# Amazon-Web-Services

## Exam Questions SCS-C02

AWS Certified Security - Specialty

**NEW QUESTION 1**
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.

**Answer:** A

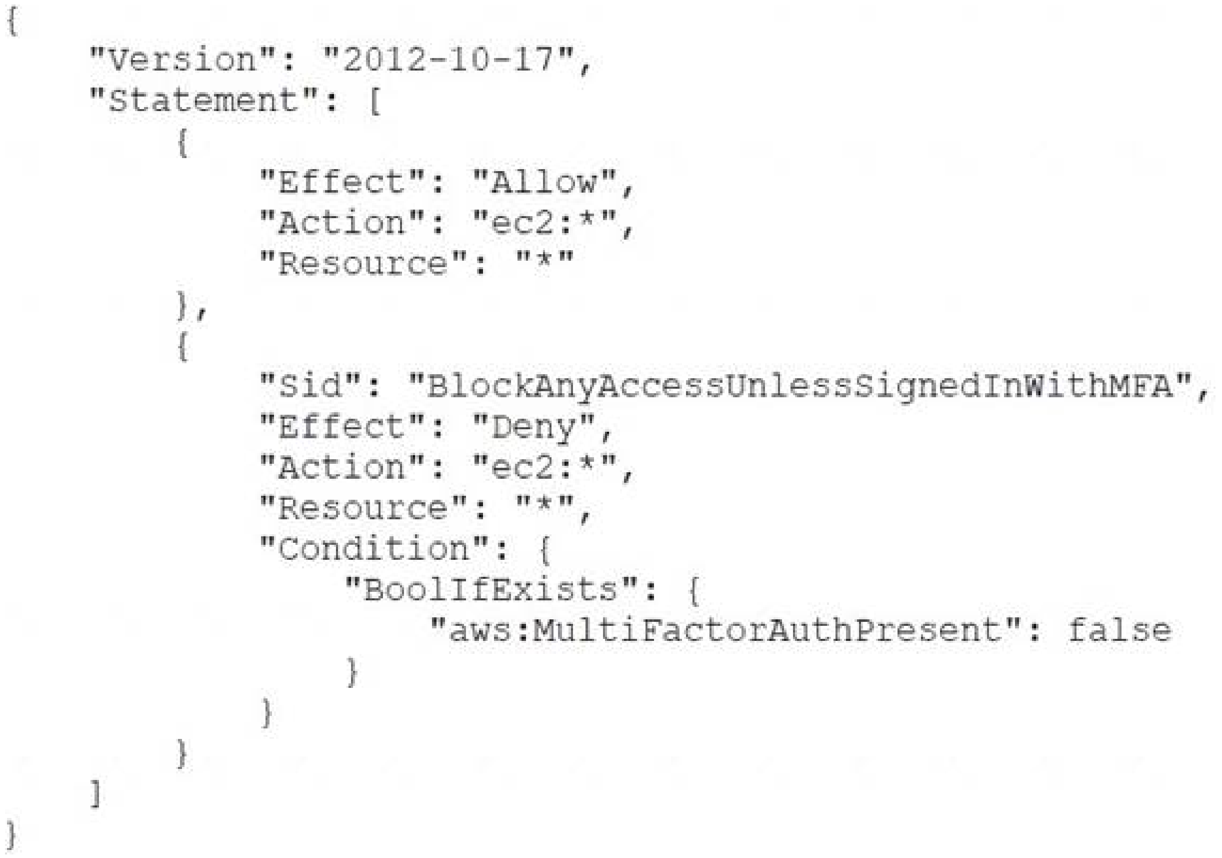
**Explanation:**
To configure end-to-end encryption between the Elastic Load Balancer and the EC2 instances with the least operational effort, the most appropriate solution would be to use Amazon issued AWS Certificate Manager (ACM) certificates on the EC2 instances and the Elastic Load Balancer to configure 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 - Amazo Web Services

**NEW QUESTION 2**
A company developed an application by using AWS Lambda, Amazon S3, Amazon Simple Notification Service (Amazon SNS), and Amazon DynamoDB. An external application puts objects into the company's S3 bucket and tags the objects with date and time. A Lambda function periodically pulls data from the company's S3 bucket based on date and time tags and inserts specific values into a DynamoDB table for further processing.
The data includes personally identifiable information (Pll). The company must remove data that is older than 30 days from the S3 bucket and the DynamoDB table.
Which solution will meet this requirement with the MOST operational efficiency?

A. Update the Lambda function to add a TTL S3 flag to S3 object
B. Create an S3 Lifecycle policy to expire objects that are older than 30 days by using the TTL S3 flag.
C. Create an S3 Lifecycle policy to expire objects that are older than 30 day
D. Update the Lambda function to add the TTL attribute in the DynamoDB tabl
E. Enable TTL on the DynamoDB table to expire entires that are older than 30 days based on the TTL attribute.
F. Create an S3 Lifecycle policy to expire objects that are older than 30 days and to add all prefixes to the S3 bucke
G. Update the Lambda function to delete entries that are older than 30 days.
H. Create an S3 Lifecycle policy to expire objects that are older than 30 days by using object tag
I. Update the Lambda function to delete entries that are older than 30 days.

**Answer:** B

**NEW QUESTION 3**
An AWS account administrator created an IAM group and applied the following managed policy to require that each individual user authenticate using multi-factor authentication:



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

After implementing the policy, the administrator receives reports that users are unable to perform Amazon EC2 commands using the AWS CLI.
What should the administrator do to resolve this problem while still enforcing multi-factor authentication?

A. Change the value of aws:MultiFactorAuthPresent to true.
B. Instruct users to run the aws sts get-session-token CLI command and pass the multi-factor authentication--serial-number and --token-code parameter
C. Use these resulting values to make API/CLI calls.
D. Implement federated API/CLI access using SAML 2.0, then configure the identity provider to enforce multi-factor authentication.
E. Create a role and enforce multi-factor authentication in the role trust polic
F. Instruct users to run the sts assume-role CLI command and pass --serial-number and --token-code parameter
G. Store the resultingvalues in environment variable
H. Add sts:AssumeRole to NotAction in the policy.

**Answer:** B

**Explanation:**
The correct answer is B. Instruct users to run the aws sts get-session-token CLI command and pass the multi-factor authentication --serial-number and --token-code parameters. Use these resulting values to make API/CLI calls.
According to the AWS documentation1, the aws sts get-session-token CLI command returns a set of temporary credentials for an AWS account or IAM user. The credentials consist of an access key ID, a secret access key, and a security token. These credentials are valid for the specified duration only. The session duration for IAM users can be between 15 minutes and 36 hours, with a default of 12 hours.
You can use the --serial-number and --token-code parameters to provide the MFA device serial number and the MFA code from the device. The MFA device must be associated with the user who is making the
get-session-token call. If you do not provide these parameters when your IAM user or role has a policy that requires MFA, you will receive an Access Denied error.
The temporary security credentials that are returned by the get-session-token command can then be used to make subsequent API or CLI calls that require MFA authentication. You can use environment variables or a profile in your AWS CLI configuration file to specify the temporary credentials.
Therefore, this solution will resolve the problem of users being unable to perform EC2 commands using the AWS CLI, while still enforcing MFA.
The other options are incorrect because:

- A. Changing the value of aws:MultiFactorAuthPresent to true will not work, because this is a condition key that is evaluated by AWS when a request is made. You cannot set this value manually in your policy or request. You must provide valid MFA information to AWS for this condition key to be true.
- C. Implementing federated API/CLI access using SAML 2.0 may work, but it requires more operational effort than using the get-session-token command. You would need to configure a SAML identity provider and trust relationship with AWS, and use a custom SAML client to request temporary credentials from AWS STS. This solution may also introduce additional security risks if the identity provider is compromised.
- D. Creating a role and enforcing MFA in the role trust policy may work, but it also requires more operational effort than using the get-session-token command. You would need to create a role for each user or group that needs to perform EC2 commands, and specify a trust policy that requires MFA. You would also need to grant the users permission to assume the role, and instruct them to use the sts assume-role command instead of the get-session-token command.

References:
1: get-session-token — AWS CLI Command Reference

**NEW QUESTION 4**
A security engineer wants to forward custom application-security logs from an Amazon EC2 instance to Amazon CloudWatch. The security engineer installs the CloudWatch agent on the EC2 instance and adds the path of the logs to the CloudWatch configuration file. However, CloudWatch does not receive the logs. The security engineer verifies that the awslogs service is running on the EC2 instance.
What should the security engineer do next to resolve the issue?

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

**Answer:** D

**Explanation:**
The correct answer is D. Attach the CloudWatchAgentServerPolicy AWS managed policy to the EC2 instance role.
According to the AWS documentation1, the CloudWatch agent is a software agent that you can install on your EC2 instances to collect system-level metrics and logs. To use the CloudWatch agent, you need to attach an IAM role or user to the EC2 instance that grants permissions for the agent to perform actions on your behalf. The CloudWatchAgentServerPolicy is an AWS managed policy that provides the necessary permissions for the agent to write metrics and logs to CloudWatch2. By attaching this policy to the EC2 instance role, the security engineer can resolve the issue of CloudWatch not receiving the custom application-security logs.
The other options are incorrect for the following reasons:

- A. Adding AWS CloudTrail to the trust policy of the EC2 instance is not relevant, because CloudTrail is a service that records API activity in your AWS account, not custom application logs3. Sending the custom logs to CloudTrail instead of CloudWatch would not meet the requirement of forwarding them to CloudWatch.
- B. Adding Amazon S3 to the trust policy of the EC2 instance is not necessary, because S3 is a storage service that does not require any trust relationship with EC2 instances4. Configuring the application to write the custom logs to an S3 bucket that CloudWatch can use to ingest the logs would be an alternative solution, but it would be more complex and costly than using the CloudWatch agent directly.
- C. Adding Amazon Inspector to the trust policy of the EC2 instance is not helpful, because Inspector is a service that scans EC2 instances for software vulnerabilities and unintended network exposure, not custom application logs5. Using Amazon Inspector instead of the CloudWatch agent would not meet the requirement of forwarding them to CloudWatch.

References:
1: Collect metrics, logs, and traces with the CloudWatch agent - Amazon CloudWatch 2: CloudWatchAgentServerPolicy - AWS Managed Policy 3: What Is AWS CloudTrail? - AWS CloudTrail 4: Amazon S3 FAQs - Amazon Web Services 5: Automated Software Vulnerability Management - Amazon
Inspector - AWS

**NEW QUESTION 5**
A company has AWS accounts in an organization in AWS Organizations. The organization includes a dedicated security account.
All AWS account activity across all member accounts must be logged and reported to the dedicated security account. The company must retain all the activity logs in a secure storage location within the dedicated security account for 2 years. No changes or deletions of the logs are allowed.
Which combination of steps will meet these requirements with the LEAST operational overhead? (Select TWO.)

A. In the dedicated security account, create an Amazon S3 bucke
B. Configure S3 Object Lock in compliance mode and a retention period of 2 years on the S3 bucke
C. Set the bucket policy to allow the organization's management account to write to the S3 bucket.
D. In the dedicated security account, create an Amazon S3 bucke
E. Configure S3 Object Lock in compliance mode and a retention period of 2 years on the S3 bucke
F. Set the bucket policy to allow the organization's member accounts to write to the S3 bucket.
G. In the dedicated security account, create an Amazon S3 bucket that has an S3 Lifecycle configuration that expires objects after 2 year
H. Set the bucket policy to allow the organization's member accounts to write to the S3 bucket.
I. Create an AWS Cloud Trail trail for the organizatio
J. Configure logs to be delivered to the logging Amazon S3 bucket in the dedicated security account.

K. Turn on AWS CloudTrail in each accoun
L. Configure logs to be delivered to an Amazon S3 bucket that is created in the organization's management accoun
M. Forward the logs to the S3 bucket in the dedicated security account by using AWS Lambda and Amazon Kinesis Data Firehose.

**Answer:** BD

**Explanation:**
The correct answer is B and D. In the dedicated security account, create an Amazon S3 bucket. Configure S3 Object Lock in compliance mode and a retention period of 2 years on the S3 bucket. Set the bucket policy to allow the organization’s member accounts to write to the S3 bucket. Create an AWS CloudTrail trail for the organization. Configure logs to be delivered to the logging Amazon S3 bucket in the dedicated security account.
According to the AWS documentation, AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services.
To use CloudTrail with multiple AWS accounts and regions, you need to enable AWS Organizations with all features enabled. This allows you to centrally manage your accounts and apply policies across your organization. You can also use CloudTrail as a service principal for AWS Organizations, which lets you create an organization trail that applies to all accounts in your organization. An organization trail logs events for all AWS Regions and delivers the log files to an S3 bucket that you specify.
To create an organization trail, you need to use an administrator account, such as the organization’s management account or a delegated administrator account. You can then configure the trail to deliver logs to an S3 bucket in the dedicated security account. This will ensure that all account activity across all member accounts and regions is logged and reported to the security account.
According to the AWS documentation, Amazon S3 is an object storage service that offers scalability, data availability, security, and performance. You can use S3 to store and retrieve any amount of data from anywhere on the web. You can also use S3 features such as lifecycle management, encryption, versioning, and replication to optimize your storage.
To use S3 with CloudTrail logs, you need to create an S3 bucket in the dedicated security account that will store the logs from the organization trail. You can then configure S3 Object Lock on the bucket to prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. You can also enable compliance mode on the bucket, which prevents any user, including the root user in your account, from deleting or modifying a locked object until it reaches its retention date.
To set a retention period of 2 years on the S3 bucket, you need to create a default retention configuration for the bucket that specifies a retention mode (either governance or compliance) and a retention period (either a number of days or a date). You can then set the bucket policy to allow the organization’s member accounts to write to the S3 bucket. This will ensure that all logs are retained in a secure storage location within the security account for 2 years and no changes or deletions are allowed.
Option A is incorrect because setting the bucket policy to allow the organization’s management account to write to the S3 bucket is not sufficient, as it will not grant access to the other member accounts in the organization.
Option C is incorrect because using an S3 Lifecycle configuration that expires objects after 2 years is not secure, as it will allow users to delete or modify objects before they expire.
Option E is incorrect because using Lambda and Kinesis Data Firehose to forward logs from one S3 bucket to another is not necessary, as CloudTrail can directly deliver logs to an S3 bucket in another account. It also introduces additional operational overhead and complexity.

**NEW QUESTION 6**
A company has several workloads running on AWS. Employees are required to authenticate using on-premises ADFS and SSO to access the AWS Management Console. Developers migrated an existing legacy web application to an Amazon EC2 instance. Employees need to access this application from anywhere on the internet, but currently, there is no authentication system built into the application.
How should the Security Engineer implement employee-only access to this system without changing the application?

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

**Answer:** A

**Explanation:**
https://docs.aws.amazon.com/elasticloadbalancing/latest/application/listener-authenticate-users.html

**NEW QUESTION 7**
A company is building an application on AWS that will store sensitive information. The company has a support team with access to the IT infrastructure, including databases. The company's security engineer must introduce measures to protect the sensitive data against any data breach while minimizing management overhead. The credentials must be regularly rotated.
What should the security engineer recommend?

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

Q. Set up TLS for the connection to the RDS hosted database.

**Answer:** C

**NEW QUESTION 8**
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:** ABC

**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

**NEW QUESTION 9**
A Security Engineer receives alerts that an Amazon EC2 instance on a public subnet is under an SFTP brute force attack from a specific IP address, which is a known malicious bot. What should the Security Engineer do to block the malicious bot?

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

**Answer:** D

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

**NEW QUESTION 10**
A security engineer must troubleshoot an administrator's inability to make an existing Amazon S3 bucket public in an account that is part of an organization n IAM Organizations. The administrator switched the role from the master account to a member account and then attempted to make one S3 bucket public. This action was immediately denied
Which actions should the security engineer take to troubleshoot the permissions issue? (Select TWO.)

A. Review the cross-account role permissions and the S3 bucket policy Verify that the Amazon S3 block public access option in the member account is deactivated.
B. Review the role permissions m the master account and ensure it has sufficient privileges to perform S3 operations
C. Filter IAM CloudTrail logs for the master account to find the original deny event and update the cross-account role m the member account accordingly Verify that the Amazon S3 block public access option in the master account is deactivated.
D. Evaluate the SCPs covering the member account and the permissions boundary of the role in the member account for missing permissions and explicit denies.
E. Ensure the S3 bucket policy explicitly allows the s3 PutBucketPublicAccess action for the role m the member account

**Answer:** DE

**Explanation:**

- A is incorrect because reviewing the cross-account role permissions and the S3 bucket policy is not enough to troubleshoot the permissions issue. You also need to verify that the Amazon S3 block public access option in the member account is deactivated, as well as the permissions boundary and the SCPs of the role in the member account.
- D is correct because evaluating the SCPs and the permissions boundary of the role in the member account can help you identify any missing permissions or explicit denies that could prevent the administrator from making the S3 bucket public.
- E is correct because ensuring that the S3 bucket policy explicitly allows the s3 PutBucketPublicAccess action for the role in the member account can help you override any block public access settings that could prevent the administrator from making the S3 bucket public.

**NEW QUESTION 10**
A security engineer needs to implement a write-once-read-many (WORM) model for data that a company will store in Amazon S3 buckets. The company uses the S3 Standard storage class for all of its S3 buckets. The security engineer must en-sure that objects cannot be overwritten or deleted by any user, including the AWS account root user.
Which solution will meet these requirements?

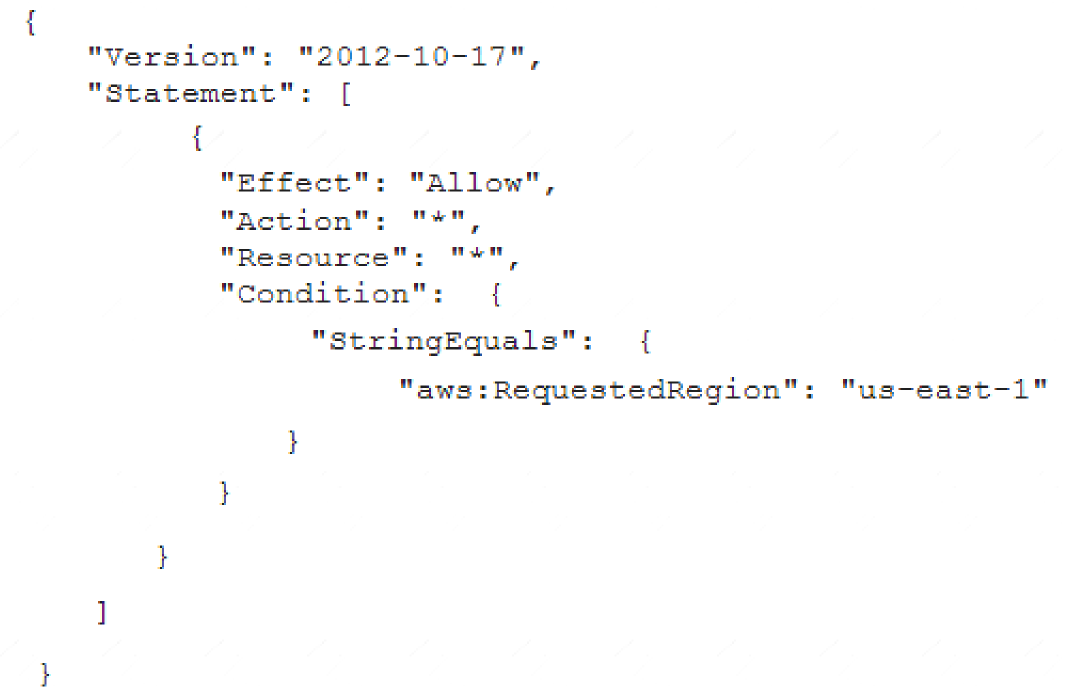
A. Create new S3 buckets with S3 Object Lock enabled in compliance mod
B. Place objects in the S3 buckets.
C. Use S3 Glacier Vault Lock to attach a Vault Lock policy to new S3 bucket
D. Wait 24 hours to complete the Vault Lock proces
E. Place objects in the S3 buckets.

F. Create new S3 buckets with S3 Object Lock enabled in governance mod
G. Place objects in the S3 buckets.
H. Create new S3 buckets with S3 Object Lock enabled in governance mod
I. Add a legal hold to the S3 bucket
J. Place objects in the S3 buckets.

**Answer:** A

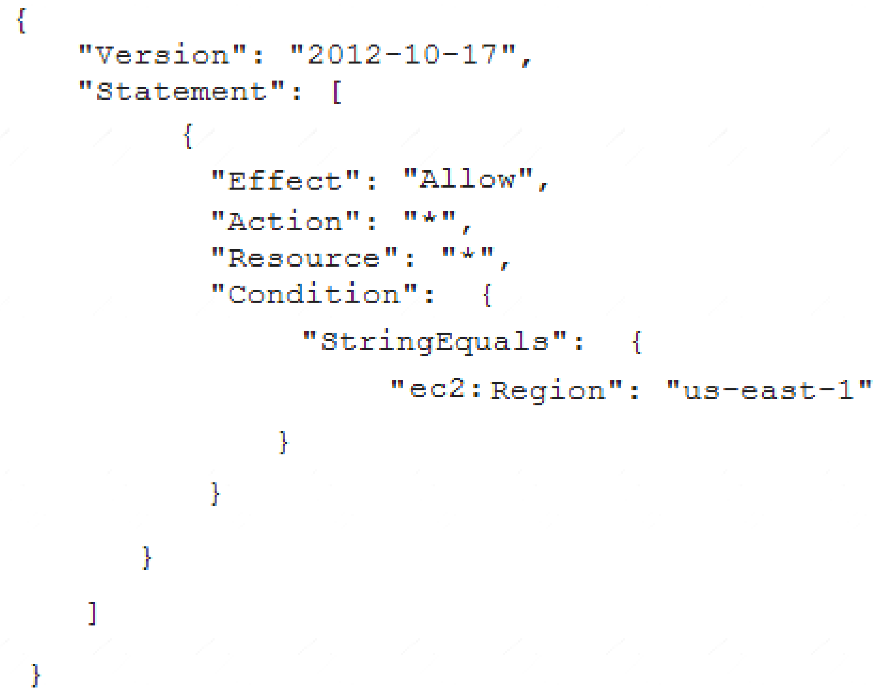
**NEW QUESTION 11**
To meet regulatory requirements, a Security Engineer needs to implement an IAM policy that restricts the use of AWS services to the us-east-1 Region.
What policy should the Engineer implement?

A.



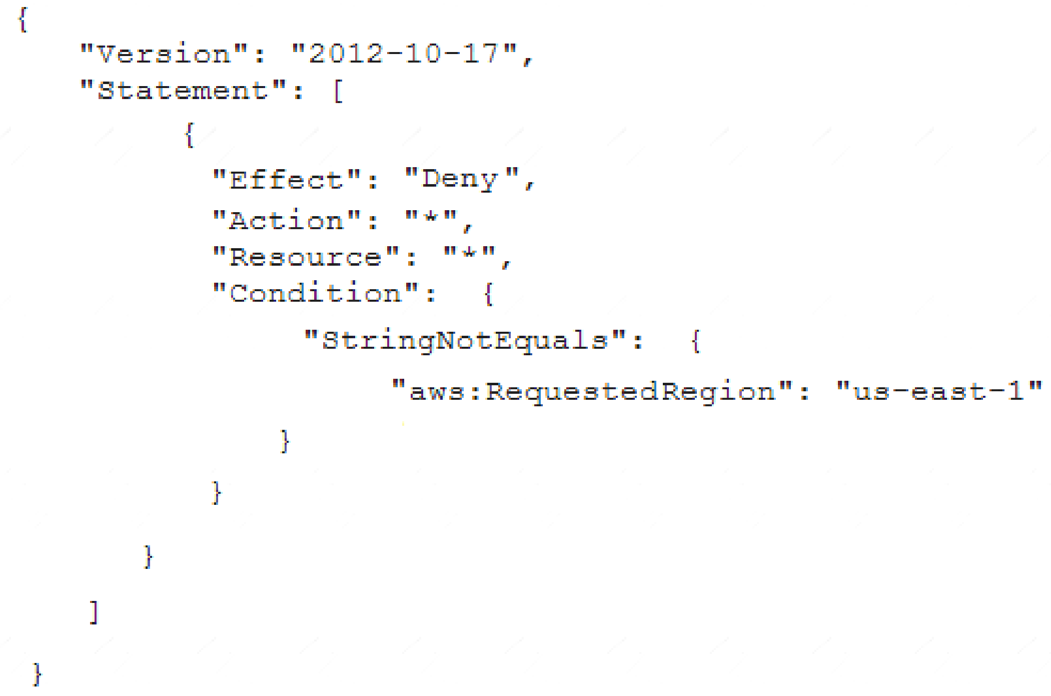
```
{
    "Version": "2012-10-17",
    "Statement": [
         {
          "Effect": "Allow",
          "Action": "*",
          "Resource": "*",
          "Condition":  {
               "StringEquals":  {
                    "aws:RequestedRegion": "us-east-1"
               }
          }
      }
  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

B. A computer code with black text Description automatically generated



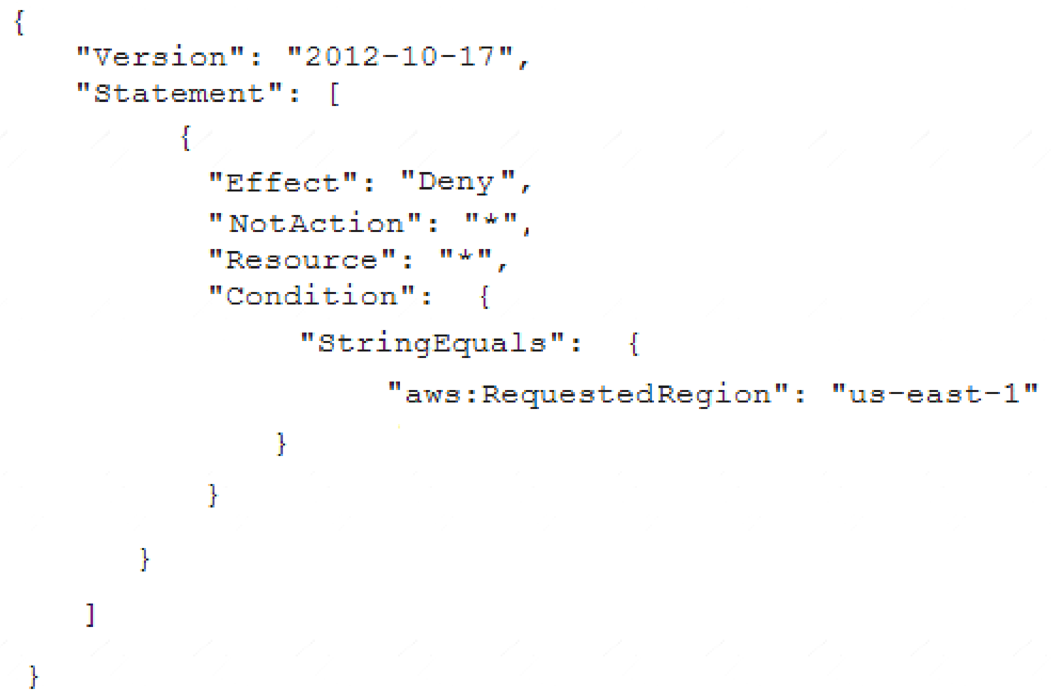
```
{
    "Version": "2012-10-17",
    "Statement": [
         {
          "Effect": "Allow",
          "Action": "*",
          "Resource": "*",
          "Condition":  {
               "StringEquals":  {
                    "ec2:Region":  "us-east-1"
               }
          }
      }
    ]
}
```

C. A computer code with black text Description automatically generated



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

D. A computer code with text Description automatically generated



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

**Answer:** C

**Explanation:**
https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_examples_aws_deny-requested-region.h

**NEW QUESTION 16**
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

**Answer:** C

**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.
References: : AWS Systems Manager Session Manager - AWS Systems Manager : AWS Systems Manage AWS Management Console : AWS Identity and Access Management - AWS Management Console : Am Elastic Compute Cloud - Amazon Web Services : Amazon Linux 2 - Amazon Web Services : AWS Syst Manager - AWS Management Console : AWS Systems Manager - AWS Management Console : AWS Systems Manager - AWS Management Console

**NEW QUESTION 21**
Your CTO thinks your IAM account was hacked. What is the only way to know for certain if there was unauthorized access and what they did, assuming your hackers are very sophisticated IAM engineers and doing everything they can to cover their tracks?
Please select:

A. Use CloudTrail Log File Integrity Validation.
B. Use IAM Config SNS Subscriptions and process events in real time.
C. Use CloudTrail backed up to IAM S3 and Glacier.
D. Use IAM Config Timeline forensics.

**Answer:** A

**Explanation:**
The IAM Documentation mentions the following
To determine whether a log file was modified, deleted, or unchanged after CloudTrail delivered it you can use CloudTrail log file integrity validation. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. You can use the IAM CLI to validate the files in the location where CloudTrail delivered them
Validated log files are invaluable in security and forensic investigations. For example, a validated log file enables you to assert positively that the log file itself has not changed, or that particular user credentials performed specific API activity. The CloudTrail log file integrity validation process also lets you know if a log file has been deleted or changed, or assert positively that no log files were delivered to your account during a given period of time.
Options B.C and D is invalid because you need to check for log File Integrity Validation for cloudtrail logs For more information on Cloudtrail log file validation, please visit the below URL: http://docs.IAM.amazon.com/IAMcloudtrail/latest/userguide/cloudtrail-log-file-validation-intro.html
The correct answer is: Use CloudTrail Log File Integrity Validation. omit your Feedback/Queries to our Expert

**NEW QUESTION 22**

A company uses AWS Organizations and has production workloads across multiple AWS accounts. A security engineer needs to design a solution that will proactively monitor for suspicious behavior across all the accounts that contain production workloads.
The solution must automate remediation of incidents across the production accounts. The solution also must publish a notification to an Amazon Simple Notification Service (Amazon SNS) topic when a critical security finding is detected. In addition, the solution must send all security incident logs to a dedicated account.
Which solution will meet these requirements?

A. Activate Amazon GuardDuty in each production accoun
B. In a dedicated logging accoun
C. aggregate all GuardDuty logs from each production accoun
D. Remediate incidents by configuring GuardDuty to directly invoke an AWS Lambda functio
E. Configure the Lambda function to also publish notifications to the SNS topic.
F. Activate AWS security Hub in each production accoun
G. In a dedicated logging accoun
H. aggregate all security Hub findings from each production accoun
I. Remediate incidents by ustng AWS Config and AWS Systems Manage
J. Configure Systems Manager to also pub11Sh notifications to the SNS topic.
K. Activate Amazon GuardDuty in each production accoun
L. In a dedicated logging accoun
M. aggregate all GuardDuty logs from each production account Remediate incidents by using Amazon EventBridge to invoke a custom AWS Lambda function from the GuardDuty finding
N. Configure the Lambda function to also publish notifications to the SNS topic.
O. Activate AWS Security Hub in each production accoun
P. In a dedicated logging accoun
Q. aggregate all Security Hub findings from each production accoun
R. Remediate incidents by using Amazon EventBridge to invoke a custom AWS Lambda function from the Security Hub finding
S. Configure the Lambda function to also publish notifications to the SNS topic.

**Answer:** D

**Explanation:**
The correct answer is D.
To design a solution that will proactively monitor for suspicious behavior across all the accounts that contain production workloads, the security engineer needs to use a service that can aggregate and analyze security findings from multiple sources. AWS Security Hub is a service that provides a comprehensive view of your security posture across your AWS accounts and enables you to check your environment against security standards and best practices. Security Hub also integrates with other AWS services, such as Amazon GuardDuty, AWS Config, and AWS Systems Manager, to collect and correlate security findings.
To automate remediation of incidents across the production accounts, the security engineer needs to use a service that can trigger actions based on events. Amazon EventBridge is a serverless event bus service that allows you to connect your applications with data from a variety of sources. EventBridge can use rules to match events and route them to targets for processing. You can use EventBridge to invoke a custom AWS Lambda function from the Security Hub findings. Lambda is a serverless compute service that lets you run code without provisioning or managing servers.
To publish a notification to an Amazon SNS topic when a critical security finding is detected, the security engineer needs to use a service that can send messages to subscribers. Amazon SNS is a fully managed messaging service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SNS can deliver messages to a variety of endpoints, such as email, SMS, or HTTP. You can configure the Lambda function to also publish notifications to the SNS topic.
To send all security incident logs to a dedicated account, the security engineer needs to use a service that can aggregate and store log data from multiple sources. AWS Security Hub allows you to aggregate security findings from multiple accounts into a single account using the delegated administrator feature. This feature enables you to designate an AWS account as the administrator for Security Hub in an organization. The administrator account can then view and manage Security Hub findings from all member accounts.
Therefore, option D is correct because it meets all the requirements of the solution. Option A is incorrect because GuardDuty does not provide a comprehensive view of your security posture across your AWS accounts. GuardDuty is primarily a threat detection service that monitors for malicious or unauthorized behavior. Option B is incorrect because Config and Systems Manager are not designed to automate remediation of incidents based on Security Hub findings. Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources, while Systems Manager is a service that allows you to manage your infrastructure on AWS at scale. Option C is incorrect because GuardDuty does not provide a comprehensive view of your security posture across your AWS accounts.
References:

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

**NEW QUESTION 24**
A security engineer must use AWS Key Management Service (AWS KMS) to design a key management solution for a set of Amazon Elastic Block Store (Amazon EBS) volumes that contain sensitive data. The solution needs to ensure that the key material automatically expires in 90 days.
Which solution meets these criteria?

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

**Answer:** A

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

The correct answer is A. A customer managed CMK that uses customer provided key material.
A customer managed CMK is a KMS key that you create, own, and manage in your AWS account. You have full control over the key configuration, permissions, rotation, and deletion. You can use a customer managed CMK to encrypt and decrypt data in AWS services that are integrated with AWS KMS, such as Amazon EBS1.
A customer managed CMK can use either AWS provided key material or customer provided key material. AWS provided key material is generated by AWS KMS and never leaves the service unencrypted. Customer provided key material is generated outside of AWS KMS and imported into a customer managed CMK. You can specify an expiration date for the imported key material, after which the CMK becomes unusable until you reimport new key material2.
To meet the criteria of automatically expiring the key material in 90 days, you need to use customer provided key material and set the expiration date accordingly. This way, you can ensure that the data encrypted with the CMK will not be accessible after 90 days unless you reimport new key material and re-encrypt the data.
The other options are incorrect for the following reasons:
* B. A customer managed CMK that uses AWS provided key material does not expire automatically. You can enable automatic rotation of the key material every year, but this does not prevent access to the data encrypted with the previous key material. You would need to manually delete the CMK and its backing key material to make the data inaccessible3.
* C. An AWS managed CMK is a KMS key that is created, owned, and managed by an AWS service on your behalf. You have limited control over the key configuration, permissions, rotation, and deletion. You cannot use an AWS managed CMK to encrypt data in other AWS services or applications. You also cannot set an expiration date for the key material of an AWS managed CMK4.
* D. Operation system-native encryption that uses GnuPG is not a solution that uses AWS KMS. GnuPG is a command line tool that implements the OpenPGP standard for encrypting and signing data. It does not integrate with Amazon EBS or other AWS services. It also does not provide a way to automatically expire the key material used for encryption5.
References:
1: Customer Managed Keys - AWS Key Management Service 2: [Importing Key Material in AWS Key Management Service (AWS KMS) - AWS Key Management Service] 3: [Rotating Customer Master Keys - AWS Key Management Service] 4: [AWS Managed Keys - AWS Key Management Service] 5: The GNU Privacy Guard

**NEW QUESTION 27**
A company purchased a subscription to a third-party cloud security scanning solution that integrates with AWS Security Hub. A security engineer needs to implement a solution that will remediate the findings
from the third-party scanning solution automatically. Which solution will meet this requirement?

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

**Answer:** A

**NEW QUESTION 29**
A company deploys a distributed web application on a fleet of Amazon EC2 instances. The fleet is behind an Application Load Balancer (ALB) that will be configured to terminate the TLS connection. All TLS traffic to the ALB must stay secure, even if the certificate private key is compromised.
How can a security engineer meet this requirement?

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

**Answer:** A

**NEW QUESTION 34**
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:** BD

**NEW QUESTION 36**
A company is using IAM Secrets Manager to store secrets for its production Amazon RDS database. The Security Officer has asked that secrets be rotated every 3 months. Which solution would allow the company to securely rotate the secrets? (Select TWO.)

A. Place the RDS instance in a public subnet and an IAM Lambda function outside the VP
B. Schedule the Lambda function to run every 3 months to rotate the secrets.
C. Place the RDS instance in a private subnet and an IAM Lambda function inside the VPC in the private subne
D. Configure the private subnet to use a NAT gatewa
E. Schedule the Lambda function to run every 3 months to rotate the secrets.
F. Place the RDS instance in a private subnet and an IAM Lambda function outside the VP
G. Configure the private subnet to use an internet gatewa
H. Schedule the Lambda function to run every 3 months lo rotate the secrets.
I. Place the RDS instance in a private subnet and an IAM Lambda function inside the VPC in the private subne
J. Schedule the Lambda function to run quarterly to rotate the secrets.
K. Place the RDS instance in a private subnet and an IAM Lambda function inside the VPC in the private subne

L. Configure a Secrets Manager interface endpoin
M. Schedule the Lambda function to run every 3 months to rotate the secrets.

**Answer:** BE

**Explanation:**
these are the solutions that can securely rotate the secrets for the production RDS database using Secrets Manager. Secrets Manager is a service that helps you manage secrets such as database credentials, API keys, and passwords. You can use Secrets Manager to rotate secrets automatically by using a Lambda function that runs on a schedule. The Lambda function needs to have access to both the RDS instance and the Secrets Manager service. Option B places the RDS instance in a private subnet and the Lambda function in the same VPC in another private subnet. The private subnet with the Lambda function needs to use a NAT gateway to access Secrets Manager over the internet. Option E places the RDS instance and the Lambda function in the same private subnet and configures a Secrets Manager interface endpoint, which is a private connection between the VPC and Secrets Manager. The other options are either insecure or incorrect for rotating secrets using Secrets Manager.

**NEW QUESTION 41**
A company's public Application Load Balancer (ALB) recently experienced a DDoS attack. To mitigate this issue. the company deployed Amazon CloudFront in front of the ALB so that users would not directly access the Amazon EC2 instances behind the ALB.
The company discovers that some traffic is still coming directly into the ALB and is still being handled by the EC2 instances.
Which combination of steps should the company take to ensure that the EC2 instances will receive traffic only from CloudFront? (Choose two.)

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

**Answer:** BC

**Explanation:**
To prevent users from directly accessing an Application Load Balancer and allow access only through CloudFront, complete these high-level steps: Configure CloudFront to add a custom HTTP header to requests that it sends to the Application Load Balancer. Configure the Application Load Balancer to only forward requests that contain the custom HTTP header. (Optional) Require HTTPS to improve the security of this solution.
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/restrict-access-to-load-balancer.html

**NEW QUESTION 45**
The Security Engineer is managing a traditional three-tier web application that is running on Amazon EC2 instances. The application has become the target of increasing numbers of malicious attacks from the Internet.
What steps should the Security Engineer take to check for known vulnerabilities and limit the attack surface? (Choose two.)

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

**Answer:** BD

**Explanation:**
The steps that the Security Engineer should take to check for known vulnerabilities and limit the attack surface are:
➢ B. Review the application security groups to ensure that only the necessary ports are open. This is a good practice to reduce the exposure of the EC2 instances to potential attacks from the Internet. Application security groups are a feature of Azure that allow you to group virtual machines and define network security policies based on those groups1.
➢ D. Use Amazon Inspector to periodically scan the backend instances. This is a service that helps you to identify vulnerabilities and exposures in your EC2 instances and applications. Amazon Inspector can perform automated security assessments based on predefined or custom rules packages2.

**NEW QUESTION 46**
A company's Security Team received an email notification from the Amazon EC2 Abuse team that one or more of the company's Amazon EC2 instances may have been compromised
Which combination of actions should the Security team take to respond to (be current modem? (Select TWO.)

A. Open a support case with the IAM Security team and ask them to remove the malicious code from the affected instance
B. Respond to the notification and list the actions that have been taken to address the incident
C. Delete all IAM users and resources in the account
D. Detach the internet gateway from the VPC remove aft rules that contain 0.0.0.0V0 from the security groups, and create a NACL rule to deny all traffic Inbound from the internet
E. Delete the identified compromised instances and delete any associated resources that the Security team did not create.

**Answer:** DE

**Explanation:**
these are the recommended actions to take when you receive an abuse notice from AWS8. You should review the abuse notice to see what content or activity was reported and detach the internet gateway from the VPC to isolate the affected instances from the internet. You should also remove any rules that allow inbound traffic from 0.0.0.0/0 from the security groups and create a network access control list (NACL) rule to deny all traffic inbound from the internet. You should then delete the compromised instances and any associated resources
that you did not create. The other options are either inappropriate or unnecessary for responding to the abuse notice.

**NEW QUESTION 48**
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

**Answer:** CD

**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.

**NEW QUESTION 50**
A security engineer is working with a company to design an ecommerce application. The application will run on Amazon EC2 instances that run in an Auto Scaling group behind an Application Load Balancer (ALB). The application will use an Amazon RDS DB instance for its database.
The only required connectivity from the internet is for HTTP and HTTPS traffic to the application. The application must communicate with an external payment provider that allows traffic only from a preconfigured allow list of IP addresses. The company must ensure that communications with the external payment provider are not interrupted as the environment scales.
Which combination of actions should the security engineer recommend to meet these requirements? (Select THREE.)

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

**Answer:** ACE

**NEW QUESTION 54**
A company’s security team needs to receive a notification whenever an AWS access key has not been rotated in 90 or more days. A security engineer must develop a solution that provides these notifications automatically.
Which solution will meet these requirements with the LEAST amount of effort?

A. Deploy an AWS Config managed rule to run on a periodic basis of 24 hour
B. Select theaccess-keys-rotated managed rule, and set the maxAccessKeyAge parameter to 90 day
C. Create an Amazon EventBridge (Amazon CloudWatch Events) rule with an event pattern that matches the compliance type of NON_COMPLIANT from AWS Config for the managed rul
D. Configure EventBridge (CloudWatch Events) to send an Amazon Simple Notification Service (Amazon SNS) notification to the security team.
E. Create a script to export a .csv file from the AWS Trusted Advisor check for IAM access key rotation.Load the script into an AWS Lambda function that will upload the .csv file to an Amazon S3 bucke
F. Create an Amazon Athena table query that runs when the .csv file is uploaded to the S3 bucke
G. Publish the results for any keys older than 90 days by using an invocation of an Amazon Simple Notification Service (Amazon SNS) notification to the security team.
H. Create a script to download the IAM credentials report on a periodic basi
I. Load the script into an AWS Lambda function that will run on a schedule through Amazon EventBridge (Amazon CloudWatch Events). Configure the Lambda script to load the report into memory and to filter the report for recordsin which the key was last rotated at least 90 days ag
J. If any records are detected, send an Amazon Simple Notification Service (Amazon SNS) notification to the security team.
K. Create an AWS Lambda function that queries the IAM API to list all the user
L. Iterate through the users by using the ListAccessKeys operatio
M. Verify that the value in the CreateDate field is not at least 90 days ol
N. Send an Amazon Simple Notification Service (Amazon SNS) notification to the security team if the value is at least 90 days ol
O. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to schedule the Lambda function to run each day.

**Answer:** A

**NEW QUESTION 58**
You need to create a policy and apply it for just an individual user. How could you accomplish this in the right way?
Please select:

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

**Answer:** D

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

The IAM Documentation mentions the following
An inline policy is a policy that's embedded in a principal entity (a user, group, or role)—that is, the policy is an inherent part of the principal entity. You can create a policy and embed it in a principal entity, either when you create the principal entity or later.
For more information on IAM Access and Inline policies, just browse to the below URL: https://docs.IAM.amazon.com/IAM/latest/UserGuide/access
The correct answer is: Add an inline policy for the user Submit your Feedback/Queries to our Experts

**NEW QUESTION 60**
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 Regio
E. Attach the SCP to the AWS account in AWS Organizations.

**Answer:** D

**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.htm

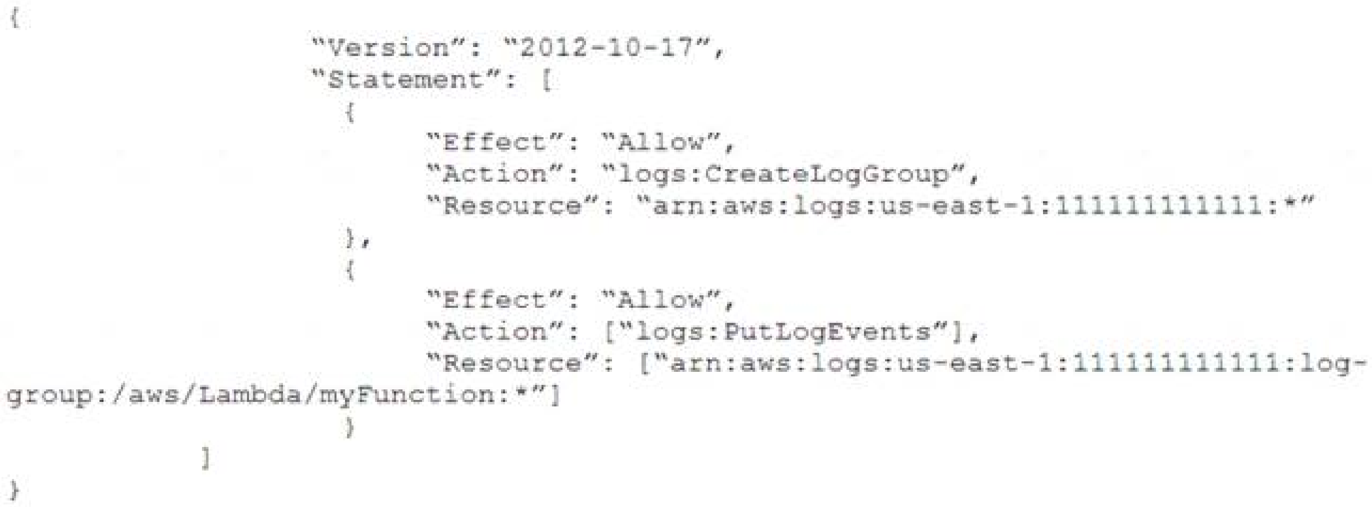
**NEW QUESTION 62**
An international company has established a new business entity in South Korea. The company also has established a new AWS account to contain the workload for the South Korean region. The company has set up the workload in the new account in the ap-northeast-2 Region. The workload consists of three Auto Scaling groups of Amazon EC2 instances. All workloads that operate in this Region must keep system logs and application logs for 7 years.
A security engineer must implement a solution to ensure that no logging data is lost for each instance during scaling activities. The solution also must keep the logs for only the required period of 7 years.
Which combination of steps should the security engineer take to meet these requirements? (Choose three.)

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

**Answer:** ABC

**Explanation:**
The correct combination of steps that the security engineer should take to meet these requirements are A. Ensure that the Amazon CloudWatch agent is installed on all the EC2 instances that the Auto Scaling groups launch. Generate a CloudWatch agent configuration file to forward the required logs to Amazon CloudWatch Logs., B. Set the log retention for desired log groups to 7 years., and C. Attach an IAM role to the launch configuration or launch template that the Auto Scaling groups use. Configure the role to provide the necessary permissions to forward logs to Amazon CloudWatch Logs.
* A. This answer is correct because it meets the requirement of ensuring that no logging data is lost for each instance during scaling activities. By installing the CloudWatch agent on all the EC2 instances, the security engineer can collect and send system logs and application logs to CloudWatch Logs, which is a service that stores and monitors log data. By generating a CloudWatch agent configuration file, the security engineer can specify which logs to forward and how often.
* B. This answer is correct because it meets the requirement of keeping the logs for only the required period of 7 years. By setting the log retention for desired log groups, the security engineer can control how long
CloudWatch Logs retains log events before deleting them. The security engineer can choose a predefined retention period of 7 years, or use a custom value.
* C. This answer is correct because it meets the requirement of providing the necessary permissions to forward logs to CloudWatch Logs. By attaching an IAM role to the launch configuration or launch template that the Auto Scaling groups use, the security engineer can grant permissions to the EC2 instances that are launched by the Auto Scaling groups. By configuring the role to provide the necessary permissions, such as cloudwatch:PutLogEvents and cloudwatch:CreateLogStream, the security engineer can allow the EC2 instances to send log data to CloudWatch Logs.

**NEW QUESTION 63**
A security engineer logs in to the AWS Lambda console with administrator permissions. The security engineer is trying to view logs in Amazon CloudWatch for a Lambda function that is named my Function.
When the security engineer chooses the option in the Lambda console to view logs in CloudWatch, an “error loading Log Streams" message appears.
The IAM policy for the Lambda function's execution role contains the following:



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

How should the security engineer correct the error?

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

**Answer:** D

**Explanation:**
CloudWatchLogsReadOnlyAccess doesn't include "logs:CreateLogStream" but it includes "logs:Get*"
https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/iam-identity-based-access-control-cwl.html#:~:te

**NEW QUESTION 67**
An organization wants to log all IAM API calls made within all of its IAM accounts, and must have a central place to analyze these logs. What steps should be taken to meet these requirements in the MOST secure manner? (Select TWO)

A. Turn on IAM CloudTrail in each IAM account
B. Turn on CloudTrail in only the account that will be storing the logs
C. Update the bucket ACL of the bucket in the account that will be storing the logs so that other accounts can log to it
D. Create a service-based role for CloudTrail and associate it with CloudTrail in each account
E. Update the bucket policy of the bucket in the account that will be storing the logs so that other accounts can log to it

**Answer:** AE

**Explanation:**
these are the steps that can meet the requirements in the most secure manner. CloudTrail is a service that records AWS API calls and delivers log files to an S3 bucket. Turning on CloudTrail in each IAM account can help capture all IAM API calls made within those accounts. Updating the bucket policy of the bucket in the account that will be storing the logs can help grant other accounts permission to write log files to that bucket. The other options are either unnecessary or insecure for logging and analyzing IAM API calls.

**NEW QUESTION 72**
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 accoun
B. Grant the appropriate permissions to the resources that are neede
C. Share the password only with the users that need access.
D. Create cross-account access with an IAM role in the developer accoun
E. Grant the appropriate permissions to this rol
F. Allow users in the developer account to assume this role to access the production resources.
G. Create cross-account access with an IAM user account in the production accoun
H. Grant the appropriate permissions to this user accoun
I. Allow users in the developer account to use this user account to access the production resources.
J. Create cross-account access with an IAM role in the production accoun
K. Grant the appropriate permissions to this rol
L. Allow users in the developer account to assume this role to access the production resources.

**Answer:** D

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

**NEW QUESTION 74**
A company has deployed Amazon GuardDuty and now wants to implement automation for potential threats. The company has decided to start with RDP brute force attacks that come from Amazon EC2 instances in the company's AWS environment. A security engineer needs to implement a solution that blocks the detected communication from a suspicious instance until investigation and potential remediation can occur.
Which solution will meet these requirements?

A. Configure GuardDuty to send the event to an Amazon Kinesis data strea
B. Process the event with an Amazon Kinesis Data Analytics for Apache Flink application that sends a notification to the company through Amazon Simple Notification Service (Amazon SNS). Add rules to the network ACL to block traffic to and from the suspicious instance.
C. Configure GuardDuty to send the event to Amazon EventBridge (Amazon CloudWatch Events). Deploy an AWS WAF web AC
D. Process the event with an AWS Lambda function that sends a notification to the company through Amazon Simple Notification Service (Amazon SNS) and adds a web ACL rule to block traffic to and from the suspicious instance.

E. Enable AWS Security Hub to ingest GuardDuty findings and send the event to Amazon EventBridge (Amazon CloudWatch Events). Deploy AWS Network Firewal
F. Process the event with an AWS Lambda function that adds a rule to a Network Firewall firewall policy to block traffic to and from the suspicious instance.
G. Enable AWS Security Hub to ingest GuardDuty finding
H. Configure an Amazon Kinesis data stream as an event destination for Security Hu
I. Process the event with an AWS Lambda function that replaces the security group of the suspicious instance with a security group that does not allow any connections.

**Answer:** C

**Explanation:**
https://aws.amazon.com/blogs/security/automatically-block-suspicious-traffic-with-aws-network-firewall-and-a

**NEW QUESTION 76**
A company is developing an ecommerce application. The application uses Amazon EC2 instances and an Amazon RDS MySQL database. For compliance reasons, data must be secured in transit and at rest. The company needs a solution that minimizes operational overhead and minimizes cost.
Which solution meets these requirements?

A. Use TLS certificates from AWS Certificate Manager (ACM) with an Application Load Balancer.Deploy self-signed certificates on the EC2 instance
B. Ensure that the database client software uses a TLS connection to Amazon RD
C. Enable encryption of the RDS DB instanc
D. Enable encryption on the Amazon Elastic Block Store (Amazon EBS) volumes that support the EC2 instances.
E. Use TLS certificates from a third-party vendor with an Application Load Balance
F. Install the same certificates on the EC2 instance
G. Ensure that the database client software uses a TLS connection to Amazon RD
H. Use AWS Secrets Manager for client-side encryption of application data.
I. Use AWS CloudHSM to generate TLS certificates for the EC2 instance
J. Install the TLS certificates on the EC2 instance
K. Ensure that the database client software uses a TLS connection to Amazon RD
L. Use the encryption keys form CloudHSM for client-side encryption of application data.
M. Use Amazon CloudFront with AWS WA
N. Send HTTP connections to the origin EC2 instance
O. Ensure that the database client software uses a TLS connection to Amazon RD
P. Use AWS Key Management Service (AWS KMS) for client-side encryption of application data before the data is stored in the RDS database.

**Answer:** A

**NEW QUESTION 77**
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 finding
B. Use Amazon Simple Notification Service (Amazon SNS) to send the email alert
C. Create an Amazon EventBridge rule to invoke the functions on a schedule.
D. Create an Amazon EventBridge rule with a pattern that matches Security Hub findings events with high severit
E. Configure the rule to send the findings to a target Amazon Simple Notification Service (Amazon SNS) topi
F. Subscribe the desired email addresses to the SNS topic.
G. Create an Amazon EventBridge rule with a pattern that matches AWS Control Tower events with high severit
H. Configure the rule to send the findings to a target Amazon Simple Notification Service (Amazon SNS) topi
I. Subscribe the desired email addresses to the SNS topic.
J. 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 topi
K. Subscribe the desired email addresses to the SNS topic.

**Answer:** B

**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.
References: : AWS Security Hub User Guide

**NEW QUESTION 82**
A company's Security Engineer has been tasked with restricting a contractor's IAM account access to the company's Amazon EC2 console without providing access to any other AWS services. The contractor's IAM account must not be able to gain access to any other AWS service, even if the IAM account is assigned additional permissions based on IAM group membership.
What should the Security Engineer do to meet these requirements?

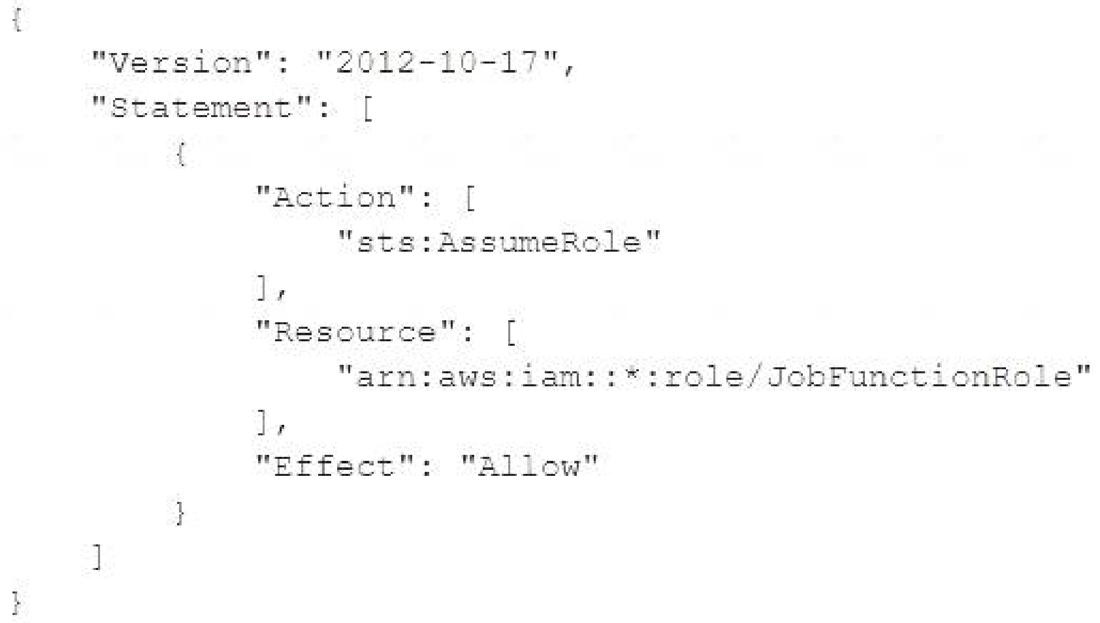
A. Create an Inline IAM user policy that allows for Amazon EC2 access for the contractor's IAM user.
B. Create an IAM permissions boundary policy that allows Amazon EC2 acces
C. Associate the contractor's IAM account with the IAM permissions boundary policy.
D. Create an IAM group with an attached policy that allows for Amazon EC2 acces
E. Associate the contractor's IAM account with the IAM group.
F. Create an IAM role that allows for EC2 and explicitly denies all other service
G. Instruct the contractor to always assume this role.

**Answer:** B

**NEW QUESTION 84**

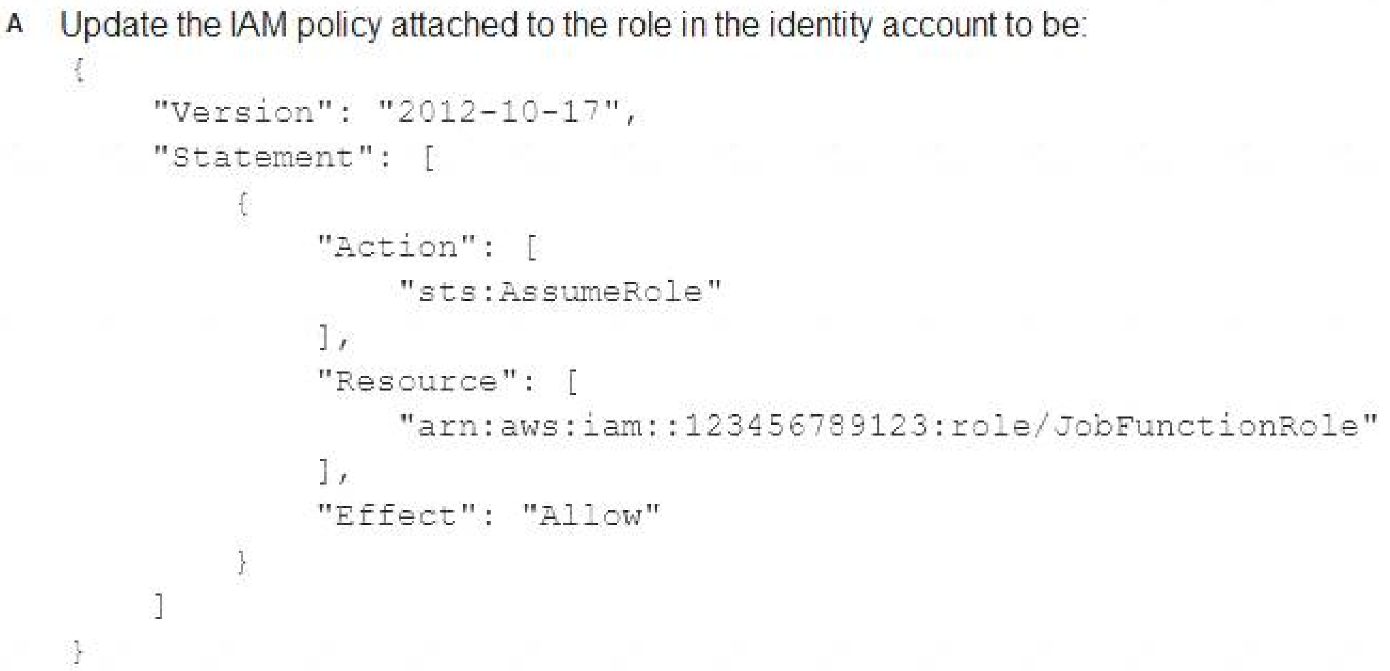
A company uses identity federation to authenticate users into an identity account (987654321987) where the users assume an IAM role named IdentityRole. The users then assume an IAM role named JobFunctionRole in the target IAM account (123456789123) to perform their job functions.

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



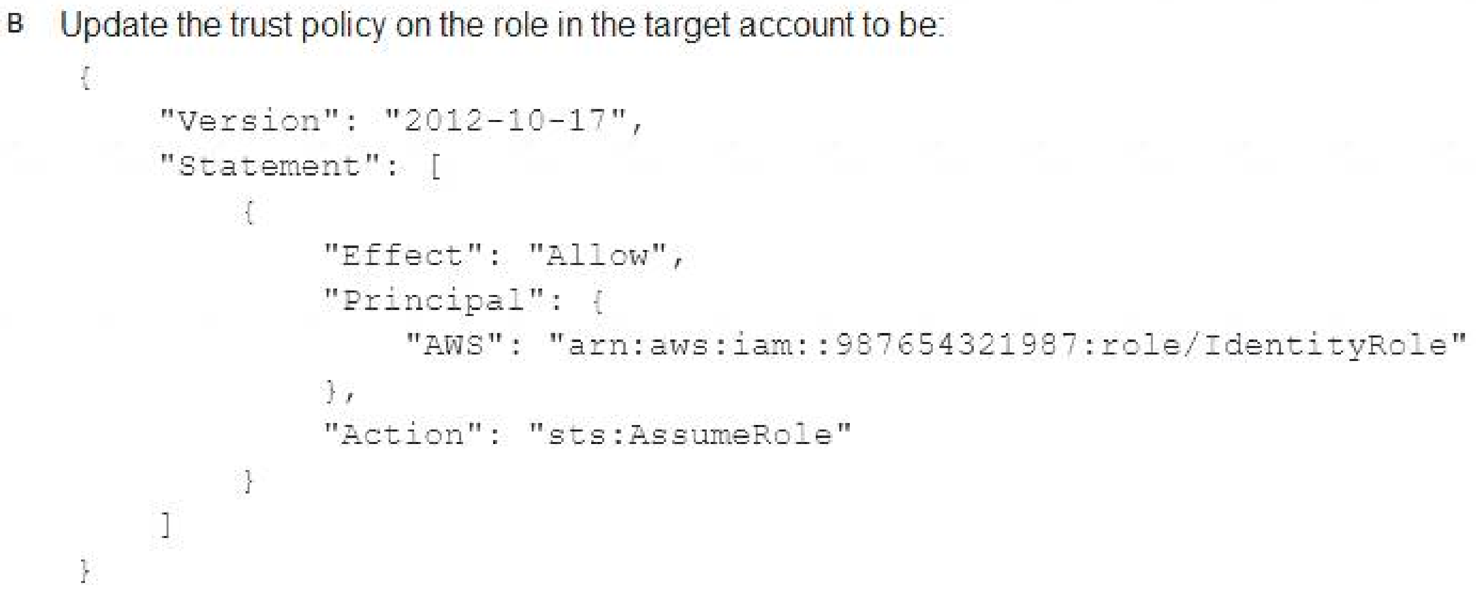
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/JobFunctionRole"
            ],
            "Effect": "Allow"
        }
    ]
}
```

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



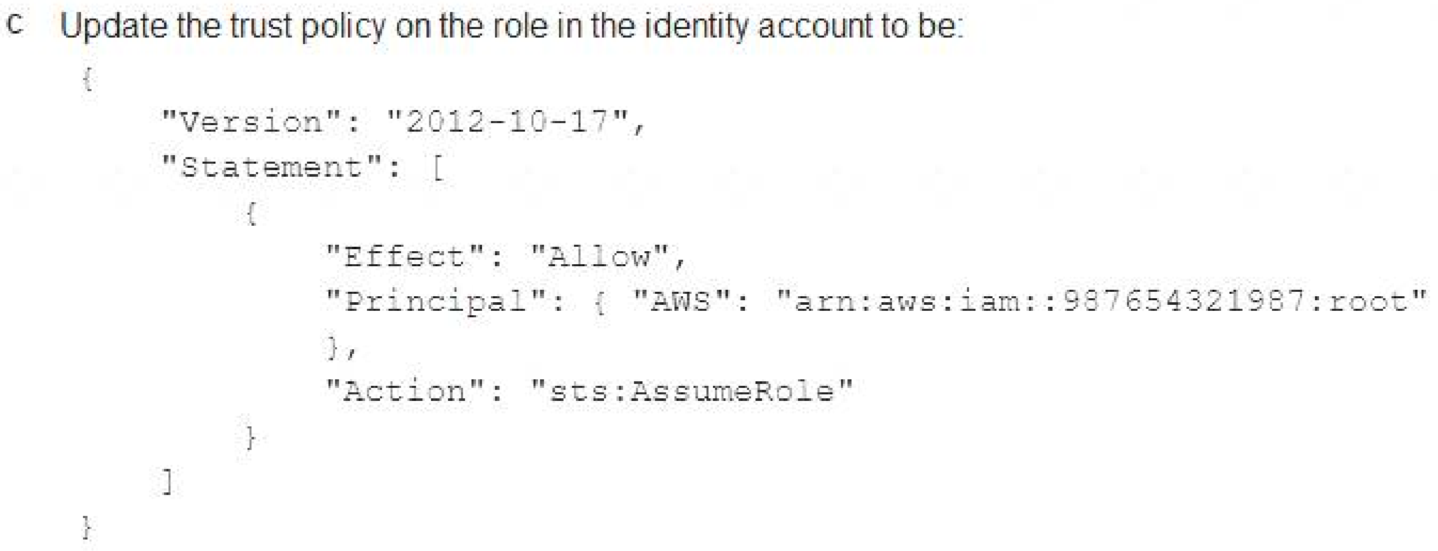
A Update the IAM policy attached to the role in the identity account to be:

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



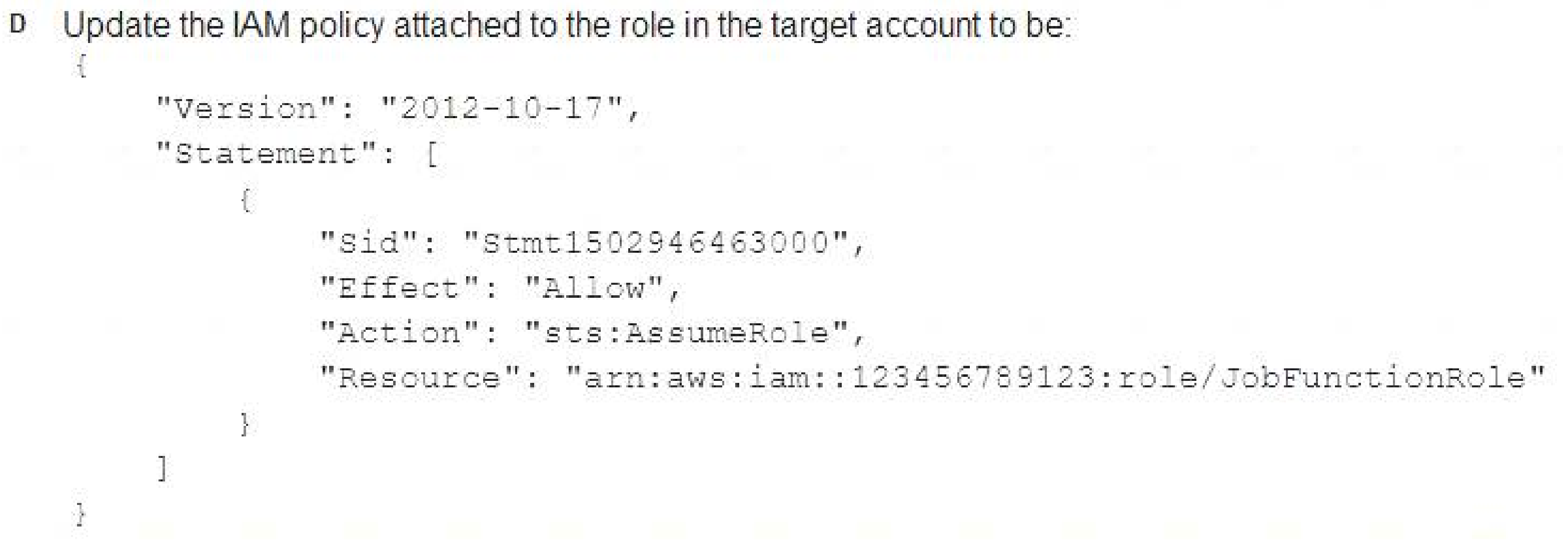
B Update the trust policy on the role in the target account to be:

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



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

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



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

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

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

**Answer:** B

**Explanation:**
https://aws.amazon.com/blogs/security/how-to-use-trust-policies-with-iam-roles/

**NEW QUESTION 86**
A company's security engineer has been tasked with restricting a contractor's IAM account access to the company's Amazon EC2 console without providing access to any other IAM services The contractors IAM account must not be able to gain access to any other IAM service, even it the IAM account rs assigned additional permissions based on IAM group membership
What should the security engineer do to meet these requirements"

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

**Answer:** B

**Explanation:**
To restrict the contractor’s IAM account access to the EC2 console without providing access to any other AWS services, the security engineer should do the following:

- Create an IAM permissions boundary policy that allows EC2 access. This is a policy that defines the maximum permissions that an IAM entity can have.
- Associate the contractor’s IAM account with the IAM permissions boundary policy. This means that even if the contractor’s IAM account is assigned additional permissions based on IAM group membership, those permissions are limited by the permissions boundary policy.

**NEW QUESTION 87**
A website currently runs on Amazon EC2, wan mostly statics content on the site. Recently the site was subjected to a DDoS attack a security engineer was (asked was redesigning the edge security to help
Mitigate this risk in the future.
What are some ways the engineer could achieve this (Select THREE)?

A. Use IAM X-Ray to inspect the trafc going to the EC2 instances.
B. Move the static content to Amazon S3, and front this with an Amazon Cloud Front distribution.
C. Change the security group conguration to block the source of the attack trafc
D. Use IAM WAF security rules to inspect the inbound trafc.
E. Use Amazon Inspector assessment templates to inspect the inbound traffic.
F. Use Amazon Route 53 to distribute trafc.

**Answer:** BDF

**Explanation:**
To redesign the edge security to help mitigate the DDoS attack risk in the future, the engineer could do the following:

- Move the static content to Amazon S3, and front this with an Amazon CloudFront distribution. This allows the engineer to use a global content delivery network that can cache static content at edge locations and reduce the load on the origin servers.
- Use AWS WAF security rules to inspect the inbound traffic. This allows the engineer to use web application firewall rules that can filter malicious requests based on IP addresses, headers, body, or URI strings, and block them before they reach the web servers.
- Use Amazon Route 53 to distribute traffic. This allows the engineer to use a scalable and highly available DNS service that can route traffic based on different policies, such as latency, geolocation, or health checks.

**NEW QUESTION 91**
A security engineer is configuring a new website that is named example.com. The security engineer wants to secure communications with the website by requiring users to connect to example.com through HTTPS.
Which of the following is a valid option for storing SSL/TLS certificates?

A. Custom SSL certificate that is stored in AWS Key Management Service (AWS KMS)

B. Default SSL certificate that is stored in Amazon CloudFront.
C. Custom SSL certificate that is stored in AWS Certificate Manager (ACM)
D. Default SSL certificate that is stored in Amazon S3

**Answer:** C

**NEW QUESTION 96**
A company has contracted with a third party to audit several AWS accounts. To enable the audit, cross- account IAM roles have been created in each account targeted for audit. The Auditor is having trouble accessing some of the accounts.
Which of the following may be causing this problem? (Choose three.)

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

**Answer:** ACF

**Explanation:**
The following may be causing the problem for the Auditor:

- A. The external ID used by the Auditor is missing or incorrect. This is a possible cause, because the external ID is a unique identifier that is used to establish a trust relationship between the accounts. The external ID must match the one that is specified in the role’s trust policy in the destination account1.
- C. The Auditor has not been granted sts:AssumeRole for the role in the destination account. This is a possible cause, because sts:AssumeRole is the API action that allows the Auditor to assume the
cross-account role and obtain temporary credentials. The Auditor must have an IAM policy that allows them to call sts:AssumeRole for the role ARN in the destination account2.
- F. The role ARN used by the Auditor is missing or incorrect. This is a possible cause, because the role ARN is the Amazon Resource Name of the cross-account role that the Auditor wants to assume. The role ARN must be valid and exist in the destination account3.

**NEW QUESTION 99**
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 role
C. Remove all permissions that grant access to Signer.
D. Re-encrypt all source code with a new AWS Key Management Service (AWS KMS) key.
E. 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

**NEW QUESTION 104**
Your company uses IAM to host its resources. They have the following requirements
1) Record all API calls and Transitions
2) Help in understanding what resources are there in the account

3) Facility to allow auditing credentials and logins
Which services would suffice the above requirements Please select:

A. IAM Inspector, CloudTrail, IAM Credential Reports
B. CloudTrai
C. IAM Credential Reports, IAM SNS
D. CloudTrail, IAM Config, IAM Credential Reports
E. IAM SQS, IAM Credential Reports, CloudTrail

**Answer:** C

**Explanation:**
You can use IAM CloudTrail to get a history of IAM API calls and related events for your account. This history includes calls made with the IAM Management Console, IAM Command Line Interface, IAM SDKs, and other IAM services.
Options A,B and D are invalid because you need to ensure that you use the services of CloudTrail, IAM Config, IAM Credential Reports
For more information on Cloudtrail, please visit the below URL:
http://docs.IAM.amazon.com/IAMcloudtrail/latest/userguide/cloudtrail-user-guide.html
IAM Config is a service that enables you to assess, audit and evaluate the configurations of your IAM resources. Config continuously monitors and records your IAM resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. With Config, you can review changes in configurations and relationships between IAM resources, dive into detailed resource configuration histories, and determine your overall compliance against the configurations specified in your internal guidelines. This enables you to simplify compliance auditing, security analysis, char management and operational troubleshooting.
For more information on the config service, please visit the below URL https://IAM.amazon.com/config/
You can generate and download a credential report that lists all users in your account and the status of their various credentials, including passwords, access keys, and MFA devices. You can get a credential report from the IAM Management Console, the IAM SDKs and Command Line Tools, or the IAM API.
For more information on Credentials Report, please visit the below URL: http://docs.IAM.amazon.com/IAM/latest/UserGuide/id credentials_getting-report.html
The correct answer is: CloudTrail, IAM Config, IAM Credential Reports Submit your Feedback/Queries to our Experts

**NEW QUESTION 109**
You work at a company that makes use of IAM resources. One of the key security policies is to ensure that all data i encrypted both at rest and in transit. Which of the following is one of the right ways to implement this.
Please select:

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

**Answer:** A

**Explanation:**
By disabling SSL termination, you are leaving an unsecure connection from the ELB to the back end instances. Hence this means that part of the data transit is not being encrypted.
Option B is incorrect because this would not guarantee complete encryption of data in transit Option C and D are incorrect because these would not guarantee encryption
For more information on SSL Listeners for your load balancer, please visit the below URL: http://docs.IAM.amazon.com/elasticloadbalancine/latest/classic/elb-https-load-balancers.htmll The correct answer is: Use S3 SSE and use SSL for data in transit
Submit your Feedback/Queries to our Experts

**NEW QUESTION 114**
A company has an AWS account that hosts a production application. The company receives an email notification that Amazon GuardDuty has detected an Impact:IAMUser/AnomalousBehavior finding in the account. A security engineer needs to run the investigation playbook for this security incident and must collect and analyze the information without affecting the application.
Which solution will meet these requirements MOST quickly?

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

**Answer:** B

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

**NEW QUESTION 117**
A company is using Amazon Elastic Container Service (Amazon ECS) to run its container-based application on AWS. The company needs to ensure that the container images contain no severe vulnerabilities. The company also must ensure that only specific IAM roles and specific AWS accounts can access the container images.

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

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

**Answer:** C

**Explanation:**
The correct answer is C. Pull images from the public container registry. Publish the images to Amazon Elastic Container Registry (Amazon ECR) repositories with scan on push configured in a centralized AWS account.
Use a CI/CD pipeline to deploy the images to different AWS accounts. Use repository policies and identity-based policies to restrict access to which IAM principals and accounts can access the images.
This solution meets the requirements because:

- Amazon ECR is a fully managed container registry service that supports Docker and OCI images and artifacts1. It integrates with Amazon ECS and other AWS services to simplify the development and deployment of container-based applications.
- Amazon ECR provides image scanning on push, which uses the Common Vulnerabilities and Exposures (CVEs) database from the open-source Clair project to detect software vulnerabilities in container images2. The scan results are available in the AWS Management Console, AWS CLI, or AWS SDKs2.
- Amazon ECR supports cross-account access to repositories, which allows sharing images across multiple AWS accounts3. This can be achieved by using repository policies, which are resource-based policies that specify which IAM principals and accounts can access the repositories and what actions they can perform4. Additionally, identity-based policies can be used to control which IAM roles in each account can access the repositories5.

The other options are incorrect because:

- A. This option does not use repository policies to restrict cross-account access to the images, which is a requirement. Identity-based policies alone are not sufficient to control access to Amazon ECR repositories5.
- B. This option does not use Amazon ECR, which is a fully managed service that provides image scanning and cross-account access features. Hosting a private container registry on EC2 instances would require more management overhead and additional security measures.
- D. This option uses AWS CodeArtifact, which is a fully managed artifact repository service that supports Maven, npm, NuGet, PyPI, and generic package formats6. However, AWS CodeArtifact does not support Docker or OCI container images, which are required for Amazon ECS applications.

**NEW QUESTION 119**
A security engineer configures Amazon S3 Cross-Region Replication (CRR) for all objects that are in an S3 bucket in the us-east-1. Region Some objects in this S3 bucket use server-side encryption with AWS KMS keys (SSE-KMS) for encryption at test. The security engineer creates a destination S3 bucket in the us-west-2 Region. The destination S3 bucket is in the same AWS account as the source S3 bucket.
The security engineer also creates a customer managed key in us-west-2 to encrypt objects at rest in the destination S3 bucket. The replication configuration is set to use the key in us-west-2 to encrypt objects in the destination S3 bucket. The security engineer has provided the S3 replication configuration with an IAM role to perform the replication in Amazon S3.
After a day, the security engineer notices that no encrypted objects from the source S3 bucket are replicated to the destination S3 bucket. However, all the unencrypted objects are replicated.
Which combination of steps should the security engineer take to remediate this issue? (Select THREE.)

A. Change the replication configuration to use the key in us-east-1 to encrypt the objects that are in the destination S3 bucket.
B. Grant the IAM role the km
C. Encrypt permission for the key in us-east-1 that encrypts source objects.
D. Grant the IAM role the s3 GetObjectVersionForReplication permission for objects that are in the source S3 bucket.
E. Grant the IAM role the km
F. Decrypt permission for the key in us-east-1 that encrypts source objects.
G. Change the key policy of the key in us-east-1 to grant the km
H. Decrypt permission to the security engineer's IAM account.
I. Grant the IAM role the kms Encrypt permission for the key in us-west-2 that encrypts objects that are in the destination S3 bucket.

**Answer:** BF

**Explanation:**
To enable S3 Cross-Region Replication (CRR) for objects that are encrypted with SSE-KMS, the following steps are required:

- Grant the IAM role the kms.Decrypt permission for the key in us-east-1 that encrypts source objects.

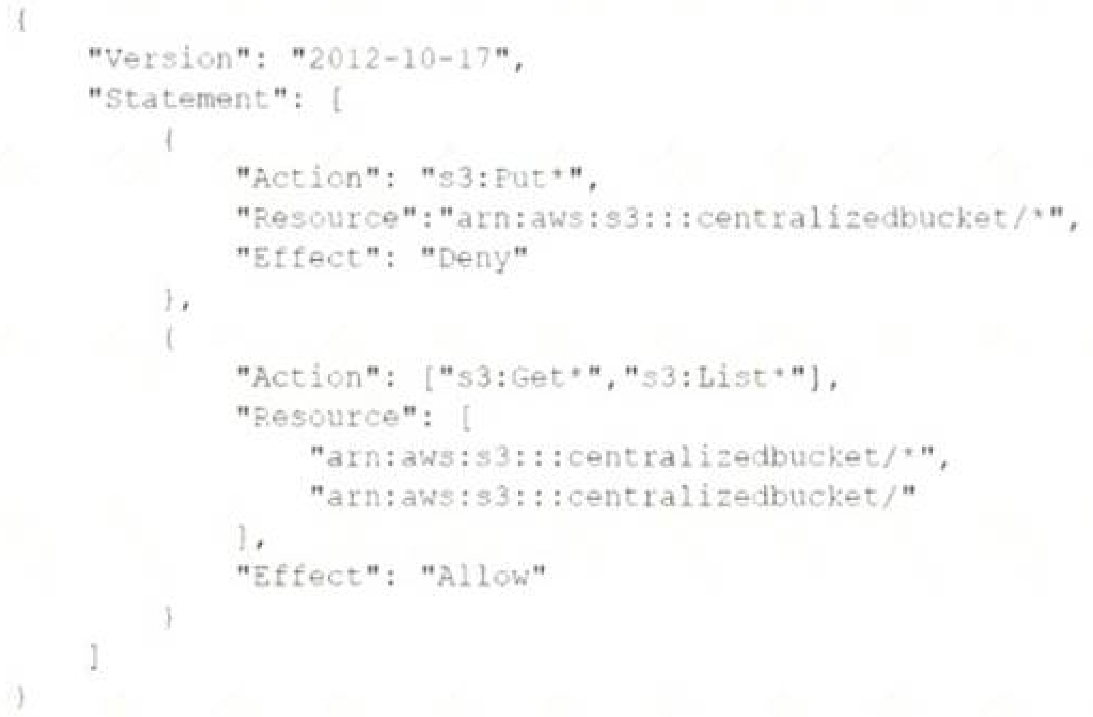
This will allow the IAM role to decrypt the source objects before replicating them to the destination bucket. The kms.Decrypt permission must be granted in the key policy of the source KMS key or in an IAM policy attached to the IAM role.

- Grant the IAM role the kms.Encrypt permission for the key in us-west-2 that encrypts objects that are in the destination S3 bucket. This will allow the IAM role to encrypt the replica objects with the destination KMS key before storing them in the destination bucket. The kms.Encrypt permission must be granted in the key policy of the destination KMS key or in an IAM policy attached to the IAM role.

This solution will remediate the issue of encrypted objects not being replicated to the destination bucket.
The other options are incorrect because they either do not grant the necessary permissions for CRR (A, C, D), or do not use a valid encryption method for CRR (E).
Verified References:

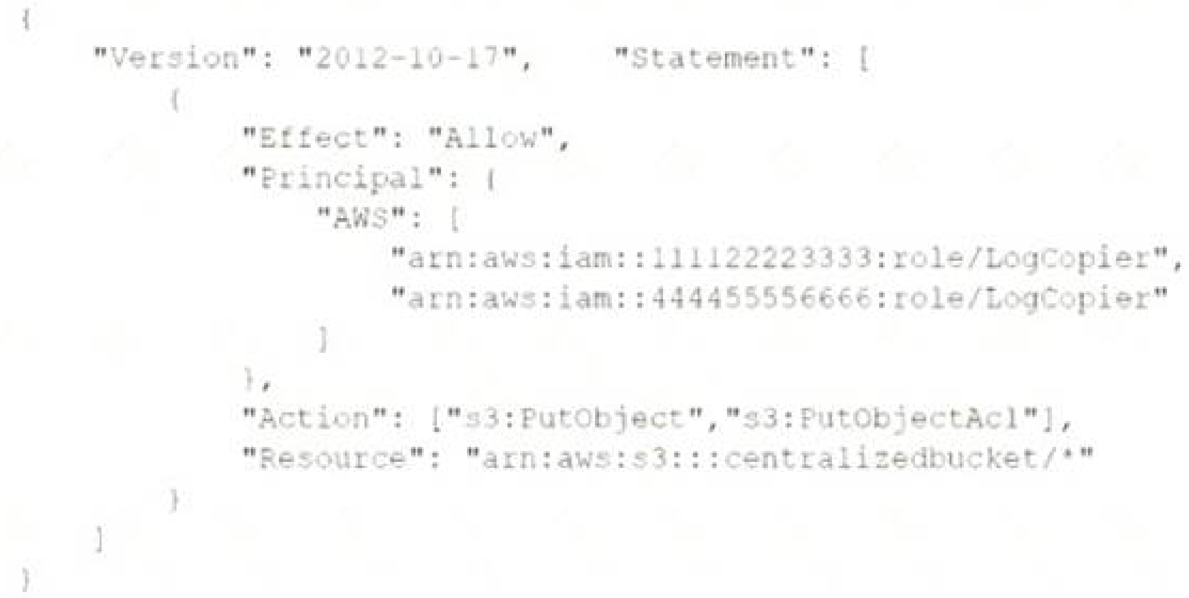
- https://docs.aws.amazon.com/AmazonS3/latest/userguide/replication-config-for-kms-objects.html

**NEW QUESTION 120**
A company's Security Engineer is copying all application logs to centralized Amazon S3 buckets. Currently, each of the company's applications is in its own IAM account, and logs are pushed into S3 buckets associated with each account. The Engineer will deploy an IAM Lambda function into each account that copies the relevant log files to the centralized S3 bucket.
The Security Engineer is unable to access the log files in the centralized S3 bucket. The Engineer's IAM user policy from the centralized account looks like this:



```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "s3:Put*",
            "Resource":"arn:aws:s3:::centralizedbucket/*",
            "Effect": "Deny"
        },
        {
            "Action": ["s3:Get*","s3:List*"],
            "Resource": [
                "arn:aws:s3:::centralizedbucket/*",
                "arn:aws:s3:::centralizedbucket/"
            ],
            "Effect": "Allow"
        }
    ]
}
```

The centralized S3 bucket policy looks like this:



```
{
    "Version": "2012-10-17",     "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:role/LogCopier",
                    "arn:aws:iam::444455556666:role/LogCopier"
                ]
            },
            "Action": ["s3:PutObject","s3:PutObjectAcl"],
            "Resource": "arn:aws:s3:::centralizedbucket/*"
        }
    ]
}
```

Why is the Security Engineer unable to access the log files?

A. The S3 bucket policy does not explicitly allow the Security Engineer access to the objects in the bucket.
B. The object ACLs are not being updated to allow the users within the centralized account to access the objects
C. The Security Engineers IAM policy does not grant permissions to read objects in the S3 bucket
D. The s3:PutObject and s3:PutObjectAcl permissions should be applied at the S3 bucket level

**Answer:** C

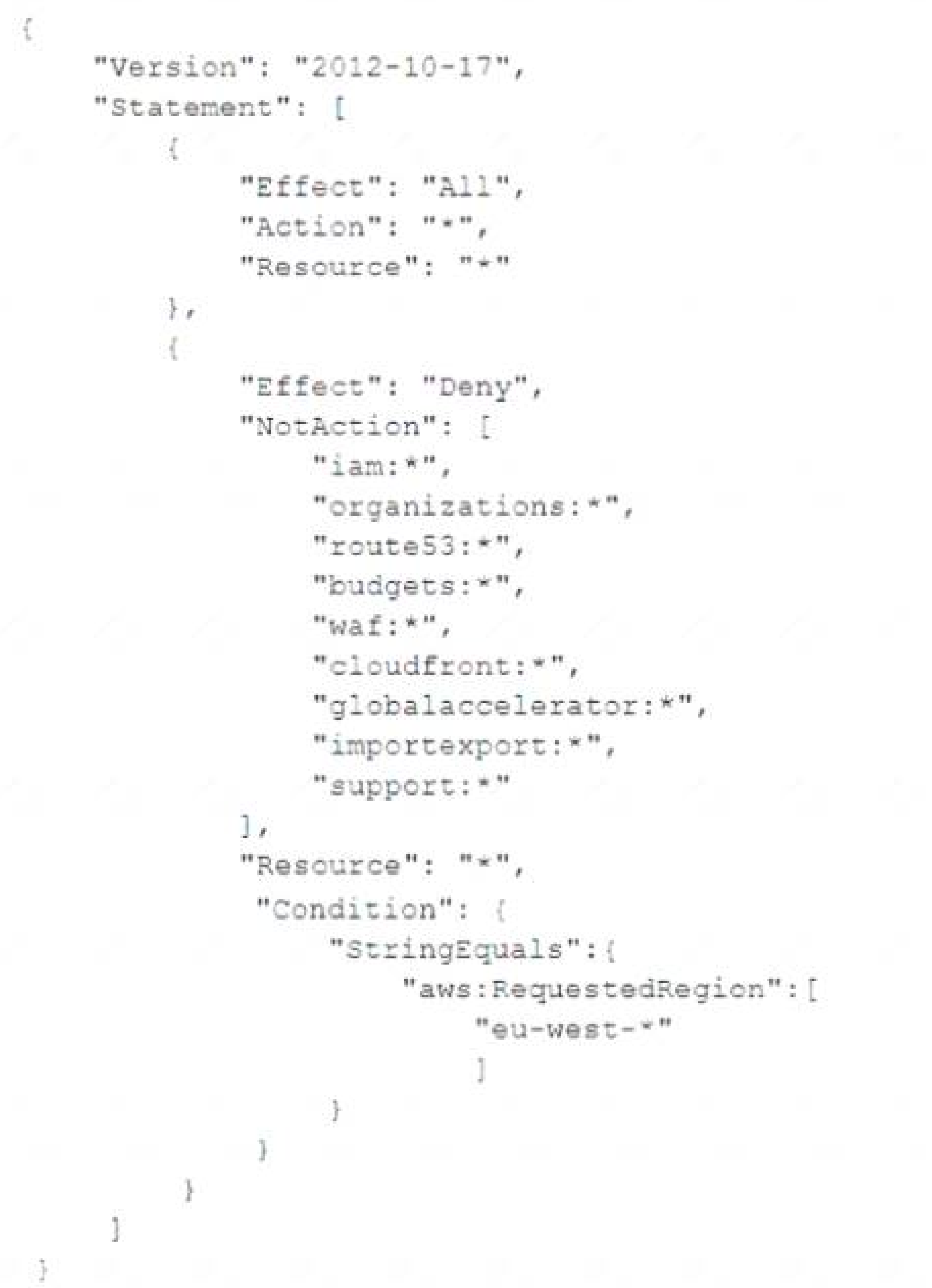
**NEW QUESTION 123**
An organization has a multi-petabyte workload that it is moving to Amazon S3, but the CISO is concerned about cryptographic wear-out and the blast radius if a key is compromised. How can the CISO be assured that IAM KMS and Amazon S3 are addressing the concerns? (Select TWO )

A. There is no API operation to retrieve an S3 object in its encrypted form.
B. Encryption of S3 objects is performed within the secure boundary of the KMS service.
C. S3 uses KMS to generate a unique data key for each individual object.
D. Using a single master key to encrypt all data includes having a single place to perform audits and usage validation.
E. The KMS encryption envelope digitally signs the master key during encryption to prevent cryptographic wear-out

**Answer:** CE

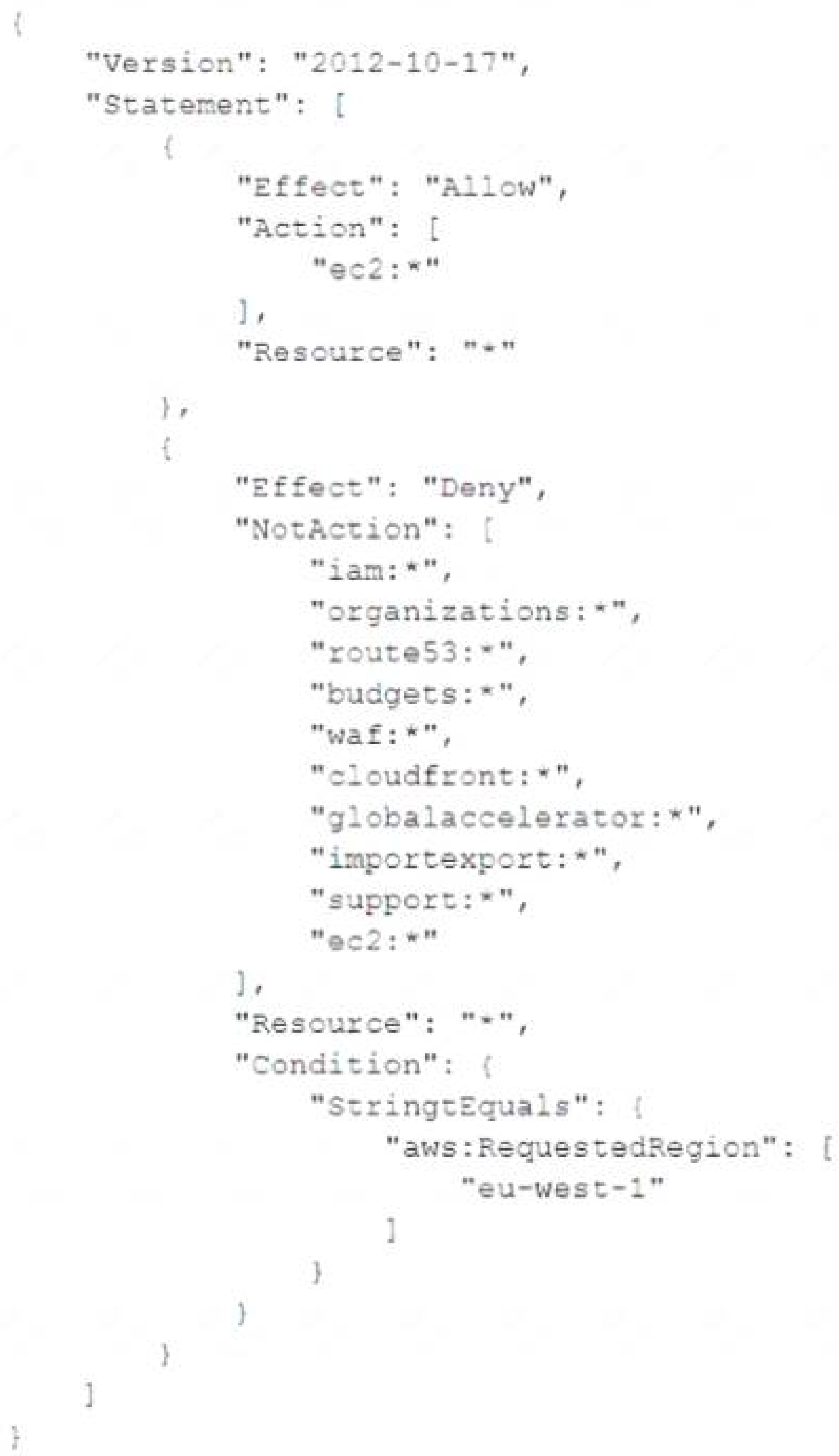
**Explanation:**
because these are the features that can address the CISO’s concerns about cryptographic wear-out and blast radius. Cryptographic wear-out is a phenomenon that occurs when a key is used too frequently or for too long, which increases the risk of compromise or degradation. Blast radius is a measure of how much damage a compromised key can cause to the encrypted data. S3 uses KMS to generate a unique data key for each individual object, which reduces both cryptographic wear-out and blast radius. The KMS encryption envelope digitally signs the master key during encryption, which prevents cryptographic wear-out by ensuring that only authorized parties can use the master key. The other options are either incorrect or irrelevant for addressing the CISO’s concerns.

**NEW QUESTION 128**
A System Administrator is unable to start an Amazon EC2 instance in the eu-west-1 Region using an IAM role The same System Administrator is able to start an EC2 instance in the eu-west-2 and eu-west-3 Regions. The IAMSystemAdministrator access policy attached to the System Administrator IAM role allows unconditional access to all IAM services and resources within the account
Which configuration caused this issue?
A) An SCP is attached to the account with the following permission statement:



```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "All",
            "Action": "*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "NotAction": [
                "iam:*",
                "organizations:*",
                "route53:*",
                "budgets:*",
                "waf:*",
                "cloudfront:*",
                "globalaccelerator:*",
                "importexport:*",
                "support:*"
            ],
            "Resource": "*",
             "Condition": {
                 "StringEquals":{
                     "aws:RequestedRegion":[
                         "eu-west-*"
                         ]
                 }
             }
        }
    ]
}
```

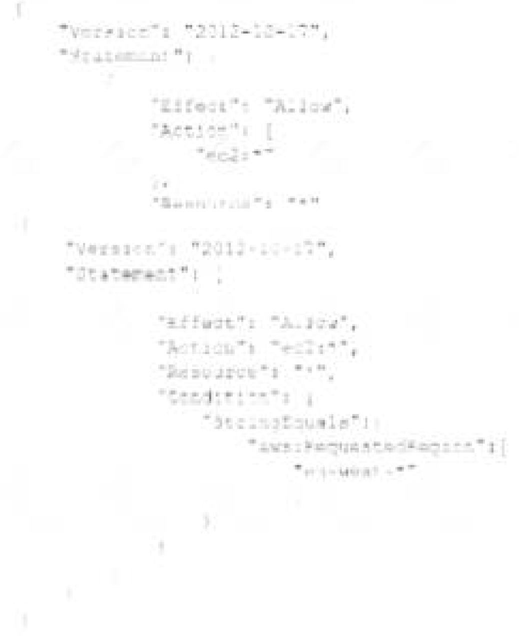
B)
A permission boundary policy is attached to the System Administrator role with the following permission statement:



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

        },
        {
            "Effect": "Deny",
            "NotAction": [
                "iam:*",
                "organizations:*",
                "route53:*",
                "budgets:*",
                "waf:*",
                "cloudfront:*",
                "globalaccelerator:*",
                "importexport:*",
                "support:*",
                "ec2:*"
            ],
            "Resource": "*",
            "Condition": {
                "StringtEquals": {
                    "aws:RequestedRegion": [
                        "eu-west-1"
                    ]
                }
            }
        }
    ]
}
```

C)
A permission boundary is attached to the System Administrator role with the following permission statement:

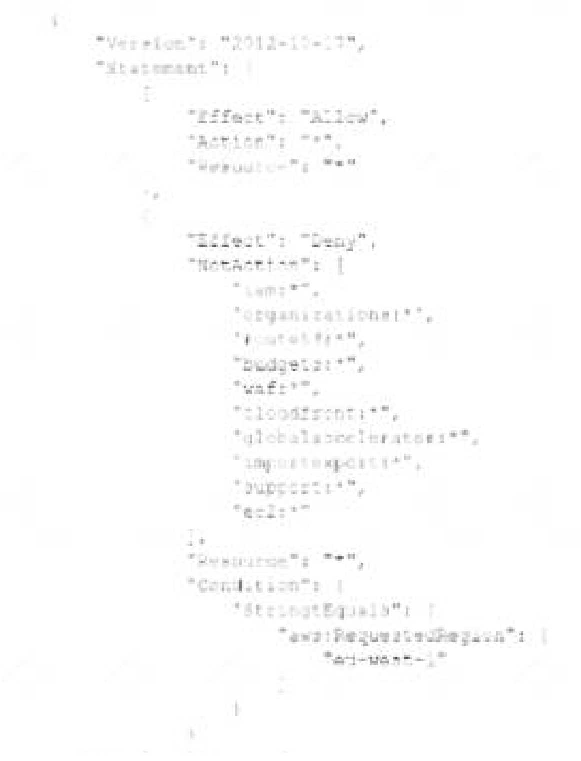


```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*"
            ],
            "Resource": "*"
{
    "Version": "2012-10-17",
    "Statement": [

            "Effect": "Allow",
            "Action": "ec2:*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestedRegion": [
                        "eu-west-1"

                }
            }
        }
    ]
}
```

D)
An SCP is attached to the account with the following statement:



```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "NotAction": [
                "iam:*",
                "organizations:*",
                "route53:*",
                "budgets:*",
                "waf:*",
                "cloudfront:*",
                "globalaccelerator:*",
                "importexport:*",
                "support:*",
                "ec2:*"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestedRegion": [
                        "eu-west-1"
                    ]
                }
            }
        }
```

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

**Answer:** B

**NEW QUESTION 131**
A company has a batch-processing system that uses Amazon S3, Amazon EC2, and AWS Key Management Service (AWS KMS). The system uses two AWS accounts: Account A and Account B.
Account A hosts an S3 bucket that stores the objects that will be processed. The S3 bucket also stores the results of the processing. All the S3 bucket objects are encrypted by a KMS key that is managed in
Account A.
Account B hosts a VPC that has a fleet of EC2 instances that access the S3 buck-et in Account A by using statements in the bucket policy. The VPC was created with DNS hostnames enabled and DNS resolution enabled.
A security engineer needs to update the design of the system without changing any of the system's code. No AWS API calls from the batch-processing EC2 instances can travel over the internet.
Which combination of steps will meet these requirements? (Select TWO.)

A. In the Account B VPC, create a gateway VPC endpoint for Amazon S3. For the gateway VPC endpoint,create a resource policy that allows the s3:GetObject, s3:ListBucket, s3:PutObject, and s3:PutObjectAcl actions for the S3 bucket.
B. In the Account B VPC, create an interface VPC endpoint for Amazon S3. For the interface VPC endpoint, create a resource policy that allows the s3:GetObject, s3:ListBucket, s3:PutObject, and s3:PutObjectAcl actions for the S3 bucket.
C. In the Account B VPC, create an interface VPC endpoint for AWS KM
D. For the interface VPC endpoint, create a resource policy that allows the kms:Encrypt, kms:Decrypt, and kms:GenerateDataKey actions for the KMS ke
E. Ensure that private DNS is turned on for the endpoint.
F. In the Account B VPC, create an interface VPC endpoint for AWS KM
G. For the interface VPC endpoint, create a resource policy that allows the kms:Encrypt, kms:Decrypt, and kms:GenerateDataKey actions for the KMS ke
H. Ensure that private DNS is turned off for the endpoint.
I. In the Account B VPC, verify that the S3 bucket policy allows the s3:PutObjectAcl action for cross-account us
J. In the Account B VPC, create a gateway VPC endpoint for Amazon S3. For the gateway VPC endpoint, create a resource policy that allows the s3:GetObject, s3:ListBucket, and s3:PutObject actions for the S3 bucket.

**Answer:** BC

**NEW QUESTION 134**
A recent security audit found that IAM CloudTrail logs are insufficiently protected from tampering and unauthorized access Which actions must the Security Engineer take to address these audit findings? (Select THREE )

A. Ensure CloudTrail log file validation is turned on
B. Configure an S3 lifecycle rule to periodically archive CloudTrail logs into Glacier for long-term storage
C. Use an S3 bucket with tight access controls that exists m a separate account
D. Use Amazon Inspector to monitor the file integrity of CloudTrail log files.
E. Request a certificate through ACM and use a generated certificate private key to encrypt CloudTrail log files
F. Encrypt the CloudTrail log files with server-side encryption with IAM KMS-managed keys (SSE-KMS)

**Answer:** ADE

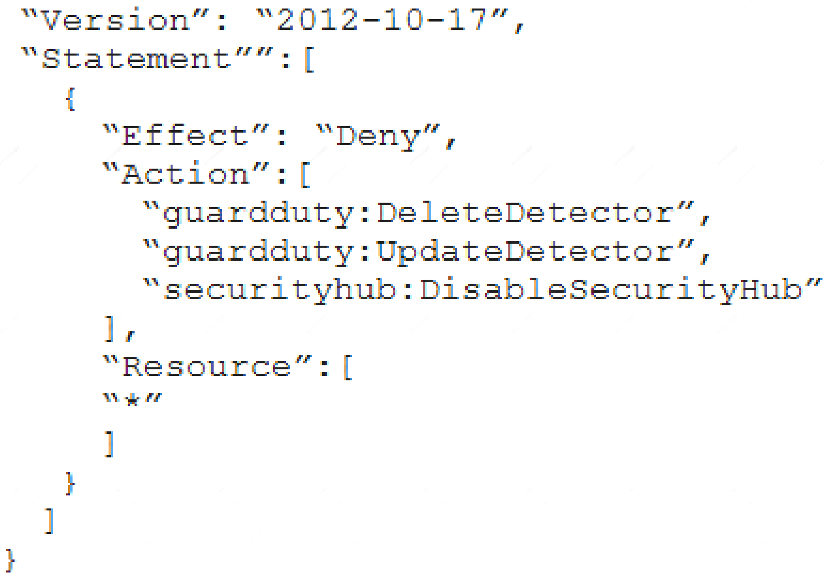
**NEW QUESTION 139**
A company wants to monitor the deletion of customer managed CMKs A security engineer must create an alarm that will notify the company before a CMK is deleted The security engineer has configured the integration of IAM CloudTrail with Amazon CloudWatch
What should the security engineer do next to meet this requirement?

A. Use inbound rule 100 to allow traffic on TCP port 443 Use inbound rule 200 to deny traffic on TCP port 3306 Use outbound rule 100 to allow traffic on TCP port 443
B. Use inbound rule 100 to deny traffic on TCP port 3306. Use inbound rule 200 to allow traffic on TCP port range 1024-65535. Use outbound rule 100 to allow

traffic on TCP port 443
C. Use inbound rule 100 to allow traffic on TCP port range 1024-65535 Use inbound rule 200 to deny traffic on TCP port 3306 Use outbound rule 100 to allow traffic on TCP port 443
D. Use inbound rule 100 to deny traffic on TCP port 3306 Use inbound rule 200 to allow traffic on TCP port 443 Use outbound rule 100 to allow traffic on TCP port 443

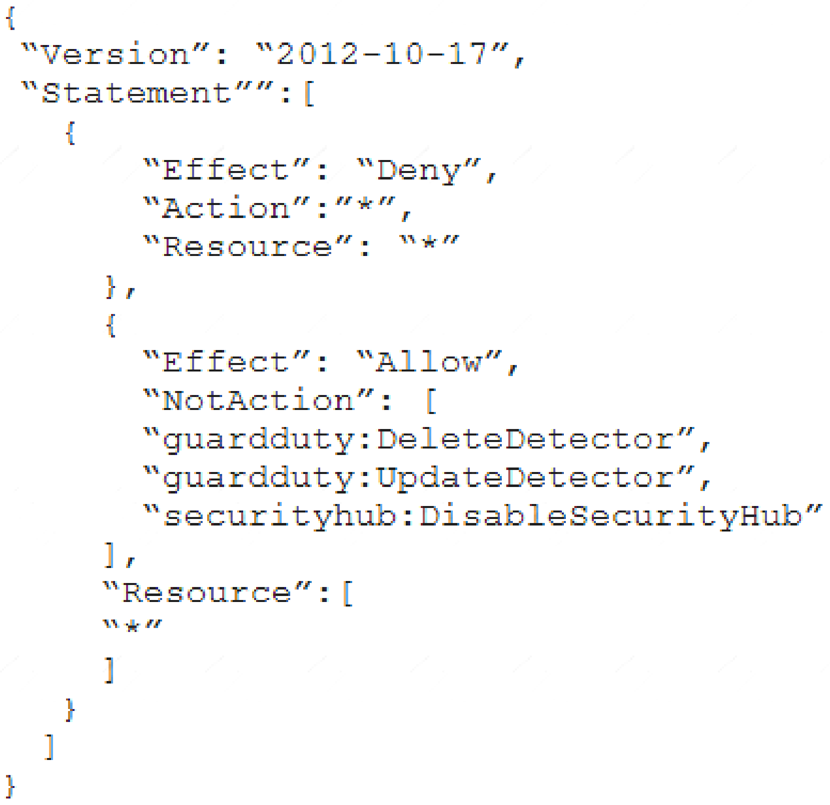
**Answer:** A

**NEW QUESTION 141**
A company deploys a set of standard IAM roles in AWS accounts. The IAM roles are based on job functions within the company. To balance operational efficiency and security, a security engineer implemented AWS Organizations SCPs to restrict access to critical security services in all company accounts.
All of the company's accounts and OUs within AWS Organizations have a default FullAWSAccess SCP that is attached. The security engineer needs to ensure that no one can disable Amazon GuardDuty and AWS Security Hub. The security engineer also must not override other permissions that are granted by IAM policies that are defined in the accounts.
Which SCP should the security engineer attach to the root of the organization to meet these requirements? A)



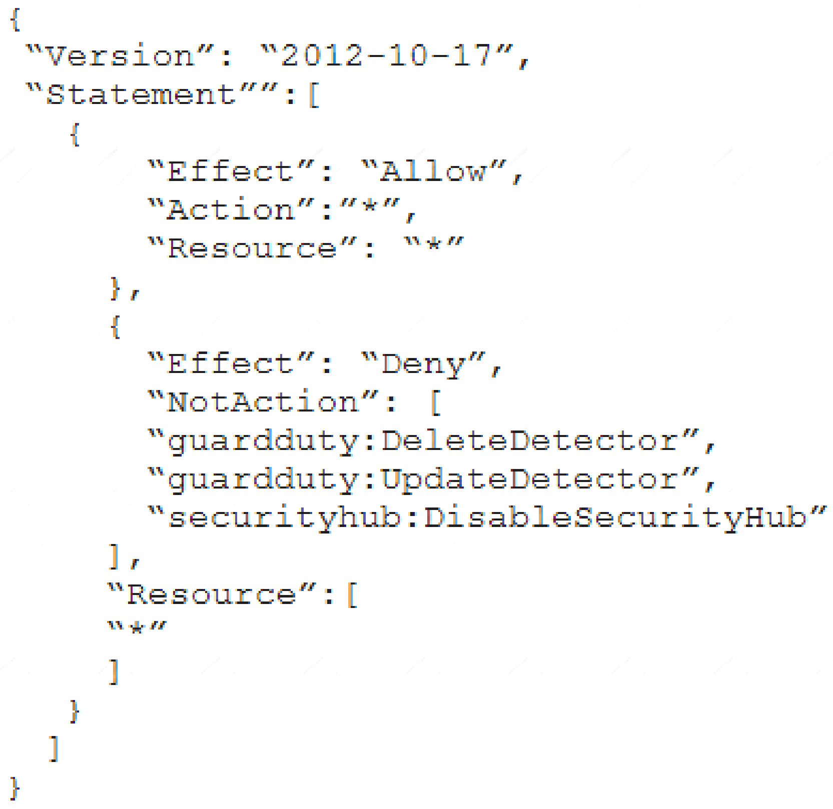
```
 “Version”: “2012-10-17”,
 “Statement””:[
   {
     “Effect”: “Deny”,
     “Action”:[
       “guardduty:DeleteDetector”,
       “guardduty:UpdateDetector”,
       “securityhub:DisableSecurityHub”
     ],
     “Resource”:[
     “*”
     ]
   }
  ]
}
```

B)



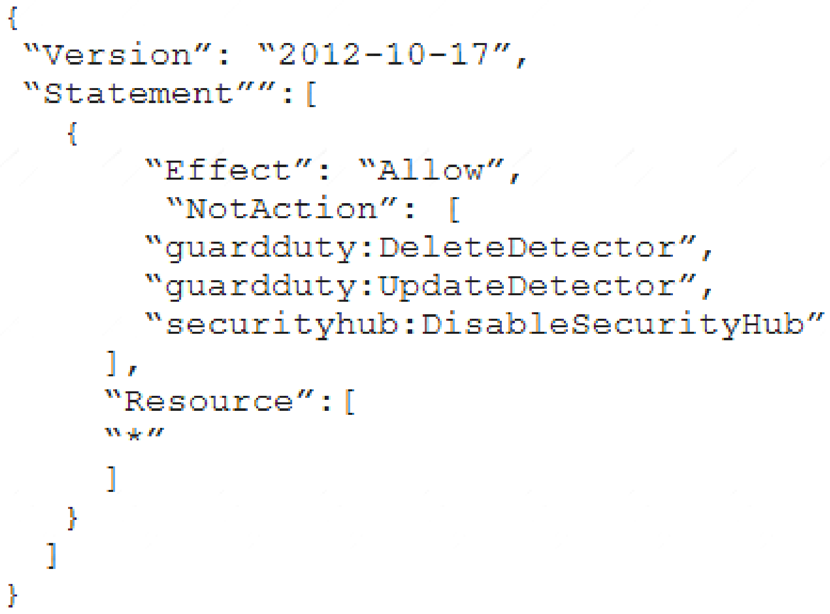
```
{
 “Version”: “2012-10-17”,
 “Statement””:[
   {
       “Effect”: “Deny”,
       “Action”:”*”,
       “Resource”: “*”
     },
     {
       “Effect”: “Allow”,
       “NotAction”: [
       “guardduty:DeleteDetector”,
       “guardduty:UpdateDetector”,
       “securityhub:DisableSecurityHub”
     ],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

C)



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

D)



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

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

**Answer:** A

**NEW QUESTION 143**
A company has two IAM accounts within IAM Organizations. In Account-1. Amazon EC2 Auto Scaling is launched using a service-linked role. In Account-2. Amazon EBS volumes are encrypted with an IAM KMS key A Security Engineer needs to ensure that the service-linked role can launch instances with these encrypted volumes
Which combination of steps should the Security Engineer take in both accounts? (Select TWO.)

A. Allow Account-1 to access the KMS key in Account-2 using a key policy
B. Attach an IAM policy to the service-linked role in Account-1 that allows these actions CreateGrant.DescnbeKey, Encrypt, GenerateDataKey, Decrypt, and ReEncrypt
C. Create a KMS grant for the service-linked role with these actions CreateGrant, DescnbeKey Encrypt GenerateDataKey Decrypt, and ReEncrypt
D. Attach an IAM policy to the role attached to the EC2 instances with KMS actions and then allow Account-1 in the KMS key policy.
E. Attach an IAM policy to the user who is launching EC2 instances and allow the user to access the KMS key policy of Account-2.

**Answer:** CD

**Explanation:**
because these are the steps that can ensure that the service-linked role can launch instances with encrypted volumes. A service-linked role is a type of IAM role that is linked to an AWS service and allows the service to perform actions on your behalf. A KMS grant is a mechanism that allows you to delegate permissions to use a customer master key (CMK) to a principal such as a service-linked role. A KMS grant specifies the actions that the principal can perform, such as encrypting and decrypting data. By creating a KMS grant for the service-linked role with the specified actions, you can allow the service-linked role to use the CMK in Account-2 to launch instances with encrypted volumes. By attaching an IAM policy to the role attached to the EC2 instances with KMS actions and then allowing Account-1 in the KMS key policy, you can also enable cross-account access to the CMK and allow the EC2 instances to use the encrypted volumes. The other options are either incorrect or unnecessary for meeting the requirement.

**NEW QUESTION 145**
A company wants to prevent SSH access through the use of SSH key pairs for any Amazon Linux 2 Amazon EC2 instances in its AWS account. However, a system administrator occasionally will need to access these EC2 instances through SSH in an emergency. For auditing purposes, the company needs to record any commands that a user runs in an EC2 instance.
What should a security engineer do to configure access to these EC2 instances to meet these requirements?

A. Use the EC2 serial console Configure the EC2 serial console to save all commands that are entered to an Amazon S3 bucke
B. Provide the EC2 instances with an IAM role that allows the EC2 serial console to access Amazon S3. Configure an IAM account for the system administrato
C. Provide an IAM policy that allows the IAM account to use the EC2 serial console.
D. Use EC2 Instance Connect Configure EC2 Instance Connect to save all commands that are entered to Amazon CloudWatch Log
E. Provide the EC2 instances with an IAM role that allows the EC2 instances to access CloudWatch Logs Configure an IAM account for the system administrato
F. Provide an IAM policy that allows the IAM account to use EC2 Instance Connect.
G. Use an EC2 key pair with an EC2 instance that needs SSH access Access the EC2 instance with this key pair by using SS
H. Configure the EC2 instance to save all commands that are entered to Amazon CloudWatch Log
I. Provide the EC2 instance with an IAM role that allows the EC2 instance to access Amazon S3 and CloudWatch Logs.
J. Use AWS Systems Manager Session Manager Configure Session Manager to save all commands that are entered in a session to an Amazon S3 bucke
K. Provide the EC2 instances with an IAM role that allows Systems Manager to manage the EC2 instance
L. Configure an IAM account for the system administrator Provide an IAM policy that allows the IAM account to use Session Manager.

**Answer:** D

**Explanation:**
Open the AWS Systems Manager console at https://console.aws.amazon.com/systems-manager/. In the navigation pane, choose Session Manager. Choose the Preferences tab, and then choose Edit. Select the check box next to Enable under S3 logging. (Recommended) Select the check box next to Allow only encrypted S3 buckets. With this option turned on, log data is encrypted using the server-side encryption key specified for the bucket. If you don't want to encrypt the log data that is sent to Amazon S3, clear the check box. You must also clear the check box if encryption isn't allowed on the S3 bucket.

**NEW QUESTION 147**

A company wants to protect its website from man in-the-middle attacks by using Amazon CloudFront. Which solution will meet these requirements with the LEAST operational overhead?

A. Use the SimpleCORS managed response headers policy.
B. Use a Lambda@Edge function to add the Strict-Transport-Security response header.
C. Use the SecurityHeadersPolicy managed response headers policy.
D. Include the X-XSS-Protection header in a custom response headers policy.

**Answer:** C

**Explanation:**
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/using-managed-response-headers-poli The SecurityHeadersPolicy is a managed policy provided by Amazon CloudFront that includes a set of recommended security headers to enhance the security of your website. These headers help protect against various types of attacks, including man-in-the-middle attacks. By applying the SecurityHeadersPolicy to your CloudFront distribution, the necessary security headers will be automatically added to the responses sent by CloudFront. This reduces operational overhead because you don't have to manually configure or manage the headers yourself.

**NEW QUESTION 151**
A company manages three separate IAM accounts for its production, development, and test environments, Each Developer is assigned a unique IAM user under the development account. A new application hosted on an Amazon EC2 instance in the developer account requires read access to the archived documents stored in an Amazon S3 bucket in the production account.
How should access be granted?

A. Create an IAM role in the production account and allow EC2 instances in the development account to assume that role using the trust polic
B. Provide read access for the required S3 bucket to this role.
C. Use a custom identity broker to allow Developer IAM users to temporarily access the S3 bucket.
D. Create a temporary IAM user for the application to use in the production account.
E. Create a temporary IAM user in the production account and provide read access to Amazon S3.Generate the temporary IAM user's access key and secret key and store these on the EC2 instance used by the application in the development account.

**Answer:** A

**Explanation:**
https://IAM.amazon.com/premiumsupport/knowledge-center/cross-account-access-s3/

**NEW QUESTION 156**
A company discovers a billing anomaly in its AWS account. A security consultant investigates the anomaly and discovers that an employee who left the company 30 days ago still has access to the account.
The company has not monitored account activity in the past.
The security consultant needs to determine which resources have been deployed or reconfigured by the employee as quickly as possible.
Which solution will meet these requirements?

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

**Answer:** C

**NEW QUESTION 160**
......

# Thank You for Trying Our Product

## We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

## SCS-C02 Practice Exam Features:

* SCS-C02 Questions and Answers Updated Frequently

* SCS-C02 Practice Questions Verified by Expert Senior Certified Staff

* SCS-C02 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SCS-C02 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The SCS-C02 Practice Test Here