developers to view the exported log data in Amazon S3.

- C. Export the CloudWatch Logs data to an Amazon S3 bucket. Set up automated discovery by using Amazon Macie on the S3 bucket. Specify the appropriate managed data identifiers. Remove the developers' access to CloudWatch Logs. Grant permissions for the developers to view the exported log data in Amazon S3.
- D. Create a CloudWatch Logs data protection policy for each log group. Specify the appropriate data identifiers for the policy. Ensure that the developers do not have the logs:Unmask IAM permission.

Correct Answer: *A*
Explanation:
AWS CloudWatch Logs account-level data protection policies allow organizations to mask or redact sensitive data automatically across all log groups in an AWS account. This is the most scalable solution because it applies automatically to all current and future log groups, ensuring sensitive data is always protected.

Question:230 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A security engineer needs to implement a solution to identify any sensitive data that is stored in an Amazon S3 bucket. The solution must report on sensitive data in the S3 bucket by using an existing Amazon Simple Notification Service (Amazon SNS) topic.

Which solution will meet these requirements with the LEAST implementation effort?

- A. Enable AWS Config. Configure AWS Config to monitor for sensitive data in the S3 bucket and to send notifications to the SNS topic.
- B. Create an AWS Lambda function to scan the S3 bucket for sensitive data that matches a pattern. Program the Lambda function to send notifications to the SNS topic.
- C. Configure Amazon Macie to use managed data identifiers to identify and categorize sensitive data. Create an Amazon EventBridge rule to send notifications to the SNS topic.
- D. Enable Amazon GuardDuty. Configure AWS CloudTrail S3 data events. Create an Amazon CloudWatch alarm that reacts to GuardDuty findings and sends notifications to the SNS topic.

Correct Answer: *C*
Explanation:
Amazon Macie is designed specifically for automated discovery and classification of sensitive data in Amazon S3 using managed data identifiers. It can identify PII, financial data, and credentials with minimal setup. Macie findings can be integrated with Amazon EventBridge, which can send alerts to an SNS topic for notifications.

This option requires the least implementation effort because:
✅ Macie is a fully managed service – No custom scripting or manual configuration needed.
✅ Uses built-in managed data identifiers – No need to define custom regex patterns.
✅ Seamless EventBridge integration – Automatically triggers notifications.
✅ Scales automatically across S3 buckets and objects.

Question:231 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company has an application on Amazon EC2 instances that store confidential customer data. The company must restrict access to customer data. A security engineer requires secure access to the instances that host the application. According to company policy, users must not open any inbound ports, maintain bastion hosts, or manage SSH keys for the EC2 instances.

The security engineer wants to monitor, store, and access all session activity logs. The logs must be encrypted.

Which solution will meet these requirements?

- A. Use AWS Control Tower to connect to the EC2 instances. Configure Amazon CloudWatch logging for the sessions. Select the upload session logs option and allow only encrypted CloudWatch Logs log groups.
- B. Use AWS Security Hub to connect to the EC2 instances. Configure Amazon CloudWatch logging for the sessions. Select the upload session logs option and allow only encrypted CloudWatch Logs log groups.
- C. Use AWS Systems Manager Session Manager to connect to the EC2 instances. Configure Amazon

CloudWatch monitoring to record the sessions. Select the store session logs option for the desired CloudWatch Logs log groups.
- D. Use AWS Systems Manager Session Manager to connect to the EC2 instances. Configure Amazon CloudWatch logging. Select the upload session logs option and allow only encrypted CloudWatch Logs log groups.

Correct Answer: *D*
Reference:
https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager-logging-cloudwatch-logs.html

Question:232

A company uses an organization in AWS Organizations to help separate its Amazon EC2 instances and VPCs. The company has separate OUs for development workloads and production workloads.

A security engineer must ensure that only AWS accounts in the production OU can write VPC flow logs to an Amazon S3 bucket. The security engineer is configuring the S3 bucket policy with a Condition element to allow the s3:PutObject action for VPC flow logs.

How should the security engineer configure the Condition element to meet these requirements?

- A. Set the value of the aws:SourceOrgID condition key to be the organization ID.
- B. Set the value of the aws:SourceOrgPaths condition key to be the Organizations entity path of the production OU.
- C. Set the value of the aws:ResourceOrgID condition key to be the organization ID.
- D. Set the value of the aws:ResourceOrgPaths condition key to be the Organizations entity path of the production OU.

Correct Answer: *B*

Question:233

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

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

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

Correct Answer: *AB*
Explanation:
A. File permissions issue – If the file permissions change (e.g., log rotation modifies ownership or access rights), the CloudWatch Logs agent may lose access to the logs and stop forwarding them.

B. Log rotation issue – Many operating systems use log rotation mechanisms (e.g., logrotate in Linux). If a log file is rotated and the CloudWatch Logs agent is not configured to handle rotation correctly, it may lose track of the log stream and stop sending logs.

Question:234

A security engineer has designed a VPC to segment private traffic from public traffic. The VPC includes two Availability Zones. The security engineer has provisioned each Availability Zone with one private subnet and one public subnet. The security engineer has created three route tables for use with the environment. One route table is for the public subnets, and two route tables are for the private subnets (one route table for the private subnet in each Availability Zone).

The security engineer discovers that all four subnets are attempting to route traffic out through the internet gateway that is attached to the VPC.

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

- A. Verify that a NAT gateway has been provisioned in the public subnet in each Availability Zone.
- B. Verify that a NAT gateway has been provisioned in the private subnet in each Availability Zone.
- C. Modify the route tables that are associated with each of the public subnets. Create a new route for local destinations to the VPC CIDR range.
- D. Modify the route tables that are associated with each of the private subnets. Create a new route for the destination 0.0.0.0/0. Specify the NAT gateway in the public subnet of the same Availability Zone as the target of the route.
- E. Modify the route tables that are associated with each of the private subnets. Create a new route for the destination 0.0.0.0/0. Specify the internet gateway in the public subnet of the same Availability Zone as the target of the route.

Correct Answer: *AD*
Explanation:
A. NAT Gateway Provisioning: NAT gateways need to be in the public subnet of each Availability Zone to enable instances in the private subnets to connect to the internet for updates and other tasks, without exposing these instances directly to the internet.

D. Route Table Modification: Private subnets should route their outbound internet traffic to the NAT gateway in the corresponding public subnet. This ensures that private subnet traffic passes through the NAT gateway, which then routes it to the internet gateway, maintaining security by preventing direct internet access.

Question:235

A company hired an external consultant who needs to use a laptop to access the company's VPCs. Specifically, the consultant needs access to two VPCs that are peered together in the same AWS Region. The company wants to provide the consultant with access to these VPCs without also providing any unnecessary access to other network resources.

Which solution will meet these requirements?

- A. Create an AWS Site-to-Site VPN endpoint in the same Region as the VPCs. Configure access through an appropriate subnet and authorization rule.
- B. Create an AWS account. Use the VPC sharing feature through AWS Resource Access Manager to allow the consultant to access the VPCs.
- C. Create an AWS Client VPN endpoint in the same Region as the VPCs. Configure access through an appropriate subnet and authorization rule.
- D. Create a gateway VPC endpoint in the same Region as the VPCs. Configure access through an appropriate subnet and authorization rule.

Correct Answer: *C*

Question:236

A company uses AWS Organizations to manage a small number of AWS accounts. However, the company plans to add 1,000 more accounts soon. The company allows only a centralized security team to create IAM roles for all AWS accounts and teams. Application teams submit requests for IAM roles to the security team. The security team has a backlog of IAM role requests and cannot review and provision the IAM roles quickly.

The security team must create a process that will allow application teams to provision their own IAM roles. The process must also limit the scope of IAM roles and prevent privilege escalation.

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

- A. Create an IAM group for each application team. Associate policies with each IAM group. Provision IAM users for each application team member. Add the new IAM users to the appropriate IAM group by using

role-based access control (RBAC).
- B. Delegate application team leads to provision IAM roles for each team. Conduct a quarterly review of the IAM roles the team leads have provisioned. Ensure that the application team leads have the appropriate training to review IAM roles.
- C. Put each AWS account in its own OU. Add an SCP to each OU to grant access to only the AWS services that the teams plan to use. Include conditions in the AWS account of each team.
- D. Create an SCP and a permissions boundary for IAM roles. Add the SCP to the root OU so that only roles that have the permissions boundary attached can create any new IAM roles.

Correct Answer: *D*
Explanation:
Service Control Policies (SCPs) and permissions boundaries are effective tools for controlling the maximum permissions an IAM role can have within an AWS Organization. By attaching an SCP to the root organizational unit (OU), you ensure that only roles with the permissions boundary can be created, which enforces strict controls on what these roles can do. This approach allows application teams to create roles within the defined boundaries, reducing the security team's workload and preventing privilege escalation.

Question:237 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A developer is receiving AccessDenied errors when the developer invokes API calls to AWS services from a workstation. The developer previously configured environment variables and configuration files on the workstation to use multiple roles with other AWS accounts.

A security engineer needs to help the developer configure authentication. The current credentials must be evaluated without conflicting with other credentials that were previously configured on the workstation.

Where these credentials should be configured to meet this requirement?
- A. In the local AWS CLI configuration file
- B. As environment variables on the local workstation
- C. As variables in the AWS CLI command line options
- D. In the AWS shared configuration file

Correct Answer: *C*
Explanation:
This approach ensures that the specific set of credentials needed for the current task can be provided directly in the CLI command itself, thus avoiding any potential conflicts with the environment variables or configuration files that might contain other credentials for different roles or accounts. Configuring credentials this way ensures that each command can be executed with its own specific set of credentials, without affecting the global or shared configurations on the workstation.

Question:238 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A medical company recently completed an acquisition and inherited an existing AWS environment. The company has an upcoming audit and is concerned about the compliance posture of its acquisition.

The company must identify personal health information inside Amazon S3 buckets and must identify S3 buckets that are publicly accessible. The company needs to prepare for the audit by collecting evidence in the environment.

Which combination of steps will meet these requirements with the LEAST operational overhead? (Choose three.)
- A. Enable Amazon Macie. Run an on-demand sensitive data discovery job that uses the PERSONAL_INFORMATION managed data identifier.
- B. Use AWS Glue with the Detect PII transform to identify sensitive data and to mask the sensitive data.
- C. Enable AWS Audit Manager. Create an assessment by using a supported framework.
- D. Enable Amazon GuardDuty S3 Protection. Document any findings that are related to suspicious access of S3 buckets.
- E. Enable AWS Security Hub. Use the AWS Foundational Security Best Practices standard. Review the controls dashboard for evidence of failed S3 Block Public Access controls.
- F. Enable AWS Config. Set up the s3-bucket-public-write-prohibited AWS Config managed rule.

Correct Answer: *ACE*
Explanation:
A. Amazon Macie specializes in discovering sensitive data, such as personal health information, within your S3 buckets. This directly addresses the need to identify such data.

C. AWS Audit Manager helps you create assessments and gather evidence based on compliance frameworks, preparing you thoroughly for the audit.

E. AWS Security Hub provides a consolidated view of your security posture and identifies public access issues for S3 buckets, helping you review and document compliance with best practices.

Question:239 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

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.

Correct Answer: *BCE*
Explanation:
B. Enable termination protection for the EC2 instance if termination protection has not been enabled. This prevents accidental termination of the instance during the investigation.

C. Take snapshots of the Amazon Elastic Block Store (Amazon EBS) data volumes that are attached to the EC2 instance. Creating snapshots ensures that you have a backup of the current state of your data volumes, which is crucial for forensic analysis.

E. Capture the EC2 instance metadata, and then tag the EC2 instance as under quarantine. Capturing metadata provides information about the instance that could be useful during the investigation, and tagging the instance helps in tracking and managing the investigation process.

Question:240 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company is implementing a customized notification solution to detect repeated unauthorized authentication attempts to bastion hosts. The company's security engineer needs to implement a solution that will provide notification when 5 failed attempts occur within a 5-minute period. The solution must use native AWS services and must notify only the designated system administrator who is assigned to the specific bastion host.

Which solution will meet these requirements?

- A. Use the Amazon CloudWatch agent to collect operating system logs. Use Amazon EventBridge to configure an alarm based on a metric filter for failed login attempts. Send an alert to Amazon Simple Notification Service (Amazon SNS) when the defined threshold for the alarm is exceeded. Use Amazon EC2 instance tags to determine which SNS topics receive notifications.
- B. Use AWS Systems Manager Agent to collect operating system logs. Use the Systems Manager Run Command AWS-ConfigureCloudWatch document to configure an Amazon EventBridge event based on a metric filter for failed login attempts. Send an alert to Amazon Simple Notification Service (Amazon SNS) when the defined threshold for the alarm is exceeded. Use SNS messaging filters to control who receives notifications.
- C. Use the Amazon CloudWatch agent to collect operating system logs. Create a CloudWatch alarm based on a metric filter for failed login attempts. Send an alert to Amazon Simple Notification Servige (Amazon SNS) when the defined threshold for the alarm is exceeded. Use SNS messaging filters to control who receives

notifications.

- D. Use AWS Systems Manager Agent to collect operating system logs. Use the Systems Manager Run Command AWS-ConfigureCloudWatch document to configure an Amazon CloudWatch alarm based on a metric filter for failed login attempts. Send an alert to Amazon Simple Notification Service (Amazon SNS) when the defined threshold for the alarm is exceeded. Use EC2 instance tags to determine which SNS topics receive notifications.

Correct Answer: *C*
Explanation:
CloudWatch Agent and Logs: The Amazon CloudWatch agent is configured to collect operating system logs, making it an ideal choice for monitoring failed login attempts.

CloudWatch Alarm and Metric Filter: Creating a CloudWatch alarm based on a metric filter for failed login attempts ensures that you can set up precise conditions, such as 5 failed attempts within a 5-minute period.

SNS and Messaging Filters: Amazon SNS is used to send alerts when the threshold is exceeded. SNS messaging filters can be used to control who receives notifications, ensuring that only the designated system administrator for the specific bastion host is notified.

Question:241 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

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.

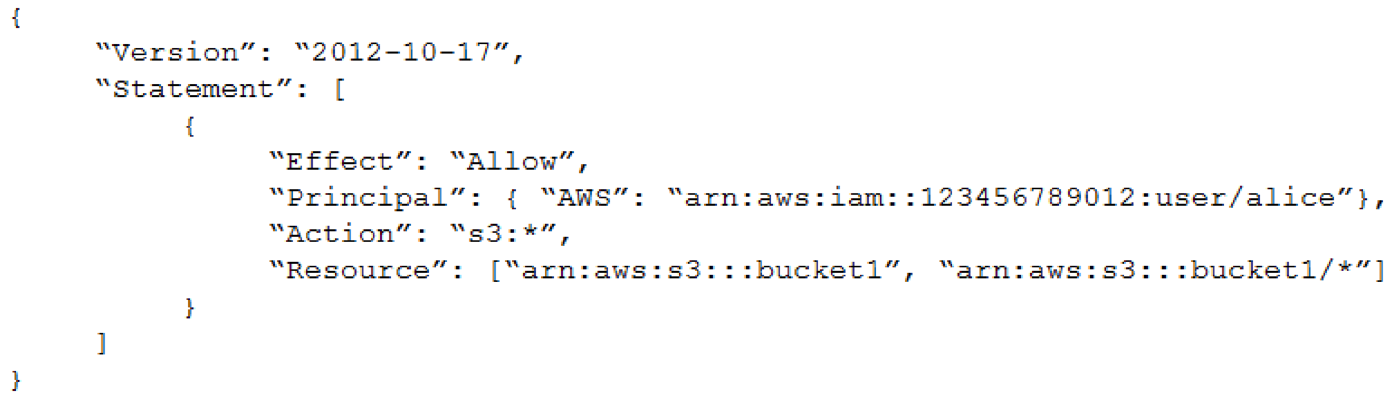
Which steps would help achieve this? (Choose two.)

- 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 EventBridge 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.

Correct Answer: *BE*
Explanation:
B. Provides enhanced protection against DDoS attacks, including advanced mitigation capabilities. Includes 24/7 access to the AWS DDoS Response Team (DRT) for immediate assistance during an attack. Also provides cost protection to prevent unexpected charges due to scaling during a DDoS attack.
E. AWS WAF can help create custom rules to detect and block malicious traffic patterns (e.g., rate-based rules, IP address blocking, or patterns indicative of DDoS).
It integrates with AWS Shield and CloudFront for real-time traffic filtering.
By setting up rate-limiting rules, WAF can help mitigate volumetric attacks.

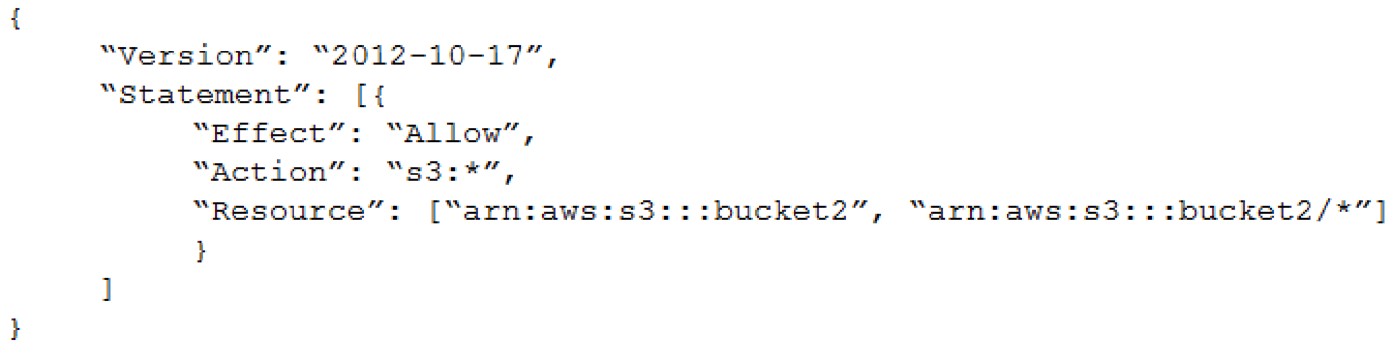
Question:242 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

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



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

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



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

Which buckets can user “alice” access?

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

Correct Answer: *C*
Explanation:
bucket1 has a policy that explicitly allows user "alice" access to arn:aws:s3:::bucket1/*.

bucket2 has no bucket policy, but "alice"'s IAM policy allows access to arn:aws:s3:::bucket2/*.

Here's the access situation:

bucket1: User "alice" can access bucket1 because the bucket policy explicitly allows it.

bucket2: User "alice" can access bucket2 because her IAM policy grants her permission to it, and there is no bucket policy to restrict this access.

So, user "alice" can access both bucket1 and bucket2.

Question:243 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company plans to create Amazon S3 buckets to store log data. All the S3 buckets will have versioning enabled and will use the S3 Standard storage class.

A security engineer needs to implement a solution that protects objects in the S3 buckets from deletion for 90 days. The solution must ensure that no object can be deleted during this time period, even by an administrator or the AWS account root user.

Which solution will meet these requirements?

- A. Enable S3 Object Lock in governance mode. Set a legal hold of 90 days.
- B. Enable S3 Object Lock in governance mode. Set a retention period of 90 days.

- C. Enable S3 Object Lock in compliance mode. Set a retention period of 90 days.
- D. Create an S3 Glacier Vault Lock policy that prevents deletion for 90 days.

Correct Answer: *C*

Question:244 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company has used AWS Lambda functions to build an application on AWS. The company's security engineer implemented Amazon Inspector and activated Lambda standard scanning and Lambda code scanning.

The security engineer reviews the Amazon Inspector console and learns that Amazon Inspector is not scanning some of the Lambda functions. The provided reason is that the scan eligibility expired.

What should the security engineer do to investigate the reason that the scans are failing?

- A. Validate that the AmazonInspector2ServiceRolePolicy AWS managed policy grants permissions to access Lambda.
- B. Increase the timeout value of the Lambda functions to complete the scans successfully while the code is running.
- C. Build a custom runtime for the unscanned Lambda functions. Include the Amazon Inspector agent in the runtime.
- D. Determine whether the unscanned Lambda functions have been invoked in the last 90 days.

Correct Answer: *D*
Explanation:
Amazon Inspector's eligibility for scanning Lambda functions is typically based on activity. If a Lambda function has not been invoked in the last 90 days, it may no longer be eligible for scanning. This helps ensure that only active and potentially vulnerable functions are scanned, optimizing resource usage and focusing on functions that are in use.
Reference:
https://docs.aws.amazon.com/inspector/latest/user/scanning-lambda.html#lambda-scan-behavior

Question:245 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A security engineer received an Amazon GuardDuty alert indicating a finding involving the Amazon EC2 instance that hosts the company's primary website. The GuardDuty finding received read:

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.

The security engineer confirmed that a malicious actor used API access keys intended for the EC2 instance from a country where the company does not operate. The security engineer needs to deny access to the malicious actor.

What is the first step the security engineer should take?

- A. Open the EC2 console and remove any security groups that allow inbound traffic from 0.0.0.0/0.
- B. Install the AWS Systems Manager Agent on the EC2 instance and run an inventory report.
- C. Install the Amazon Inspector agent on the host and run an assessment with the CVE rules package.
- D. Open the IAM console and revoke all IAM sessions that are associated with the instance profile.

Correct Answer: *D*

Question:246 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company is testing incident response procedures for destination containment. The company needs to contain a critical Amazon EC2 instance as quickly as possible while keeping the EC2 instance running. The EC2 instance is the only resource in a public subnet and has active connections to other resources.

Which solution will contain the EC2 instance IMMEDIATELY?

- A. Create a new security group that has no inbound rules or outbound rules. Attach the new security group to the EC2 instance.
- B. Configure the existing security group for the EC2 instance. Remove all existing inbound rules and outbound rules from the security group.
- C. Create a new network ACL that has a single Deny rule for inbound traffic and outbound traffic. Associate

the new network ACL with the subnet that contains the EC2 instance.
- D. Create a new VPC for isolation. Stop the EC2 instance. Create a new AMI from the EC2 instance. Use the new AMI to launch a new EC2 instance in the new VPC.

Correct Answer: *C*
Explanation:
This approach will instantly isolate the EC2 instance from the network by denying all inbound and outbound traffic at the subnet level, ensuring no accidental connections can be made.

Question:247

A company needs to use HTTPS when connecting to its web applications to meet compliance requirements. These web applications run in Amazon VPC on Amazon EC2 instances behind an Application Load Balancer (ALB). A security engineer wants to ensure that the load balancer will only accept connections over port 443, even if the ALB is mistakenly configured with an HTTP listener.

Which configuration steps should the security engineer take to accomplish this task?
- A. Create a security group with a rule that denies inbound connections from 0.0.0.0/0 on port 80. Attach this security group to the ALB to overwrite more permissive rules from the ALB’s default security group.
- B. Create a network ACL that denies inbound connections from 0.0.0.0/0 on port 80. Associate the network ACL with the VPC’s internet gateway.
- C. Create a network ACL that allows outbound connections to the VPC IP range on port 443 only. Associate the network ACL with the VPC’s internet gateway.
- D. Create a security group with a single inbound rule that allows connections from 0.0.0.0/0 on port 443. Ensure this security group is the only one associated with the ALB.

Correct Answer: *D*
Reference:
https://docs.aws.amazon.com/vpc/latest/userguide/security-group-rules.html

Question:248

A consultant agency needs to perform a security audit for a company’s production AWS account. Several consultants need access to the account. The consultant agency already has its own AWS account.

The company requires multi-factor authentication (MFA) for all access to its production account. The company also forbids the use of long-term credentials.

Which solution will provide the consultant agency with access that meets these requirements?
- A. Create an IAM group. Create an IAM user for each consultant. Add each user to the group. Turn on MFA for each consultant.
- B. Configure Amazon Cognito on the company’s production account to authenticate against the consultant agency’s identity provider (IdP). Add MFA to a Cognito user pool.
- C. Create an IAM role in the consultant agency’s AWS account. Define a trust policy that requires MFA. In the trust policy, specify the company’s production account as the principal. Attach the trust policy to the role.
- D. Create an IAM role in the company’s production account. Define a trust policy that requires MFA. In the trust policy, specify the consultant agency’s AWS account as the principal. Attach the trust policy to the role.

Correct Answer: *D*
Explanation:
Security: By creating an IAM role in the company's production account, the consultants will only have temporary access to the specific resources granted by the role. This limits the potential damage if credentials are compromised.

MFA Enforcement: The trust policy can be configured to require MFA for all access to the role, ensuring that consultants are authenticated with a strong second factor.

No Long-Term Credentials: The consultants will not need long-term access keys, as they will use temporary credentials generated by their AWS account.

Granular Access Control: The IAM role can be configured with specific permissions to limit access to only the necessary resources, reducing the risk of unauthorized actions.

This approach provides a secure, flexible, and compliant solution for granting temporary access to the consultant agency while enforcing strong security measures.

Question:249 *SCS-C02: Actual Exam Q&A | CLEARCATNET*

A company uses AWS Lambda functions to implement application logic. The company uses an organization in AWS Organizations to manage hundreds of AWS accounts.

The company needs to implement a solution to continuously monitor the Lambda functions for vulnerabilities in all accounts. The solution must publish detected issues to a dashboard. Lambda functions that are being tested or are in development must not appear on the dashboard.

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

- A. Designate a delegated Amazon GuardDuty administrator account in the organization's management account. Use the GuardDuty Summary dashboard to obtain an overview of Lambda functions that have vulnerabilities.
- B. Designate a delegated Amazon Inspector administrator account in the organization's management account. Use the Amazon Inspector dashboard to obtain an overview of Lambda functions that have vulnerabilities.
- C. Apply tags of "test" or "development" to all Lambda functions that are in testing or development. Use a suppression filter that suppresses findings that contain these tags.
- D. Enable AWS Shield Advanced in the organization's management account. Use Amazon CloudWatch to build a dashboard for Lambda functions that have vulnerabilities.
- E. Enable Lambda Protection in GuardDuty for all accounts. Auto-enable Lambda Protection for new accounts. Apply a tag to the Lambda functions that are in testing or development. Use GuardDutyExclusion as the tag key and LambdaStandardScanning as the tag value.

Correct Answer: *BC*

Question:250 *SCS-C02: Actual Exam Q&A | CLEARCATNET*

A company has an organization in AWS Organizations that includes dedicated accounts for each of its business units. The company is collecting all AWS CloudTrail logs from the accounts in a single Amazon S3 bucket in the top-level account. The company's IT governance team has access to the top-level account. A security engineer needs to allow each business unit to access its own CloudTrail logs.

The security engineer creates an IAM role in the top-level account for each of the other accounts. For each role, the security engineer creates an IAM policy to allow read-only permissions to objects in the S3 bucket with the prefix of the respective logs.

Which action must the security engineer take in each business unit account to allow an IAM user in that account to read the logs?

- A. Attach a policy to the IAM user to allow the user to assume the role that was created in the top-level account. Specify the role's ARN in the policy.
- B. Create an SCP that grants permissions to the top-level account.
- C. Use the root account of the business unit account to assume the role that was created in the top-level account. Specify the role's ARN in the policy.
- D. Forward the credentials of the IAM role in the top-level account to the IAM user in the business unit account.

Correct Answer: *A*
Explanation:
The IAM role in the top-level account is created to allow read-only access to specific CloudTrail logs.
To allow an IAM user in a business unit account to access the logs, the user must assume the role in the top-level account.
An IAM policy must be attached to the IAM user in the business unit account, allowing them to assume the role using

the role's Amazon Resource Name (ARN).

Question:251 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company has configured an organization in AWS Organizations for its AWS accounts. AWS CloudTrail is enabled in all AWS Regions.

A security engineer must implement a solution to prevent CloudTrail from being disabled.

Which solution will meet this requirement?

- A. Enable CloudTrail log file integrity validation from the organization's management account.
- B. Enable server-side encryption with AWS KMS keys (SSE-KMS) for CloudTrail logs. Create a KMS key. Attach a policy to the key to prevent decryption of the logs.
- C. Create an SCP that includes an explicit Deny rule for the StopLogging action and the DeleteTrail action. Attach the SCP to the root OU.
- D. Create IAM policies for all the company's users to prevent the users from performing the DescribeTrails action and the GetTrailStatus action.

Correct Answer: *C*

Explanation:

AWS Organizations allows Service Control Policies (SCPs) to restrict actions across all accounts in an organization or organizational units (OUs). An SCP with an explicit Deny for the StopLogging and DeleteTrail actions will prevent CloudTrail from being stopped or deleted, ensuring continuous logging. SCPs override any IAM permissions in the member accounts, making this the best and most effective solution.

Question:252 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company runs its microservices architecture in Kubernetes containers on AWS by using Amazon Elastic Kubernetes Service (Amazon EKS) and Amazon Aurora The company has an organization in AWS Organizations to manage hundreds of AWS accounts that host different microservices.

The company needs to implement a monitoring solution for logs from all AWS resources across all accounts. The solution must include automatic detection of security-related issues.

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

- A. Designate an Amazon GuardDuty administrator account in the organization's management account. Enable GuardDuty for all accounts. Enable EKS Protection and RDS Protection in the GuardDuty administrator account.
- B. Designate a monitoring account. Share Amazon CloudWatch logs from all accounts with the monitoring account. Configure Aurora to publish all logs to CloudWatch. Use Amazon Inspector in the monitoring account to evaluate the CloudWatch logs.
- C. Create a central Amazon S3 bucket in the organization's management account. Configure AWS CloudTrail in all AWS accounts to deliver CloudTrail logs to the S3 bucket. Configure Aurora to publish all logs to CloudTrail. Use Amazon Athena to query the CloudTrail logs in the S3 bucket for security issues.
- D. Designate a monitoring account. Share Amazon CloudWatch logs from all accounts with the monitoring account. Subscribe an Amazon Kinesis data stream to the CloudWatch logs. Create AWS Lambda functions to process log records in the data stream to detect security issues.

Correct Answer: *A*

Explanation:

Centralized Management: Designating a GuardDuty administrator account allows for centralized management and monitoring across all AWS accounts in the organization.

Automated Threat Detection: GuardDuty provides continuous monitoring for malicious or unauthorized behavior to help protect your AWS accounts, workloads, and data.

EKS and RDS Protection: Enabling EKS Protection and RDS Protection ensures that GuardDuty can monitor and detect security issues specific to your Kubernetes clusters and Aurora databases.

Minimal Operational Overhead: Once enabled, GuardDuty operates continuously and automatically, requiring minimal ongoing management.

The other options, while valid, involve more complex setups and manual processes which increase operational overhead:

Question:253 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

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

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

The security engineer has verified the following:

1. The rule set in the security groups is correct.
2. The rule set in the network ACLs is correct.
3. The rule set in the virtual appliance is correct.

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

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

Correct Answer: *BD*

Question:254 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company has a strict policy against using root credentials. The company's security team wants to be alerted as soon as possible when root credentials are used to sign in to the AWS Management Console.

How should the security team achieve this goal?

- A. Use AWS Lambda to periodically query AWS CloudTrail for console login events and send alerts using Amazon Simple Notification Service (Amazon SNS).
- B. Use Amazon EventBridge to monitor console logins and direct them to Amazon Simple Notification Service (Amazon SNS).
- C. Use Amazon Athena to query AWS IAM Identity Center logs and send alerts using Amazon Simple Notification Service (Amazon SNS) for root login events.
- D. Configure AWS Resource Access Manager to review the access logs and send alerts using Amazon Simple Notification Service (Amazon SNS).

Correct Answer: *B*
Explanation:
The most effective way to achieve this goal is to use Amazon EventBridge.

EventBridge Rule: Create an EventBridge rule that triggers on console login events.
Target SNS Topic: Configure the rule to send notifications to an SNS topic.
SNS Subscriptions: Subscribe relevant security team members or security tools to the SNS topic.
This approach offers several advantages:

Real-time Monitoring: EventBridge can detect and respond to events in real-time, ensuring immediate alerts for root logins.
Scalability: EventBridge can handle a large volume of events efficiently, making it suitable for large-scale environments.

Flexibility: EventBridge can be integrated with various AWS services, allowing for customization and automation of response actions.
Cost-Effective: EventBridge is a serverless service, so you only pay for the resources consumed.

Question:255 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

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.

Correct Answer: *B*

Question:256 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A security engineer is designing security controls for a fleet of Amazon EC2 instances that run sensitive workloads in a VPC. The security engineer needs to implement a solution to detect and mitigate software vulnerabilities on the EC2 instances.

Which solution will meet this requirement?

- A. Scan the EC2 instances by using Amazon Inspector. Apply security patches and updates by using AWS Systems Manager Patch Manager.
- B. Install host-based firewall and antivirus software on each EC2 instance. Use AWS Systems Manager Run Command to update the firewall and antivirus software.
- C. Install the Amazon CloudWatch agent on the EC2 instances. Enable detailed logging. Use Amazon EventBridge to review the software logs for anomalies.
- D. Scan the EC2 instances by using Amazon GuardDuty Malware Protection. Apply security patches and updates by using AWS Systems Manager Patch Manager.

Correct Answer: *A*
Explanation:
Amazon Inspector: It provides automated vulnerability management for your EC2 instances. It continuously scans for vulnerabilities and deviations from best practices, giving you detailed findings and recommendations.

AWS Systems Manager Patch Manager: This tool automates the process of applying security patches and updates, ensuring your instances are always up-to-date with the latest security patches.

This combination offers a comprehensive approach to both detecting and mitigating vulnerabilities with minimal manual intervention, ensuring continuous compliance and security.

Question:257 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company stores sensitive data in AWS Secrets Manager. A security engineer needs to design a solution to generate a notification email when anomalous GetSecretValue API calls occur. The security engineer has configured an Amazon EventBridge rule for all Secrets Manager events that AWS CloudTrail delivers.

Which solution will meet these requirements?

- A. Configure CloudTrail as the target of the EventBridge rule. Set up an attribute filter on the IncomingBytes attribute and enable anomaly detection. Create an Amazon Simple Notification Service (Amazon SNS) topic. Configure a CloudTrail alarm that uses the SNS topic to send the notification.
- B. Configure CloudTrail as the target of the EventBridge rule. Set up an attribute filter on the IncomingBytes attribute and enable anomaly detection. Create an Amazon Simple Queue Service (Amazon SQS) queue. Configure a CloudTrail alarm that uses the SQS queue to send the notification.
- C. Configure Amazon CloudWatch Logs as the target of the EventBridge rule. Set up a metric filter on the IncomingBytes metric and enable anomaly detection. Create an Amazon Simple Notification Service (Amazon SNS) topic. Configure a CloudWatch alarm that uses the SNS topic to send the notification.
- D. Configure Amazon CloudWatch Logs as the target of the EventBridge rule. Use CloudWatch Logs Insights query syntax to search for anomalous GetSecretValue API calls. Create an Amazon Simple Queue Service (Amazon SQS) queue. Configure a CloudWatch alarm that uses the SQS queue to send the notification.

Correct Answer: *C*
Explanation:
EventBridge Rule and CloudWatch Logs: By configuring CloudWatch Logs as the target of the EventBridge rule, you can capture and store all relevant logs for further analysis.

Metric Filter and Anomaly Detection: Setting up a metric filter on the IncomingBytes metric enables detailed monitoring and anomaly detection for specific API call patterns, such as the GetSecretValue API.

SNS Topic for Notifications: Creating an SNS topic ensures that alerts are sent out immediately when an anomaly is detected. CloudWatch alarms can be configured to trigger notifications via SNS, providing timely alerts to the security team.

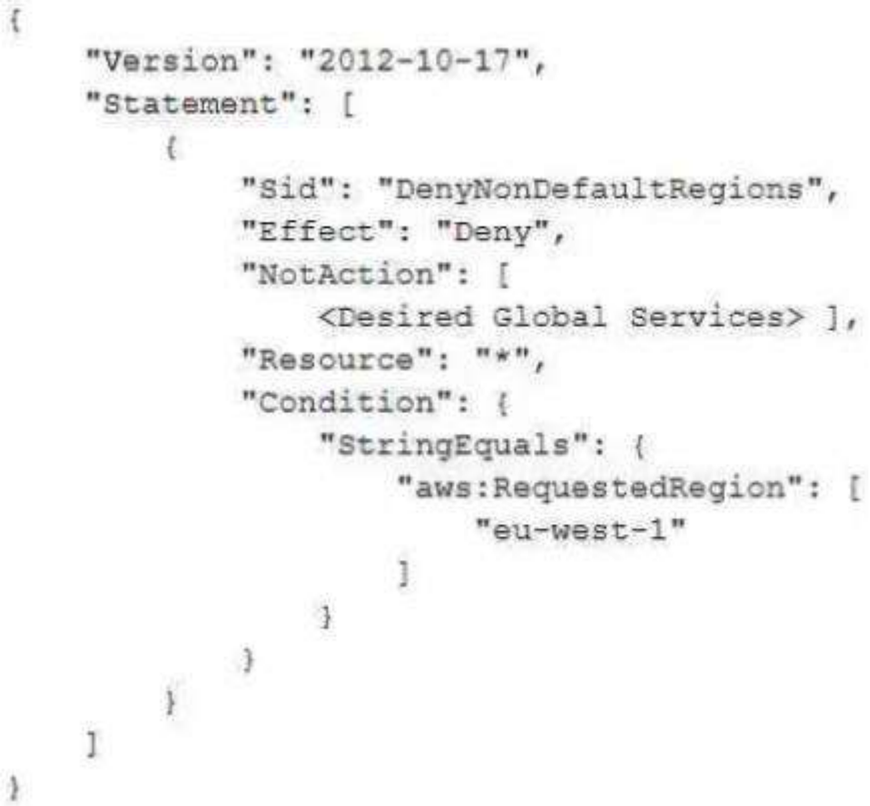
Question:258

A company is using AWS Organizations with the default SCP. The company needs to restrict AWS usage for all AWS accounts that are in a specific OU.

Except for some desired global services, the AWS usage must occur only in the eu-west-1 Region for all accounts in the OU. A security engineer must create an SCP that applies the restriction to existing accounts and any new accounts in the OU.

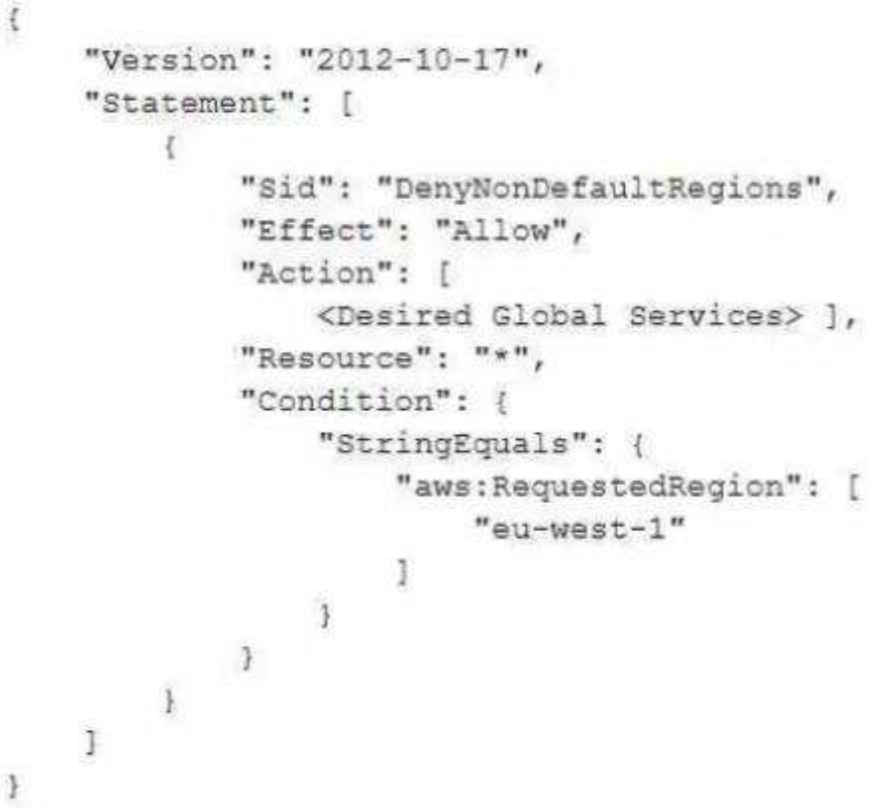
Which SCP will meet these requirements?

- A.



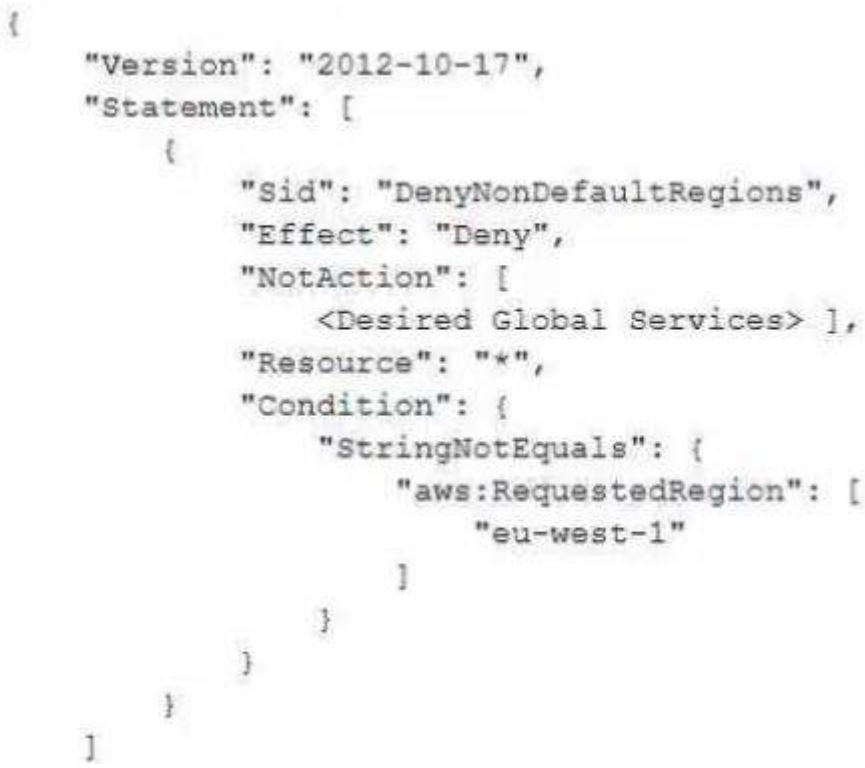
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyNonDefaultRegions",
            "Effect": "Deny",
            "NotAction": [
                <Desired Global Services> ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestedRegion": [
                        "eu-west-1"
                    ]
                }
            }
        }
    ]
}
```

- B.



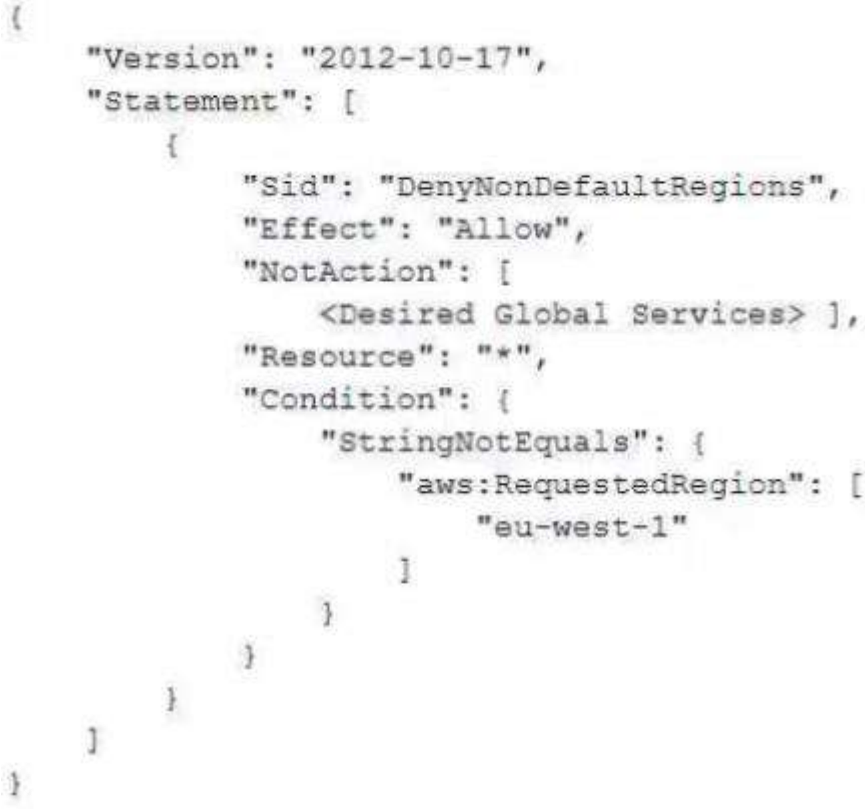
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyNonDefaultRegions",
            "Effect": "Allow",
            "Action": [
                <Desired Global Services> ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestedRegion": [
                        "eu-west-1"
                    ]
                }
            }
        }
    ]
}
```

- C.



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

- D.



```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyNonDefaultRegions",
            "Effect": "Allow",
            "NotAction": [
                <Desired Global Services> ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                        "eu-west-1"
                    ]
                }
            }
        }
    ]
}
```

Correct Answer: *C*

Explanation:

The requirement is to restrict AWS usage to only eu-west-1 region (except for global services).

This means we need to:

Use "Deny" effect to block access

Use "StringNotEquals" condition to deny requests to any region that is NOT eu-west-1

Use "NotAction" to exclude the desired global services from this restriction

Question:259 *SCS-C02: Actual Exam Q&A | CLEARCATNET*

A company is planning to migrate its applications to AWS in a single AWS Region. The company's applications will use a combination of Amazon EC2 instances, Elastic Load Balancing (ELB) load balancers, and Amazon S3 buckets. The company wants to complete the migration as quickly as possible. All the applications must meet the following requirements:

• Data must be encrypted at rest.
• Data must be encrypted in transit.
• Endpoints must be monitored for anomalous network traffic.

Which combination of steps should a security engineer take to meet these requirements with the LEAST effort? (Choose three.)

- A. Install the Amazon Inspector agent on EC2 instances by using AWS Systems Manager Automation.
- B. Enable Amazon GuardDuty in all AWS accounts.
- C. Create VPC endpoints for Amazon EC2 and Amazon S3. Update VPC route tables to use only the secure VPC endpoints.
- D. Configure AWS Certificate Manager (ACM). Configure the load balancers to use certificates from ACM.
- E. Use AWS Key Management Service (AWS KMS) for key management. Create an S3 bucket policy to deny any PutObject command with a condition for x-amz-meta-side-encryption.
- F. Use AWS Key Management Service (AWS KMS) for key management. Create an S3 bucket policy to deny any PutObject command with a condition for x-amz-server-side-encryption.

Correct Answer: *BDF*

Question:260

A security engineer is working with a development team to design a supply chain application that stores sensitive inventory data in an Amazon S3 bucket. The application will use an AWS Key Management Service (AWS KMS) customer managed key to encrypt the data in Amazon S3.

The inventory data in Amazon S3 will be shared with hundreds of vendors. All vendors will use AWS principals from their own AWS accounts to access the data in Amazon S3. The vendor list might change weekly. The security engineer needs to find a solution that supports cross-account access.

Which solution is the MOST operationally efficient way to manage access control for the customer managed key?

- A. Use KMS grants to manage key access. Programmatically create and revoke grants to manage vendor access.
- B. Use am 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.

Correct Answer: *A*
Explanation:
Create KMS Key: Create a customer managed key in your AWS account. Create KMS Grants: For each vendor, create a KMS grant that allows them to encrypt and decrypt data using the key. You can specify the principal (the vendor's AWS account) and the permitted operations. Revoke Grants: When a vendor is no longer authorized, revoke their grant. By using KMS grants, you can efficiently manage access to your sensitive data, ensuring that only authorized vendors can access it. This approach eliminates the need for complex IAM role management and provides a more streamlined and secure solution.
Reference:
https://docs.aws.amazon.com/kms/latest/developerguide/grants.html

Question:261

A company runs an application on a fleet of Amazon EC2 instances behind an Application Load Balancer (ALB). A security engineer needs to provide secure access to the application without requiring the use of a VPN. Users should be able to access the application only when they meet specific security conditions, including a defined device posture.

Which solution will meet these requirements?

- A. Create an AWS WAF web ACL. Configure a custom response to block traffic that does not align with the defined device posture.
- B. Configure AWS Verified Access. Add the application by creating an endpoint for the ALB.
- C. Configure Amazon Verified Permissions. Use a policy-based access control (PBAC) policy to perform authorization.
- D. Configure Amazon Verified Permissions. Add the application by creating an endpoint for the ALB.

Correct Answer: *B*
Explanation:
AWS Verified Access: This service provides secure access to corporate applications without requiring a VPN. It evaluates each application request in real-time and ensures that users can access the application only when they meet specific security conditions, including device posture. Endpoint for ALB: By creating an endpoint for the Application Load Balancer (ALB), you can integrate Verified Access with your application, ensuring that access is controlled and secure. This solution aligns with the requirement of providing secure access without a VPN and ensuring that access is granted based on specific security conditions.

Question:262 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company needs to retain data that is stored in Amazon CloudWatch Logs log groups. The company must retain this data for 90 days. The company must receive notification in AWS Security Hub when log group retention is not compliant with this requirement.

Which solution will provide the appropriate notification?

- A. Create a Security Hub custom action to assess the log group retention period.
- B. Create a data protection policy in CloudWatch Logs to assess the log group retention period.
- C. Create a Security Hub automation rule. Configure the automation rule to assess the log group retention period.
- D. Use the AWS Config managed rule that assesses the log group retention period. Ensure that AWS Config integration is enabled in Security Hub.

Correct Answer: *D*
Explanation:
AWS Config Managed Rule: AWS Config provides a managed rule specifically for assessing the retention period of CloudWatch Logs log groups. This rule will automatically evaluate whether log groups comply with the specified retention period (in this case, 90 days). Integration with Security Hub: By enabling AWS Config integration with Security Hub, non-compliant configurations identified by AWS Config can trigger notifications in Security Hub. This ensures that any deviations from the retention policy are promptly reported.

Question:263 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company needs to prevent Amazon S3 objects from being shared with IAM identities outside of the company's organization in AWS Organizations. A security engineer is creating and deploying an SCP to accomplish this goal. The company has enabled the S3 Block Public Access feature on all of its S3 buckets.

What should the SCP do to meet these requirements?

- A. Deny the S3:* action with a Condition element that comprises an operator of StringNotEquals, a key of aws:ResourceOrgID, and a value of S{aws PrincipalOrgID}.
- B. Deny the S3:PutAccountPublicAccessBlock action with a Condition element that comprises an operator of StringLike, a key of aws:PrincipalArn, and the values of the external IAM principals.
- C. Allow the S3:* action with a Condition element that comprises an operator of StringNotEquals, a key of aws:PrincipalOrgID, and a value of S{aws:PrincipalOrgID}.
- D. Deny the S3:* action with a Condition element that comprises an operator of StringLike, a key of aws:PrincipalArn, and the values of the external IAM principals

Correct Answer: *A*
Explanation:
Use an SCP (Service Control Policy) – SCPs define what actions are allowed or denied across all accounts in an AWS Organization. Block access to resources for IAM principals outside of the organization – This ensures that only

identities within the company's AWS Organization can access the S3 objects. Use the correct condition key: aws:PrincipalOrgID refers to the organization ID of the AWS principal making the request. aws:ResourceOrgID refers to the organization ID of the AWS account that owns the resource. StringNotEquals ensures that the action is denied unless the resource belongs to the company's organization.

Question:264 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A security engineer is implementing authentication for a multi-account environment by using federated access with SAML 2.0. The security engineer has configured AWS IAM Identity Center as an identity provider (IdP). The security engineer also has created IAM roles to grant access to the AWS accounts.

A federated user reports an authentication failure when the user attempts to authenticate with the new system.

What should the security engineer do to troubleshoot this issue in the MOST operationally efficient way?

- A. Review the SAML IdP logs to identify errors. Check AWS CloudTrail to verify the API calls that the user made.
- B. Review the SAML IdP logs to identify errors. Use the IAM policy simulator to validate access to the IAM roles.
- C. Use IAM access advisor to review recent service access. Use the IAM policy simulator to validate access to the IAM roles.
- D. Recreate the SAML IdP in a separate account to confirm the behavior that the user is experiencing.

Correct Answer: *A*
Explanation:
When troubleshooting authentication failures in a federated SAML 2.0 authentication setup with AWS IAM Identity Center, you need to check two key areas: SAML IdP logs (Identity Provider logs) – This helps identify issues related to SAML assertions, incorrect attributes, or user authentication failures before reaching AWS. AWS CloudTrail logs – This helps verify whether the authentication request reached AWS, if it was processed correctly, and if any errors occurred at the IAM role level.

Question:265 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company stores sensitive data in an Amazon S3 bucket. The company encrypts the data at rest by using server-side encryption with Amazon S3 managed keys (SSE-S3).

A security engineer must prevent any modifications to the data in the S3 bucket.

Which solution will meet this requirement?

- A. Configure S3 bucket policies to deny DELETE and PUT object permissions.
- B. Configure S3 Object Lock in compliance mode with S3 bucket versioning enabled.
- C. Change the encryption on the S3 bucket to use AWS Key Management Service (AWS KMS) customer managed keys.
- D. Configure the S3 bucket with multi-factor authentication (MFA) delete protection.

Correct Answer: *B*
Explanation:
S3 Object Lock in compliance mode ensures that the objects cannot be deleted or overwritten for a fixed amount of time or indefinitely, providing a strong safeguard against accidental or malicious changes. Enabling versioning adds an additional layer of protection by keeping multiple versions of an object, which can be useful for recovery purposes.

Question:266 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company is developing a new serverless application that uses AWS Lambda functions. The company uses AWS CloudFormation to deploy the Lambda functions.

The company's developers are trying to debug a Lambda function that is deployed. The developers cannot debug the Lambda function because the Lambda function is not logging its output to Amazon CloudWatch Logs.

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

- A. Check the role that is defined in the CloudFormation template and is passed to the Lambda function. Ensure that the role has a trust policy that allows the sts:AssumeRole action by the service principal lambda amazonaws.com.
- B. Check the execution role that is configured in the CloudFormation template for the Lambda function. Ensure that the execution role has the necessary permissions to write to CloudWatch Logs.
- C. Check the Lambda function configuration in the CloudFormation template. Ensure that the Lambda function has an AWS X-Ray tracing configuration that is set to Active mode or PassThrough mode.
- D. Check the resource policy that is configured in the CloudFormation template for the Lambda function. Ensure that the resource policy has the necessary permissions to write to CloudWatch Logs.
- E. Check the role that the developers use to debug the Lambda function. Ensure that the role has a trust policy that allows the sts:AssumeRole action by the service principal lambda.amazonaws.com.

Correct Answer: *AB*
Explanation:
Trust policy check (A):

Allows Lambda to assume role
Required for function execution
Basic Lambda requirement
Must be properly configured

Execution role permissions (B):

Needed for CloudWatch Logs access
Required for log writing
Must include logging permissions
Essential for logging functionality

Question:267 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company uses a collaboration application. A security engineer needs to configure automated alerts from AWS Security Hub in the us-west-2 Region for the application. The security engineer wants to receive an alert in a channel in the application every time Security Hub receives a new finding.

The security engineer creates an AWS Lambda function to convert the message to the format that the application requires. The Lambda function also sends the message to the application's API. The security engineer configures a corresponding Amazon EventBridge rule that specifies the Lambda function as the target.

After the EventBridge rule is implemented, the channel begins to constantly receive alerts from Security Hub. Many of the alerts are Amazon Inspector alerts that do not require any action. The security engineer wants to stop the Amazon Inspector alerts.

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

- A. Update the Lambda function code to find pattern matches of events from Amazon Inspector and to suppress the findings.
- B. Create a Security Hub custom action that automatically sends findings from all services except Amazon Inspector to the EventBridge event bus.
- C. Modify the value of the ProductArn attribute in the event pattern of the EventBridge rule to "anything-but": ["arn:aws:securityhub:us-west-2::product/aws/inspector"].
- D. Create an Amazon Simple Notification Service (Amazon SNS) topic to send messages to the application. Set a filter policy on the topic subscriptions to reject any messages that contain the product/aws/inspector string.

Correct Answer: *C*

Question:268 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company has an organization in AWS Organizations. The organization consists of multiple OUs. The company must prevent IAM principals from outside the organization from accessing the organization’s Amazon S3 buckets. The solution must not affect the existing access that the OUs have to the S3 buckets.

Which solution will meet these requirements?

- A. Configure S3 Block Public Access for all S3 buckets.
- B. Configure S3 Block Public Access for all AWS accounts.
- C. Deploy an SCP that includes the “aws:ResourceOrgPaths”: “${aws:PrincipalOrgPaths}” condition.
- D. Deploy an SCP that includes the “aws:ResourceOrgID”: “${aws:PrincipalOrgID}" condition.

Correct Answer: *D*

Question:269 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company needs to implement data lifecycle management for Amazon RDS snapshots. The company will use AWS Backup to manage the snapshots.

The company must retain RDS automated snapshots for 5 years and will use Amazon S3 for long-term archival storage.

Which solution will meet these requirements?

- A. Use AWS Backup to apply a 5-year retention tag to the RDS snapshots.
- B. Enable versioning on the S3 bucket that AWS Backup uses for the RDS snapshots. Configure a 5-year retention period.
- C. Create an S3 Lifecycle policy. Include a 5-year retention period for the S3 bucket that AWS Backup uses for the RDS snapshots.
- D. Create a backup plan in AWS Backup. Configure a 5-year retention period.

Correct Answer: *D*

Question:270 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company’s security policy requires all Amazon EC2 instances to use the Amazon Time Sync Service. AWS CloudTrail trails are enabled in all of the company’s AWS accounts. VPC flow logs are enabled for all VPCs.

A security engineer must identify any EC2 instances that attempt to use Network Time Protocol (NTP) servers on the internet.

Which solution will meet these requirements?

- A. Monitor CloudTrail logs for API calls to non-standard time servers.
- B. Monitor CloudTrail logs for API calls to the Amazon Time Sync Service.
- C. Monitor VPC flow logs for traffic to non-standard time servers.
- D. Monitor VPC flow logs for traffic to the Amazon Time Sync Service.

Correct Answer: *C*
Explanation:
VPC Flow Logs is able to capture information about the IP traffic going to and from network interfaces in a VPC.

Question:271 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company has a multi-account strategy that uses an organization in AWS Organizations with all features enabled. The company has enabled trusted access for AWS Account Management. New accounts are provisioned through AWS Control Tower Account Factory.

The company must ensure that all new accounts in the organization become AWS Security Hub member accounts.

Which solution will meet these requirements with the LEAST development effort?

- A. Enable Security Hub in the organization’s management account. Create an AWS Step Functions workflow. Create an Amazon EventBridge rule to invoke the workflow when a CreateAccount event occurs.
- B. Enable Security Hub in the organization’s management account. Wait for all new accounts to complete automatic onboarding.

- C. Enable Security Hub in the organization’s management account. Create an AWS Lambda function to enable Security Hub for new accounts. Invoke the Lambda function by using an AWS Control Tower lifecycle event that occurs when a new account is provisioned.
- D. Use the organization’s management account to designate a Security Hub delegated administrator account. In the delegated administrator account, create a configuration policy to enable Security Hub. Associate the configuration policy with the organization root.

Correct Answer: *D*
Explanation:
It's best practice to designate a delegated security administrator account.
Reference:
https://docs.aws.amazon.com/securityhub/latest/userguide/designate-orgs-admin-account.html
https://docs.aws.amazon.com/securityhub/latest/userguide/create-associate-policy.html

Question:272

A company uses Amazon Elastic Kubernetes Service (Amazon EKS) clusters to run its Kubernetes-based applications. The company uses Amazon GuardDuty to protect the applications.

EKS Protection is enabled in GuardDuty. However, the corresponding GuardDuty feature is not monitoring the Kubernetes-based applications.

Which solution will cause GuardDuty to monitor the Kubernetes-based applications?

- A. Enable VPC flow logs for the VPC that hosts the EKS clusters.
- B. Assign the CloudWatchEventsFullAccess AWS managed policy to the EKS clusters.
- C. Ensure that the AmazonGuardDutyFullAccess AWS managed policy is attached to the GuardDuty service role.
- D. Enable the control plane logs in Amazon EKS. Ensure that the logs are ingested into Amazon CloudWatch.

Correct Answer: *D*
Explanation:
When you enable EKS Protection, GuardDuty will be able to access your Amazon EKS audit logs only for continuous threat detection. So you need to ensure the audit logs is enabled first.
Reference:
https://docs.aws.amazon.com/eks/latest/userguide/integration-guardduty.html

Question:273

A company needs to log object-level activity in its Amazon S3 buckets. The company also needs to validate the integrity of the log file by using a digital signature.

Which solution will meet these requirements?

- A. Create an AWS CloudTrail trail with log file validation enabled. Enable data events. Specify Amazon S3 as the data event type.
- B. Create a new S3 bucket for S3 server access logs. Configure the existing S3 buckets to send their S3 server access logs to the new S3 bucket.
- C. Create an Amazon CloudWatch Logs log group. Configure the existing S3 buckets to send their S3 server access logs to the log group.
- D. Create a new S3 bucket for S3 server access logs with log file validation enabled. Enable data events. Specify Amazon S3 as the data event type.

Correct Answer: *A*
Explanation:
Object-Level Logging: By enabling data events in AWS CloudTrail and specifying Amazon S3 as the data event type, you can log object-level activities such as GET, PUT, DELETE, and other operations on your S3 objects. Log File Validation: AWS CloudTrail provides the option to enable log file integrity validation. When this feature is enabled, CloudTrail creates a hash for each log file and delivers it alongside the log file. This ensures that you can verify the integrity and authenticity of your log files, confirming they haven't been tampered with.

Question:274 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company has a new web-based account management system for an online game. Players create a unique username and password to log in to the system.

The company has implemented an AWS WAF web ACL for the system. The web ACL includes the core rule set (CRS) AWS managed rule group on the Application Load Balancer that serves the system.

The company's security team finds that the system was the target of a credential stuffing attack. Credentials that were exposed in other breaches were used to try to log in to the system.

The security team must implement a solution to reduce the chance of a successful credential stuffing attack in the future. The solution also must minimize impact on legitimate users of the system.

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

- A. Create an Amazon CloudWatch custom metric to analyze the number of successful login responses from a single IP address.
- B. Add the account takeover prevention (ATP) AWS managed rule group to the web ACL. Configure the rule group to inspect login requests to the system. Block any requests that have the awswaf:managed:aws:atp:signal:credential_compromised label.
- C. Configure a default web ACL action that requires all users to solve a CAPTCHA puzzle when they log in.
- D. Implement IP-based match rules in the web ACL for any IP addresses that generate many successful login responses. Block any IP addresses that generate many successful logins.
- E. Create a custom block response that redirects users to a secure workflow to reset their password inside the system.

Correct Answer: *AB*
Explanation:
By monitoring and analysing successful login attempts from individual IP addresses, you can detect patterns that suggest credential stuffing. This allows you to take targeted actions against suspicious IPs, improving security without impacting legitimate users.

B. This managed rule group specifically targets account takeover attempts, including credential stuffing. By automatically inspecting and blocking compromised login requests, you add a critical layer of defense without disrupting legitimate user access.

Question:275 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company is running workloads on AWS. The workloads are in separate AWS accounts for development, testing, and production. All the company's developers can access the development account. A subset of the developers can access the testing account and the production account.

The company is spending too much time managing individual credentials for every developer across every environment. A security engineer must implement a more scalable solution that the company can use when a developer needs different access. The solution must allow developers to access resources across multiple accounts. The solution also must minimize credential sharing.

Which solution will meet these requirements?

- A. Use AWS Identity and Access Management Access Analyzer to identify the permissions that the developers need on each account. Configure IAM Access Analyzer to automatically provision the correct access for each developer.
- B. Create an Amazon Simple Workflow Service (Amazon SWF) workflow. Instruct the developers to use the workflow to request access to other accounts when additional access is necessary.
- C. Create IAM roles in the testing account and production account. Add a policy that allows the sts:AssumeRole action to the roles. Create IAM roles in the development account for the developers who have access to the testing and production accounts. Add these roles to the trust policy on the new roles in the testing and production accounts.
- D. Create service accounts in the testing environment and production environment. Give the access keys for the service accounts to developers who require access to the testing account and the production account.

Rotate the access keys for the service accounts periodically.

Correct Answer: *C*

Question:276 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

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.

Correct Answer: *A*

Question:277 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company runs an application that sends logs to a log group in Amazon CloudWatch Logs. The email addresses of the application users are in the logs.

The company's developers need to view the logs in CloudWatch Logs. A security engineer must ensure that the developers who access the log group cannot see the user email addresses.

Which solution will meet this requirement?

- A. Use Amazon Macie to scan the log group. Configure Macie to use a custom data identifier that uses a regular expression to identify an email address pattern. Activate automated data discovery in Macie.
- B. Create an AWS Key Management Service (AWS KMS) key. Configure the log group to use the key to encrypt the logs. Configure the key policy to deny access to the IAM role that the developers assume to use CloudWatch Logs.
- C. Create a subscription filter for the log group. Configure the log subscription to send the log data to an AWS Lambda function. Program the Lambda function to parse the log entries and to mask values that are email addresses.
- D. Configure a data protection policy for the log group. Specify the AWS managed data identifier of EmailAddress for the type of data to mask. Activate data protection for the log group.

Correct Answer: *D*

Question:278 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A security engineer is implementing a logging solution for a company's AWS environment. The security engineer has configured an AWS CloudTrail trail in the company's AWS account. The logs are stored in an Amazon S3 bucket for a third-party service provider to monitor. The service provider has a designated IAM role to access the S3 bucket.

The company requires all logs to be encrypted at rest with a customer managed key. The security engineer uses AWS

Key Management Service (AWS KMS) to create the customer managed key and key policy. The security engineer also configures CloudTrail to use the key to encrypt the trail.

When the security engineer implements this configuration, the service provider no longer can read the logs.

What should the security engineer do to allow the service provider to read the logs?

- A. Ensure that the S3 bucket policy allows access to the service provider’s role to decrypt objects.
- B. Add a statement to the key policy to allow the service provider’s role the kms:Decrypt action for the key.
- C. Add the AWSKeyManagementServicePowerUser AWS managed policy to the service provider’s role.
- D. Migrate the key to AWS Certificate Manager (ACM) to create a shared endpoint for access to the key.

Correct Answer: *B*

Question:279 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company runs workloads on Amazon EC2 instances. The company needs to continually monitor the EC2 instances for software vulnerabilities and must display the findings in AWS Security Hub. The company must not install agents on the EC2 instances.

Which solution will meet these requirements?

- A. Enable Amazon Inspector. Set the scan mode to hybrid scanning. Enable the integration for Amazon Inspector in Security Hub.
- B. Use Security Hub to enable the AWS Foundational Security Best Practices standard. Wait for Security Hub to generate the findings.
- C. Enable Amazon GuardDuty. Initiate on-demand malware scans by using GuardDuty Malware Protection. Enable the integration for GuardDuty in Security Hub.
- D. Use AWS Config managed rules to detect EC2 software vulnerabilities. Ensure that Security Hub has the AWS Config integration enabled.

Correct Answer: *A*
Reference:
https://docs.aws.amazon.com/inspector/latest/user/scanning-ec2.html#agentless

Question:280 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company runs a custom online gaming application. The company uses Amazon Cognito for user authentication and authorization.

A security engineer wants to use AWS to implement fine-grained authorization on resources in the custom application. The security engineer must implement a solution that uses the user attributes that exist in Cognito. The company has already set up a user pool and an identity pool in Cognito.

Which solution will meet these requirements?

- A. Create a set of IAM roles and IAM policies. Configure the Cognito identity pool to assign users to the IAM roles.
- B. Create a policy store in Amazon Verified Permissions. Configure Cognito as the identity source. Map Cognito access tokens to the Verified Permissions schema.
- C. Create customer managed permissions by using AWS Resource Access Manager (AWS RAM). Configure the Cognito identity pool to assign users to the customer managed permissions.
- D. Create a set of IAM users and IAM policies. Configure the Cognito user pool to assign users to the IAM users.

Correct Answer: *B*
Explanation:
Verified Permissions works closely with Amazon Cognito user pools. Amazon Cognito JWTs have a predictable structure. Verified Permissions recognizes this structure and draws maximum benefit from the information that it contains. For example, you can implement a role-based access control (RBAC) authorization model with either ID tokens or access tokens.
Reference:

https://docs.aws.amazon.com/verifiedpermissions/latest/userguide/identity-sources.html

Question:281 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company wants to automate the creation of a security report. The company has an AWS Lambda function that gathers data from Amazon Inspector findings stored in AWS Security Hub in the us-west-2 Region. The Lambda function then needs to create a daily report by using an Amazon EventBridge schedule.

A security engineer discovers that the Lambda function is failing to create the report. The security engineer must implement a solution that corrects the issue and provides least privilege permissions.

Which solution will meet these requirements?

- A. Create a resource-based policy that allows Security Hub access to the ARN of the Lambda function.
- B. Attach the AWSSecurityHubReadOnlyAccess AWS managed policy to the Lambda function’s execution role.
- C. Grant the Lambda function’s execution role read-only permissions to access Amazon Inspector and Security Hub.
- D. Create a custom IAM policy that grants the Security Hub Get*, List*, Batch*, and Describe* permissions on the arn:aws:securityhub:us-west-2::product/aws/inspector/* resource. Attach the policy to the Lambda function’s execution role.

Correct Answer: *B*

Explanation:

There's no need for permissions to Inspector as logs already populated in Security Hub.

Question:282 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company must retain backup copies of Amazon RDS DB instances and Amazon Elastic Block Store (Amazon EBS) volumes. The company must retain the backup copies in data centers that are several hundred miles apart.

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

- A. Configure AWS Backup to create the backups according to the needed schedule. In the backup plan, specify multiple Availability Zones as backup destinations.
- B. Configure Amazon Data Lifecycle Manager to create the backups. Configure the Amazon Data Lifecycle Manager policy to copy the backups to an Amazon S3 bucket. Enable replication on the S3 bucket.
- C. Configure AWS Backup to create the backups according to the needed schedule. Create a destination backup vault in a different AWS Region. Configure AWS Backup to copy the backups to the destination backup vault.
- D. Configure Amazon Data Lifecycle Manager to create the backups. Create an AWS Lambda function to copy the backups to a different AWS Region. Use Amazon EventBridge to invoke the Lambda function on a schedule.

Correct Answer: *C*

Explanation:

This approach leverages AWS Backup's built-in capabilities to automate the backup process and copy backups across regions, ensuring data redundancy and compliance with the requirement to retain backups in data centers that are several hundred miles apart. It minimizes operational overhead by using AWS Backup's native features.

Question:283 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

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.

Correct Answer: *B*
Explanation:
WS WAF (Web Application Firewall) allows you to create rate-based rules that can limit the number of requests from a specific IP address. This way, you can control the traffic without completely blocking the IP address, ensuring that legitimate traffic is still allowed through at a controlled rate.

Question:284 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company runs workloads that are spread across hundreds of Amazon EC2 instances. During a recent security incident, an EC2 instance was compromised and ran malware code until the company manually terminated the instance.

The company is now using Amazon GuardDuty to detect malware on EC2 instances. A security engineer needs to implement a solution that automates a response when GuardDuty determines that an instance is infected. The solution must mitigate the incident and must comply with the AWS Well-Architected Framework guidance for incident response.

Which solution will meet these requirements?

- A. Configure AWS Systems Manager Run Command to run when a GuardDuty scan determines that an instance is infected. Use Run Command to remove all network adapters from the operating system of the infected instance. Use Run Command to also add a tag of “Infected” to the instance.
- B. Create an AWS Lambda function that runs when a GuardDuty scan determines that an instance is infected. Program the Lambda function to delete all elastic network interfaces that are associated with the instance. Program the Lambda function to also add a tag of “Infected” to the instance.
- C. Create an AWS Lambda function that runs when a GuardDuty scan determines that an instance is infected. Program the Lambda function to detach all Amazon Elastic Block Store (Amazon EBS) volumes from the instance. Program the Lambda function to also add a tag of “Infected” to the EBS volumes and to terminate the instance afterward.
- D. Define a separate VPC to isolate EC2 instances. Define a security group that does not allow any network traffic. Create an AWS Lambda function that runs when a GuardDuty scan determines that an instance is infected. Program the Lambda function to move the instance into the separate VPC and to assign the security group to the instance.

Correct Answer: *C*
Explanation:
Based on this doc, none of the above options is good, for a compromise ec2, we first need to isolate it with the security group and network ACL and turn on the termination protection, gather all metadata, then detach its EBS volume, tag it, then terminate it.

Question:285 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A public subnet contains two Amazon EC2 instances. The subnet has a custom network ACL. A security engineer is designing a solution to improve the subnet security.

The solution must allow outbound traffic to an internet service that uses TLS through port 443. The solution also must deny inbound traffic that is destined for MySQL port 3306.

Which network ACL rule set meets these requirements?

- A. Use inbound rule 100 to allow traffic on TCP port 443. Use inbound rule 200 to deny traffic on TCP port 3306. Use outbound rule 100 to allow traffic on TCP port 443.
- B. Use inbound rule 100 to deny traffic on TCP port 3306. Use inbound rule 200 to allow traffic on TCP port range 1024-65535. Use outbound rule 100 to allow traffic on TCP port 443.
- C. Use inbound rule 100 to allow traffic on TCP port range 1024-65535. Use inbound rule 200 to deny traffic on TCP port 3306. Use outbound rule 100 to allow traffic on TCP port 443.
- D. Use inbound rule 100 to deny traffic on TCP port 3306. Use inbound rule 200 to allow traffic on TCP port 443. Use outbound rule 100 to allow traffic on TCP port 443.

Correct Answer: *D*

Explanation:
Inbound Rule 100 to deny traffic on TCP port 3306: This rule denies inbound traffic on MySQL's default port (3306). It ensures that no traffic can reach the EC2 instances on that port from external sources.

Inbound Rule 200 to allow traffic on TCP port 443: This rule allows inbound HTTPS (TLS) traffic on port 443, which is required for your application to communicate with an external internet service over HTTPS.

Outbound Rule 100 to allow traffic on TCP port 443: This rule allows outbound traffic from the EC2 instances on port 443. It ensures that the EC2 instances can establish outbound connections to the internet over HTTPS.

This rule set allows secure internet access for outbound TLS traffic on port 443 while denying inbound MySQL traffic on port 3306, fulfilling both requirements for security.

Question:286 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company is investigating actions that an IAM role performed. The company must find out when the role last accessed AWS Security Hub and when the role last used the DeleteInsight action in Security Hub.

Which solution will provide this information?

- A. Use the checks for the security category in AWS Trusted Advisor. Search for the role and examine the actions taken.
- B. Use the Access Advisor tab in AWS Identity and Access Management (IAM). Search for Security Hub and the actions taken.
- C. Use AWS Identity and Access Management (IAM) to generate a credential report. Search the report for Security Hub activity.
- D. Create an analyzer in AWS Identity and Access Management Access Analyzer. Examine the findings for the role's actions in Security Hub.

Correct Answer: *B*

Question:287 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company hosts its microservices application on Amazon Elastic Kubernetes Service (Amazon EKS). The company has set up continuous deployments to update the application on demand.

A security engineer must implement a solution to provide automatic detection of anomalies in application logs in near real time. The solution also must send notifications about these anomalies to the security team.

Which solution will meet these requirements?

- A. Configure Amazon CloudWatch Container Insights to collect and aggregate EKS application logs. Create a CloudWatch alarm to monitor for anomalies. Configure the alarm to launch an AWS Lambda function to alert the security team when anomalies are detected.
- B. Configure Amazon EKS to send application logs to Amazon CloudWatch. Create a CloudWatch alarm based on a log group metric filter. Specify anomaly detection as the threshold type. Configure the alarm to use Amazon Simple Notification Service (Amazon SNS) to alert the security team.
- C. Configure Amazon EKS to export logs to Amazon S3. Use Amazon Athena queries to analyze the logs for anomalies. Use Amazon QuickSight to visualize and monitor user access requests for anomalies. Configure Amazon Simple Notification Service (Amazon SNS) notifications to alert the security team.
- D. Configure AWS App Mesh to monitor the traffic to the microservices in Amazon EKS. Integrate App Mesh with AWS CloudTrail for logging. Use Amazon Detective to analyze the logs for anomalies and to alert the security team when anomalies are detected.

Correct Answer: *B*

Question:288 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company is migrating container workloads from a data center to Amazon Elastic Container Service (Amazon ECS) clusters. The company must implement a solution to detect potential threats in the workloads and to improve the security posture of the container clusters.

Which solution will meet these requirements?

- A. Configure Amazon Inspector on the VPC that is running the ECS clusters.
- B. Enable Amazon GuardDuty Runtime Monitoring on the ECS clusters.
- C. Audit Amazon ECS API access by using Amazon CloudWatch logs to identify unauthorized access.
- D. Create container clusters in the same VPC. Use VPC flow logs to centrally monitor network traffic.

Correct Answer: *B*
Explanation:
To detect potential threats in the workloads and improve the security posture of Amazon ECS clusters, the best approach is:

Enable Amazon GuardDuty Runtime Monitoring ✅
GuardDuty Runtime Monitoring provides real-time threat detection for ECS workloads by analyzing runtime activity. It detects suspicious activities like file access anomalies, privilege escalation, or unauthorized network connections. This feature integrates with Amazon ECS Fargate and EC2-based ECS clusters to improve container security.

Question:289 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A security engineer needs to implement a solution to determine whether a company's Amazon EC2 instances are being used to mine cryptocurrency. The solution must provide notifications of cryptocurrency-related activity to an Amazon Simple Notification Service (Amazon SNS) topic.

Which solution will meet these requirements?

- A. Create AWS Config custom rules by using Guard custom policy. Configure the AWS Config rules to detect when an EC2 instance queries a DNS domain name that is associated with cryptocurrency-related activity. Configure AWS Config to initiate alerts to the SNS topic.
- B. Enable Amazon GuardDuty. Create an Amazon EventBridge rule to send alerts to the SNS topic when GuardDuty creates a finding that is associated with cryptocurrency-related activity.
- C. Enable Amazon Inspector. Create an Amazon EventBridge rule to send alerts to the SNS topic when Amazon Inspector creates a finding that is associated with cryRtocurrency-related activity.
- D. Enable VPC flow logs. Send the flow logs to an Amazon S3 bucket. Set up a query in Amazon Athena to detect when an EC2 instance queries a DNS domain name that is associated with cryptocurrency-related activity. Configure the Athena query to initiate alerts to the SNS topic.

Correct Answer: *B*
Explanation:
Amazon GuardDuty is the best solution for detecting cryptocurrency mining on EC2 instances. It provides:
Threat Detection for Cryptocurrency Mining ✅
GuardDuty has built-in detection for malicious activities, including crypto-mining behavior. It analyzes VPC Flow Logs, DNS logs, and CloudTrail logs to detect suspicious activity. Automated Alerts via EventBridge & SNS ✅
GuardDuty findings are automatically sent to Amazon EventBridge. EventBridge rules can trigger an SNS notification whenever GuardDuty detects cryptocurrency mining activity.

Question:290 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company controls user access by using IAM users and groups in AWS accounts across an organization in AWS Organizations. The company uses an external identity provider (IdP) for workforce single sign-on (SSO).

The company needs to implement a solution to provide a single management portal to access accounts within the organization. The solution must support the external IdP as a federation source.

Which solution will meet these requirements?

- A. Enable AWS IAM Identity Center. Specify the external IdP as the identity source.
- B. Enable federation with AWS Identity and Access Management (IAM). Specify the external IdP as the identity source.
- C. Migrate to Amazon Verified Permissions. Implement fine-grained access to AWS by using policy-based access control (PBAC).
- D. Migrate users to AWS Directory Service. Use AWS Control Tower to centralize security across the

organization.

Correct Answer: *A*
Explanation:
AWS IAM Identity Center (formerly AWS Single Sign-On) allows you to centrally manage access to multiple AWS accounts and applications. By specifying the external IdP as the identity source, you can integrate your existing SSO solution with AWS, providing a seamless and unified access management experience

Question:291 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***
A company must create annual snapshots of Amazon Elastic Block Store (Amazon EBS) volumes. The company must retain the snapshots for 10 years. The company will use AWS Key Management Service (AWS KMS) to encrypt the EBS volumes and snapshots.

The encryption keys must be rotated automatically every year. Snapshots that were created in previous years must be readable after rotation of the encryption keys.

Which type of KMS keys should the company use for encryption to meet these requirements?

- A. Asymmetric AWS managed KMS keys with key material created by AWS KMS
- B. Symmetric customer managed KMS keys with key material created by AWS KMS
- C. Symmetric customer managed KMS keys with custom imported key material
- D. Asymmetric AWS managed KMS keys with custom imported key material

Correct Answer: *B*

Question:292 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***
A company has hundreds of AWS accounts and uses AWS Organizations. The company plans to create many different IAM roles and policies for its product team, security team, and platform team. Some IAM policies will be shared across teams.

A security engineer needs to implement a solution to logically group together the IAM roles of each team. The solution must allow only the platform team to delegate IAM permissions to AWS services.

Which solution will meet these requirements?

- A. Set up an IAM path with the IAM roles for each team. Deploy an SCP that denies the iam:PassRole permission to all entities except the IAM path of the platform team.
- B. Apply different tags for each team to the IAM roles. Deploy an SCP that denies the sts:AssumeRole permission to all entities except the roles of the platform team.
- C. Apply different tags for each team to the IAM policies. Deploy an SCP that denies the iam:PassRole permission to all entities except the policies of the platform team.
- D. Set up an IAM path with the IAM roles for each team. Use IAM permissions boundaries to deny the sts:AssumeRole permission to the IAM roles for the product team and the security team.

Correct Answer: *A*

Question:293 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***
A company's developers are using AWS Lambda function URLs to invoke functions directly. The company must ensure that developers cannot configure or deploy unauthenticated functions in production accounts. The company wants to meet this requirement by using AWS Organizations. The solution must not require additional work for the developers.

Which solution will meet these requirements?

- A. Require the developers to configure all function URL to support cross-origin resource sharing (CORS) when the functions are called from a different domain.
- B. Use an AWS WAF delegated administrator account to view and block unauthenticated access to function URLs in production accounts, based on the OU of accounts that are using the functions.
- C. Use SCPs to allow all lambda:CreateFunctionUrlConfig and lambda:UpdateFunctionUrlConfig actions that have a lambda:FunctionUrlAuthType condition key value of AWS_IAM.

- D. Use SCPs to deny all lambda:CreateFunctionUrlConfig and lambda:UpdateFunctionUrlConfig actions that have a lambda:FunctionUrlAuthType condition key value of NONE.

Correct Answer: *D*

Question:294

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.

Correct Answer: *A*

Question:295

A security engineer wants to evaluate configuration changes to a specific AWS resource to ensure that the resource meets compliance standards. However, the security engineer is concerned about a situation in which several configuration changes are made to the resource in quick succession. The security engineer wants to record only the latest configuration of that resource to indicate the cumulative impact of the set of changes.

Which solution will meet this requirement in the MOST operationally efficient way?

- A. Use AWS CloudTrail to detect the configuration changes by filtering API calls to monitor the changes. Use the most recent API call to indicate the cumulative impact of multiple calls.
- B. Use AWS Config to detect the configuration changes and to record the latest configuration in case of multiple configuration changes.
- C. Use Amazon CloudWatch to detect the configuration changes by filtering API calls to monitor the changes. Use the most recent API call to indicate the cumulative impact of multiple calls.
- D. Use AWS Cloud Map to detect the configuration changes. Generate a report of configuration changes from AWS Cloud Map to track the latest state by using a sliding time window.

Correct Answer: *B*

Question:296

A company uses AWS Organizations to manage an organization that consists of three workload OUs. Production, Development, and Testing. The company uses AWS CloudFormation templates to define and deploy workload infrastructure in AWS accounts that are associated with the OUs. Different SCPs are attached to each workload OU.

The company successfully deployed a CloudFormation stack update to workloads in the Development OU and the Testing OU. When the company uses the same CloudFormation template to deploy the stack update in.an account in the Production OU, the update fails. The error message reports insufficient IAM permissions.

What is the FIRST step that a security engineer should take to troubleshoot this issue?

- A. Review the AWS CloudTrail logs in the account in the Production OU. Search for any failed API calls from CloudFormation during the deployment attempt.
- B. Remove all the SCPs that are attached to the Production OU. Rerun the CloudFormation stack update to determine if the SCPs were preventing the CloudFormation API calls.
- C. Confirm that the role used by CloudFormation has sufficient permissions to create, update, and delete the resources that are referenced in the CloudFormation template.
- D. Make all the SCPs that are attached to the Production OU the same as the SCPs that are attached to the Testing OU.

Correct Answer: *A*

Question:297 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company hosts a web-based application that captures and stores sensitive data in an Amazon DynamoDB table. The company needs to implement a solution that provides end-to-end data protection and the ability to detect unauthorized data changes.

Which solution will meet these requirements?

- A. Use an AWS Key Management Service (AWS KMS) customer managed key. Encrypt the data at rest.
- B. Use AWS Private Certificate Authority. Encrypt the data in transit.
- C. Use the DynamoDB Encryption Client. Use client-side encryption. Sign the table items.
- D. Use the AWS Encryption SDK. Use client-side encryption. Sign the table items.

Correct Answer: *C*
Explanation:
End-to-end protection: Encrypts data before sending it to DynamoDB and provides a way to verify the data integrity through signing. Comprehensive solution: Meets both requirements of encrypting data and detecting

Question:298 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A security engineer has created an Amazon GuardDuty detector in several AWS accounts. The accounts are in an organization in AWS Organizations. The security engineer needs centralized visibility of the security findings from the detectors.

Which solution will meet this requirement?

- A. Configure Amazon CloudWatch Logs Insights.
- B. Create an Amazon CloudWatch dashboard.
- C. Configure AWS Security Hub integrations.
- D. Query the findings by using Amazon Athena.

Correct Answer: *C*

Question:299 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company runs workloads on Amazon EC2 instances in VPCs. The EC2 instances make requests to Amazon S3 buckets through VPC endpoints. The company uses AWS Organizations to manage its AWS accounts.

The company needs the requests from the EC2 instances to originate from the same VPC that the EC2 instance credentials were issued to.

Which solution will meet this requirement?

- A. Deploy an SCP that includes the S3:* action with the “aws:SourceVpc”: “${aws:Ec2InstanceSourceVpc}” condition.
- B. Edit the VPC endpoints to include the S3:* action with the “aws:Ec2InstanceSourcePrivateIPv4”: “${aws:VpcSourceIp}” condition.
- C. Limit all actions in the S3 bucket policies by using the aws:SourceVpce condition key with the value of the allowed VPC endpoint.
- D. Limit all actions in the S3 bucket policies by using the aws:SourceVpc condition key with the value of the allowed VPC ID.

Correct Answer: *D*

Question:300

A company uses Amazon Cognito for external user authentication for a web application. External users report that they can no longer log in to the application.

What is the FIRST step that a security engineer should take to troubleshoot the problem?

- A. Review AWS CloudTrail logs to identify authentication errors that relate to Cognito users.
- B. Use AWS Identity and Access Management Access Analyzer to delete all unused IAM roles and users.
- C. Review any recent changes in Cognito configuration, IAM policies, and role trust policies to identify issues.
- D. Write a script that uses CLI commands to reset all user passwords in the Cognito user pool.

Correct Answer: *C*

Question:301

A company is running its application on AWS. Malicious users exploited a recent promotion event and created many fake accounts.

The application currently uses Amazon CloudFront in front of an Amazon API Gateway API. AWS Lambda functions serve the different API endpoints. The GET registration endpoint is behind the path of /store/registration. The URI for submission of the new account details is at /store/newaccount.

A security engineer needs to design a solution that prevents similar exploitations for future promotion events.

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

- A. Create an AWS WAF web ACL. Add the AWSManagedRulesACFPRuleSet rule group to the web ACL. Associate the web ACL with the CloudFront distribution.
- B. Create an AWS WAF web ACL. Add a rate limit rule to the web ACL. Include a RateBasedStatement entry that has a SearchString value that points to /store/registration.
- C. Specify /store/registration as the registration page path. Specify /store/newaccount as the account creation path.
- D. Enable AWS Shield Advanced for the account that hosts the CloudFront distribution. Configure a DNS-specific custom mitigation that uses the Shield Response Team (SRT) for /store/newaccount.
- E. Enable Amazon GuardDuty for the account that hosts the CloudFront distribution. Enable Lambda Protection for the Lambda functions that answer calls to /store/registration and /store/newaccount.

Correct Answer: *AB*

Question:302

A company is investigating an increase in its AWS monthly bill. The company discovers that bad actors compromised some Amazon EC2 instances and served webpages for a large email phishing campaign.

A security engineer must implement a solution to monitor for cost increases in the future to help detect malicious activity.

Which solution will offer the company the EARLIEST detection of cost increases?

- A. Create an Amazon EventBridge rule that invokes an AWS Lambda function hourly. Program the Lambda function to download an AWS usage report from AWS Data Exports about usage of all services. Program the Lambda function to analyze the report and to send a notification when anomalies are detected.
- B. Create a cost monitor in AWS Cost Anomaly Detection. Configure an individual alert to notify an Amazon Simple Notification Service (Amazon SNS) topic when the percentage above the expected cost exceeds a threshold.
- C. Review AWS Cost Explorer daily to detect anomalies in cost from prior months. Review the usage of any services that experience a significant cost increase from prior months.
- D. Capture VPC flow logs from the VPC where the EC2 instances run. Use a third-party network analysis tool to analyze the flow logs and to detect anomalies in network traffic that might increase cost.

Correct Answer: *B*

Question:303 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company's network security policy requires encryption for all data in transit. The company must encrypt data that is sent between Amazon EC2 instances and Amazon Elastic Block Store (Amazon EBS) volumes.

Which solution will meet this requirement?

- A. Configure Amazon EC2 to enable encryption in the EC2 network interface properties.
- B. Configure Amazon EBS to enable volume encryption with AWS Key Management Service (AWS KMS) for data at rest.
- C. Configure Amazon EBS to enable TLS encryption in the volume configuration properties.
- D. Configure Amazon EC2 to enable TLS encryption with certificates that are stored in AWS Certificate Manager (ACM).

Correct Answer: *B*

Question:304 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company runs a web application on a fleet of Amazon EC2 instances that are in an Auto Scaling group. The EC2 instances are in the same VPC subnet as other workloads.

A security engineer deploys an Amazon GuardDuty detector in the same AWS Region as the EC2 instances. The security engineer also sets up an AWS Security Hub integration with GuardDuty.

The security engineer needs to implement an automated solution to detect and appropriately respond to anomalous traffic patterns for the web application. The solution must comply with AWS best practices for initial response to security incidents and must minimize disruption to the web application.

Which solution will meet these requirements?

- A. Create an Amazon EventBridge rule that detects the Behavior:EC2/TrafficVolumeUnusual GuardDuty finding. Configure the rule to invoke an AWS Lambda function to disable the EC2 instance profile access keys.
- B. Create an Amazon EventBridge rule that invokes an AWS Lambda function when GuardDuty detects anomalous traffic. Program the Lambda function to disassociate the identified instance from the Auto Scaling group and to isolate the instance by using a new restricted security group.
- C. Create a Security Hub automated response that updates the network ACL that is associated with the subnet of the EC2 instances. Configure the response to update the network ACL to deny traffic from the source of detected anomalous traffic.
- D. Create an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the security engineer's email address to the SNS topic. Configure GuardDuty to send all findings to the SNS topic.

Correct Answer: *B*

Question:305 ***SCS-C02: Actual Exam Q&A | CLEARCATNET***

A company has an application that needs to read objects from an Amazon S3 bucket. The company configures an IAM policy and attaches the policy to an IAM role that the application uses. When the application tries to read objects from the S3 bucket, the application receives AccessDenied errors.

A security engineer must resolve this problem without decreasing the security of the S3 bucket or the application.

Which solution will meet these requirements?

- A. Attach a resource policy to the S3 bucket to grant read access to the role.
- B. Launch a new deployment of the application in a different AWS Region. Attach the role to the application.
- C. Review the IAM policy by using AWS Identity and Access Management Access Analyzer to ensure that the policy grants the right permissions. Validate that the application is assuming the role correctly.
- D. Ensure that the S3 Block Public Access feature is disabled on the S3 bucket. Review AWS CloudTrail logs to validate that the application is assuming the role correctly.

Correct Answer: *C*

Question:306

A security engineer is designing a solution that will provide end-to-end encryption between clients and Docker containers running in Amazon Elastic Container Service (Amazon ECS). This solution will also handle volatile traffic patterns.

Which solution would have the MOST scalability and LOWEST latency?

- A. Configure a Network Load Balancer to terminate the TLS traffic and then re-encrypt the traffic to the containers.
- B. Configure an Application Load Balancer to terminate the TLS traffic and then re-encrypt the traffic to the containers.
- C. Configure a Network Load Balancer with a TCP listener to pass through TLS traffic to the containers.
- D. Configure Amazon Route 53 to use multivalue answer routing to send traffic to the containers.

Correct Answer: *C*

Question:307

A company has a large fleet of Amazon Linux 2 Amazon EC2 instances that run an application. The application processes sensitive data and has the following compliance requirements:

• No remote access management ports to the EC2 instances can be exposed internally or externally.
• All remote session activity must be recorded in an audit log.
• All remote access to the EC2 instances must be authenticated and authorized by AWS IAM Identity Center.

The company’s DevOps team occasionally needs to connect to one of the EC2 instances to troubleshoot issues.

Which solution will provide remote access to the EC2 instances while meeting the compliance requirements?

- A. Grant access to the EC2 serial console at the account level. Create an IAM policy that allows an IAM role of the DevOps team to access the EC2 serial console.
- B. Enable EC2 instance Connect on the AMI of the EC2 instances. Configure the appropriate security group rules. Grant EC2 console access to the DevOps team for access to EC2 instance Connect.
- C. Assign an EC2 instance role that allows access to AWS Systems Manager. Create an IAM policy that grants access to Systems Manager Session Manager. Assign the policy to an IAM role of the DevOps team.
- D. Use AWS Systems Manager Automation runbooks to open remote access ports to the EC2 instances. Attach a role to the EC2 instances to allow the runbooks to run.

Correct Answer: *C*

Thank you

Thank you for being so interested in the premium exam material.
We’re glad to hear that you found it informative and helpful.

If you have any feedback or thoughts on the dumps, we would love to hear them. Your insights can help us improve our writing and better understand our readers.

Best of Luck

You have worked hard to get to this point, and you are well-prepared for the exam Keep your head up, stay positive, and go show that exam what you're made of!

VIST US to Purchase easily any IT Exam Dumps – WWW.CLEARCATNET.COM

STAY CONNECTED WITH US-

Send us your request/inquiry at **clearcat.net@gmail.com** or connect us for 💡 Live Support any time for **any certification exam dumps pdf** Or for **most asked Interview Q&A PDFs** to ensure your success in first try!!

✅ **Follow us on:** Facebook | Instagram | LinkedIn | reddit | Twitter | Quora | YouTube

IT Certifications Exam – Best Practice Q&A
Clearcat.net
Be Certified Now!
Get Any Full Premium PDF Now
97.5% Success Rate
WWW.CLEARCATNET.COM
Mail us- clearcat.net@gmail.com
Live Chat t.Me/CLEARCATNET
Watch us- YouTube/CLEARCATNET
Microsoft Azure
aws
Google
cisco
CompTIA Get IT Certified
Latest Real Exam Q&A, FIRST ATTEMPT PASS