NO.1 A company's application team needs to host a MySQL database on IAM. According to the company's security policy, all data that is stored on IAM must be encrypted at rest. In addition, all cryptographic material must be compliant with FIPS 140-2 Level 3 validation.
The application team needs a solution that satisfies the company's security requirements and minimizes operational overhead.
Which solution will meet these requirements?
A. Host the database on Amazon RDS. Use Amazon Elastic Block Store (Amazon EBS) for encryption. Use an IAM Key Management Service (IAM KMS) custom key store that is backed by IAM CloudHSM for key management.
B. Host the database on Amazon RDS. Use Amazon Elastic Block Store (Amazon EBS) for encryption. Use an IAM managed CMK in IAM Key Management Service (IAM KMS) for key management.
C. Host the database on an Amazon EC2 instance. Use Amazon Elastic Block Store (Amazon EBS) for encryption. Use a customer managed CMK in IAM Key Management Service (IAM KMS) for key management.
D. Host the database on an Amazon EC2 instance. Use Transparent Data Encryption (TDE) for encryption and key management.
Answer: B

NO.2 A company is undergoing a layer 3 and layer 4 DDoS attack on its web servers running on IAM. Which combination of IAM services and features will provide protection in this scenario? (Select THREE).
A. Amazon Route 53
B. IAM Certificate Manager (ACM)
C. Amazon S3
D. IAM Shield
E. Elastic Load Balancer
F. Amazon GuardDuty
Answer: D E F

NO.3 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.
Answer: A

Explanation:
https://aws.amazon.com/about-aws/whats-new/2020/10/now-use-aws-systems-manager-to-view-vulnerability-ide

NO.4 A company created an IAM account for its developers to use for testing and learning purposes Because MM account will be shared among multiple teams of developers, the company wants to restrict the ability to stop and terminate Amazon EC2 instances so that a team can perform these actions only on the instances it owns.
Developers were Instructed to tag al their instances with a Team tag key and use the team name in the tag value One of the first teams to use this account is Business Intelligence A security engineer needs to develop a highly scalable solution for providing developers with access to the appropriate resources within the account The security engineer has already created individual IAM roles for each team.
Which additional configuration steps should the security engineer take to complete the task?
A. For each team, create an AM policy similar to the one that fellows Populate the ec2: ResourceTag/Team condition key with a proper team name Attach resulting policies to the corresponding IAM roles.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "NotAction": [
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ]
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/Team": "BusinessIntelligence"
                }
            }
        }
    ]
}
```

B. For each team create an IAM policy similar to the one that follows Populate the IAM TagKeys/Team condition key with a proper team name. Attach the resuming policies to the corresponding IAM roles.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "NotAction": [
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys/Team": "BusinessIntelligence"
                }
            }
        }
    ]
}
```

C. Tag each IAM role with a Team lag key. and use the team name in the tag value. Create an IAM policy similar to the one that follows, and attach 4 to all the IAM roles used by developers.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "NotAction": [
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/Team": "${aws:PrincipalTag/Team}"
                }
            }
        }
    ]
}
```

D. Tag each IAM role with the Team key, and use the team name in the tag value. Create an IAM policy similar to the one that follows, and it to all the IAM roles used by developers.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "NotAction": [
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys/Team": "${aws:PrincipalTag/Team}"
                }
            }
        }
    ]
}
```

Answer: A

NO.5 A company uses AWS Signer with all of the company's AWS Lambda functions. A developer recently stopped working for the company. The company wants to ensure that all the code that the developer wrote can no longer be deployed to the Lambda functions.
Which solution will meet this requirement?

A. Revoke all versions of the signing profile assigned to the developer.

B. Examine the developer's IAM roles. Remove all permissions that grant access to Signer.

C. Re-encrypt all source code with a new AWS Key Management Service (AWS KMS) key.

D. Use Amazon CodeGuru to profile all the code that the Lambda functions use.

Answer: A

Explanation:
The correct answer is A. Revoke all versions of the signing profile assigned to the developer.
According to the AWS documentation1, AWS Signer is a fully managed code-signing service that helps you ensure the trust and integrity of your code. You can use Signer to sign code artifacts, such as Lambda deployment packages, with code-signing certificates that you control and manage.
A signing profile is a collection of settings that Signer uses to sign your code artifacts. A signing profile includes information such as the following:
* The type of signature that you want to create (for example, a code-signing signature).
* The signing algorithm that you want Signer to use to sign your code.
* The code-signing certificate and its private key that you want Signer to use to sign your code.
You can create multiple versions of a signing profile, each with a different code-signing certificate. You can also revoke a version of a signing profile if you no longer want to use it for signing code artifacts.
In this case, the company wants to ensure that all the code that the developer wrote can no longer be deployed to the Lambda functions. One way to achieve this is to revoke all versions of the signing profile that was assigned to the developer. This will prevent Signer from using that signing profile to

sign any new code artifacts, and also invalidate any existing signatures that were created with that signing profile. This way, the company can ensure that only trusted and authorized code can be deployed to the Lambda functions.
The other options are incorrect because:
* B. Examining the developer's IAM roles and removing all permissions that grant access to Signer may not be sufficient to prevent the deployment of the developer's code. The developer may have already signed some code artifacts with a valid signing profile before leaving the company, and those signatures may still be accepted by Lambda unless the signing profile is revoked.
* C. Re-encrypting all source code with a new AWS Key Management Service (AWS KMS) key may not be effective or practical. AWS KMS is a service that lets you create and manage encryption keys for your data. However, Lambda does not require encryption keys for deploying code artifacts, only valid signatures from Signer. Therefore, re-encrypting the source code may not prevent the deployment of the developer's code if it has already been signed with a valid signing profile. Moreover, re-encrypting all source code may be time-consuming and disruptive for other developers who are working on the same code base.
* D. Using Amazon CodeGuru to profile all the code that the Lambda functions use may not help with preventing the deployment of the developer's code. Amazon CodeGuru is a service that provides intelligent recommendations to improve your code quality and identify an application's most expensive lines of code. However, CodeGuru does not perform any security checks or validations on your code artifacts, nor does it interact with Signer or Lambda in any way. Therefore, using CodeGuru may not prevent unauthorized or untrusted code from being deployed to the Lambda functions.
References:
1: What is AWS Signer? - AWS Signer

NO.6 A company uses infrastructure as code (IaC) to create AWS infrastructure. The company writes the code as AWS CloudFormation templates to deploy the infrastructure. The company has an existing CI/CD pipeline that the company can use to deploy these templates.
After a recent security audit, the company decides to adopt a policy-as-code approach to improve the company's security posture on AWS. The company must prevent the deployment of any infrastructure that would violate a security policy, such as an unencrypted Amazon Elastic Block Store (Amazon EBS) volume.
Which solution will meet these requirements?
A. Turn on AWS Trusted Advisor. Configure security notifications as webhooks in the preferences section of the CI/CD pipeline.
B. Turn on AWS Config. Use the prebuilt rules or customized rules. Subscribe the CI/CD pipeline to an Amazon Simple Notification Service (Amazon SNS) topic that receives notifications from AWS Config.
C. Create rule sets in AWS CloudFormation Guard. Run validation checks for CloudFormation templates as a phase of the CI/CD process.
D. Create rule sets as SCPs. Integrate the SCPs as a part of validation control in a phase of the CI/CD process.
Answer: C
Explanation:
The correct answer is C. Create rule sets in AWS CloudFormation Guard. Run validation checks for CloudFormation templates as a phase of the CI/CD process.
This answer is correct because AWS CloudFormation Guard is a tool that helps you implement policy-as-code for your CloudFormation templates. You can use Guard to write rules that define your

security policies, such as requiring encryption for EBS volumes, and then validate your templates against those rules before deploying them. You can integrate Guard into your CI/CD pipeline as a step that runs the validation checks and prevents the deployment of any non-compliant templates12.
The other options are incorrect because:
* A. Turning on AWS Trusted Advisor and configuring security notifications as webhooks in the preferences section of the CI/CD pipeline is not a solution, because AWS Trusted Advisor is not a policy-as-code tool, but a service that provides recommendations to help you follow AWS best practices. Trusted Advisor does not allow you to define your own security policies or validate your CloudFormation templates against them3.
* B. Turning on AWS Config and using the prebuilt or customized rules is not a solution, because AWS Config is not a policy-as-code tool, but a service that monitors and records the configuration changes of your AWS resources. AWS Config does not allow you to validate your CloudFormation templates before deploying them, but only evaluates the compliance of your resources after they are created4.
* D. Creating rule sets as SCPs and integrating them as a part of validation control in a phase of the CI/CD process is not a solution, because SCPs are not policy-as-code tools, but policies that you can use to manage permissions in your AWS Organizations. SCPs do not allow you to validate your CloudFormation templates, but only restrict the actions that users and roles can perform in your accounts5.
References:
1: What is AWS CloudFormation Guard? 2: Introducing AWS CloudFormation Guard 2.0 3: AWS Trusted Advisor 4: What Is AWS Config? 5: Service control policies - AWS Organizations

NO.7 An Application team has requested a new IAM KMS master key for use with Amazon S3, but the organizational security policy requires separate master keys for different IAM services to limit blast radius.
How can an IAM KMS customer master key (CMK) be constrained to work with only Amazon S3?
A. Configure the CMK key policy to allow only the Amazon S3 service to use the kms Encrypt action
B. Configure the CMK key policy to allow IAM KMS actions only when the kms ViaService condition matches the Amazon S3 service name.
C. Configure the IAM user's policy lo allow KMS to pass a rote lo Amazon S3
D. Configure the IAM user's policy to allow only Amazon S3 operations when they are combined with the CMK
Answer: B
Explanation:
the kms:ViaService condition key can be used to restrict a CMK to work with only a specific AWS service6. By configuring the CMK key policy to allow KMS actions only when the kms:ViaService condition matches the Amazon S3 service name, you can ensure that only Amazon S3 can use the CMK7. The other options are either incorrect or insufficient for constraining a CMK to work with only Amazon S3.

NO.8 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

Answer: A

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.

References: : Amazon Elastic Container Service Developer Guide

NO.9 A security engineer wants to evaluate configuration changes to a specific AWS resource to ensure that the resource meets compliance standards. However, the security engineer is concerned about a situation in which several configuration changes are made to the resource in quick succession. The security engineer wants to record only the latest configuration of that resource to indicate the cumulative impact of the set of changes.

Which solution will meet this requirement in the MOST operationally efficient way?

A. Use AWS CloudTrail to detect the configuration changes by filtering API calls to monitor the changes.

Use the most recent API call to indicate the cumulative impact of multiple calls

B. Use AWS Config to detect the configuration changes and to record the latest configuration in case of multiple configuration changes.

C. Use Amazon CloudWatch to detect the configuration changes by filtering API calls to monitor the changes. Use the most recent API call to indicate the cumulative impact of multiple calls.

D. Use AWS Cloud Map to detect the configuration changes. Generate a report of configuration changes from AWS Cloud Map to track the latest state by using a sliding time window.

Answer: B

Explanation:

AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. AWS Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations.

To evaluate configuration changes to a specific AWS resource and ensure that it meets compliance standards, the security engineer should use AWS Config to detect the configuration changes and to record the latest configuration in case of multiple configuration changes. This will allow the security engineer to view the current state of the resource and its compliance status, as well as its configuration history and timeline.

AWS Config records configuration changes as ConfigurationItems, which are point-in-time snapshots of the resource's attributes, relationships, and metadata. If multiple configuration changes occur within a short period of time, AWS Config records only the latest ConfigurationItem for that resource. This indicates the cumulative impact of the set of changes on the resource's configuration.

This solution will meet the requirement in the most operationally efficient way, as it leverages AWS Config's features to monitor, record, and evaluate resource configurations without requiring

additional tools or services.
The other options are incorrect because they either do not record the latest configuration in case of multiple configuration changes (A, C), or do not use a valid service for evaluating resource configurations (D).
Verified References:
* https://docs.aws.amazon.com/config/latest/developerguide/WhatIsConfig.html
* https://docs.aws.amazon.com/config/latest/developerguide/config-item-table.html

NO.10 A Security Engineer is troubleshooting an issue with a company's custom logging application. The application logs are written to an Amazon S3 bucket with event notifications enabled to send events lo an Amazon SNS topic. All logs are encrypted at rest using an IAM KMS CMK. The SNS topic is subscribed to an encrypted Amazon SQS queue. The logging application polls the queue for new messages that contain metadata about the S3 object. The application then reads the content of the object from the S3 bucket for indexing.
The Logging team reported that Amazon CloudWatch metrics for the number of messages sent or received is showing zero. No togs are being received.
What should the Security Engineer do to troubleshoot this issue?
A) Add the following statement to the IAM managed CMKs:

```
{
    "Sid": "Allow Amazon SNS to use this key",
    "Effect": "Allow",
    "Principal": {
        "Service": ["sns.amazonaws.com", "sqs.amazonaws.com", "s3.amazonaws.com"]
    },
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey*"
    ],
    "Resource": "*"
}
```

B)
Add the following statement to the CMK key policy:

```
{
    "Sid": "Allow Amazon SNS to use this key",
    "Effect": "Allow",
    "Principal": {
        "Service": "sns.amazonaws.com"
    },
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey*"
    ],
    "Resource": "*"
}
```

C)
Add the following statement to the CMK key policy:

```
{
    "Sid": "Allow Amazon SNS to use this key",
    "Effect": "Allow",
    "Principal": {
        "Service": "sqs.amazonaws.com"
    },
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey*"
    ],
    "Resource": "*"
}
```

D)
Add the following statement to the CMK key policy:

```
{
    "Sid": "Allow Amazon SNS to use this key",
    "Effect": "Allow",
    "Principal": {
        "Service": "s3.amazonaws.com"
    },
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey*"
    ],
    "Resource": "*"
}
```

A. Option A
B. Option B
C. Option C
D. Option D
Answer: D

NO.11 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.

Answer: A

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 References:

* 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

NO.12 An ecommerce website was down for 1 hour following a DDoS attack Users were unable to connect to the website during the attack period. The ecommerce company's security team is worried about future potential attacks and wants to prepare for such events The company needs to minimize downtime in its response to similar attacks in the future.

Which steps would help achieve this9 (Select TWO)

A. Enable Amazon GuardDuty to automatically monitor for malicious activity and block unauthorized access.

B. Subscribe to IAM Shield Advanced and reach out to IAM Support in the event of an attack.

C. Use VPC Flow Logs to monitor network: traffic and an IAM Lambda function to automatically block an attacker's IP using security groups.

D. Set up an Amazon CloudWatch Events rule to monitor the IAM CloudTrail events in real time use IAM Config rules to audit the configuration, and use IAM Systems Manager for remediation.

E. Use IAM WAF to create rules to respond to such attacks

Answer: B E

Explanation:

To minimize downtime in response to DDoS attacks, the company should do the following:

* Subscribe to AWS Shield Advanced and reach out to AWS Support in the event of an attack. This provides access to 24x7 support from the AWS DDoS Response Team (DRT), as well as advanced detection and mitigation capabilities for network and application layer attacks.
* Use AWS WAF to create rules to respond to such attacks. This allows the company to filter web requests based on IP addresses, headers, body, or URI strings, and block malicious requests before

they reach the web applications.

NO.13 A company is using AWS to run a long-running analysis process on data that is stored in Amazon S3 buckets.
The process runs on a fleet of Amazon EC2 instances that are in an Auto Scaling group. The EC2 instances are deployed in a private subnet Of a VPC that does not have internet access. The EC2 instances and the S3 buckets are in the same AWS account The EC2 instances access the S3 buckets through an S3 gateway endpoint that has the default access policy.
Each EC2 instance is associated With an instance profile role that has a policy that explicitly allows the s3:GetObject action and the s3:PutObject action for only the required S3 buckets.
The company learns that one or more of the EC2 instances are compromised and are exfiltrating data to an S3 bucket that is outside the companys organization in AWS Organizations. A security engtneer must implement a solution to stop this exfiltration of data and to keep the EC2 processing job functional.
Which solution will meet these requirements?
A. Update the policy on the S3 gateway endpoint to allow the S3 actions CY11y if the values of the aws:ResourceOrglD and aws:PrincipalOrglD condition keys match the companys values.
B. Update the policy on the instance profile role to allow the S3 actions only if the value of the aws:ResourceOrglD condition key matches the company's value.
C. Add a network ACL rule to the subnet of the EC2 instances to block outgoing connections on port 443.
D. Apply an SCP on the AWS account to allow the $3 actions only if the values of the aws:ResourceOrglD and aws:PrincipalOrglD condition keys match the company's values.
Answer: D
Explanation:
The correct answer is D.
To stop the data exfiltration from the compromised EC2 instances, the security engineer needs to implement a solution that can deny access to any S3 bucket that is outside the company's organization. The solution should also allow the EC2 instances to access the required S3 buckets within the company's organization for the analysis process.
Option A is incorrect because updating the policy on the S3 gateway endpoint will not affect the access to S3 buckets that are outside the company's organization. The S3 gateway endpoint only applies to S3 buckets that are in the same AWS Region as the VPC. The compromised EC2 instances can still access S3 buckets in other Regions or other AWS accounts through the internet gateway or NAT device.
Option B is incorrect because updating the policy on the instance profile role will not prevent the compromised EC2 instances from using other credentials or methods to access S3 buckets outside the company's organization. The instance profile role only applies to requests that are made using the credentials of that role. The compromised EC2 instances can still use other IAM users, roles, or access keys to access S3 buckets outside the company's organization.
Option C is incorrect because adding a network ACL rule to block outgoing connections on port 443 will also block legitimate connections to S3 buckets within the company's organization. The network ACL rule will prevent the EC2 instances from accessing any S3 bucket through HTTPS, regardless of whether it is inside or outside the company's organization.
Option D is correct because applying an SCP on the AWS account will effectively deny access to any S3 bucket that is outside the company's organization. The SCP will apply to all IAM users, roles, and

resources in the AWS account, regardless of how they access S3. The SCP will use the aws:ResourceOrgID and aws:PrincipalOrgID condition keys to check whether the S3 bucket and the principal belong to the same organization as the AWS account. If they do not match, the SCP will deny the S3 actions.
References:
* Using service control policies
* AWS Organizations service control policy examples

NO.14 A company uses AWS Organizations to manage several AWs accounts. The company processes a large volume of sensitive data. The company uses a serverless approach to microservices. The company stores all the data in either Amazon S3 or Amazon DynamoDB. The company reads the data by using either AWS lambda functions or container-based services that the company hosts on Amazon Elastic Kubernetes Service (Amazon EKS) on AWS Fargate.
The company must implement a solution to encrypt all the data at rest and enforce least privilege data access controls. The company creates an AWS Key Management Service (AWS KMS) customer managed key.
What should the company do next to meet these requirements?
A. Create a key policy that allows the kms:Decrypt action only for Amazon S3 and DynamoDB. Create an SCP that denies the creation of S3 buckets and DynamoDB tables that are not encrypted with the key.
B. Create an 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.
Answer: B

NO.15 A security engineer needs to build a solution to turn IAM CloudTrail back on in multiple IAM Regions in case it is ever turned off.
What is the MOST efficient way to implement this solution?
A. Use IAM Config with a managed rule to trigger the IAM-EnableCloudTrail remediation.
B. Create an Amazon EventBridge (Amazon CloudWatch Events) event with a cloudtrail.amazonIAM.com event source and a StartLogging event name to trigger an IAM Lambda function to call the StartLogging API.
C. Create an Amazon CloudWatch alarm with a cloudtrail.amazonIAM.com event source and a StopLogging event name to trigger an IAM Lambda function to call the StartLogging API.
D. Monitor IAM Trusted Advisor to ensure CloudTrail logging is enabled.
Answer: B

NO.16 A company is storing data in Amazon S3 Glacier. A security engineer implemented a new vault lock policy for

10 TB of data and called the initiate-vault-lock operation 12 hours ago. The audit team identified a typo in the policy that is allowing unintended access to the vault.
What is the MOST cost-effective way to correct this error?

A. Call the abort-vault-lock operation. Update the policy. Call the initiate-vault-lock operation again.

B. Copy the vault data to a new S3 bucket. Delete the vault. Create a new vault with the data.

C. Update the policy to keep the vault lock in place

D. Update the policy. Call the initiate-vault-lock operation again to apply the new policy.

Answer: A

Explanation:
The most cost-effective way to correct a typo in a vault lock policy during the 24-hour initiation period is to call the abort-vault-lock operation. This action stops the vault lock process, allowing the security engineer to correct the policy and re-initiate the vault lock with the corrected policy. This approach avoids the need for data transfer or creating a new vault, thus minimizing costs and operational overhead.

NO.17 There are currently multiple applications hosted in a VPC. During monitoring it has been noticed that multiple port scans are coming in from a specific IP Address block. The internal security team has requested that all offending IP Addresses be denied for the next 24 hours. Which of the following is the best method to quickly and temporarily deny access from the specified IP Address's.
Please select:

A. Create an AD policy to modify the Windows Firewall settings on all hosts in the VPC to deny access from the IP Address block.

B. Modify the Network ACLs associated with all public subnets in the VPC to deny access from the IP Address block.

C. Add a rule to all of the VPC Security Groups to deny access from the IP Address block.

D. Modify the Windows Firewall settings on all AMI'S that your organization uses in that VPC to deny access from the IP address block.

Answer: B

Explanation:
NACL acts as a firewall at the subnet level of the VPC and we can deny the offending IP address block at the subnet level using NACL rules to block the incoming traffic to the VPC instances. Since NACL rules are applied as per the Rule numbers make sure that this rule number should take precedence over other rule numbers if there are any such rules that will allow traffic from these IP ranges. The lowest rule number has more precedence over a rule that has a higher number.
The IAM Documentation mentions the following as a best practices for IAM users For extra security, enable multi-factor authentication (MFA) for privileged IAM users (users who are allowed access to sensitive resources or APIs). With MFA, users have a device that generates a unique authentication code (a one-time password, or OTP). Users must provide both their normal credentials (like their user name and password) and the OTP. The MFA device can either be a special piece of hardware, or it can be a virtual device (for example, it can run in an app on a smartphone).
Options C is invalid because these options are not available
Option D is invalid because there is not root access for users
For more information on IAM best practices, please visit the below URL:
https://docs.IAM.amazon.com/IAM/latest/UserGuide/best-practices.html
The correct answer is: Modify the Network ACLs associated with all public subnets in the VPC to deny

access from the IP Address block.
omit your Feedback/Queries to our Experts

NO.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

Answer: A B C

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

NO.19 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

Answer: C
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.
References: : AWS Security Best Practices

NO.20 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.

Answer: A D

NO.21 A security engineer is designing a cloud architecture to support an application. The application runs on Amazon EC2 instances and processes sensitive information, including credit card numbers.
The application will send the credit card numbers to a component that is running in an isolated environment.
The component will encrypt, store, and decrypt the numbers.
The component then will issue tokens to replace the numbers in other parts of the application.
The component of the application that manages the tokenization process will be deployed on a separate set of EC2 instances. Other components of the application must not be able to store or access the credit card numbers.
Which solution will meet these requirements?

A. Use EC2 Dedicated Instances for the tokenization component of the application.

B. Place the EC2 instances that manage the tokenization process into a partition placement group.

C. Create a separate VPC. Deploy new EC2 instances into the separate VPC to support the data tokenization.

D. Deploy the tokenization code onto AWS Nitro Enclaves that are hosted on EC2 instances.

Answer: D
Explanation:
AWS Nitro Enclaves are isolated and hardened virtual machines that run on EC2 instances and

provide a secure environment for processing sensitive data. Nitro Enclaves have no persistent storage, interactive access, or external networking, and they can only communicate with the parent instance through a secure local channel. Nitro Enclaves also support cryptographic attestation, which allows verifying the identity and integrity of the enclave and its code. Nitro Enclaves are ideal for implementing data protection solutions such as tokenization, encryption, and key management. Using Nitro Enclaves for the tokenization component of the application meets the requirements of isolating the sensitive data from other parts of the application, encrypting and storing the credit card numbers securely, and issuing tokens to replace the numbers. Other components of the application will not be able to access or store the credit card numbers, as they are only available within the enclave.

NO.22 A security engineer is troubleshooting an AWS Lambda function that is named MyLambdaFunction. The function is encountering an error when the function attempts to read the objects in an Amazon S3 bucket that is named DOC-EXAMPLE-BUCKET. The S3 bucket has the following bucket policy:

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

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

A. Remove the Condition element. Change the Principal element to the following:
{
"AWS": "arn "aws" ::: lambda ::: function:MyLambdaFunction"
}

B. Change the Action element to the following:
" s3:GetObject*"
" s3:GetBucket*"

C. Change the Resource element to "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*".

D. Change the Resource element to "arn:aws:lambda:::function:MyLambdaFunction". Change the Principal element to the following:
{
"Service": "s3.amazonaws.com"
}

Answer: C

Explanation:
The correct answer is C. Change the Resource element to "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*".

The reason is that the Resource element in the bucket policy specifies which objects in the bucket are affected by the policy. In this case, the policy only applies to the bucket itself, not the objects inside it. Therefore, the Lambda function cannot access the objects with the s3:GetObject permission. To fix this, the Resource element should include a wildcard (*) to match all objects in the bucket. This way, the policy grants the Lambda function permission to read any object in the bucket.
The other options are incorrect for the following reasons:
* A. Removing the Condition element would not help, because it only restricts access based on the source IP address of the request. The Principal element should not be changed to the Lambda function ARN, because it specifies who is allowed or denied access by the policy. The policy should allow access to any principal ("*") and rely on IAM roles or policies to control access to the Lambda function.
* B. Changing the Action element to include s3:GetBucket* would not help, because it would grant additional permissions that are not needed by the Lambda function, such as s3:GetBucketAcl or s3:GetBucketPolicy. The s3:GetObject* permission is sufficient for reading objects in the bucket.
* D. Changing the Resource element to the Lambda function ARN would not make sense, because it would mean that the policy applies to the Lambda function itself, not the bucket or its objects. The Principal element should not be changed to s3.amazonaws.com, because it would grant access to any AWS service that uses S3, not just Lambda.

NO.23 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

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/

NO.24 A company is using AWS Organizations to create OUs for its accounts. The company has more than 20 accounts that are all part of the OUs. A security engineer must implement a solution to ensure that no account can stop to file delivery to AWS CloudTrail.
Which solution will meet this requirement?
A. Use the --is-multi-region-trail option while running the create-trail command to ensure that logs are configured across all AWS Regions.
B. Create an SCP that includes a Deny rule tor the cloudtrail. StopLogging action Apply the SCP to all accounts in the OUs.
C. Create an SCP that includes an Allow rule for the cloudtrail. StopLogging action Apply the SCP to all accounts in the OUs.
D. Use AWS Systems Manager to ensure that CloudTrail is always turned on.
Answer: B
Explanation:
This SCP prevents users or roles in any affected account from disabling a CloudTrail log, either directly as a command or through the console. https://asecure.cloud/a/scp_cloudtrail/

NO.25 A company has deployed servers on Amazon EC2 instances in a VPC. External vendors access these servers over the internet. Recently, the company deployed a new application on EC2 instances in a new CIDR range.
The company needs to make the application available to the vendors.
A security engineer verified that the associated security groups and network ACLs are allowing the required ports in the inbound diction. However, the vendors cannot connect to the application.
Which solution will provide the vendors access to the application?
A. Modify the security group that is associated with the EC2 instances to have the same outbound rules as inbound rules.
B. Modify the network ACL that is associated with the CIDR range to allow outbound traffic to ephemeral ports.
C. Modify the inbound rules on the internet gateway to allow the required ports.
D. Modify the network ACL that is associated with the CIDR range to have the same outbound rules

as inbound rules.

Answer: B

Explanation:

The correct answer is B. Modify the network ACL that is associated with the CIDR range to allow outbound traffic to ephemeral ports.

This answer is correct because network ACLs are stateless, which means that they do not automatically allow return traffic for inbound connections. Therefore, the network ACL that is associated with the CIDR range of the new application must have outbound rules that allow traffic to ephemeral ports, which are the temporary ports used by the vendors' machines to communicate with the application servers. Ephemeral ports are typically in the range of 1024-655351. If the network ACL does not have such rules, the vendors will not be able to connect to the application.

The other options are incorrect because:

* A. Modifying the security group that is associated with the EC2 instances to have the same outbound rules as inbound rules is not a solution, because security groups are stateful, which means that they automatically allow return traffic for inbound connections. Therefore, there is no need to add outbound rules to the security group for the vendors to access the application2.
* C. Modifying the inbound rules on the internet gateway to allow the required ports is not a solution, because internet gateways do not have inbound or outbound rules. Internet gateways are VPC components that enable communication between instances in a VPC and the internet. They do not filter traffic based on ports or protocols3.
* D. Modifying the network ACL that is associated with the CIDR range to have the same outbound rules as inbound rules is not a solution, because it does not address the issue of ephemeral ports. The outbound rules of the network ACL must match the ephemeral port range of the vendors' machines, not necessarily the inbound rules of the network ACL4.

References:

1: Ephemeral port - Wikipedia 2: Security groups for your VPC - Amazon Virtual Private Cloud 3 : Internet gateways - Amazon Virtual Private Cloud 4: Network ACLs - Amazon Virtual Private Cloud

NO.26 A company is using an Amazon CloudFront distribution to deliver content from two origins. One origin is a dynamic application that is hosted on Amazon EC2 instances. The other origin is an Amazon S3 bucket for static assets.

A security analysis shows that HTTPS responses from the application do not comply with a security requirement to provide an X-Frame-Options HTTP header to prevent frame-related cross-site scripting attacks.

A security engineer must ipake the full stack compliant by adding the missing HTTP header to the responses.

Which solution will meet these requirements?

A. Create a Lambda@Edge function. Include code to add the X-Frame-Options header to the response.

Configure the function to run in response to the CloudFront origin response event.

B. Create a Lambda@Edge function. Include code to add the X-Frame-Options header to the response.

Configure the function to run in response to the CloudFront viewer request event.

C. Update the CloudFront distribution by adding X-Frame-Options to custom headers in the origin settings.

D. D. Customize the EC2 hosted application to add the X-Frame-Options header to the responses that

are returned to CloudFront.

Answer: A

Explanation:

The correct answer is A because it allows the security engineer to add the X-Frame-Options header to the HTTPS responses from the application origin without modifying the origin itself. A Lambda@Edge function is a Lambda function that runs in response to CloudFront events, such as viewer request, origin request, origin response, or viewer response. By configuring the function to run in response to the origin response event, the security engineer can modify the response headers that CloudFront receives from the origin before sending them to the viewer1. The function can include code to add the X-Frame-Options header with the desired value, such as DENY or SAMEORIGIN, to prevent frame-related cross-site scripting attacks2.

The other options are incorrect because they are either less efficient or less secure than option A. Option B is incorrect because configuring the Lambda@Edge function to run in response to the viewer request event is not optimal, as it adds latency to the request processing and does not modify the response headers that CloudFront receives from the origin. Option C is incorrect because adding X-Frame-Options to custom headers in the origin settings does not affect the response headers that CloudFront sends to the viewer. Custom headers are only used to send additional information to the origin when CloudFront forwards a request3. Option D is incorrect because customizing the EC2 hosted application to add the X-Frame-Options header to the responses requires changing the origin code, which may not be feasible or desirable for the security engineer.

NO.27 A developer 15 building a serverless application hosted on IAM that uses Amazon Redshift in a data store.

The application has separate modules for read/write and read-only functionality. The modules need their own database users tor 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 read/write.

B. Configure a VPC endpoint for Amazon Redshift Configure an endpoint policy that maps database users to each application module, and allow access to the tables that are required for read-only and read/write

C. Configure an IAM poky for each module Specify the ARN of an Amazon Redshift database user that allows the GetClusterCredentials API call

D. Create focal 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: C D

Explanation:

To grant appropriate access to the application modules, the security engineer should do the following:

* Configure an IAM policy for each module. Specify the ARN of an Amazon Redshift database user that

* allows the GetClusterCredentials API call. This allows the application modules to use temporary credentials to access the database with the permissions of the specified user.

* Create local database users for each module. This allows the security engineer to create separate users for read/write and read-only functionality, and to assign them different privileges on the database tables.

NO.28 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
Answer: B D

NO.29 A company uses an Amazon S3 bucket to store reports Management has mandated that all new objects stored in this bucket must be encrypted at rest using server-side encryption with a client-specified IAM Key Management Service (IAM KMS) CMK owned by the same account as the S3 bucket. The IAM account number is 111122223333, and the bucket name Is report bucket. The company's security specialist must write the S3 bucket policy to ensure the mandate can be Implemented Which statement should the security specialist include in the policy?
A.

```
{
    "Effect": "Deny",
    "Principal": "*",
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::reportbucket/*",
    "Condition": {
        "StringEquals": {
            "s3:x-amz-server-side-encryption": "AES256"
        }
    }
}
```

B.

```
{
    "Effect": "Deny",
    "Principal": "*",
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::reportbucket/*",
    "Condition": {
        "StringNotLike": {
            "s3:x-amz-server-side-encryption-aws-kms-key-id": "arn:aws:kms:*:111122223333:key/*"
        }
    }
}
```

C.

```
{
    "Effect": "Deny",
    "Principal": "*",
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::reportbucket/*",
    "Condition": {
        "StringNotLike": {
            "s3:x-amz-server-side-encryption": "aws:kms"
        }
    }
}
```

D.

```
{
    "Effect": "Deny",
    "Principal": "*",
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::reportbucket/*",
    "Condition": {
        "StringNotLikeIfExists": {
            "s3:x-amz-server-side-encryption-aws-kms-key-id": "arn:aws:kms:*:111122223333:key/*"
        }
    }
}
```

Answer: D

NO.30 A company uses Amazon GuardDuty. The company's security team wants all High severity findings to automatically generate a ticket in a third-party ticketing system through email integration. Which solution will meet this requirement?

A. Create a verified identity for the third-party ticketing email system in Amazon Simple Email Service (Amazon SES). Create an Amazon EventBridge rule that includes an event pattern that matches High severity GuardDuty findings. Specify the SES identity as the target for the EventBridge rule.

B. Create an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the third-party ticketing email system to the SNS topic. Create an Amazon EventBridge rule that includes an event pattern that matches High severity GuardDuty findings. Specify the SNS topic as the target for the EventBridge rule.

C. Use the GuardDuty CreateFilter API operation to build a filter in GuardDuty to monitor for High severity findings. Export the results of the filter to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the third-party ticketing email system to the SNS topic.

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

Answer: B

Explanation:

The correct answer is B. Create an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the third-party ticketing email system to the SNS topic. Create an Amazon EventBridge rule that includes an event pattern that matches High severity GuardDuty findings. Specify the SNS topic as the target for the Event-Bridge rule.

According to the AWS documentation1, you can use Amazon EventBridge to create rules that match events from GuardDuty and route them to targets such as Amazon SNS topics. You can use event patterns to filter events based on criteria such as severity, type, or resource. For example, you can create a rule that matches only High severity findings and sends them to an SNS topic that is subscribed by a third-party ticketing email system. This way, you can automate the creation of tickets for High severity findings and notify the security team.

NO.31 A company's cloud operations team is responsible for building effective security for IAM cross-account access. The team asks a security engineer to help troubleshoot why some developers in the developer account (123456789012) in the developers group are not able to assume a cross-account role (ReadS3) into a production account (999999999999) to read the contents of an Amazon S3 bucket (productionapp). The two account policies are as follows:

Developer account 123456789012:
Developer group permissions:

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "sts:AssumeRole",
        "Resource": "arn:aws:iam::999999999999:role/ReadS3"
    }
}
```

Production account 999999999999:
Production account ReadS3 role policy:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:ListAllMyBuckets",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
```

Production account ReadS3 role policy - trust relationship:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::888888888888:root"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "BoolIfExists": {
                    "aws:MultiFactorAuthPresent": "true"
                }
            }
        }
    ]
}
```

Which recommendations should the security engineer make to resolve this issue? (Select TWO.)

A. Ask the developers to change their password and use a different web browser.

B. Ensure that developers are using multi-factor authentication (MFA) when they log in to their developer account as the developer role.

C. Modify the production account ReadS3 role policy to allow the PutBucketPolicy action on the productionapp S3 bucket.

D. Update the trust relationship policy on the production account S3 role to allow the account number of the developer account.

E. Update the developer group permissions in the developer account to allow access to the productionapp S3 bucket.

Answer: A D

NO.32 An organization must establish the ability to delete an IAM KMS Customer Master Key (CMK) within a
24-hour timeframe to keep it from being used for encrypt or decrypt operations Which of tne following actions will address this requirement?

A. Manually rotate a key within KMS to create a new CMK immediately

B. Use the KMS import key functionality to execute a delete key operation

C. Use the schedule key deletion function within KMS to specify the minimum wait period for deletion

D. Change the KMS CMK alias to immediately prevent any services from using the CMK.

Answer: C

Explanation:
the schedule key deletion function within KMS allows you to specify a waiting period before deleting a customer master key (CMK)4. The minimum waiting period is 7 days and the maximum is 30 days5. This function prevents the CMK from being used for encryption or decryption operations during the waiting period4. The other options are either invalid or ineffective for deleting a CMK within a 24-hour timeframe.