

SCS-C01 Dumps

AWS Certified Security- Specialty

<https://www.certleader.com/SCS-C01-dumps.html>



NEW QUESTION 1

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 day
- B. Export the results to a data tabl
- C. Group the data table by re-source.
- D. Use AWS Cost Anomaly Detection to create a cost monito
- E. Access the detec-tion histor
- F. Set the time frame to Last 30 day
- G. In the search area, choose the service category.
- H. In AWS CloudTrail, filter the event history to display results from the past 30 day
- I. Create an Amazon Athena table that contains the dat
- J. Parti-tion the table by event source.
- K. Use AWS Audit Manager to create an assessment for the past 30 day
- L. Apply a usage-based framework to the assessmen
- M. Configure the assessment to as-sess by resource.

Answer: C

NEW QUESTION 2

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

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

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

Answer: B

Explanation:

"If you copy an encrypted snapshot across Regions, you must specify a KMS key valid in the destination AWS Region. It can be a Region-specific KMS key, or a multi-Region key." <https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-copy-snapshot.html#aurora-copy-sna>

NEW QUESTION 3

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? (Select TWO.)

- A. Create a local individual break glass IAM user for the security tea
- B. Create a trail in AWS CloudTrail that has Amazon CloudWatch Logs turned o
- C. Use Amazon EventBridge to monitor local user activities.
- D. Create a break glass EC2 key pair for the AWS accoun
- E. Provide the key pair to the security tea
- F. Use AWS CloudTrail to monitor key pair activit
- G. Send notifications to the security team by using Amazon Simple Notification Service (Amazon SNS).
- H. Create a break glass IAM role for the accoun
- I. Allow security team members to perform the AssumeRoleWithSAML operatio
- J. Create an AWS Cloud Trail trail that has Amazon CloudWatch Logs turned o
- K. Use Amazon EventBridge to monitor security team activities.
- L. 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.
- M. Configure AWS Systems Manager Session Manager for Amazon EC2. Configure an AWS Cloud Trail filter based on Session Manage
- N. Send the results to an Amazon Simple Notification Service (Amazon SNS) topic.

Answer: AE

Explanation:

The combination of solutions that will meet the requirements are:

- 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. This is a valid solution because it allows the security team to access the workload AWS account and instances using a local IAM user that does not depend on SAML federation. It also enables logging and monitoring of the break glass user activities using AWS CloudTrail, Amazon CloudWatch Logs, and Amazon EventBridge123.
- 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. This is a valid solution because it allows the security team to access the workload instances without opening any inbound ports or managing SSH keys or bastion hosts. It also enables logging and notification of the break glass user activities using AWS CloudTrail, Session Manager, and Amazon SNS456.

The other options are incorrect because:

- B. Creating a break glass EC2 key pair for the AWS account and providing it to the security team is not a valid solution, because it requires opening inbound

ports on the instances and managing SSH keys, which increases the security risk and complexity7.

- C. Creating a break glass IAM role for the account and allowing security team members to perform the AssumeRoleWithSAML operation is not a valid solution, because it still depends on SAML federation, which might not work in case of SAML errors8.
- D. Creating a local individual break glass IAM user on the operating system level of each workload instance and configuring unrestricted security groups on the instances to grant access to the break glass IAM users is not a valid solution, because it requires opening inbound ports on the instances and managing multiple local users, which increases the security risk and complexity9.

References:

1: Creating an IAM User in Your AWS Account 2: Creating a Trail - AWS CloudTrail 3: Using Amazon EventBridge with AWS CloudTrail 4: Setting up Session Manager - AWS Systems Manager 5: Logging Session Manager sessions - AWS Systems Manager 6: Amazon Simple Notification Service 7: Connecting to your Linux instance using SSH - Amazon Elastic Compute Cloud 8: AssumeRoleWithSAML - AWS Security Token Service 9: IAM Users - AWS Identity and Access Management

NEW QUESTION 4

A development team is attempting to encrypt and decode a secure string parameter from the IAM Systems Manager Parameter Store using an IAM Key Management Service (IAM KMS) CMK. However, each attempt results in an error message being sent to the development team. Which CMK-related problems possibly account for the error? (Select two.)

- A. The CMK is used in the attempt does not exist.
- B. The CMK is used in the attempt needs to be rotated.
- C. The CMK is used in the attempt is using the CMK's key ID instead of the CMK ARN.
- D. The CMK is used in the attempt is not enabled.
- E. The CMK is used in the attempt is using an alias.

Answer: AD

Explanation:

<https://docs.IAM.amazon.com/kms/latest/developerguide/services-parameter-store.html#parameter-store-cmk-fa>

NEW QUESTION 5

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

The security team is unable to get objects from the S3 bucket Which factors could cause this issue? (Select THREE.)

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

Answer: ADE

Explanation:

<https://docs.aws.amazon.com/vpc/latest/userguide/security-group-rules.html>

To get objects from an S3 bucket that are encrypted with a KMS customer managed key, the security team needs to have the following factors in place:

- The IAM instance profile that is attached to the EC2 instance must allow the s3:GetObject action to the S3 bucket or object in the AWS account. This permission is required to read the object from S3. Option A is incorrect because it specifies the s3:ListBucket action, which is only required to list the objects in the bucket, not to get them.
- The KMS key policy that encrypts the object in the S3 bucket must allow the kms:Decrypt action to the EC2 instance profile ARN. This permission is required to decrypt the object using the KMS key. Option D is correct.
- The security group that is attached to the EC2 instance must have an outbound rule to the S3 managed prefix list over port 443. This rule is required to allow HTTPS traffic from the EC2 instance to S3 within the AWS infrastructure. Option E is correct. Option B is incorrect because it specifies the s3:ListParts action, which is only required for multipart uploads, not for getting objects. Option C is incorrect because it specifies the kms:ListKeys action, which is not required for getting objects. Option F is incorrect because it specifies an inbound rule from the S3 managed prefix list, which is not required for getting objects. Verified References:
- <https://docs.aws.amazon.com/kms/latest/developerguide/control-access.html>
- <https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints-s3.html>

NEW QUESTION 6

An Incident Response team is investigating an IAM access key leak that resulted in Amazon EC2 instances being launched. The company did not discover the incident until many months later The Director of Information Security wants to implement new controls that will alert when similar incidents happen in the future Which controls should the company implement to achieve this? {Select TWO.)

- A. Enable VPC Flow Logs in all VPCs Create a scheduled IAM Lambda function that downloads and parses the logs, and sends an Amazon SNS notification for violations.
- B. Use IAM CloudTrail to make a trail, and apply it to all Regions Specify an Amazon S3 bucket to receive all the CloudTrail log files
- C. Add the following bucket policy to the company's IAM CloudTrail bucket to prevent log tampering{"Version": "2012-10-17-","Statement": { "Effect": "Deny","Action": "s3:PutObject", "Principal": "-", "Resource": "arn:IAM:s3:::cloudtrail/IAMLogs/111122223333/*"}}Create an Amazon S3 data event for an PutObject attempts, which sends notifications to an Amazon SNS topic.
- D. Create a Security Auditor role with permissions to access Amazon CloudWatch Logs m all Regions Ship the logs to an Amazon S3 bucket and make a lifecycle policy to ship the logs to Amazon S3 Glacier.
- E. Verify that Amazon GuardDuty is enabled in all Regions, and create an Amazon CloudWatch Events rule for Amazon GuardDuty findings Add an Amazon SNS topic as the rule's target

Answer: AE

NEW QUESTION 7

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 snapshot
- B. Enable Amazon Elastic Block Store (Amazon EBS) encryption on Amazon EC2 instance
- C. Include the database credential in the EC2 user data field
- D. Use an AWS Lambda function to rotate database credential
- E. Set up TLS for the connection to the database.
- F. Install a database on an Amazon EC2 instance
- G. Enable third-party disk encryption to encrypt Amazon Elastic Block Store (Amazon EBS) volume
- H. Store the database credentials in AWS CloudHSM with automatic rotation
- I. Set up TLS for the connection to the database.
- J. Enable Amazon RDS encryption to encrypt the database and snapshot
- K. Enable Amazon Elastic Block Store (Amazon EBS) encryption on Amazon EC2 instance
- L. Store the database credentials in AWS Secrets Manager with automatic rotation
- M. Set up TLS for the connection to the RDS hosted database.
- N. Set up an AWS CloudHSM cluster with AWS Key Management Service (AWS KMS) to store KMS key
- O. Set up Amazon RDS encryption using AWS KMS to encrypt the database
- P. Store the database credentials in AWS Systems Manager Parameter Store with automatic rotation
- Q. Set up TLS for the connection to the RDS hosted database.

Answer: C

NEW QUESTION 8

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

Which solution will meet these requirements?

- A. Install the Amazon CloudWatch agent on each EC2 instance in the VPC
- B. Use the CloudWatch agent to stream the DNS query logs to an Amazon CloudWatch Logs log group
- C. Use CloudWatch metric filters to automatically generate metrics that list the most common DNS queries.
- D. Install a BIND DNS server in the VPC
- E. Create a bash script to list the DNS request number of common DNS queries from the BIND logs.
- F. Create VPC flow logs for all subnets in the VPC
- G. Stream the flow logs to an Amazon CloudWatch Logs log group
- H. Use CloudWatch Logs Insights to list the most common DNS queries for the log group in a custom dashboard.
- I. Configure Amazon Route 53 Resolver query logging
- J. Add an Amazon CloudWatch Logs log group as the destination
- K. Use Amazon CloudWatch Contributor Insights to analyze the data and create time series that display the most common DNS queries.

Answer: D

Explanation:

<https://aws.amazon.com/blogs/aws/log-your-vpc-dns-queries-with-route-53-resolver-query-logs/>

NEW QUESTION 9

A company is attempting to conduct forensic analysis on an Amazon EC2 instance, but the company is unable to connect to the instance by using AWS Systems Manager Session Manager. The company has installed AWS Systems Manager Agent (SSM Agent) on the EC2 instance.

The EC2 instance is in a subnet in a VPC that does not have an internet gateway attached. The company has associated a security group with the EC2 instance. The security group does not have inbound or outbound rules. The subnet's network ACL allows all inbound and outbound traffic.

Which combination of actions will allow the company to conduct forensic analysis on the EC2 instance without compromising forensic data? (Select THREE.)

- A. Update the EC2 instance security group to add a rule that allows outbound traffic on port 443 for 0.0.0.0/0.
- B. Update the EC2 instance security group to add a rule that allows inbound traffic on port 443 to the VPC's CIDR range.
- C. Create an EC2 key pair
- D. Associate the key pair with the EC2 instance.
- E. Create a VPC interface endpoint for Systems Manager in the VPC where the EC2 instance is located.
- F. Attach a security group to the VPC interface endpoint
- G. Allow inbound traffic on port 443 to the VPC's CIDR range.
- H. Create a VPC interface endpoint for the EC2 instance in the VPC where the EC2 instance is located.

Answer: BCF

NEW QUESTION 10

A company wants to monitor the deletion of AWS Key Management Service (AWS KMS) customer managed keys. A security engineer needs to create an alarm that will notify the company before a KMS key is deleted. The security engineer has configured the integration of AWS CloudTrail with Amazon CloudWatch.

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

- A. Specify the deletion time of the key material during KMS key creation
- B. Create a custom AWS Config rule to assess the key's scheduled deletion
- C. Configure the rule to trigger upon a configuration change
- D. Send a message to an Amazon Simple Notification Service (Amazon SNS) topic if the key is scheduled for deletion.
- E. Create an Amazon EventBridge rule to detect KMS API calls of DeleteAlias
- F. Create an AWS Lambda function to send an Amazon Simple Notification Service (Amazon SNS) message to the company
- G. Add the Lambda function as the target of the EventBridge rule.
- H. Create an Amazon EventBridge rule to detect KMS API calls of DisableKey and ScheduleKeyDeletion. Create an AWS Lambda function to send an Amazon Simple Notification Service (Amazon SNS) message to the company

- I. Add the Lambda function as the target of the EventBridge rule.
- J. Create an Amazon Simple Notification Service (Amazon SNS) policy to detect KMS API calls of RevokeGrant and ScheduleKeyDeletion. Create an AWS Lambda function to generate the alarm and send the notification to the company.
- K. Add the Lambda function as the target of the SNS policy.

Answer: C

Explanation:

The AWS documentation states that you can create an Amazon EventBridge rule to detect KMS API calls of DisableKey and ScheduleKeyDeletion. You can then create an AWS Lambda function to send an Amazon Simple Notification Service (Amazon SNS) message to the company. You can add the Lambda function as the target of the EventBridge rule. This method will meet the requirements.

References: : AWS KMS Developer Guide

NEW QUESTION 10

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

Answer: B

NEW QUESTION 13

A Security Engineer receives alerts that an Amazon EC2 instance on a public subnet is under an SFTP brute force attack from a specific IP address, which is a known malicious bot. What should the Security Engineer do to block the malicious bot?

- A. Add a deny rule to the public VPC security group to block the malicious IP
- B. Add the malicious IP to IAM WAF blocked IPs
- C. Configure Linux iptables or Windows Firewall to block any traffic from the malicious IP
- D. Modify the hosted zone in Amazon Route 53 and create a DNS sinkhole for the malicious IP

Answer: D

Explanation:

What the Security Engineer should do to block the malicious bot. SFTP is a protocol that allows secure file transfer over SSH. EC2 is a service that provides virtual servers in the cloud. A public subnet is a subnet that has a route to an internet gateway, which allows it to communicate with the internet. A brute force attack is a type of attack that tries to guess passwords or keys by trying many possible combinations. A malicious bot is a software program that performs automated tasks for malicious purposes. Route 53 is a service that provides DNS resolution and domain name registration. A DNS sinkhole is a technique that redirects malicious or unwanted traffic to a different destination, such as a black hole server or a honeypot. By modifying the hosted zone in Route 53 and creating a DNS sinkhole for the malicious IP, the Security Engineer can block the malicious bot from reaching the EC2 instance on the public subnet. The other options are either ineffective or inappropriate for blocking the malicious bot.

NEW QUESTION 15

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
- B. Associate policies with each IAM group
- C. Provision IAM users for each application team member
- D. Add the new IAM users to the appropriate IAM group by using role-based access control (RBAC).
- E. Delegate application team leads to provision IAM roles for each team
- F. Conduct a quarterly review of the IAM roles the team leads have provisioned
- G. Ensure that the application team leads have the appropriate training to review IAM roles.
- H. Put each AWS account in its own OU
- I. Add an SCP to each OU to grant access to only the AWS services that the teams plan to use
- J. Include conditions in the AWS account of each team.
- K. Create an SCP and a permissions boundary for IAM roles
- L. Add the SCP to the root OU so that only roles that have the permissions boundary attached can create any new IAM roles.

Answer: D

Explanation:

To create a process that will allow application teams to provision their own IAM roles, while limiting the scope of IAM roles and preventing privilege escalation, the following steps are required:

- Create a service control policy (SCP) that defines the maximum permissions that can be granted to any IAM role in the organization. An SCP is a type of policy that you can use with AWS Organizations to manage permissions for all accounts in your organization. SCPs restrict permissions for entities in member accounts, including each AWS account root user, IAM users, and roles. For more information, see [Service control policies overview](#).
 - Create a permissions boundary for IAM roles that matches the SCP. A permissions boundary is an advanced feature for using a managed policy to set the maximum permissions that an identity-based policy can grant to an IAM entity. A permissions boundary allows an entity to perform only the actions that are allowed by both its identity-based policies and its permissions boundaries. For more information, see [Permissions boundaries for IAM entities](#).
 - Add the SCP to the root organizational unit (OU) so that it applies to all accounts in the organization. This will ensure that no IAM role can exceed the permissions defined by the SCP, regardless of how it is created or modified.
 - Instruct the application teams to attach the permissions boundary to any IAM role they create. This will prevent them from creating IAM roles that can escalate their own privileges or access resources they are not authorized to access. This solution will meet the requirements with the least operational overhead, as it leverages AWS Organizations and IAM features to delegate and limit IAM role creation without requiring manual reviews or approvals. The other options are incorrect because they either do not allow application teams to provision their own IAM roles (A), do not limit the scope of IAM roles or prevent privilege escalation (B), or do not take advantage of managed services whenever possible ©.
- Verified References:
- https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_boundaries.html

NEW QUESTION 20

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 policie
- B. View the findings from policy validation checks.
- C. Review AWS Trusted Advisor checks for all accounts in the organization.
- D. Set up AWS Audit Manage
- E. Run an assessment for all AWS Regions for all accounts.
- F. Ensure that Amazon Inspector agents are installed on all Amazon EC2 in-stances in all accounts.

Answer: A

NEW QUESTION 24

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 in-stances. 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 grou
- B. Configure the load balancers to send logs to the log grou
- C. Use the CloudWatch Logs console to search the log
- D. Create CloudWatch Logs filters on the logs for the required met-rics.
- E. Create an Amazon S3 bucke
- F. Configure the load balancers to send logs to the S3 bucke
- G. Use Amazon Athena to search the logs that are in the S3 bucke
- H. Create Amazon CloudWatch filters on the S3 log files for the re-quired metrics.
- I. Create an Amazon S3 bucke
- J. Configure the load balancers to send logs to the S3 bucke
- K. Use Amazon Athena to search the logs that are in the S3 bucke
- L. Create Athena queries for the required metric
- M. Publish the metrics to Amazon CloudWatch.
- N. Create an Amazon CloudWatch Logs log grou
- O. Configure the load balancers to send logs to the log grou
- P. Use the AWS Management Console to search the log
- Q. Create Amazon Athena queries for the required metric
- R. Publish the metrics to Amazon CloudWatch.

Answer: C

Explanation:

- Amazon S3 is a service that provides scalable, durable, and secure object storage. You can use Amazon S3 to store and retrieve any amount of data from anywhere on the web1
- AWS Elastic Load Balancing is a service that distributes incoming application or network traffic across multiple targets, such as EC2 instances, containers, or IP addresses. You can use Elastic Load Balancing to increase the availability and fault tolerance of your applications2
- Elastic Load Balancing supports access logging, which captures detailed information about requests sent to your load balancer. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. You can use access logs to analyze traffic patterns and troubleshoot issues3
- You can configure your load balancer to store access logs in an Amazon S3 bucket that you specify. You can also specify the interval for publishing the logs, which can be 5 or 60 minutes. The logs are stored in a hierarchical folder structure by load balancer name, IP address, year, month, day, and time.
- Amazon Athena is a service that allows you to analyze data in Amazon S3 using standard SQL. You can use Athena to run ad-hoc queries and get results in seconds. Athena is serverless, so there is no infrastructure to manage and you pay only for the queries that you run.
- You can use Athena to search the access logs that are stored in your S3 bucket. You can create a table in Athena that maps to your S3 bucket and then run SQL queries on the table. You can also use the Athena console or API to view and download the query results.
- You can also use Athena to create queries for the required metrics, such as the number of requests per cipher or protocol. You can then publish the metrics to Amazon CloudWatch, which is a service that monitors and manages your AWS resources and applications. You can use CloudWatch to collect and track metrics,

create alarms, and automate actions based on the state of your resources.

➤ By using this solution, you can meet the requirements of ensuring that all the load balancer logs are centralized and searchable for auditing and that metrics are generated to show which ciphers are in use.

NEW QUESTION 27

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

Answer: C

Explanation:

Q: Which data sources does GuardDuty analyze? GuardDuty analyzes CloudTrail management event logs, CloudTrail S3 data event logs, VPC Flow Logs, DNS query logs, and Amazon EKS audit logs. GuardDuty can also scan EBS volume data for possible malware when GuardDuty Malware Protection is enabled and identifies suspicious behavior indicative of malicious software in EC2 instance or container workloads. The service is optimized to consume large data volumes for near real-time processing of security detections. GuardDuty gives you access to built-in detection techniques developed and optimized for the cloud, which are maintained and continuously improved upon by GuardDuty engineering.

NEW QUESTION 32

A company is implementing a new application in a new IAM 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 IAM 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 VP
- B. Add a new network ACL rule on the database subnet
- C. Configure the rule to TCP port 1521 from the IP address range of the application VP
- D. Attach the new security group to the database instances that the application instances need to access.
- E. 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.
- F. Create a new security group in the application VPC with no inbound rule
- G. 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 VP
- H. Attach the application security group to the application instances that need database access, and attach the database security group to the database instances.
- I. 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 subnet
- J. Configure the rule to allow all traffic from the IP address range of the application VP
- K. Attach the new security group to the application instances that need database access.

Answer: C

NEW QUESTION 36

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

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

Answer: A

Explanation:

To grant appropriate access to separate modules for read-write and read-only functionality in a serverless application hosted on AWS that uses Amazon Redshift as a data store, a security engineer should configure cluster security groups for each application module to control access to database users that are required for read-only and readwrite, and configure an IAM policy for each module specifying the ARN of an IAM user that allows the GetClusterCredentials API call.

References: : Amazon Redshift - Amazon Web Services : Amazon Redshift - Amazon Web Services : Identity and Access Management - AWS Management Console : AWS Identity and Access Management - AWS Management Console

NEW QUESTION 39

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.
- D. Subscribe the security team's email distribution list to the topic.
- E. Create an Amazon Simple Queue Service (Amazon SQS) queue.
- F. Subscribe the security team's email distribution list to the queue.
- G. Create an Amazon EventBridge (Amazon CloudWatch Events) rule for GuardDuty findings of high severity.
- H. Configure the rule to publish a message to the topic.
- I. Create an Amazon EventBridge (Amazon CloudWatch Events) rule for Security Hub findings of high severity.
- J. Configure the rule to publish a message to the queue.

Answer: BCE

NEW QUESTION 41

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.
- B. In a dedicated logging account, aggregate all GuardDuty logs from each production account.
- C. Remediate incidents by configuring GuardDuty to directly invoke an AWS Lambda function.
- D. Configure the Lambda function to also publish notifications to the SNS topic.
- E. Activate AWS security Hub in each production account.
- F. In a dedicated logging account, aggregate all security Hub findings from each production account.
- G. Remediate incidents by using AWS Config and AWS Systems Manager to publish notifications to the SNS topic.
- H. Configure Systems Manager to also publish notifications to the SNS topic.
- I. Activate Amazon GuardDuty in each production account.
- J. In a dedicated logging account, aggregate all GuardDuty logs from each production account.
- K. Remediate incidents by using Amazon EventBridge to invoke a custom AWS Lambda function from the GuardDuty finding.
- L. Configure the Lambda function to also publish notifications to the SNS topic.
- M. Activate AWS Security Hub in each production account.
- N. In a dedicated logging account, aggregate all Security Hub findings from each production account.
- O. Remediate incidents by using Amazon EventBridge to invoke a custom AWS Lambda function from the Security Hub finding.
- P. Configure the Lambda function to also publish notifications to the SNS topic.

Answer: D

Explanation:

The correct answer is D.

To design a solution that will proactively monitor for suspicious behavior across all the accounts that contain production workloads, the security engineer needs to use a service that can aggregate and analyze security findings from multiple sources. AWS Security Hub is a service that provides a comprehensive view of your security posture across your AWS accounts and enables you to check your environment against security standards and best practices. Security Hub also integrates with other AWS services, such as Amazon GuardDuty, AWS Config, and AWS Systems Manager, to collect and correlate security findings.

To automate remediation of incidents across the production accounts, the security engineer needs to use a service that can trigger actions based on events.

Amazon EventBridge is a serverless event bus service that allows you to connect your applications with data from a variety of sources. EventBridge can use rules to match events and route them to targets for processing. You can use EventBridge to invoke a custom AWS Lambda function from the Security Hub findings.

Lambda is a serverless compute service that lets you run code without provisioning or managing servers.

To publish a notification to an Amazon SNS topic when a critical security finding is detected, the security engineer needs to use a service that can send messages to subscribers. Amazon SNS is a fully managed messaging service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SNS can deliver messages to a variety of endpoints, such as email, SMS, or HTTP. You can configure the Lambda function to also publish notifications to the SNS topic.

To send all security incident logs to a dedicated account, the security engineer needs to use a service that can aggregate and store log data from multiple sources. AWS Security Hub allows you to aggregate security findings from multiple accounts into a single account using the delegated administrator feature. This feature enables you to designate an AWS account as the administrator for Security Hub in an organization. The administrator account can then view and manage Security Hub findings from all member accounts.

Therefore, option D is correct because it meets all the requirements of the solution. Option A is incorrect because GuardDuty does not provide a comprehensive view of your security posture across your AWS accounts. GuardDuty is primarily a threat detection service that monitors for malicious or unauthorized behavior.

Option B is incorrect because Config and Systems Manager are not designed to automate remediation of incidents based on Security Hub findings. Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources, while Systems Manager is a service that allows you to manage your infrastructure on AWS at scale. Option C is incorrect because GuardDuty does not provide a comprehensive view of your security posture across your AWS accounts.

References:

- AWS Security Hub
- Amazon EventBridge
- AWS Lambda
- Amazon SNS
- Aggregating Security Hub findings across accounts

NEW QUESTION 42

Within a VPC, a corporation runs an Amazon RDS Multi-AZ DB instance. The database instance is connected to the internet through a NAT gateway via two subnets.

Additionally, the organization has application servers that are hosted on Amazon EC2 instances and use the RDS database. These EC2 instances have been deployed onto two more private subnets inside the same VPC. These EC2 instances connect to the internet through a default route via the same NAT gateway. Each VPC subnet has its own route table.

The organization implemented a new security requirement after a recent security examination. Never allow the database instance to connect to the internet. A security engineer must perform this update promptly without interfering with the network traffic of the application servers.

How will the security engineer be able to comply with these requirements?

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

Answer: C

Explanation:

Each subnet has a route table, so modify the routing associated with DB instance subnets to prevent internet access.

NEW QUESTION 47

A startup company is using a single AWS account that has resources in a single AWS Region. A security engineer configures an AWS Cloud Trail 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
- B. Select the new Regions where the company added resources.
- C. Change the S3 bucket to receive notifications to track all actions from all Regions.
- D. Create a new CloudTrail trail that applies to all Regions.
- E. Change the existing CloudTrail trail so that it applies to all Regions.

Answer: D

Explanation:

The correct answer is D. Change the existing CloudTrail trail so that it applies to all Regions.

According to the AWS documentation¹, you can configure CloudTrail to deliver log files from multiple Regions to a single S3 bucket for a single account. To change an existing single-Region trail to log in all Regions, you must use the AWS CLI and add the `--is-multi-region-trail` option to the `update-trail` command². This will ensure that you log global service events and capture all management event activity in your account.

Option A is incorrect because creating a new CloudTrail trail for each Region will incur additional costs and increase operational overhead. Option B is incorrect because changing the S3 bucket to receive notifications will not affect the delivery of log files from other Regions. Option C is incorrect because creating a new CloudTrail trail that applies to all Regions will result in duplicate log files for the original Region and also incur additional costs.

NEW QUESTION 51

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

Which solution meets these criteria?

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

Answer: A

Explanation:

```
https://awscli.amazonaws.com/v2/documentation/api/latest/reference/kms/import-key-material.html aws kms import-key-material \
--key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
--encrypted-key-material fileb://EncryptedKeyMaterial.bin \
--import-token fileb://ImportToken.bin \
--expiration-model KEY_MATERIAL_EXPIRES \
--valid-to 2021-09-21T19:00:00Z
```

The correct answer is A. A customer managed CMK that uses customer provided key material.

A customer managed CMK is a KMS key that you create, own, and manage in your AWS account. You have full control over the key configuration, permissions, rotation, and deletion. You can use a customer managed CMK to encrypt and decrypt data in AWS services that are integrated with AWS KMS, such as Amazon EBS¹.

A customer managed CMK can use either AWS provided key material or customer provided key material. AWS provided key material is generated by AWS KMS and never leaves the service unencrypted. Customer provided key material is generated outside of AWS KMS and imported into a customer managed CMK. You can specify an expiration date for the imported key material, after which the CMK becomes unusable until you reimport new key material².

To meet the criteria of automatically expiring the key material in 90 days, you need to use customer provided key material and set the expiration date accordingly. This way, you can ensure that the data encrypted with the CMK will not be accessible after 90 days unless you reimport new key material and re-encrypt the data. The other options are incorrect for the following reasons:

* B. A customer managed CMK that uses AWS provided key material does not expire automatically. You can enable automatic rotation of the key material every year, but this does not prevent access to the data encrypted with the previous key material. You would need to manually delete the CMK and its backing key material to make the data inaccessible³.

* C. An AWS managed CMK is a KMS key that is created, owned, and managed by an AWS service on your behalf. You have limited control over the key configuration, permissions, rotation, and deletion. You cannot use an AWS managed CMK to encrypt data in other AWS services or applications. You also cannot set an expiration date for the key material of an AWS managed CMK⁴.

* D. Operation system-native encryption that uses GnuPG is not a solution that uses AWS KMS. GnuPG is a command line tool that implements the OpenPGP standard for encrypting and signing data. It does not integrate with Amazon EBS or other AWS services. It also does not provide a way to automatically expire the

key material used for encryption.

References:

1: Customer Managed Keys - AWS Key Management Service 2: [Importing Key Material in AWS Key Management Service (AWS KMS) - AWS Key Management Service] 3: [Rotating Customer Master Keys - AWS Key Management Service] 4: [AWS Managed Keys - AWS Key Management Service] 5: The GNU Privacy Guard

NEW QUESTION 56

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 IAM features should be used as much as possible. The security engineer has set up IAM Organizations with all features activated and IAM SSO 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 IAM accounts. Assign AD Connector groups to IAM accounts and link to the IAM roles in accordance with the employees' job functions and access requirements. Instruct employees to access IAM accounts by using the IAM Directory Service user portal.
- B. Use an IAM SSO default directory to create users and groups for all employees that require access to IAM account.
- C. Assign groups to IAM accounts and link to permission sets in accordance with the employees' job functions and access requirement.
- D. Instruct employees to access IAM accounts by using the IAM SSO user portal.
- E. Use an IAM SSO default directory to create users and groups for all employees that require access to IAM account.
- F. Link IAM SSO groups to the IAM users present in all accounts to inherit existing permission.
- G. Instruct employees to access IAM accounts by using the IAM SSO user portal.
- H. Use IAM Directory Service for Microsoft Active Directory to create users and groups for all employees that require access to IAM accounts. Enable IAM Management Console access in the created directory and specify IAM SSO as a source of information for integrated accounts and permission set.
- I. Instruct employees to access IAM accounts by using the IAM Directory Service user portal.

Answer: B

NEW QUESTION 61

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 IAM 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).

Answer: A

NEW QUESTION 66

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).

Answer: BC

Explanation:

To prevent users from directly accessing an Application Load Balancer and allow access only through CloudFront, complete these high-level steps: Configure CloudFront to add a custom HTTP header to requests that it sends to the Application Load Balancer. Configure the Application Load Balancer to only forward requests that contain the custom HTTP header. (Optional) Require HTTPS to improve the security of this solution.

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/restrict-access-to-load-balancer.html>

NEW QUESTION 67

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

Answer: B

NEW QUESTION 71

There is a requirement for a company to transfer large amounts of data between IAM and an on-premise location. There is an additional requirement for low latency and high consistency traffic to IAM. Given these requirements how would you design a hybrid architecture? Choose the correct answer from the options below
Please select:

- A. Provision a Direct Connect connection to an IAM region using a Direct Connect partner.
- B. Create a VPN tunnel for private connectivity, which increases network consistency and reduces latency.
- C. Create an IPSec tunnel for private connectivity, which increases network consistency and reduces latency.
- D. Create a VPC peering connection between IAM and the Customer gateway.

Answer: A

Explanation:

IAM Direct Connect makes it easy to establish a dedicated network connection from your premises to IAM. Using IAM Direct Connect you can establish private connectivity between IAM and your datacenter, office, or colocation environment which in many cases can reduce your network costs, increase bandwidth throughput and provide a more consistent network experience than Internet-based connections.

Options B and C are invalid because these options will not reduce network latency Options D is invalid because this is only used to connect 2 VPC's

For more information on IAM direct connect, just browse to the below URL: <https://IAM.amazon.com/directconnect>

The correct answer is: Provision a Direct Connect connection to an IAM region using a Direct Connect partner. omit your Feedback/Queries to our Experts

NEW QUESTION 75

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 event
- B. Run the script with the existing AWS managed IAM policies
- C. Use IAM Access Analyzer to generate a new IAM policy that is based on access activity in the trail
- D. Replace the existing AWS managed IAM policies with the generated IAM policy for the role.
- E. Remove the existing AWS managed IAM policies from the role
- F. Attach the IAM Access Analyzer Role Policy Generator to the role
- G. Run the script
- H. Return to IAM Access Analyzer and generate a least privilege IAM policy
- I. Attach the new IAM policy to the role.
- J. Create an account analyzer in IAM Access Analyzer
- K. Create an archive rule that has a filter that checks whether the PrincipalArn value matches the ARN of the role
- L. Run the script
- M. Remove the existing AWS managed IAM policies from the role.
- N. In AWS CloudTrail, create a trail for management event
- O. Remove the existing AWS managed IAM policies from the role
- P. Run the script
- Q. Find the authorization failure in the trail event that is associated with the script
- R. Create a new IAM policy that includes the action and resource that caused the authorization failure
- S. Repeat the process until the script succeeds
- T. Attach the new IAM policy to the role.

Answer: A

NEW QUESTION 78

A company has multiple Amazon S3 buckets encrypted with customer-managed CMKs. Due to regulatory requirements the keys must be rotated every year. The company's Security Engineer has enabled automatic key rotation for the CMKs; however the company wants to verify that the rotation has occurred.

What should the Security Engineer do to accomplish this?

- A. Filter IAM CloudTrail logs for KeyRotation events
- B. Monitor Amazon CloudWatch Events for any IAM KMS CMK rotation events
- C. Using the IAM CLI
- D. run the IAM kms get-key-rotation-status operation with the --key-id parameter to check the CMK rotation date
- E. Use Amazon Athena to query IAM CloudTrail logs saved in an S3 bucket to filter Generate New Key events

Answer: C

Explanation:

the aws kms get-key-rotation-status command returns a boolean value that indicates whether automatic rotation of the customer master key (CMK) is enabled¹. This command also shows the date and time when the CMK was last rotated². The other options are not valid ways to check the CMK rotation status.

NEW QUESTION 79

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?

- A. A computer code with black text Description automatically generated


```

    "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-la2b3c4d"
          }
        }
      }
    ]
  }
}

```

B. A computer code with black text Description automatically generated

```

    "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-la2b3c4d"
          }
        }
      }
    ]
  }
}

```

C. A computer code with black text Description automatically generated

```

    "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-la2b3c4d"
          }
        }
      }
    ]
  }
}

```

D. A computer code with black text Description automatically generated

```

    "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": {
          "StringEquals": {
            "aws:sourceVpce": "vpce-la2b3c4d"
          }
        }
      }
    ]
  }
}

```

Answer: B

Explanation:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/example-bucket-policies-vpc-endpoint.html>

NEW QUESTION 83

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 variable
- C. Access the environment variables at runtime
- D. Use IAM permissions to restrict access to the environment variables to only the Lambda functions that require access.
- E. Store the environment variables in AWS Secrets Manager, and access them at runtime

- F. Use IAM permissions to restrict access to the secrets to only the Lambda functions that require access.
- G. Store the environment variables in AWS Systems Manager Parameter Store as secure string parameters, and access them at runtime.
- H. Use IAM permissions to restrict access to the parameters to only the Lambda functions that require access.

Answer: D

Explanation:

Storing sensitive information in environment variables is not a secure practice, as anyone who has access to the Lambda console or the Lambda function code can view them as plaintext. To address this security issue, the security engineer needs to use a service that can store and encrypt the environment variables, and access them at runtime using IAM permissions. The most cost-effective way to do this is to use AWS Systems Manager Parameter Store, which is a service that provides secure, hierarchical storage for configuration data management and secrets management. Parameter Store allows you to store values as standard parameters (plaintext) or secure string parameters (encrypted). Secure string parameters use a AWS Key Management Service (AWS KMS) customer master key (CMK) to encrypt the parameter value. To access the parameter value at runtime, the Lambda function needs to have IAM permissions to decrypt the parameter using the KMS CMK.

The other options are incorrect because:

- Option A is incorrect because setting up IAM policies from the Lambda console to hide access to the environment variables will not prevent someone who has access to the Lambda function code from viewing them as plaintext. IAM policies can only control who can perform actions on AWS resources, not what they can see in the code or the console.
- Option B is incorrect because using AWS Step Functions to store the environment variables is not a secure or cost-effective solution. AWS Step Functions is a service that lets you coordinate multiple AWS services into serverless workflows. Step Functions does not provide any encryption or secrets management capabilities, and it will incur additional charges for each state transition in the workflow. Moreover, storing environment variables in Step Functions will make them visible in the execution history of the workflow, which can be accessed by anyone who has permission to view the Step Functions console or API.
- Option C is incorrect because storing the environment variables in AWS Secrets Manager and accessing them at runtime is not a cost-effective solution. AWS Secrets Manager is a service that helps you protect secrets needed to access your applications, services, and IT resources. Secrets Manager enables you to rotate, manage, and retrieve secrets throughout their lifecycle. While Secrets Manager can securely store and encrypt environment variables using KMS CMKs, it will incur higher charges than Parameter Store for storing and retrieving secrets. Unless the security engineer needs the advanced features of Secrets Manager, such as automatic rotation of secrets or integration with other AWS services, Parameter Store is a cheaper and simpler option.

NEW QUESTION 87

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.

Answer: D

Explanation:

The possible reason that the IAM user cannot access the objects in the S3 bucket is D. The KMS key policy has been edited to remove the ability for the AWS account to have full access to the key.

This answer is correct because the KMS key policy is the primary way to control access to the KMS key, and it must explicitly allow the AWS account to have full access to the key. If the KMS key policy has been edited to remove this permission, then the IAM policy that grants kms:Decrypt permission to the IAM user has no effect, and the IAM user cannot decrypt the objects in the S3 bucket¹².

The other options are incorrect because:

- A. The IAM policy does not need to allow the kms:DescribeKey permission, because this permission is not required for decrypting objects in S3 using SSE-KMS. The kms:DescribeKey permission allows getting information about a KMS key, such as its creation date, description, and key state³.
- B. The S3 bucket has not been changed to use the AWS managed key to encrypt objects at rest, because this would not cause an Access Denied message for the IAM user. The AWS managed key is a default KMS key that is created and managed by AWS for each AWS account and Region. The IAM user does not need any permissions on this key to use it for SSE-KMS⁴.
- C. An S3 bucket policy does not need to be added to allow the IAM user to access the objects, because the IAM user already has s3:List* and s3:Get* permissions for the S3 bucket and its objects through an IAM policy. An S3 bucket policy is an optional way to grant cross-account access or public access to an S3 bucket⁵.

References:

1: Key policies in AWS KMS 2: Using server-side encryption with AWS KMS keys (SSE-KMS) 3: AWS KMS API Permissions Reference 4: Using server-side encryption with Amazon S3 managed keys (SSE-S3) 5: Bucket policy examples

NEW QUESTION 92

A company uses AWS Organizations to run workloads in multiple AWS accounts. Currently, the individual team members at the company access all Amazon EC2 instances remotely by using SSH or Remote Desktop Protocol (RDP). The company does not have any audit trails, and security groups are occasionally open. The company must secure access management and implement a centralized logging solution.

Which solution will meet these requirements MOST securely?

- A. Configure trusted access for AWS Systems Manager in Organizations. Configure a bastion host from the management account. Replace SSH and RDP by using Systems Manager Session Manager from the management account. Configure Session Manager logging to Amazon CloudWatch Logs.
- B. Replace SSH and RDP with AWS Systems Manager Session Manager. Install Systems Manager Agent (SSM Agent) on the instances. Attach the AmazonSSMManagedInstanceCore role to the instances. Configure session data streaming to Amazon CloudWatch Logs. Create a separate logging account that has appropriate cross-account permissions to audit the log data.
- C. Install a bastion host in the management account. Reconfigure all SSH and RDP to allow access only from the bastion host. Install AWS Systems Manager Agent (SSM Agent) on the bastion host. Attach the AmazonSSMManagedInstanceCore role to the bastion host. Configure session data streaming to Amazon CloudWatch Logs in a separate logging account to audit log data.
- D. Replace SSH and RDP with AWS Systems Manager State Manager. Install Systems Manager Agent (SSM Agent) on the instances. Attach the AmazonSSMManagedInstanceCore role to the instances. Configure session data streaming to Amazon CloudTrail. Use CloudTrail Insights to analyze the trail data.

Answer: C

Explanation:

To meet the requirements of securing access management and implementing a centralized logging solution, the most secure solution would be to:

- Install a bastion host in the management account.
- Reconfigure all SSH and RDP to allow access only from the bastion host.
- Install AWS Systems Manager Agent (SSM Agent) on the bastion host.
- Attach the AmazonSSMManagedInstanceCore role to the bastion host.
- Configure session data streaming to Amazon CloudWatch Logs in a separate logging account to audit log data

This solution provides the following security benefits:

- It uses AWS Systems Manager Session Manager instead of traditional SSH and RDP protocols, which provides a secure method for accessing EC2 instances without requiring inbound firewall rules or open ports.
- It provides audit trails by configuring Session Manager logging to Amazon CloudWatch Logs and creating a separate logging account to audit the log data.
- It uses the AWS Systems Manager Agent to automate common administrative tasks and improve the security posture of the instances.
- The separate logging account with cross-account permissions provides better data separation and improves security posture.

<https://aws.amazon.com/solutions/implementations/centralized-logging/>

NEW QUESTION 93

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? (Select 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.

Answer: ACE

NEW QUESTION 95

You need to create a policy and apply it for just an individual user. How could you accomplish this in the right way?

Please select:

- A. Add an IAM managed policy for the user
- B. Add a service policy for the user
- C. Add an IAM role for the user
- D. Add an inline policy for the user

Answer: D

Explanation:

Options A and B are incorrect since you need to add an inline policy just for the user Option C is invalid because you don't assign an IAM role to a user

The IAM Documentation mentions the following

An inline policy is a policy that's embedded in a principal entity (a user, group, or role)—that is, the policy is an inherent part of the principal entity. You can create a policy and embed it in a principal entity, either when you create the principal entity or later.

For more information on IAM Access and Inline policies, just browse to the below URL: <https://docs.IAM.amazon.com/IAM/latest/UserGuide/access>

The correct answer is: Add an inline policy for the user Submit your Feedback/Queries to our Experts

NEW QUESTION 97

A company hosts multiple externally facing applications, each isolated in its own IAM account The company's Security team has enabled IAM WAF. IAM Config. and Amazon GuardDuty on all accounts. The company's Operations team has also joined all of the accounts to IAM Organizations and established centralized logging for CloudTrail. IAM Config, and GuardDuty. The company wants the Security team to take a reactive remediation in one account, and automate implementing this remediation as proactive prevention in all the other accounts.

How should the Security team accomplish this?

- A. Update the IAM WAF rules in the affected account and use IAM Firewall Manager to push updated IAM WAF rules across all other accounts.
- B. Use GuardDuty centralized logging and Amazon SNS to set up alerts to notify all application teams of security incidents.
- C. Use GuardDuty alerts to write an IAM Lambda function that updates all accounts by adding additional NACLs on the Amazon EC2 instances to block known malicious IP addresses.
- D. Use IAM Shield Advanced to identify threats in each individual account and then apply the account-based protections to all other accounts through Organizations.

Answer: C

NEW QUESTION 98

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 instance
- B. Use Patch Manager also to automate the patching process.
- C. Use AWS Shield Advanced to view vulnerability identifiers for missing patches on the instance
- D. Use AWS Systems Manager Patch Manager to automate the patching process.
- E. Use Amazon GuardDuty to view vulnerability identifiers for missing patches on the instance
- F. Use Amazon Inspector to automate the patching process.
- G. Use Amazon Inspector to view vulnerability identifiers for missing patches on the instance
- H. Use Amazon Inspector also to automate the patching process.

Answer: A

Explanation:

<https://aws.amazon.com/about-aws/whats-new/2020/10/how-use-aws-systems-manager-to-view-vulnerability-id>

NEW QUESTION 101

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

Answer: ABC

Explanation:

The correct combination of steps that the security engineer should take to meet these requirements are 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., and 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.

* A. This answer is correct because it meets the requirement of ensuring that no logging data is lost for each instance during scaling activities. By installing the CloudWatch agent on all the EC2 instances, the security engineer can collect and send system logs and application logs to CloudWatch Logs, which is a service that stores and monitors log data. By generating a CloudWatch agent configuration file, the security engineer can specify which logs to forward and how often.

* B. This answer is correct because it meets the requirement of keeping the logs for only the required period of 7 years. By setting the log retention for desired log groups, the security engineer can control how long CloudWatch Logs retains log events before deleting them. The security engineer can choose a predefined retention period of 7 years, or use a custom value.

* C. This answer is correct because it meets the requirement of providing the necessary permissions to forward logs to CloudWatch Logs. By attaching an IAM role to the launch configuration or launch template that the Auto Scaling groups use, the security engineer can grant permissions to the EC2 instances that are launched by the Auto Scaling groups. By configuring the role to provide the necessary permissions, such as cloudwatch:PutLogEvents and cloudwatch:CreateLogStream, the security engineer can allow the EC2 instances to send log data to CloudWatch Logs.

NEW QUESTION 104

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? (Select THREE.)

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

Answer: BDF

NEW QUESTION 106

You have an S3 bucket defined in IAM. You want to ensure that you encrypt the data before sending it across the wire. What is the best way to achieve this. Please select:

- A. Enable server side encryption for the S3 bucket
- B. This request will ensure that the data is encrypted first.
- C. Use the IAM Encryption CLI to encrypt the data first

- D. Use a Lambda function to encrypt the data before sending it to the S3 bucket.
E. Enable client encryption for the bucket

Answer: B

Explanation:

One can use the IAM Encryption CLI to encrypt the data before sending it across to the S3 bucket. Options A and C are invalid because this would still mean that data is transferred in plain text Option D is invalid because you cannot just enable client side encryption for the S3 bucket For more information on Encrypting and Decrypting data, please visit the below URL:

<https://IAM.amazonaws.com/blogs/security/how-to-encrypt-and-decrypt-your-data-with-the-IAM-encryption-cli> The correct answer is: Use the IAM Encryption CLI to encrypt the data first Submit your Feedback/Queries to our Experts

NEW QUESTION 108

A company has multiple accounts in the AWS Cloud. Users in the developer account need to have access to specific resources in the production account. What is the MOST secure way to provide this access?

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

Answer: D

Explanation:

https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html

NEW QUESTION 109

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 Balance
B. Create two listeners one listener on port 80 and one listener on port 443. Create one target group
C. 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.
D. Create a public Application Load Balance
E. Create two listeners one listener on port 80 and one listener on port 443. Create one target group
F. 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.
G. Create a public Network Load Balance
H. Create two listeners one listener on port 80 and one listener on port 443. Create one target group
I. 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.
J. Create a public Network Load Balance
K. Create a listener on port 443. Create one target group
L. Create a rule to forward traffic from port 443 to the target group
M. Set the protocol for the listener on port 443 to TLS.

Answer: A

Explanation:

An Application Load Balancer (ALB) is a type of load balancer that operates at the application layer (layer 7) of the OSI model. It can distribute incoming traffic based on the content of the request, such as the host

header, path, or query parameters. An ALB can also terminate TLS connections and decrypt requests from clients before sending them to the targets.

To implement TLS for incoming traffic to the application, the following steps are required:

- Create a public ALB in a public subnet and register the EC2 instances as targets in a target group.
- Create two listeners for the ALB, one on port 80 for HTTP traffic and one on port 443 for HTTPS traffic.
- Create a rule for the listener on port 80 to redirect HTTP requests to HTTPS using the same host, path, and query parameters.
- Provision a public TLS certificate in AWS Certificate Manager (ACM) for the domain name of the application. ACM is a service that lets you easily provision, manage, and deploy public and private SSL/TLS certificates for use with AWS services and your internal connected resources.
- Attach the certificate to the listener on port 443 and configure the security policy to negotiate secure connections between clients and the ALB.
- Configure the security groups for the ALB and the EC2 instances to allow inbound traffic on ports 80 and 443 from the internet and outbound traffic on any port to the EC2 instances.

This solution will meet the requirements of implementing TLS for incoming traffic without impacting performance or requiring end-to-end encryption. The ALB will handle the TLS termination and decryption, while forwarding unencrypted requests to the EC2 instances.

Verified References:

- <https://docs.aws.amazon.com/elasticloadbalancing/latest/application/introduction.html>
- <https://docs.aws.amazon.com/elasticloadbalancing/latest/application/create-https-listener.html>
- <https://docs.aws.amazon.com/acm/latest/userguide/acm-overview.html>

NEW QUESTION 110

A developer signed in to a new account within an IAM Organization organizational unit (OU) containing multiple accounts. Access to the Amazon S3 service is restricted with the following SCP.

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

How can the security engineer provide the developer with Amazon S3 access without affecting other account?

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

Answer: C

NEW QUESTION 111

A company is developing a highly resilient application to be hosted on multiple Amazon EC2 instances. The application will store highly sensitive user data in Amazon RDS tables.

The application must

- Include migration to a different IAM Region in the application disaster recovery plan.
- Provide a full audit trail of encryption key administration events
- Allow only company administrators to administer keys.
- Protect data at rest using application layer encryption

A Security Engineer is evaluating options for encryption key management.

Why should the Security Engineer choose IAM CloudHSM over IAM KMS for encryption key management in this situation?

- A. The key administration event logging generated by CloudHSM is significantly more extensive than IAM KMS.
- B. CloudHSM ensures that only company support staff can administer encryption keys, whereas IAM KMS allows IAM staff to administer keys.
- C. The ciphertext produced by CloudHSM provides more robust protection against brute force decryption attacks than the ciphertext produced by IAM KMS.
- D. CloudHSM provides the ability to copy keys to a different Region, whereas IAM KMS does not.

Answer: B

Explanation:

CloudHSM allows full control of your keys such as including Symmetric (AES), Asymmetric (RSA), SHA-256, SHA-512, Hash Based, Digital Signatures (RSA). On the other hand, AWS Key Management Service is a multi-tenant key storage that is owned and managed by AWS.

References: 1: What are the differences between AWS Cloud HSM and KMS?

NEW QUESTION 116

Your development team is using access keys to develop an application that has access to S3 and DynamoDB. A new security policy has outlined that the credentials should not be older than 2 months, and should be rotated. How can you achieve this?

Please select:

- A. Use the application to rotate the keys in every 2 months via the SDK
- B. Use a script to query the creation date of the key
- C. If older than 2 months, create new access key and update all applications to use it; deactivate the old key and delete it.
- D. Delete the user associated with the keys after every 2 months
- E. Then recreate the user again.
- F. Delete the IAM Role associated with the keys after every 2 months
- G. Then recreate the IAM Role again.

Answer: B

Explanation:

One can use the CLI command `list-access-keys` to get the access keys. This command also returns the "CreateDate" of the keys. If the CreateDate is older than 2 months, then the keys can be deleted.

The `list-access-keys` CLI command returns information about the access key IDs associated with the specified IAM user. If there are none, the action returns an empty list.

Option A is incorrect because you might as use a script for such maintenance activities. Option C is incorrect because you would not rotate the users themselves.

Option D is incorrect because you don't use IAM roles for such a purpose. For more information on the CLI command, please refer to the below link:

<http://docs.IAM.amazon.com/cli/latest/reference/iam/list-access-keys.html>

The correct answer is: Use a script to query the creation date of the keys. If older than 2 months, create new access key and update all applications to use it; deactivate the old key and delete it.

Submit your Feedback/Queries to our Experts

NEW QUESTION 120

A security engineer recently rotated the host keys for an Amazon EC2 instance. The security engineer is trying to access the EC2 instance by using the EC2 Instance Connect feature. However, the security engineer receives an error (or failed host key validation). Before the rotation of the host keys, the EC2 Instance

Connect worked correctly with this EC2 instance.
What should the security engineer do to resolve this error?

- A. Import the key material into AWS Key Management Service (AWS KMS).
- B. Manually upload the new host key to the AWS trusted host keys database.
- C. Ensure that the AmazonSSMManagedInstanceCore policy is attached to the EC2 instance profile.
- D. Create a new SSH key pair for the EC2 instance.

Answer: B

Explanation:

To set up a CloudFront distribution for an S3 bucket that hosts a static website, and to allow only specified IP addresses to access the website, the following steps are required:

- Create a CloudFront origin access identity (OAI), which is a special CloudFront user that you can associate with your distribution. An OAI allows you to restrict access to your S3 content by using signed URLs or signed cookies. For more information, see [Using an origin access identity to restrict access to your Amazon S3 content](#).
- Create the S3 bucket policy so that only the OAI has access. This will prevent users from accessing the website directly by using S3 URLs, as they will receive an Access Denied error. To do this, use the AWS Policy Generator to create a bucket policy that grants s3:GetObject permission to the OAI, and attach it to the S3 bucket. For more information, see [Restricting access to Amazon S3 content by using an origin access identity](#).
- Create an AWS WAF web ACL and add an IP set rule. AWS WAF is a web application firewall service that lets you control access to your web applications. An IP set is a condition that specifies a list of IP addresses or IP address ranges that requests originate from. You can use an IP set rule to allow or block requests based on the IP addresses of the requesters. For more information, see [Working with IP match conditions](#).
- Associate the web ACL with the CloudFront distribution. This will ensure that the web ACL filters all requests for your website before they reach your origin. You can do this by using the AWS WAF console, API, or CLI. For more information, see [Associating or disassociating a web ACL with a CloudFront distribution](#). This solution will meet the requirements of allowing only specified IP addresses to access the website and preventing direct access by using S3 URLs. The other options are incorrect because they either do not create a CloudFront distribution for the S3 bucket (A), do not use an OAI to restrict access to the S3 bucket (C), or do not use AWS WAF to block traffic from outside the specified IP addresses (D).

Verified References:

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

NEW QUESTION 123

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 URLs.
- B. Configure a CloudWatch Logs subscription to stream the log group to an Amazon OpenSearch Service cluster.
- C. Use OpenSearch Service to analyze the logs for the specific IP address and the requested URLs.
- D. Use CloudWatch Logs Insights and a custom query syntax to analyze the CloudWatch logs for the specific IP address and the requested URLs.
- E. 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.
- F. Use AWS Glue to view the results.

Answer: C

NEW QUESTION 124

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

Answer: C

NEW QUESTION 125

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.

Answer: ACF

Explanation:

The following may be causing the problem for the Auditor:

- A. The external ID used by the Auditor is missing or incorrect. This is a possible cause, because the external ID is a unique identifier that is used to establish a trust relationship between the accounts. The external ID must match the one that is specified in the role's trust policy in the destination account.
-

C. The Auditor has not been granted sts:AssumeRole for the role in the destination account. This is a possible cause, because sts:AssumeRole is the API action that allows the Auditor to assume the cross-account role and obtain temporary credentials. The Auditor must have an IAM policy that allows them to call sts:AssumeRole for the role ARN in the destination account2.

➤ F. The role ARN used by the Auditor is missing or incorrect. This is a possible cause, because the role ARN is the Amazon Resource Name of the cross-account role that the Auditor wants to assume. The role ARN must be valid and exist in the destination account3.

NEW QUESTION 128

A company's Security Auditor discovers that users are able to assume roles without using multi-factor authentication (MFA). An example of a current policy being applied to these users is as follows:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": {
        "AWS": "arn:aws:iam::555555555555:root"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "Bool": { "aws:MultiFactorAuthPresent": false}
      }
    }
  ]
}
```

The Security Auditor finds that the users who are able to assume roles without MFA are all coming from the IAM CLI. These users are using long-term IAM credentials. Which changes should a Security Engineer implement to resolve this security issue? (Select TWO.)

A)

```
"Effect": "Deny",
"Condition": { "Bool": { "aws:MultiFactorAuthPresent": false} }
```

B)

```
"Effect": "Allow",
"Condition": { "Bool": { "aws:MultiFactorAuthPresent": true} }
```

C)

```
"Effect": "Allow","Condition": { "BoolIfExists": { "aws:MultiFactorAuthPresent": true} }
```

D)

```
"Effect": "Deny","Condition": { "BoolIfExists": { "aws:MultiFactorAuthPresent": false} }
```

E)

```
"Effect": "Deny","Condition": { "BoolIfNotExist": { "aws:MultiFactorAuthPresent": true} }
```

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

Answer: AD

NEW QUESTION 129

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.

Answer: BE

Explanation:

The most likely cause of the error is that the instance profile for the EC2 instance does not have the s3:PutObject permission for the S3 bucket. This permission is needed to upload logs to the bucket. Therefore, the security engineer should ensure that the instance profile has this permission.

One possible solution is to attach the AWSImageBuilderFullAccess policy to the instance profile for the EC2 instance. This policy grants full access to Image Builder resources and related AWS services, including the s3:PutObject permission for any bucket with "imagebuilder" in its name. However, this policy may grant more permissions than necessary, which violates the principle of least privilege.

Another possible solution is to create a custom policy that only grants the s3:PutObject permission for the specific S3 bucket that is used for logging. This policy

can be attached to the instance profile along with the other policies that are required for Image Builder functionality: EC2InstanceProfileForImageBuilder, EC2InstanceProfileForImageBuilderECRContainerBuilds, and AmazonSSMManagedInstanceCore. This solution follows the principle of least privilege more closely than the previous one.

➤ Ensure that the following policies are attached to the instance profile for the EC2 instance: EC2InstanceProfileForImageBuilder, EC2InstanceProfileForImageBuilderECRContainerBuilds, and AmazonSSMManagedInstanceCore.

➤ Ensure that the instance profile for the EC2 instance has the s3:PutObject permission for the S3 bucket.

This can be done by either attaching the AWSImageBuilderFullAccess policy or creating a custom policy with this permission.

1: Using managed policies for EC2 Image Builder - EC2 Image Builder 2: PutObject - Amazon Simple Storage Service 3: AWSImageBuilderFullAccess - AWS Managed Policy

NEW QUESTION 130

You work at a company that makes use of IAM resources. One of the key security policies is to ensure that all data is encrypted both at rest and in transit. Which of the following is one of the right ways to implement this.

Please select:

- A. Use S3 SSE and use SSL for data in transit
- B. SSL termination on the ELB
- C. Enabling Proxy Protocol
- D. Enabling sticky sessions on your load balancer

Answer: A

Explanation:

By disabling SSL termination, you are leaving an unsecure connection from the ELB to the back end instances. Hence this means that part of the data transit is not being encrypted.

Option B is incorrect because this would not guarantee complete encryption of data in transit Option C and D are incorrect because these would not guarantee encryption

For more information on SSL Listeners for your load balancer, please visit the below URL: <http://docs.IAM.amazon.com/elasticloadbalancing/latest/classic/elb-https-load-balancers.html> The correct answer is: Use S3 SSE and use SSL for data in transit

Submit your Feedback/Queries to our Experts

NEW QUESTION 131

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

Answer: B

Explanation:

This answer is correct because logging in with read-only credentials minimizes the risk of accidental or malicious changes to the AWS account. Reviewing the GuardDuty finding can help identify which API calls initiated the finding and which IAM principal was involved. Using Amazon Detective can help analyze and visualize the API calls in context, such as which resources were affected, which IP addresses were used, and how the activity deviated from normal patterns.

Amazon Detective can also help identify related findings from other sources, such as AWS Config or AWS Audit Manager.

NEW QUESTION 133

A company's on-premises networks are connected to VPCs using an IAM Direct Connect gateway. The company's on-premises application needs to stream data using an existing Amazon Kinesis Data Firehose delivery stream. The company's security policy requires that data be encrypted in transit using a private network. How should the company meet these requirements?

- A. Create a VPC endpoint for Kinesis Data Firehose
- B. Configure the application to connect to the VPC endpoint.
- C. Configure an IAM policy to restrict access to Kinesis Data Firehose using a source IP condition. Configure the application to connect to the existing Firehose delivery stream.
- D. Create a new TLS certificate in IAM Certificate Manager (ACM). Create a public-facing Network Load Balancer (NLB) and select the newly created TLS certificate
- E. Configure the NLB to forward all traffic to Kinesis Data Firehose
- F. Configure the application to connect to the NLB.
- G. Peer the on-premises network with the Kinesis Data Firehose VPC using Direct Connect
- H. Configure the application to connect to the existing Firehose delivery stream.

Answer: A

Explanation:

To stream data using an existing Amazon Kinesis Data Firehose delivery stream and encrypt it in transit using a private network, the company should do the following:

➤ Create a VPC endpoint for Kinesis Data Firehose. This allows the company to use a private connection between their VPC and Kinesis Data Firehose without

requiring an internet gateway or NAT device.

➤ Configure the application to connect to the VPC endpoint. This allows the application to stream data using Kinesis Data Firehose over AWS PrivateLink, which encrypts all traffic with TLS.

NEW QUESTION 137

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 file with secure gzip.
- C. Create an Amazon EventBridge (Amazon CloudWatch Events) 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.

Answer: ADE

NEW QUESTION 139

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

Answer: C

Explanation:

This solution meets the requirement of recovering the EC2 instances if the AWS account is compromised and the EBS snapshots are deleted. By creating a new AWS account with limited privileges, the company can isolate the backup snapshots from the main account and reduce the risk of accidental or malicious deletion. By allowing the new account to access the KMS key that encrypts the EBS snapshots, the company can ensure that the snapshots are copied in an encrypted form and can be decrypted when needed. By copying the encrypted snapshots to the new account on a recurring basis, the company can maintain a consistent backup schedule and minimize data loss.

NEW QUESTION 141

A company wants to monitor the deletion of customer managed CMKs. A security engineer must create an alarm that will notify the company before a CMK is deleted. The security engineer has configured the integration of IAM CloudTrail with Amazon CloudWatch. What should the security engineer do next to meet this requirement?

- 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.

Answer: A

NEW QUESTION 146

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

Answer: A

Explanation:

AWS Systems Manager Session Manager is a fully managed service that allows you to securely and remotely administer your EC2 instances without the need to open inbound ports, maintain bastion hosts, or manage SSH keys. Session Manager provides an interactive browser-based shell or CLI access to your instances, as well as port forwarding and auditing capabilities. Session Manager works with both Linux and Windows instances, and supports hybrid environments and edge devices.

EC2 Instance Connect is a feature that allows you to use SSH to connect to your Linux instances using short-lived keys that are generated on demand and delivered securely through the AWS metadata service. EC2 Instance Connect does not require any additional software installation or configuration on the instance, but it does require you to use SSH-RSA keys during the launch of new instances.

The correct answer is to use Session Manager, as it provides more security and flexibility than EC2 Instance Connect, and does not require SSH-RSA keys or inbound ports. Session Manager also works with Windows instances, while EC2 Instance Connect does not.

Verified References:

- <https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager.html>
- <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Connect-using-EC2-Instance-Connect.html>
- <https://repost.aws/questions/QUhV4R9EoeSdW0GT3cKBUR7w/what-is-the-difference-between-ec-2-ins>

NEW QUESTION 149

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

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

- A. Request a certificate (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 vacation of the domains for ACM.
- C. Request validation of the domains for ACM through DNS. Insert CNAME records into each domain's DNS zone.
- D. Create an Application Load Balancer for 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.

Answer: CDF

NEW QUESTION 152

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? (Select TWO.)

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

Answer: CD

NEW QUESTION 156

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? (Select 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.

Answer: BCE

Explanation:

https://d1.awsstatic.com/WWPS/pdf/aws_security_incident_response.pdf

NEW QUESTION 159

A company has two AWS accounts. One account is for development workloads. The other account is for production workloads. For compliance reasons, the production account contains all the AWS Key Management Service (AWS KMS) keys that the company uses for encryption.

The company applies an IAM role to an AWS Lambda function in the development account to allow secure access to AWS resources. The Lambda function must access a specific KMS customer managed key that exists in the production account to encrypt the Lambda function's data.

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

- A. Configure the key policy for the customer managed key in the production account to allow access to the Lambda service.
- B. Configure the key policy for the customer managed key in the production account to allow access to the IAM role of the Lambda function in the development account.
- C. Configure a new IAM policy in the production account with permissions to use the customer managed ke
- D. Apply the IAM policy to the IAM role that the Lambda function in the development account uses.
- E. Configure a new key policy in the development account with permissions to use the customer managed ke
- F. Apply the key policy to the IAM role that the Lambda function in the development account uses.
- G. Configure the IAM role for the Lambda function in the development account by attaching an IAM policy that allows access to the customer managed key in the production account.

Answer: BE

Explanation:

To allow a Lambda function in one AWS account to access a KMS customer managed key in another AWS account, the following steps are required:

➤ Configure the key policy for the customer managed key in the production account to allow access to the IAM role of the Lambda function in the development account. A key policy is a resource-based policy that defines who can use or manage a KMS key. To grant cross-account access to a KMS key, you must specify the AWS account ID and the IAM role ARN of the external principal in the key policy statement. For more information, see [Allowing users in other accounts to use a KMS key](#).

➤ Configure the IAM role for the Lambda function in the development account by attaching an IAM policy that allows access to the customer managed key in the production account. An IAM policy is an identity-based policy that defines what actions an IAM entity can perform on which resources. To allow an IAM role to use a KMS key in another account, you must specify the KMS key ARN and the kms:Encrypt action (or any other action that requires access to the KMS key) in the IAM policy statement. For more information, see [Using IAM policies with AWS KMS](#).

This solution will meet the requirements of allowing secure access to a KMS customer managed key across AWS accounts.

The other options are incorrect because they either do not grant cross-account access to the KMS key (A, C), or do not use a valid policy type for KMS keys (D).

Verified References:

➤ <https://docs.aws.amazon.com/kms/latest/developerguide/iam-policies.html>

NEW QUESTION 164

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your SCS-C01 Exam with Our Prep Materials Via below:

<https://www.certleader.com/SCS-C01-dumps.html>