Number: SCS-C02
Passing Score: 800
Time Limit: 120
File Version: 3.0

Exam Code: SCS-C02

Exam Name: AWS Certified Security - Specialty

Exam A

QUESTION 1
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

Correct Answer: A
Section:

QUESTION 2
A company is hosting a static website on Amazon S3 The company has configured an Amazon CloudFront distribution to serve the website contents The company has associated an IAM WAF web ACL with the CloudFront distribution. The web ACL ensures that requests originate from the United States to address compliance restrictions.
THE company is worried that the S3 URL might still be accessible directly and that requests can bypass the CloudFront distribution
Which combination of steps should the company take to remove direct access to the S3 URL? (Select TWO.)

A. Select 'Restrict Bucket Access' in the origin settings of the CloudFront distribution
B. Create an origin access identity (OAI) for the S3 origin
C. Update the S3 bucket policy to allow s3 GetObject with a condition that the IAM Referer key matches the secret value Deny all other requests
D. Configure the S3 bucket poky so that only the origin access identity (OAI) has read permission for objects in the bucket
E. Add an origin custom header that has the name Referer to the CloudFront distribution Give the header a secret value.

Correct Answer: A, D
Section:

QUESTION 3
A company's security team is building a solution for logging and visualization. The solution will assist the company with the large variety and velocity of data that it receives from IAM across multiple accounts. The security team has enabled IAM CloudTrail and VPC Flow Logs in all of its accounts. In addition, the company has an organization in IAM Organizations and has an IAM Security Hub master account.
The security team wants to use Amazon Detective However the security team cannot enable Detective and is unsure why
What must the security team do to enable Detective?

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

Correct Answer: D
Section:

QUESTION 4
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 (torn ACM in the us-west-2 Region Add the domain names that the certificate will secure
B. Send an email message to the domain administrators to request vacation of the domains for ACM
C. Request validation of the domains for ACM through DNS Insert CNAME records into each domain's DNS zone
D. Create an Application Load Balancer for me caching solution Select the newly requested certificate from ACM to be used for secure connections
E. Create an Amazon CloudFront distribution for the caching solution Enter the main CNAME record as the Origin Name Enter the subdomain names or alternate names in the Alternate Domain Names Distribution Settings Select the newly requested certificate from ACM to be used for secure connections
F. Request a certificate from ACM in the us-east-1 Region Add the domain names that the certificate wil secure

Correct Answer: C, D, F
Section:

QUESTION 5
A security engineer needs to create an IAM Key Management Service <IAM KMS) key that will De used to encrypt all data stored in a company's Amazon S3 Buckets in the us-west-1 Region. The key will use server-side encryption. Usage of the key must be limited to requests coming from Amazon S3 within the company's account.
Which statement in the KMS key policy will meet these requirements?
A)


```
{
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
    },
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:ViaService": "s3.us-west-1.amazonaws.com",
            "kms:CallerAccount": "<CustomerAccountID>"
        }
    }
}
```

B)

```
{
    "Effect": "Allow",
    "Principal": {
        "AWS": "s3.us-west-1.amazonaws.com"
    },
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:CallerAccount": "<CustomerAccountID>"
        }
    }
}
```

C)

```
{
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
    },
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:EncryptionContext:aws:s3:arn": [
                "arn:aws:s3:::*"
            ],
```


A. Option A
B. Option B
C. Option C

Correct Answer: A
Section:

QUESTION 6
A business requires a forensic logging solution for hundreds of Docker-based apps running on Amazon EC2. The solution must analyze logs in real time, provide message replay, and persist logs.
Which Amazon Web Offerings (IAM) services should be employed to satisfy these requirements? (Select two.)

A. Amazon Athena
B. Amazon Kinesis
C. Amazon SQS
D. Amazon Elasticsearch
E. Amazon EMR

Correct Answer: B, D
Section:

QUESTION 7
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. Create a new NAT gateway that only the application server subnets can use.
B. Configure the DB instances inbound network ACL to deny traffic from the security group ID of the NAT gateway.
C. Modify the route tables of the DB instance subnets to remove the default route to the NAT gateway.
D. Configure the route table of the NAT gateway to deny connections to the DB instance subnets.

Correct Answer: C
Section:
Explanation:
Each subnet has a route table, so modify the routing associated with DB instance subnets to prevent internet access.

QUESTION 8
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 CMKs 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.

Correct Answer: A, D
Section:
Explanation:
https://docs.IAM.amazon.com/kms/latest/developerguide/services-parameter-store.html#parameter-store-cmk-fail

QUESTION 9
A business stores website images in an Amazon S3 bucket. The firm serves the photos to end users through Amazon CloudFront. The firm learned lately that the photographs are being accessible from nations in which it does not have a distribution license.

Which steps should the business take to safeguard the photographs and restrict their distribution? (Select two.)

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

Correct Answer: A, C
Section:
Explanation:
For Enable Geo-Restriction, choose Yes. For Restriction Type, choose Whitelist to allow access to certain countries, or choose Blacklist to block access from certain countries.
https://IAM.amazon.com/premiumsupport/knowledge-center/cloudfront-geo-restriction/

QUESTION 10
A company has multiple departments. Each department has its own IAM account. All these accounts belong to the same organization in IAM Organizations.
A large .csv file is stored in an Amazon S3 bucket in the sales department's IAM account. The company wants to allow users from the other accounts to access the .csv file's content through the combination of IAM Glue and Amazon Athen
a. However, the company does not want to allow users from the other accounts to access other files in the same folder.
Which solution will meet these requirements?

A. Apply a user policy in the other accounts to allow IAM Glue and Athena lo access the .csv We.
B. Use S3 Select to restrict access to the .csv lie. In IAM Glue Data Catalog, use S3 Select as the source of the IAM Glue database.
C. Define an IAM Glue Data Catalog resource policy in IAM Glue to grant cross-account S3 object access to the .csv file.
D. Grant IAM Glue access to Amazon S3 in a resource-based policy that specifies the organization as the principal.

Correct Answer: A
Section:

QUESTION 11
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. Associate the key pair with the EC2 instance.
D. Create a VPC interface endpoint for Systems Manager in the VPC where the EC2 instance is located.
E. Attach a security group to the VPC interface endpoint. Allow inbound traffic on port 443 to the VPC's CIDR range.
F. Create a VPC interface endpoint for the EC2 instance in the VPC where the EC2 instance is located.

Correct Answer: B, C, F
Section:

QUESTION 12
A company uses Amazon API Gateway to present REST APIs to users. An API developer wants to analyze API access patterns without the need to parse the log files.
Which combination of steps will meet these requirements with the LEAST effort? (Select TWO.)

A. Configure access logging for the required API stage.
B. Configure an AWS CloudTrail trail destination for API Gateway events. Configure filters on the userIdentity, userAgent, and sourcelPAddress fields.
C. Configure an Amazon S3 destination for API Gateway logs. Run Amazon Athena queries to analyze API access information.
D. Use Amazon CloudWatch Logs Insights to analyze API access information.
E. Select the Enable Detailed CloudWatch Metrics option on the required API stage.

Correct Answer: C, D
Section:

QUESTION 13
A security administrator is setting up a new AWS account. The security administrator wants to secure the data that a company stores in an Amazon S3 bucket. The security administrator also wants to reduce the chance of unintended data exposure and the potential for misconfiguration of objects that are in the S3 bucket.
Which solution will meet these requirements with the LEAST operational overhead?

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

Correct Answer: D
Section:

QUESTION 14
A company needs to store multiple years of financial records. The company wants to use Amazon S3 to store copies of these documents. The company must implement a solution to prevent the documents from being edited, replaced, or deleted for 7 years after the documents are stored in Amazon S3. The solution must also encrypt the documents at rest.
A security engineer creates a new S3 bucket to store the documents.
What should the security engineer do next to meet these requirements?

A. Configure S3 server-side encryption. Create an S3 bucket policy that has an explicit deny rule for all users for s3:DeleteObject and s3:PutObject API calls. Configure S3 Object Lock to use governance mode with a retention period of 7 years.
B. Configure S3 server-side encryption. Configure S3 Versioning on the S3 bucket. Configure S3 Object Lock to use compliance mode with a retention period of 7 years.
C. Configure S3 Versioning. Configure S3 Intelligent-Tiering on the S3 bucket to move the documents to S3 Glacier Deep Archive storage. Use S3 server-side encryption immediately. Expire the objects after 7 years.
D. Set up S3 Event Notifications and use S3 server-side encryption. Configure S3 Event Notifications to target an AWS Lambda function that will review any S3 API call to the S3 bucket and deny the s3:DeleteObject and s3:PutObject API calls. Remove the S3 event notification after 7 years.

Correct Answer: B
Section:

QUESTION 15
A company uses AWS Organizations to manage several AWs accounts. The company processes a large volume of sensitive dat
a. The company uses a serverless approach to microservices. The company stores all the data in either Amazon S3 or Amazon DynamoDB. The company reads the data by using either AWS lambda functions or container-based services that the company hosts on Amazon Elastic Kubernetes Service (Amazon EKS) on AWS Fargate.

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

A. Create a key policy that allows the kms:Decrypt action only for Amazon S3 and DynamoDB. Create an SCP that denies the creation of S3 buckets and DynamoDB tables that are not encrypted with the key.
B. Create an 1AM policy that denies the kms:Decrypt action for the key. Create a Lambda function than runs on a schedule to attach the policy to any new roles. Create an AWS Config rule to send alerts for resources that are not encrypted with the key.
C. Create a key policy that allows the kms:Decrypt action only for Amazon S3, DynamoDB, Lambda, and Amazon EKS. Create an SCP that denies the creation of S3 buckets and DynamoDB tables that are not encrypted with the key.
D. Create a key policy that allows the kms:Decrypt action only for Amazon S3, DynamoDB, Lambda, and Amazon EKS. Create an AWS Config rule to send alerts for resources that are not encrypted with the key.

Correct Answer: B
Section:

QUESTION 16
A company is building a data processing application mat uses AWS Lambda functions. The application's Lambda functions need to communicate with an Amazon RDS OB instance that is deployed within a VPC in the same AWS account
Which solution meets these requirements in the MOST secure way?

A. Configure the DB instance to allow public access Update the DB instance security group to allow access from the Lambda public address space for the AWS Region
B. Deploy the Lambda functions inside the VPC Attach a network ACL to the Lambda subnet Provide outbound rule access to the VPC CIDR range only Update the DB instance security group to allow traffic from 0.0.0.0/0
C. Deploy the Lambda functions inside the VPC Attach a security group to the Lambda functions Provide outbound rule access to the VPC CIDR range only Update the DB instance security group to allow traffic from the Lambda security group
D. Peer the Lambda default VPC with the VPC that hosts the DB instance to allow direct network access without the need for security groups

Correct Answer: C
Section:
Explanation:
This solution ensures that the Lambda functions are deployed inside the VPC and can communicate with the Amazon RDS DB instance securely. The security group attached to the Lambda functions only allows outbound traffic to the VPC CIDR range, and the DB instance security group only allows traffic from the Lambda security group. This solution ensures that the Lambda functions can communicate with the DB instance securely and that the DB instance is not exposed to the public internet.

QUESTION 17
A company has launched an Amazon EC2 instance with an Amazon Elastic Block Store (Amazon EBS) volume in the us-east-1 Region The volume is encrypted with an AWS Key Management Service (AWS KMS) customer managed key that the company's security team created The security team has created an 1AM key policy and has assigned the policy to the key The security team has also created an 1AM instance profile and has assigned the profile to the instance
The EC2 instance will not start and transitions from the pending state to the shutting-down state to the terminated state
Which combination of steps should a security engineer take to troubleshoot this issue? (Select TWO)

A. Verify that the KMS key policy specifies a deny statement that prevents access to the key by using the aws SourcelP condition key Check that the range includes the EC2 instance IP address that is associated with the EBS volume
B. Verify that the KMS key that is associated with the EBS volume is set to the Symmetric key type
C. Verify that the KMS key that is associated with the EBS volume is in the Enabled state
D. Verify that the EC2 role that is associated with the instance profile has the correct 1AM instance policy to launch an EC2 instance with the EBS volume
E. Verify that the key that is associated with the EBS volume has not expired and needs to be rotated

Correct Answer: C, D
Section:
Explanation:
To troubleshoot the issue of an EC2 instance failing to start and transitioning to a terminated state when it has an EBS volume encrypted with an AWS KMS customer managed key, a security engineer should take the following steps:
C) Verify that the KMS key that is associated with the EBS volume is in the Enabled state. If the key is not enabled, it will not function properly and could cause the EC2 instance to fail.
D) Verify that the EC2 role that is associated with the instance profile has the correct IAM instance policy to launch an EC2 instance with the EBS volume. If the instance does not have the necessary permissions, it may not be able to mount the volume and could cause the instance to fail.
Therefore, options C and D are the correct answers.

QUESTION 18
Which of the following are valid configurations for using SSL certificates with Amazon CloudFront? (Select THREE)

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

Correct Answer: A, B, C
Section:
Explanation:
The key length for an RSA certificate that you use with CloudFront is 2048 bits, even though ACM supports larger keys. If you use an imported certificate with CloudFront, your key length must be 1024 or 2048 bits and cannot exceed 2048 bits. You must import the certificate in the US East (N. Virginia) Region.You must have permission to use and import the SSL/TLS certificate https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/cnames-and-https-requirements.html

QUESTION 19
A company usesAWS 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 togging solution
Which solution will meet these requirements MOST securely?

A. Configure trusted access for AWS System 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
C. 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
D. 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
E. 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

Correct Answer: C
Section:
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/

QUESTION 20
A company has an AWS Key Management Service (AWS KMS) customer managed key with imported key material Company policy requires all encryption keys to be rotated every year
What should a security engineer do to meet this requirement for this customer managed key?

A. Enable automatic key rotation annually for the existing customer managed key
B. Use the AWS CLI to create an AWS Lambda function to rotate the existing customer managed key annually
C. Import new key material to the existing customer managed key Manually rotate the key
D. Create a new customer managed key Import new key material to the new key Point the key alias to the new key

Correct Answer: A
Section:
Explanation:
To meet the requirement of rotating the AWS KMS customer managed key every year, the most appropriate solution would be to enable automatic key rotation annually for the existing customer managed key. This will ensure that AWS KMS generates new cryptographic material for the CMK every year. AWS KMS also saves the CMK's older cryptographic material in perpetuity so it can be used to decrypt data that it encrypted. AWS KMS does not delete any rotated key material until you delete the CMK.

QUESTION 21
A company is using an AWS Key Management Service (AWS KMS) AWS owned key in its application to encrypt files in an AWS account The company's security team wants the ability to change to new key material for new files whenever a potential key breach occurs A security engineer must implement a solution that gives the security team the ability to change the key whenever the team wants to do so
Which solution will meet these requirements?

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

Correct Answer: A
Section:
Explanation:
To meet the requirement of changing the key material for new files whenever a potential key breach occurs, the most appropriate solution would be to create a new customer managed key, add a key rotation schedule to the key, and invoke the key rotation schedule every time the security team requests a key change.

QUESTION 22
A company wants to remove all SSH keys permanently from a specific subset of its Amazon Linux 2 Amazon EC2 instances that are using the same 1AM instance profile However three individuals who have IAM user accounts will need to access these instances by using an SSH session to perform critical duties

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

A. Assign an 1AM policy to the instance profile to allow the EC2 instances to be managed by AWS Systems Manager Provide the 1AM user accounts with permission to use Systems Manager Remove the SSH keys from the EC2 instances Use Systems Manager Inventory to select the EC2 instance and connect
B. Assign an 1AM policy to the 1AM user accounts to provide permission to use AWS Systems Manager Run Command Remove the SSH keys from the EC2 instances Use Run Command to open an SSH connection to the EC2 instance
C. Assign an 1AM policy to the instance profile to allow the EC2 instances to be managed by AWS Systems Manager Provide the 1AM user accounts with permission to use Systems Manager Remove the SSH keys from the EC2 instances Use Systems Manager Session Manager to select the EC2 instance and connect
D. Assign an 1AM policy to the 1AM user accounts to provide permission to use the EC2 service in the AWS Management Console Remove the SSH keys from the EC2 instances Connect to the EC2 instance as the ec2-user through the AWS Management Console's EC2 SSH client method

Correct Answer: C
Section:
Explanation:
To provide access to the three individuals who have IAM user accounts to access the Amazon Linux 2 Amazon EC2 instances that are using the same IAM instance profile, the most appropriate solution would be to assign an IAM policy to the instance profile to allow the EC2 instances to be managed by AWS Systems Manager, provide the IAM user accounts with permission to use Systems Manager, remove the SSH keys from the EC2 instances, and use Systems Manager Session Manager to select the EC2 instance and connect.

QUESTION 23
A company has two VPCs in the same AWS Region and in the same AWS account Each VPC uses a CIDR block that does not overlap with the CIDR block of the other VPC One VPC contains AWS Lambda functions that run inside a subnet that accesses the internet through a NAT gateway. The Lambda functions require access to a publicly accessible Amazon Aurora MySQL database that is running in the other VPC
A security engineer determines that the Aurora database uses a security group rule that allows connections from the NAT gateway IP address that the Lambda functions use. The company's security policy states that no database should be publicly accessible.
What is the MOST secure way that the security engineer can provide the Lambda functions with access to the Aurora database?

A. Move the Aurora database into a private subnet that has no internet access routes in the database's current VPC Configure the Lambda functions to use the Aurora database's new private IP address to access the database Configure the Aurora databases security group to allow access from the private IP addresses of the Lambda functions
B. Establish a VPC endpoint between the two VPCs in the Aurora database's VPC configure a service VPC endpoint for Amazon RDS In the Lambda functions' VPC. configure an interface VPC endpoint that uses the service endpoint in the Aurora database's VPC Configure the service endpoint to allow connections from the Lambda functions.
C. Establish an AWS Direct Connect interface between the VPCs Configure the Lambda functions to use a new route table that accesses the Aurora database through the Direct Connect interface Configure the Aurora database's security group to allow access from the Direct Connect interface IP address
D. Move the Lambda functions into a public subnet in their VPC Move the Aurora database into a private subnet in its VPC Configure the Lambda functions to use the Aurora database's new private IP address to access the database Configure the Aurora database to allow access from the public IP addresses of the Lambda functions

Correct Answer: B
Section:
Explanation:
This option involves creating a VPC Endpoint between the two VPCs that allows private communication between them without going through the internet or exposing any public IP addresses. In this option, a VPC endpoint for Amazon RDS will be established, and an interface VPC endpoint will be created that points to the service endpoint in the Aurora database's VPC. This way, the Lambda functions can use the private IP address of the Aurora database to access it through the VPC endpoint without exposing any public IP addresses or allowing public internet access to the database.

QUESTION 24
A company hosts an end user application on AWS Currently the company deploys the application on Amazon EC2 instances behind an Elastic Load Balancer The company wants to configure end-to-end encryption between the Elastic Load Balancer and the EC2 instances.
Which solution will meet this requirement with the LEAST operational effort?

A. Use Amazon issued AWS Certificate Manager (ACM) certificates on the EC2 instances and the Elastic Load Balancer to configure end-to-end encryption

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

Correct Answer: A
Section:
Explanation:
To configure end-to-end encryption between the Elastic Load Balancer and the EC2 instances with the least operational effort, the most appropriate solution would be to use Amazon issued AWS Certificate Manager (ACM) certificates on the EC2 instances and the Elastic Load Balancer to configure end-to-end encryption.
AWS Certificate Manager - Amazon Web Services:Elastic Load Balancing - Amazon Web Services:Amazon Elastic Compute Cloud - Amazon Web Services:AWS Certificate Manager - Amazon Web Services

QUESTION 25
A security engineer receives a notice from the AWS Abuse team about suspicious activity from a Linux-based Amazon EC2 instance that uses Amazon Elastic Block Store (Amazon EBS>-based storage The instance is making connections to known malicious addresses
The instance is in a development account within a VPC that is in the us-east-1 Region The VPC contains an internet gateway and has a subnet in us-east-1a and us-easMb Each subnet is associate with a route table that uses the internet gateway as a default route Each subnet also uses the default network ACL The suspicious EC2 instance runs within the us-east-1 b subnet. During an initial investigation a security engineer discovers that the suspicious instance is the only instance that runs in the subnet
Which response will immediately mitigate the attack and help investigate the root cause?

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

Correct Answer: B
Section:
Explanation:
This option suggests updating the outbound network ACL for the subnet in us-east-1b to explicitly deny all connections as the first rule, replacing the security group with a new one that only allows connections from a diagnostics security group, and launching a new EC2 instance with diagnostic tools to investigate the suspicious instance. This option will immediately mitigate the attack and provide the necessary tools for investigation.

QUESTION 26
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 1AM 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 1AM policy for each module Specify the ARN of an 1AM user that allows the GetClusterCredentials API call

Correct Answer: A
Section:
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.

QUESTION 27
A company has retail stores The company is designing a solution to store scanned copies of customer receipts on Amazon S3 Files will be between 100 KB and 5 MB in PDF format Each retail store must have a unique encryption key Each object must be encrypted with a unique key
Which solution will meet these requirements?

A. Create a dedicated AWS Key Management Service (AWS KMS) customer managed key for each retail store Use the S3 Put operation to upload the objects to Amazon S3 Specify server-side encryption with AWS KMS keys (SSE-KMS) and the key ID of the store's key
B. Create a new AWS Key Management Service (AWS KMS) customer managed key every day for each retail store Use the KMS Encrypt operation to encrypt objects Then upload the objects to Amazon S3
C. Run the AWS Key Management Service (AWS KMS) GenerateDataKey operation every day for each retail store Use the data key and client-side encryption to encrypt the objects Then upload the objects to Amazon S3
D. Use the AWS Key Management Service (AWS KMS) ImportKeyMaterial operation to import new key material to AWS KMS every day for each retail store Use a customer managed key and the KMS Encrypt operation to encrypt the objects Then upload the objects to Amazon S3

Correct Answer: A
Section:
Explanation:
To meet the requirements of storing scanned copies of customer receipts on Amazon S3, where files will be between 100 KB and 5 MB in PDF format, each retail store must have a unique encryption key, and each object must be encrypted with a unique key, the most appropriate solution would be to create a dedicated AWS Key Management Service (AWS KMS) customer managed key for each retail store. Then, use the S3 Put operation to upload the objects to Amazon S3, specifying server-side encryption with AWS KMS keys (SSE-KMS) and the key ID of the store's key.

QUESTION 28
A systems engineer deployed containers from several custom-built images that an application team provided through a QA workflow The systems engineer used Amazon Elastic Container Service (Amazon ECS) with the Fargate launch type as the target platform The system engineer now needs to collect logs from all containers into an existing Amazon CloudWatch log group
Which solution will meet this requirement?

A. Turn on the awslogs log driver by specifying parameters for awslogs-group and awslogs-region m the LogConfiguration property
B. Download and configure the CloudWatch agent on the container instances
C. Set up Fluent Bit and FluentO as a DaemonSet to send logs to Amazon CloudWatch Logs
D. Configure an 1AM policy that includes the togs CreateLogGroup action Assign the policy to the container instances

Correct Answer: A
Section:
Explanation:
The AWS documentation states that you can use the awslogs log driver to send log information to CloudWatch Logs. To use this method, you specify the parameters for awslogs-group and awslogs-region in the LogConfiguration property of the container definition. This method is the easiest way to send logs to CloudWatch Logs.

QUESTION 29
A company receives a notification from the AWS Abuse team about an AWS account The notification indicates that a resource in the account is compromised The company determines that the compromised

resource is an Amazon EC2 instance that hosts a web application The compromised EC2 instance is part of an EC2 Auto Scaling group
The EC2 instance accesses Amazon S3 and Amazon DynamoDB resources by using an 1AM access key and secret key The 1AM access key and secret key are stored inside the AMI that is specified in the Auto Scaling group's launch configuration The company is concerned that the credentials that are stored in the AMI might also have been exposed
The company must implement a solution that remediates the security concerns without causing downtime for the application The solution must comply with security best practices
Which solution will meet these requirements'?

A. Rotate the potentially compromised access key that the EC2 instance uses Create a new AM I without the potentially compromised credentials Perform an EC2 Auto Scaling instance refresh
B. Delete or deactivate the potentially compromised access key Create an EC2 Auto Scaling linked 1AM role that includes a custom policy that matches the potentially compromised access key permission Associate the new 1AM role with the Auto Scaling group Perform an EC2 Auto Scaling instance refresh.
C. Delete or deactivate the potentially compromised access key Create a new AMI without the potentially compromised credentials Create an 1AM role that includes the correct permissions Create a launch template for the Auto Scaling group to reference the new AMI and 1AM role Perform an EC2 Auto Scaling instance refresh
D. Rotate the potentially compromised access key Create a new AMI without the potentially compromised access key Use a user data script to supply the new access key as environmental variables in the Auto Scaling group's launch configuration Perform an EC2 Auto Scaling instance refresh

Correct Answer: C
Section:
Explanation:
The AWS documentation states that you can create a new AMI without the potentially compromised credentials and create an 1AM role that includes the correct permissions. You can then create a launch template for the Auto Scaling group to reference the new AMI and 1AM role. This method is the most secure way to remediate the security concerns without causing downtime for the application.

QUESTION 30
A company is building a data processing application that uses AWS Lambda functions The application's Lambda functions need to communicate with an Amazon RDS OB instance that is deployed within a VPC in the same AWS account
Which solution meets these requirements in the MOST secure way?

A. Configure the DB instance to allow public access Update the DB instance security group to allow access from the Lambda public address space for the AWS Region
B. Deploy the Lambda functions inside the VPC Attach a network ACL to the Lambda subnet Provide outbound rule access to the VPC CIDR range only Update the DB instance security group to allow traffic from 0 0 0 0/0
C. Deploy the Lambda functions inside the VPC Attach a security group to the Lambda functions Provide outbound rule access to the VPC CIDR range only Update the DB instance security group to allow traffic from the Lambda security group
D. Peer the Lambda default VPC with the VPC that hosts the DB instance to allow direct network access without the need for security groups

Correct Answer: C
Section:
Explanation:
The AWS documentation states that you can deploy the Lambda functions inside the VPC and attach a security group to the Lambda functions. You can then provide outbound rule access to the VPC CIDR range only and update the DB instance security group to allow traffic from the Lambda security group. This method is the most secure way to meet the requirements.

QUESTION 31
A company's security engineer wants to receive an email alert whenever Amazon GuardDuty, AWS Identity and Access Management Access Analyzer, or Amazon Made generate a high-severity security finding. The company uses AWS Control Tower to govern all of its accounts. The company also uses AWS Security Hub with all of the AWS service integrations turned on.
Which solution will meet these requirements with the LEAST operational overhead?

A. Set up separate AWS Lambda functions for GuardDuty, 1AM Access Analyzer, and Macie to call each service's public API to retrieve high-severity findings. Use Amazon Simple Notification Service (Amazon SNS) to send the email alerts. Create an Amazon EventBridge rule to invoke the functions on a schedule.
B. Create an Amazon EventBridge rule with a pattern that matches Security Hub findings events with high severity. Configure the rule to send the findings to a target Amazon Simple Notification Service (Amazon

SNS) topic. Subscribe the desired email addresses to the SNS topic.

C. Create an Amazon EventBridge rule with a pattern that matches AWS Control Tower events with high severity. Configure the rule to send the findings to a target Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the desired email addresses to the SNS topic.

D. Host an application on Amazon EC2 to call the GuardDuty, 1AM Access Analyzer, and Macie APIs. Within the application, use the Amazon Simple Notification Service (Amazon SNS) API to retrieve high-severity findings and to send the findings to an SNS topic. Subscribe the desired email addresses to the SNS topic.

Correct Answer: B
Section:
Explanation:
The AWS documentation states that you can create an Amazon EventBridge rule with a pattern that matches Security Hub findings events with high severity. You can then configure the rule to send the findings to a target Amazon Simple Notification Service (Amazon SNS) topic. You can subscribe the desired email addresses to the SNS topic. This method is the least operational overhead way to meet the requirements.

QUESTION 32
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. Create a custom AWS Config rule to assess the key's scheduled deletion. Configure the rule to trigger upon a configuration change. Send a message to an Amazon Simple Notification Service (Amazon SNS) topic if the key is scheduled for deletion.

B. Create an Amazon EventBridge rule to detect KMS API calls of DeleteAlias. Create an AWS Lambda function to send an Amazon Simple Notification Service (Amazon SNS) message to the company. Add the Lambda function as the target of the EventBridge rule.

C. 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. Add the Lambda function as the target of the EventBridge rule.

D. 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. Add the Lambda function as the target of the SNS policy.

Correct Answer: C
Section:
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.

QUESTION 33
An AWS account that is used for development projects has a VPC that contains two subnets. The first subnet is named public-subnet-1 and has the CIDR block 192.168.1.0/24 assigned. The other subnet is named private-subnet-2 and has the CIDR block 192.168.2.0/24 assigned. Each subnet contains Amazon EC2 instances.
Each subnet is currently using the VPC's default network ACL. The security groups that the EC2 instances in these subnets use have rules that allow traffic between each instance where required. Currently, all network traffic flow is working as expected between the EC2 instances that are using these subnets.
A security engineer creates a new network ACL that is named subnet-2-NACL with default entries. The security engineer immediately configures private-subnet-2 to use the new network ACL and makes no other changes to the infrastructure. The security engineer starts to receive reports that the EC2 instances in public-subnet-1 and public-subnet-2 cannot communicate with each other.
Which combination of steps should the security engineer take to allow the EC2 instances that are running in these two subnets to communicate again? (Select TWO.)

A. Add an outbound allow rule for 192.168.2.0/24 in the VPC's default network ACL.

B. Add an inbound allow rule for 192.168.2.0/24 in the VPC's default network ACL.

C. Add an outbound allow rule for 192.168.2.0/24 in subnet-2-NACL.

D. Add an inbound allow rule for 192.168.1.0/24 in subnet-2-NACL.

E. Add an outbound allow rule for 192.168.1.0/24 in subnet-2-NACL.

Correct Answer: C, E
Section:
Explanation:
The AWS documentation states that you can add an outbound allow rule for 192.168.2.0/24 in subnet-2-NACL and add an outbound allow rule for 192.168.1.0/24 in subnet-2-NACL. This will allow the EC2 instances that are running in these two subnets to communicate again.

QUESTION 34
A company uses Amazon EC2 Linux instances in the AWS Cloud. A member of the company's security team recently received a report about common vulnerability identifiers on the instances.
A security engineer needs to verify patching and perform remediation if the instances do not have the correct patches installed. The security engineer must determine which EC2 instances are at risk and must implement a solution to automatically update those instances with the applicable patches.
What should the security engineer do to meet these requirements?

A. Use AWS Systems Manager Patch Manager to view vulnerability identifiers for missing patches on the instances. Use Patch Manager also to automate the patching process.
B. Use AWS Shield Advanced to view vulnerability identifiers for missing patches on the instances. Use AWS Systems Manager Patch Manager to automate the patching process.
C. Use Amazon GuardDuty to view vulnerability identifiers for missing patches on the instances. Use Amazon Inspector to automate the patching process.
D. Use Amazon Inspector to view vulnerability identifiers for missing patches on the instances. Use Amazon Inspector also to automate the patching process.

Correct Answer: A
Section:
Explanation:
https://aws.amazon.com/about-aws/whats-new/2020/10/now-use-aws-systems-manager-to-view-vulnerability-identifiers-for-missing-patches-on-your-linux-instances/

QUESTION 35
A company has an AWS account that includes an Amazon S3 bucket. The S3 bucket uses server-side encryption with AWS KMS keys (SSE-KMS) to encrypt all the objects at rest by using a customer managed key. The S3 bucket does not have a bucket policy.
An IAM role in the same account has an IAM policy that allows s3 List* and s3 Get' permissions for the S3 bucket. When the IAM role attempts to access an object in the S3 bucket the role receives an access denied message.
Why does the IAM rote not have access to the objects that are in the S3 bucket?

A. The IAM rote does not have permission to use the KMS CreateKey operation.
B. The S3 bucket lacks a policy that allows access to the customer managed key that encrypts the objects.
C. The IAM rote does not have permission to use the customer managed key that encrypts the objects that are in the S3 bucket.
D. The ACL of the S3 objects does not allow read access for the objects when the objects ace encrypted at rest.

Correct Answer: C
Section:
Explanation:
When using server-side encryption with AWS KMS keys (SSE-KMS), the requester must have both Amazon S3 permissions and AWS KMS permissions to access the objects. The Amazon S3 permissions are for the bucket and object operations, such as s3:ListBucket and s3:GetObject. The AWS KMS permissions are for the key operations, such as kms:GenerateDataKey and kms:Decrypt. In this case, the IAM role has the necessary Amazon S3 permissions, but not the AWS KMS permissions to use the customer managed key that encrypts the objects. Therefore, the IAM role receives an access denied message when trying to access the objects. Verified
Reference:
https://docs.aws.amazon.com/AmazonS3/latest/userguide/troubleshoot-403-errors.html
https://repost.aws/knowledge-center/s3-access-denied-error-kms
https://repost.aws/knowledge-center/cross-account-access-denied-error-s3

QUESTION 36

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

A. Use AWS Resource Access Manager (AWS RAM) to share the VPC subnet ID of the HSM that is hosted in the central account with the new dedicated account. Configure the CloudHSM security group to accept inbound traffic from the private IP addresses of client instances in the new dedicated account.
B. Use AWS Identity and Access Management (IAM) to create a cross-account rote to access the CloudHSM cluster that is in the central account Create a new IAM user in the new dedicated account Assign the cross-account rote to the new IAM user.
C. Use AWS 1AM Identity Center (AWS Single Sign-On) to create an AWS Security Token Service (AWS STS) token to authenticate from the new dedicated account to the central account. Use the cross-account permissions that are assigned to the STS token to invoke an operation on the HSM in the central account.
D. Use AWS Resource Access Manager (AWS RAM) to share the ID of the HSM that is hosted in the central account with the new dedicated account. Configure the CloudHSM security group to accept inbound traffic from the private IP addresses of client instances in the new dedicated account.

Correct Answer: A
Section:
Explanation:
https://aws.amazon.com/premiumsupport/knowledge-center/cloudhsm-share-clusters/#:~:text=In%20the%20navigation%20pane%2C%20in,subnet%20ID%20for%20your%20CloudHSM.

QUESTION 37
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.

Correct Answer: B, C, E
Section:
Explanation:
https://d1.awsstatic.com/WWPS/pdf/aws_security_incident_response.pdf

QUESTION 38
A company is using AWS Organizations to manage multiple accounts. The company needs to allow an IAM user to use a role to access resources that are in another organization's AWS account.
Which combination of steps must the company perform to meet this requirement? (Select TWO.)

A. Create an identity policy that allows the sts: AssumeRole action in the AWS account that contains the resources. Attach the identity policy to the IAM user.
B. Ensure that the sts: AssumeRole action is allowed by the SCPs of the organization that owns the resources that the IAM user needs to access.
C. Create a role in the AWS account that contains the resources. Create an entry in the role's trust policy that allows the IAM user to assume the role. Attach the trust policy to the role.
D. Establish a trust relationship between the IAM user and the AWS account that contains the resources.
E. Create a role in the IAM user's AWS account. Create an identity policy that allows the sts: AssumeRole action. Attach the identity policy to the role.

Correct Answer: B, C
Section:
Explanation:
To allow cross-account access to resources using IAM roles, the following steps are required:
Create a role in the AWS account that contains the resources (the trusting account) and specify the AWS account that contains the IAM user (the trusted account) as a trusted entity in the role's trust policy. This allows users from the trusted account to assume the role and access resources in the trusting account.
Ensure that the IAM user has permission to assume the role in their own AWS account. This can be done by creating an identity policy that allows the sts:AssumeRole action and attaching it to the IAM user or their group.
Ensure that there are no service control policies (SCPs) in the organization that owns the resources that deny or restrict access to the sts:AssumeRole action or the role itself. SCPs are applied to all accounts in an organization and can override any permissions granted by IAM policies.
Verified
Reference:
https://repost.aws/knowledge-center/cross-account-access-iam
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_accounts_access.html
https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html

QUESTION 39
A company in France uses Amazon Cognito with the Cognito Hosted Ul as an identity broker for sign-in and sign-up processes. The company is marketing an application and expects that all the application's users will come from France.
When the company launches the application the company's security team observes fraudulent sign-ups for the application. Most of the fraudulent registrations are from users outside of France.
The security team needs a solution to perform custom validation at sign-up Based on the results of the validation the solution must accept or deny the registration request.
Which combination of steps will meet these requirements? (Select TWO.)

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

Correct Answer: B
Section:
Explanation:
https://docs.aws.amazon.com/cognito/latest/developerguide/user-pool-lambda-post-authentication.html

QUESTION 40
A company is running its workloads in a single AWS Region and uses AWS Organizations. A security engineer must implement a solution to prevent users from launching resources in other Regions.
Which solution will meet these requirements with the LEAST operational overhead?

A. Create an IAM policy that has an aws RequestedRegion condition that allows actions only in the designated Region Attach the policy to all users.
B. Create an I AM policy that has an aws RequestedRegion condition that denies actions that are not in the designated Region Attach the policy to the AWS account in AWS Organizations.
C. Create an IAM policy that has an aws RequestedRegion condition that allows the desired actions Attach the policy only to the users who are in the designated Region.
D. Create an SCP that has an aws RequestedRegion condition that denies actions that are not in the designated Region. Attach the SCP to the AWS account in AWS Organizations.

Correct Answer: D
Section:
Explanation:
Although you can use a IAM policy to prevent users launching resources in other regions. The best practice is to use SCP when using AWS organizations.

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

QUESTION 41
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 kms us-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.

Correct Answer: B
Section:
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-snapshot.Encryption

QUESTION 42
A company has multiple accounts in the AWS Cloud. Users in the developer account need to have access to specific resources in the production account.
What is the MOST secure way to provide this access?

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

Correct Answer: D
Section:
Explanation:
https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html

QUESTION 43
A company has an organization in AWS Organizations that includes dedicated accounts for each of its business units. The company is collecting all AWS CloudTrail logs from the accounts in a single Amazon S3 bucket in the top-level account. The company's IT governance team has access to the top-level account. A security engineer needs to allow each business unit to access its own CloudTrail logs.
The security engineer creates an IAM role in the top-level account for each of the other accounts. For each role the security engineer creates an IAM policy to allow read-only permissions to objects in the S3 bucket with the prefix of the respective logs.
Which action must the security engineer take in each business unit account to allow an IAM user in that account to read the logs?

A. Attach a policy to the IAM user to allow the user to assume the role that was created in the top-level account. Specify the role's ARN in the policy.
B. Create an SCP that grants permissions to the top-level account.
C. Use the root account of the business unit account to assume the role that was created in the top-level account. Specify the role's ARN in the policy.

D. Forward the credentials of the IAM role in the top-level account to the IAM user in the business unit account.

Correct Answer: A
Section:
Explanation:
To allow an IAM user in one AWS account to access resources in another AWS account using IAM roles, the following steps are required:
Create a role in the AWS account that contains the resources (the trusting account) and specify the AWS account that contains the IAM user (the trusted account) as a trusted entity in the role's trust policy. This allows users from the trusted account to assume the role and access resources in the trusting account.
Attach a policy to the IAM user in the trusted account that allows the user to assume the role in the trusting account. The policy must specify the ARN of the role that was created in the trusting account.
The IAM user can then switch roles or use temporary credentials to access the resources in the trusting account.
Verified
Reference:
https://repost.aws/knowledge-center/cross-account-access-iam
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_accounts_access.html
https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html

QUESTION 44
A company has a large fleet of Linux Amazon EC2 instances and Windows EC2 instances that run in private subnets. The company wants all remote administration to be performed as securely as possible in the AWS Cloud.
Which solution will meet these requirements?

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

Correct Answer: A
Section:
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
Reference:
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/QUnV4R9EoeSdW0GT3cKBUR7w/what-is-the-difference-between-ec-2-instance-connect-and-session-manager-ssh-connections

QUESTION 45
An ecommerce company is developing new architecture for an application release. The company needs to implement TLS for incoming traffic to the application. Traffic for the application will originate from the internet TLS does not have to be implemented in an end-to-end configuration because the company is concerned about impacts on performance. The incoming traffic types will be HTTP and HTTPS The application uses ports 80 and 443.
What should a security engineer do to meet these requirements?

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

Correct Answer: A
Section:
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
Reference:
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