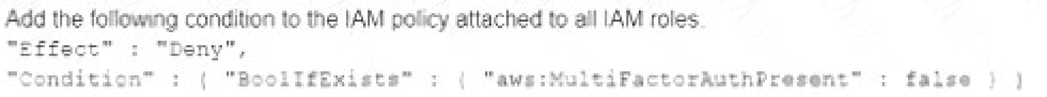
Exam Questions SCS-C01

AWS Certified Security- Specialty

https://www.2passeasy.com/dumps/SCS-C01/

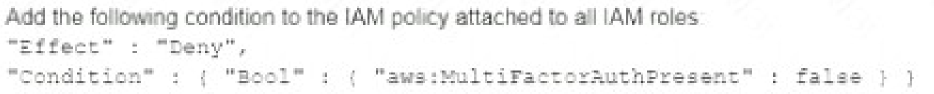
NEW QUESTION 1
- (Exam Topic 1)
A company has an AWS account and allows a third-party contractor who uses another AWS account, to assume certain IAM roles. The company wants to ensure that IAM roles can be assumed by the contractor only if the contractor has multi-factor authentication enabled on their IAM user accounts
What should the company do to accomplish this?
A)



Add the following condition to the IAM policy attached to all IAM roles.

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

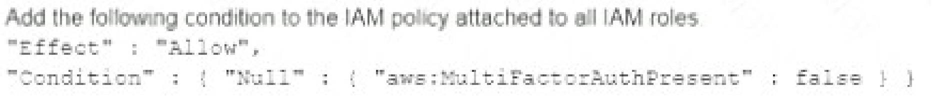
B)



Add the following condition to the IAM policy attached to all IAM roles

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

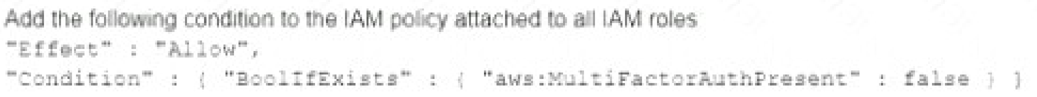
C)



Add the following condition to the IAM policy attached to all IAM roles

```
"Effect" : "Allow",
"Condition" : { "Null" : { "aws:MultiFactorAuthPresent" : false } }
```

D)



Add the following condition to the IAM policy attached to all IAM roles

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

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

Answer: A

NEW QUESTION 2
- (Exam Topic 1)
A company has an encrypted Amazon S3 bucket. An Application Developer has an IAM policy that allows access to the S3 bucket, but the Application Developer is unable to access objects within the bucket.
What is a possible cause of the issue?

A. The S3 ACL for the S3 bucket fails to explicitly grant access to the Application Developer
B. The AWS KMS key for the S3 bucket fails to list the Application Developer as an administrator
C. The S3 bucket policy fails to explicitly grant access to the Application Developer
D. The S3 bucket policy explicitly denies access to the Application Developer

Answer: C

NEW QUESTION 3
- (Exam Topic 1)
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, mere is no authentication system but 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 (or the ALB Define a SAML-based Amazon Cognito user pool and connect it to ADFSimplement AWS SSO in the master account and link it to ADFS as an identity provide' Define the EC2 instance as a managed resource, then apply an IAM policy on the resource
B. Define an Amazon Cognito identity pool then install the connector on the Active Directory server Use the Amazon Cognito SDK on the application instance to authenticate the employees using their
C. Active Directory user names and passwords
D. Create an AWS Lambda custom authorizer as the authenticator for a reverse proxy on Amazon EC2 Ensure the security group on Amazon EC2 only allows access from the Lambda function.

Answer: B

NEW QUESTION 4
- (Exam Topic 1)
A Security Engineer has been asked to troubleshoot inbound connectivity to a web server. This single web server is not receiving inbound connections from the internet, whereas all other web servers are functioning properly.
The architecture includes network ACLs, security groups, and a virtual security appliance. In addition, the Development team has implemented Application Load Balancers (ALBs) to distribute the load across all web servers. It is a requirement that traffic between the web servers and the internet flow through the virtual security appliance.
The Security Engineer has verified the following:
* 1. The rule set in the Security Groups is correct
* 2. The rule set in the network ACLs is correct
* 3. The rule set in the virtual appliance is correct
Which of the following are other valid items to troubleshoot in this scenario? (Choose two.)

A. Verify that the 0.0.0.0/0 route in the route table for the web server subnet points to a NAT gateway.

B. Verify which Security Group is applied to the particular web server’s elastic network interface (ENI).
C. Verify that the 0.0.0.0/0 route in the route table for the web server subnet points to the virtual security appliance.
D. Verify the registered targets in the ALB.
E. Verify that the 0.0.0.0/0 route in the public subnet points to a NAT gateway.

Answer: CD

Explanation:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html

NEW QUESTION 5
- (Exam Topic 1)
A company has several critical applications running on a large fleet of Amazon EC2 instances. As part of a security operations review, the company needs to apply a critical operating system patch to EC2 instances within 24 hours of the patch becoming available from the operating system vendor. The company does not have a patching solution deployed on AWS, but does have AWS Systems Manager configured. The solution must also minimize administrative overhead.
What should a security engineer recommend to meet these requirements?

A. Create an AWS Config rule defining the patch as a required configuration for EC2 instances.
B. Use the AWS Systems Manager Run Command to patch affected instances.
C. Use an AWS Systems Manager Patch Manager predefined baseline to patch affected instances.
D. Use AWS Systems Manager Session Manager to log in to each affected instance and apply the patch.

Answer: B

NEW QUESTION 6
- (Exam Topic 1)
A security engineer is designing an incident response plan to address the risk of a compromised Amazon EC2 instance. The plan must recommend a solution to meet the following requirements:
• A trusted forensic environment must be provisioned
• Automated response processes must be orchestrated
Which AWS services should be included in the plan? {Select TWO)

A. AWS CloudFormation
B. Amazon GuardDuty
C. Amazon Inspector
D. Amazon Macie
E. AWS Step Functions

Answer: AE

NEW QUESTION 7
- (Exam Topic 1)
A company has hundreds of AWS accounts, and a centralized Amazon S3 bucket used to collect AWS CloudTrail for all of these accounts. A security engineer wants to create a solution that will enable the company to run ad hoc queues against its CloudTrail logs dating back 3 years from when the trails were first enabled in the company’s AWS account.
How should the company accomplish this with the least amount of administrative overhead?

A. Run an Amazon EMP cluster that uses a MapReduce job to be examine the CloudTrail trails.
B. Use the events history/feature of the CloudTrail console to query the CloudTrail trails.
C. Write an AWS Lambda function to query the CloudTrail trails Configure the Lambda function to be executed whenever a new file is created in the CloudTrail S3 bucket.
D. Create an Amazon Athena table that tools at the S3 bucket the CloudTrail trails are being written to Use Athena to run queries against the trails.

Answer: D

NEW QUESTION 8
- (Exam Topic 1)
Authorized Administrators are unable to connect to an Amazon EC2 Linux bastion host using SSH over the internet. The connection either fails to respond or generates the following error message:
Network error: Connection timed out.
What could be responsible for the connection failure? (Select THREE)

A. The NAT gateway in the subnet where the EC2 instance is deployed has been misconfigured
B. The internet gateway of the VPC has been reconfigured
C. The security group denies outbound traffic on ephemeral ports
D. The route table is missing a route to the internet gateway
E. The NACL denies outbound traffic on ephemeral ports
F. The host-based firewall is denying SSH traffic

Answer: BDF

NEW QUESTION 9
- (Exam Topic 1)
A company has the software development teams that are creating applications that store sensitive data in Amazon S3 Each team's data must always be separate. The company's security team must design a data encryption strategy for both teams that provides the ability to audit key usage. The solution must also minimize operational overhead
what should me security team recommend?

A. Tell the application teams to use two different S3 buckets with separate AWS Key Management Service (AWS KMS) AWS managed CMKs Limit the key process to allow encryption and decryption of the CMKs to their respective teams onl
B. Force the teams to use encryption context to encrypt and decrypt
C. Tell the application teams to use two different S3 buckets with a single AWS Key Management Service (AWS KMS) AWS managed CMK Limit the key policy to allow encryption and decryption of the CMK onl
D. Do not allow the teams to use encryption context to encrypt and decrypt
E. Tell the application teams to use two different S3 buckets with separate AWS Key Management Service (AWS KMS) customer managed CMKs Limit the key policies to allow encryption and decryption of the CMKs to their respective teams only Force the teams to use encryption context to encrypt and decrypt
F. Tell the application teams to use two different S3 buckets with a single AWS Key Management Service (AWS KMS) customer managed CMK Limit the key policy to allow encryption and decryption of the CMK only Do not allow the teams to use encryption context to encrypt and decrypt

Answer: A

NEW QUESTION 10
- (Exam Topic 1)
An application running on Amazon EC2 instances generates log files in a folder on a Linux file system. The instances block access to the console and file transfer utilities, such as Secure Copy Protocol (SCP) and Secure File Transfer Protocol (SFTP). The Application Support team wants to automatically monitor the application log files so the team can set up notifications in the future.
A Security Engineer must design a solution that meets the following requirements:
• Make the log files available through an AWS managed service.
• Allow for automatic monitoring of the logs.
• Provide an Interlace for analyzing logs.
• Minimize effort.
Which approach meets these requirements^

A. Modify the application to use the AWS SD
B. Write the application logs lo an Amazon S3 bucket
C. install the unified Amazon CloudWatch agent on the instances Configure the agent to collect the application log dies on the EC2 tile system and send them to Amazon CloudWatch Logs
D. Install AWS Systems Manager Agent on the instances Configure an automation document to copy the application log files to AWS DeepLens
E. Install Amazon Kinesis Agent on the instances Stream the application log files to Amazon Kinesis Data Firehose and sot the destination to Amazon Elasticsearch Service

Answer: D

NEW QUESTION 10
- (Exam Topic 1)
A Security Engineer is setting up a new AWS account. The Engineer has been asked to continuously monitor the company's AWS account using automated compliance checks based on AWS best practices and Center for Internet Security (CIS) AWS Foundations Benchmarks
How can the Security Engineer accomplish this using AWS services?

A. Enable AWS Config and set it to record all resources in all Regions and global resource
B. Then enable AWS Security Hub and confirm that the CIS AWS Foundations compliance standard is enabled
C. Enable Amazon Inspector and configure it to scan all Regions for the CIS AWS Foundations Benchmark
D. Then enable AWS Security Hub and configure it to ingest the Amazon Inspector findings
E. Enable Amazon Inspector and configure it to scan all Regions for the CIS AWS Foundations Benchmark
F. Then enable AWS Shield in all Regions to protect the account from DDoS attacks.
G. Enable AWS Config and set it to record all resources in all Regions and global resources Then enable Amazon Inspector and configure it to enforce CIS AWS Foundations Benchmarks using AWS Config rules.

Answer: B

NEW QUESTION 13
- (Exam Topic 1)
A company uses Microsoft Active Directory for access management for on-premises resources and wants to use the same mechanism for accessing its AWS accounts. Additionally, the development team plans to launch a public-facing application for which they need a separate authentication solution.
When coma nation of the following would satisfy these requirements? (Select TWO)

A. Set up domain controllers on Amazon EC2 to extend the on-premises directory to AWS
B. Establish network connectivity between on-premises and the user's VPC
C. Use Amazon Cognito user pools for application authentication
D. Use AD Connector tor application authentication.
E. Set up federated sign-in to AWS through ADFS and SAML.

Answer: CD

NEW QUESTION 15
- (Exam Topic 1)
A company had one of its Amazon EC2 key pairs compromised. A Security Engineer must identify which current Linux EC2 instances were deployed and used the compromised key pair.
How can this task be accomplished?

A. Obtain the list of instances by directly querying Amazon EC2 using: aws ec2 describe-instances --fi1ters "Name=key-name,Values=KEYNAMEHERE".
B. Obtain the fingerprint for the key pair from the AWS Management Console, then search for the fingerprint in the Amazon Inspector logs.
C. Obtain the output from the EC2 instance metadata using: curl http: //169.254.169.254/latest/meta-data/public- keys/0/.
D. Obtain the fingerprint for the key pair from the AWS Management Console, then search for the fingerprint in Amazon CloudWatch Logs using: aws logs filter-log-events.

Answer: A

NEW QUESTION 18
- (Exam Topic 1)
A company uses HTTP Live Streaming (HLS) to stream live video content to paying subscribers by using Amazon CloudFront. HLS splits the video content into chunks so that the user can request the right chunk based on different conditions Because the video events last for several hours, the total video is made up of thousands of chunks
The origin URL is not disclosed and every user is forced to access the CloudFront URL The company has a web application that authenticates the paying users against an internal repository and a CloudFront key pair that is already issued.
What is the simplest and MOST effective way to protect the content?

A. Develop the application to use the CloudFront key pair to create signed URLs that users will use to access the content.
B. Develop the application to use the CloudFront key pair to set the signed cookies that users will use to access the content.
C. Develop the application to issue a security token that Lambda@Edge will receive to authenticate and authorize access to the content
D. Keep the CloudFront URL encrypted inside the application, and use AWS KMS to resolve the URL on-the-fly after the user is authenticated.

Answer: B

NEW QUESTION 22
- (Exam Topic 1)
A security engineer is auditing a production system and discovers several additional IAM roles that are not required and were not previously documented during the last audit 90 days ago. The engineer is trying to find out who created these IAM roles and when they were created. The solution must have the lowest operational overhead.
Which solution will meet this requirement?

A. Import AWS CloudTrail logs from Amazon S3 into an Amazon Elasticsearch Service cluster, and search through the combined logs for CreateRole events.
B. Create a table in Amazon Athena for AWS CloudTrail event
C. Query the table in Amazon Athena for CreateRole events.
D. Use AWS Config to look up the configuration timeline for the additional IAM roles and view the linked AWS CloudTrail event.
E. Download the credentials report from the IAM console to view the details for each IAM entity, including the creation dates.

Answer: A

NEW QUESTION 27
- (Exam Topic 1)
A global company that deals with International finance is investing heavily in cryptocurrencies and wants to experiment with mining technologies using AWS. The company's security team has enabled Amazon
GuardDuty and is concerned by the number of findings being generated by the accounts. The security team wants to minimize the possibility of GuardDuty finding false negatives for compromised instances that are performing mining
How can the security team continue using GuardDuty while meeting these requirements?

A. In the GuardDuty console, select the CryptoCurrency:EC2/BitcoinTool B'DNS finding and use the suppress findings option
B. Create a custom AWS Lambda function to process newly detected GuardDuty alerts Process the CryptoCurrency EC2/BitcoinTool BIDNS alert and filter outthe high-severity finding types only.
C. When creating a new Amazon EC2 Instance, provide the instance with a specific tag that indicates it is performing mining operations Create a custom AWS Lambda function to process newly detected GuardDuty alerts and filter for the presence of this tag
D. When GuardDuty produces a cryptocurrency finding, process the finding with a custom AWS Lambda function to extract the instance ID from the finding Then use the AWS Systems Manager Run Command to check for a running process performing mining operations

Answer: A

NEW QUESTION 28
- (Exam Topic 1)
A company's Security Officer is concerned about the risk of AWS account root user logins and has assigned a Security Engineer to implement a notification solution for near-real-time alerts upon account root user logins.
How should the Security Engineer meet these requirements?

A. Create a cron job that runs a script lo download the AWS IAM security credentials W
B. parse the file for account root user logins and email the Security team's distribution 1st
C. Run AWS CloudTrail logs through Amazon CloudWatch Events to detect account roo4 user logins and trigger an AWS Lambda function to send an Amazon SNS notification to the Security team'sdistribution list.
D. Save AWS CloudTrail logs to an Amazon S3 bucket in the Security team's account Process the CloudTrail logs with the Security Engineer's logging solution for account root user logins Send an Amazon SNS notification to the Security team upon encountering the account root user login events
E. Save VPC Plow Logs to an Amazon S3 bucket in the Security team's account and process the VPC Flow Logs with their logging solutions for account root user logins Send an Amazon SNS notification to the Security team upon encountering the account root user login events

Answer: B

NEW QUESTION 31
- (Exam Topic 1)
A website currently runs on Amazon EC2 with mostly static content on the site. Recently, the site was subjected to a ODoS attack, and a Security Engineer was tasked with 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 AWS X-Ray to inspect the traffic going 10 the EC2 instances
B. Move the state content to Amazon S3 and font this with an Amazon CloudFront distribution
C. Change the security group configuration to block the source of the attack traffic
D. Use AWS WAF security rules to inspect the inbound traffic
E. Use Amazon inspector assessment templates to inspect the inbound traffic
F. Use Amazon Route 53 to distribute traffic

Answer: BDF

NEW QUESTION 33
- (Exam Topic 1)
A company's web application is hosted on Amazon EC2 instances running behind an Application Load Balancer (ALB) in an Auto Scaling group. An AWS WAF web ACL is associated with the ALB. AWS CloudTrail is enabled, and stores logs in Amazon S3 and Amazon CloudWatch Logs.
The operations team has observed some EC2 instances reboot at random. After rebooting, all access logs on the instances have been deleted. During an investigation, the operations team found that each reboot happened just after a PHP error occurred on the new-user-creation.php file. The operations team needs to view log information to determine if the company is being attacked.
Which set of actions will identify the suspect attacker's IP address for future occurrences?

A. Configure VPC Flow Logs on the subnet where the ALB is located, and stream the data CloudWatch.Search for the new-user-creation.php occurrences in CloudWatch.
B. Configure the CloudWatch agent on the ALB Configure the agent to send application logs to CloudWatch Update the instance role to allow CloudWatch Logs acces
C. Export the logs to CloudWatch Search for the new-user-creation.php occurrences in CloudWatch.
D. Configure the ALB to export access logs to an Amazon Elasticsearch Service cluster, and use the service to search for the new-user-creation.php occurrences.
E. Configure the web ACL to send logs to Amazon Kinesis Data Firehose, which delivers the logs to an S3 bucket Use Amazon Athena to query the logs and find the new-user-creation php occurrences.

Answer: B

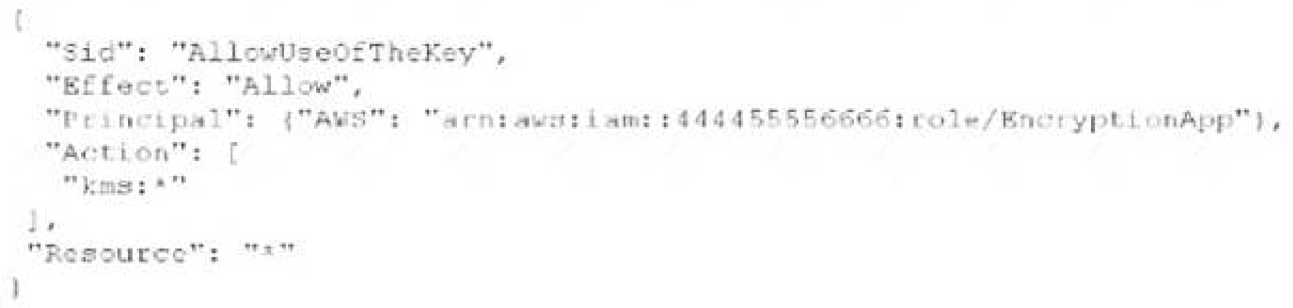
NEW QUESTION 38
- (Exam Topic 1)
A company requires that SSH commands used to access its AWS instance be traceable to the user who executed each command.
How should a Security Engineer accomplish this?

A. Allow inbound access on port 22 at the security group attached to the instance Use AWS Systems Manager Session Manager for shell access to Amazon EC2 instances with the user tag defined Enable Amazon CloudWatch togging tor Systems Manager sessions
B. Use Amazon S3 to securely store one Privacy Enhanced Mail Certificate (PEM file) for each user Allow Amazon EC2 to read from Amazon S3 and import every user that wants to use SSH to access EC2 instances Allow inbound access on port 22 at the security group attached to the instance Install the Amazon CloudWatch agent on the EC2 instance and configure it to ingest audit logs for the instance
C. Deny inbound access on port 22 at the security group attached to the instance Use AWS Systems Manager Session Manager tor shell access to Amazon EC2 instances with the user tag defined Enable Amazon CloudWatch togging for Systems Manager sessions
D. Use Amazon S3 to securely store one Privacy Enhanced Mall Certificate (PEM fie) for each team or group Allow Amazon EC2 to read from Amazon S3 and import every user that wants to use SSH to access EC2 instances Allow inbound access on pod 22 at the security group attached to the instance Install the Amazon CloudWatch agent on the EC2 instance and configure it to ingest audit logs for the instance

Answer: C

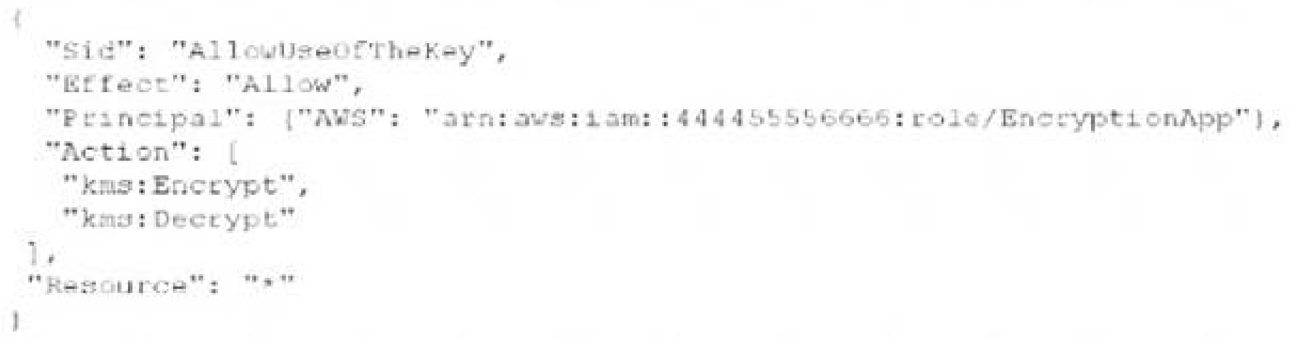
NEW QUESTION 41
- (Exam Topic 1)
An application developer is using an AWS Lambda function that must use AWS KMS to perform encrypt and decrypt operations for API keys that are less than 2 KB Which key policy would allow the application to do this while granting least privilege?

A.



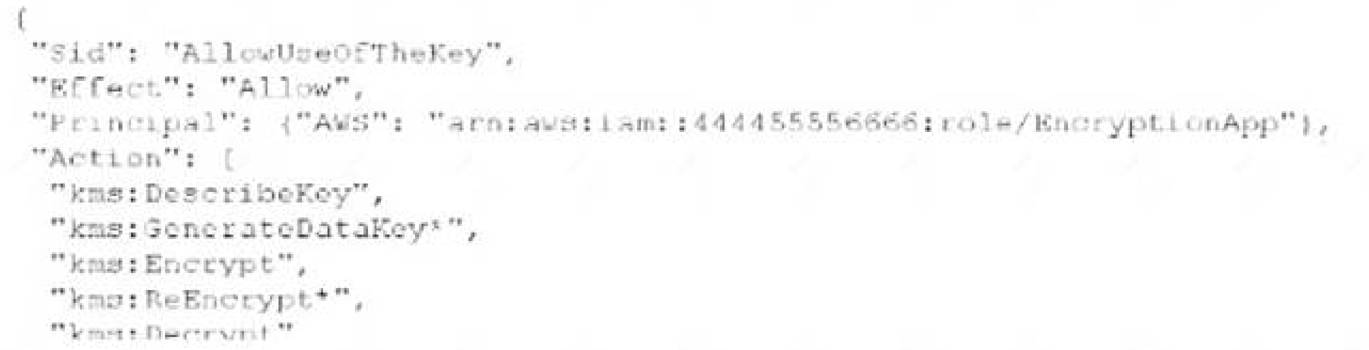
```
{
  "Sid": "AllowUseOfTheKey",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::444455556666:role/EncryptionApp"},
  "Action": [
   "kms:*"
 ],
 "Resource": "*"
}
```

B.

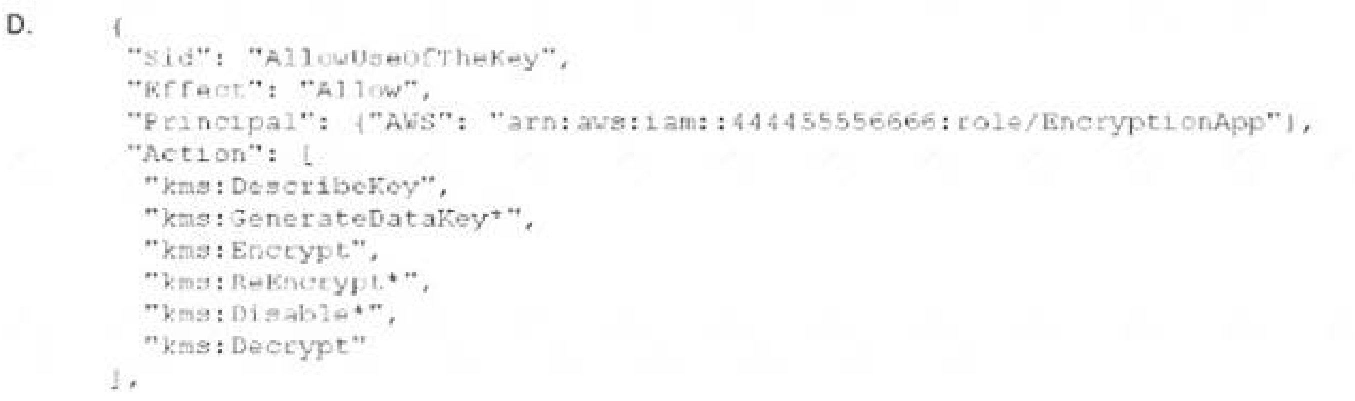


```
{
  "Sid": "AllowUseOfTheKey",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::444455556666:role/EncryptionApp"},
  "Action": [
   "kms:Encrypt",
   "kms:Decrypt"
 ],
 "Resource": "*"
}
```

C.



```
{
 "Sid": "AllowUseOfTheKey",
 "Effect": "Allow",
 "Principal": {"AWS": "arn:aws:iam::444455556666:role/EncryptionApp"},
 "Action": [
  "kms:DescribeKey",
  "kms:GenerateDataKey*",
  "kms:Encrypt",
  "kms:ReEncrypt*",
  "kms:Decrypt"
```



D.

```
{
 "Sid": "AllowUseOfTheKey",
 "Effect": "Allow",
 "Principal": {"AWS": "arn:aws:iam::444455556666:role/EncryptionApp"},
 "Action": [
  "kms:DescribeKey",
  "kms:GenerateDataKey*",
  "kms:Encrypt",
  "kms:ReEncrypt*",
  "kms:Disable*",
  "kms:Decrypt"
 ],
```

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

Answer: B

NEW QUESTION 42
- (Exam Topic 1)
A Security Engineer is looking for a way to control access to data that is being encrypted under a CMK. The Engineer is also looking to use additional authenticated data (AAD) to prevent tampering with ciphertext.
Which action would provide the required functionality?

A. Pass the key alias to AWS KMS when calling Encrypt and Decrypt API actions.
B. Use IAM policies to restrict access to Encrypt and Decrypt API actions.
C. Use kms:EncryptionContext as a condition when defining IAM policies for the CMK.
D. Use key policies to restrict access to the appropriate IAM groups.

Answer: B

NEW QUESTION 44
- (Exam Topic 1)
A company is running an application on Amazon EC2 instances in an Auto Scaling group. The application stores logs locally A security engineer noticed that logs were lost after a scale-in event. The security engineer needs to recommend a solution to ensure the durability and availability of log data All logs must be kept for a minimum of 1 year for auditing purposes
What should the security engineer recommend?

A. Within the Auto Scaling lifecycle, add a hook to create and attach an Amazon Elastic Block Store (Amazon EBS) log volume each time an EC2 instance is create
B. When the instance is terminated, the EBS volume can be reattached to another instance for log review.
C. Create an Amazon Elastic File System (Amazon EFS) file system and add a command in the user data section of the Auto Scaling launch template to mount the EFS file system during EC2 instance creation Configure a process on the instance to copy the logs once a day from an instance Amazon Elastic Block Store (Amazon EBS) volume to a directory in the EFS file system.
D. Build the Amazon CloudWatch agent into the AMI used in the Auto Scaling grou
E. Configure the CloudWatch agent to send the logs to Amazon CloudWatch Logs for review.
F. Within the Auto Scaling lifecycle, add a lifecycle hook at the terminating state transition and alert the engineering team by using a lifecycle notification to Amazon Simple Notification Service (Amazon SNS). Configure the hook to remain in the Terminating:Wait state for 1 hour to allow manual review of the security logs prior to instance termination.

Answer: B

NEW QUESTION 47
- (Exam Topic 1)
A company's on-premises data center forwards DNS logs to a third-party security incident events management (SIEM) solution that alerts on suspicious behavior. The company wants to introduce a similar capability to its AWS accounts that includes automatic remediation. The company expects to double in size within the next few months.
Which solution meets the company's current and future logging requirements?

A. Enable Amazon GuardDuty and AWS Security Hub in all Regions and all account
B. Designate a mastersecurity account to receive all alerts from the child account
C. Set up specific rules within Amazon Even;Bridge to trigger an AWS Lambda function for remediation steps.
D. Ingest all AWS CloudTrail logs, VPC Flow Logs, and DNS logs into a single Amazon S3 bucket in a designated security accoun
E. Use the current on-premises SIEM to monitor the logs and send a notification to an Amazon SNS topic to alert the security team of remediation steps.
F. Ingest all AWS CloudTrail logs, VPC Flow Logs, and DNS logs into a single Amazon S3 bucket in a designated security accoun
G. Launch an Amazon EC2 instance and install the current SIEM to monitor the logs and send a notification to an Amazon SNS topic to alert the security team of remediation steps.
H. Enable Amazon GuardDuty and AWS Security Hub in all Regions and all account
I. Designate a master security account to receive all alerts from the child account
J. Create an AWS Organizations SCP that denies access to certain API calls that are on an ignore list.

Answer: A

NEW QUESTION 52
- (Exam Topic 1)
A company is using AWS Organizations to manage multiple AWS member accounts. All of these accounts have Amazon GuardDuty enabled in all Regions. The

company's AW5 Security Operations Center has a centralized security account for logging and monitoring. One of the member accounts has received an excessively high bill A security engineer discovers that a compromised Amazon EC2 instance is being used to mine crypto currency. The Security Operations Center did not receive a GuardDuty finding in the central security account.
but there was a GuardDuty finding in the account containing the compromised EC2 instance. The security engineer needs to ensure an GuardDuty finding are available in the security account.
What should the security engineer do to resolve this issue?

A. Set up an Amazon CloudWatch Event rule to forward ail GuardDuty findings to the security account Use an AWS Lambda function as a target to raise findings
B. Set up an Amazon CloudWatch Events rule to forward all GuardDuty findings to the security account Use an AWS Lambda function as a target to raise findings in AWS Security Hub
C. Check that GuardDuty in the security account is able to assume a role in the compromised account using the GuardDuty fast findings permission Schedule an Amazon CloudWatch Events rule and an AWS Lambda function to periodically check for GuardDuty findings
D. Use the aws GuardDuty get-members AWS CLI command m the security account to see if the account is listed Send an invitation from GuardDuty m the security account to GuardDuty in the compromised account Accept the invitation to forward all future GuardDuty findings

Answer: D

NEW QUESTION 57
- (Exam Topic 1)
A convoys data lake uses Amazon S3 and Amazon Athena. The company's security engineer has been asked to design an encryption solution that meets the company's data protection requirements. The encryption solution must work with Amazon S3 and keys managed by the company. The encryption solution must be protected in a hardware security module that is validated id Federal information Processing Standards (FPS) 140-2 Level 3.
Which solution meets these requirements?

A. Use client-side encryption with an AWS KMS customer-managed key implemented with the AWS Encryption SDK
B. Use AWS CloudHSM to store the keys and perform cryptographic operations Save the encrypted text inAmazon S3
C. Use an AWS KMS customer-managed key that is backed by a custom key store using AWS CloudHSM
D. Use an AWS KMS customer-managed key with the bring your own key (BYOK) feature to import a key stored in AWS CloudHSM

Answer: B

NEW QUESTION 62
- (Exam Topic 1)
A Security Engineer discovered a vulnerability in an application running on Amazon ECS. The vulnerability allowed attackers to install malicious code. Analysis of the code shows it exfiltrates data on port 5353 in batches at random time intervals.
While the code of the containers is being patched, how can Engineers quickly identify all compromised hosts and stop the egress of data on port 5353?

A. Enable AWS Shield Advanced and AWS WA
B. Configure an AWS WAF custom filter for egress traffic on port 5353
C. Enable Amazon Inspector on Amazon ECS and configure a custom assessment to evaluate containers that have port 5353 ope
D. Update the NACLs to block port 5353 outbound.
E. Create an Amazon CloudWatch custom metric on the VPC Flow Logs identifying egress traffic on port 5353. Update the NACLs to block port 5353 outbound.
F. Use Amazon Athena to query AWS CloudTrail logs in Amazon S3 and look for any traffic on port 5353. Update the security groups to block port 5353 outbound.

Answer: C

NEW QUESTION 66
- (Exam Topic 1)
A company is operating an open-source software platform that is internet facing. The legacy software platform no longer receives security updates. The software platform operates using Amazon route 53 weighted load balancing to send traffic to two Amazon EC2 instances that connect to an Amazon POS cluster a recent report suggests this software platform is vulnerable to SQL injection attacks. with samples of attacks provided. The company's security engineer must secure this system against SQL injection attacks within 24 hours. The secure, engineer's solution involve the least amount of effort and maintain normal operations during implementation.
What should the security engineer do to meet these requirements?

A. Create an Application Load Balancer with the existing EC2 instances as a target group Create an AWS WAF web ACL containing rules mat protect the application from this attac
B. then apply it to the ALB Test to ensure me vulnerability has been mitigated, then redirect thee Route 53 records to point to the ALB Update security groups on the EC 2 instances to prevent direct access from the internet
C. Create an Amazon CloudFront distribution specifying one EC2 instance as an origin Create an AWS WAF web ACL containing rules that protect the application from this attack, then apply it to me distribution Test to ensure the vulnerability has mitigated, then redirect the Route 53 records to point toCloudFront
D. Obtain me latest source code for the platform and make ire necessary updates Test me updated code to ensure that the vulnerability has been irrigated, then deploy me patched version of the platform to the EC2 instances
E. Update the security group mat is attached to the EC2 instances, removing access from the internet to the TCP port used by the SQL database Create an AWS WAF web ACL containing rules mat protect me application from this attack, men apply it to the EC2 instances Test to ensure me vulnerability has been mitigate
F. then restore the security group to me onginal setting

Answer: A

NEW QUESTION 67
- (Exam Topic 1)
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: ACD

NEW QUESTION 71
- (Exam Topic 1)
A company plans to use custom AMIs to launch Amazon EC2 instances across multiple AWS accounts in a single Region to perform security monitoring and analytics tasks. The EC2 instances are launched in EC2 Auto Scaling groups. To increase the security of the solution, a Security Engineer will manage the lifecycle of the custom AMIs in a centralized account and will encrypt them with a centrally managed AWS KMS CMK. The Security Engineer configured the KMS key policy to allow cross-account access. However, the EC2 instances are still not being properly launched by the EC2 Auto Scaling groups.
Which combination of configuration steps should the Security Engineer take to ensure the EC2 Auto Scaling groups have been granted the proper permissions to execute tasks?

A. Create a customer-managed CMK in the centralized accoun
B. Allow other applicable accounts to use that key for cryptographical operations by applying proper cross-account permissions in the key policy.Create an IAM role in all applicable accounts and configure its access policy to allow the use of the centrally managed CMK for cryptographical operation
C. Configure EC2 Auto Scaling groups within each applicable account to use the created IAM role to launch EC2 instances.
D. Create a customer-managed CMK in the centralized accoun
E. Allow other applicable accounts to use that key for cryptographical operations by applying proper cross-account permissions in the key polic
F. Create an IAM role in all applicable accounts and configure its access policy with permissions to create grants for the centrally managed CM
G. Use this IAM role to create a grant for the centrally managed CMK with permissions to perform cryptographical operations and with the EC2 Auto Scalingservice-linked role defined as the grantee principal.
H. Create a customer-managed CMK or an AWS managed CMK in the centralized accoun
I. Allow other applicable accounts to use that key for cryptographical operations by applying proper cross-account permissions in the key polic
J. Use the CMK administrator to create a CMK grant that includes permissions to perform cryptographical operations that define EC2 Auto Scaling service-linked roles from all other accounts as the grantee principal.
K. Create a customer-managed CMK or an AWS managed CMK in the centralized accoun
L. Allow other applicable accounts to use that key for cryptographical operations by applying proper cross-account permissions in the key polic
M. Modify the access policy for the EC2 Auto Scaling roles to perform cryptographical operations against the centrally managed CMK.

Answer: B

NEW QUESTION 75
- (Exam Topic 1)
A company uses SAML federation with AWS Identity and Access Management (IAM) to provide internal users with SSO for their AWS accounts. The company's identity provider certificate was rotated as part of its normal lifecycle. Shortly after, users started receiving the following error when attempting to log in:
"Error: Response Signature Invalid (Service: AWSSecuntyTokenService; Status Code: 400; Error Code: InvalidIdentltyToken)"
A security engineer needs to address the immediate issue and ensure that it will not occur again. Which combination of steps should the security engineer take to accomplish this? (Select TWO.)

A. Download a new copy of the SAML metadata file from the identity provider Create a new IAM identity provider entit
B. Upload the new metadata file to the new IAM identity provider entity.
C. During the next certificate rotation period and before the current certificate expires, add a new certificate as the secondary to the identity provide
D. Generate a new metadata file and upload it to the IAM identity provider entit
E. Perform automated or manual rotation of the certificate when required.
F. Download a new copy of the SAML metadata file from the identity provider Upload the new metadata to the IAM identity provider entity configured for the SAML integration in question.
G. During the next certificate rotation period and before the current certificate expires, add a new certificate as the secondary to the identity provide
H. Generate a new copy of the metadata file and create a new IAM identity provider entit
I. Upload the metadata file to the new IAM identity provider entit
J. Performautomated or manual rotation of the certificate when required.
K. Download a new copy of the SAML metadata file from the identity provider Create a new IAM identity provider entit
L. Upload the new metadata file to the new IAM identity provider entit
M. Update the identity provider configurations to pass a new IAM identity provider entity name in the SAML assertion.

Answer: AD

NEW QUESTION 78
- (Exam Topic 1)
A company is outsourcing its operational support 1o an external company. The company’s security officer must implement an access solution fen delegating operational support that minimizes overhead.
Which approach should the security officer take to meet these requirements?

A. implement Amazon Cognito identity pools with a role that uses a policy that denies the actions related to Amazon Cognito API management Allow the external company to federate through its identity provider
B. Federate AWS identity and Access Management (IAM) with the external company's identity provider Create an IAM role and attach a policy with the necessary permissions
C. Create an IAM group for me external company Add a policy to the group that denies IAM modifications Securely provide the credentials to the eternal company.
D. Use AWS SSO with the external company's identity provide
E. Create an IAM group to map to the identity provider user group, and attach a policy with the necessary permissions.

Answer: B

NEW QUESTION 83
- (Exam Topic 1)
A company has an application hosted in an Amazon EC2 instance and wants the application to access secure strings stored in AWS Systems Manager Parameter Store When the application tries to access the secure string key value, it fails.
Which factors could be the cause of this failure? (Select TWO.)

A. The EC2 instance role does not have decrypt permissions on the AWS Key Management Sen/ice (AWS KMS) key used to encrypt the secret
B. The EC2 instance role does not have read permissions to read the parameters In Parameter Store

C. Parameter Store does not have permission to use AWS Key Management Service (AWS KMS) to decrypt the parameter
D. The EC2 instance role does not have encrypt permissions on the AWS Key Management Service (AWS KMS) key associated with the secret
E. The EC2 instance does not have any tags associated.

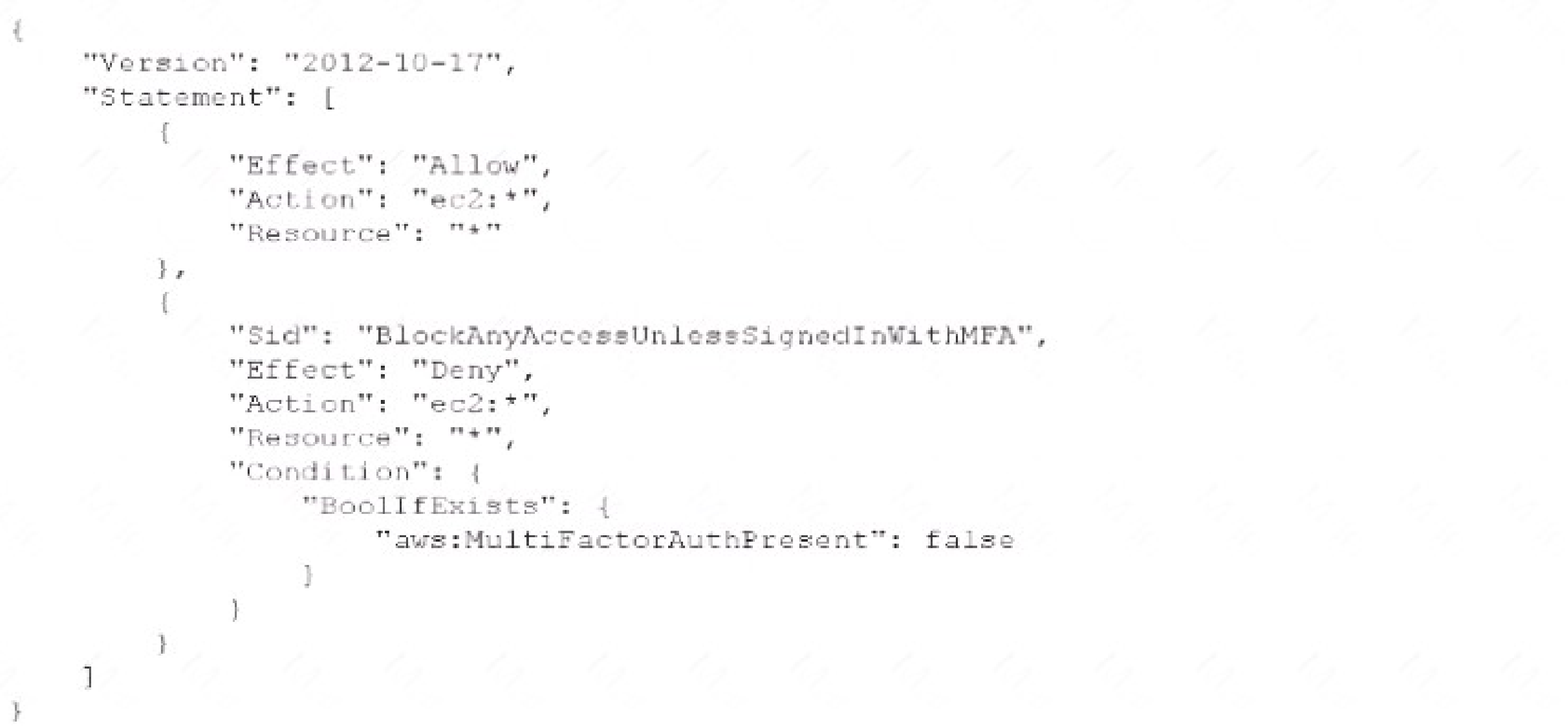
Answer: CE

NEW QUESTION 86
- (Exam Topic 1)
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

NEW QUESTION 88
- (Exam Topic 1)
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 policy Instruct users to run the sts assume-role CLI command and pass --serial-number and —token-code parameters Store the resulting values in environment variable
F. Add sts:AssumeRole to NotAction in the policy.

Answer: B

NEW QUESTION 90
- (Exam Topic 1)
A company's architecture requires that its three Amazon EC2 instances run behind an Application Load Balancer (ALB). The EC2 instances transmit sensitive data between each other Developers use SSL certificates to encrypt the traffic between the public users and the ALB However the Developers are unsure of how to encrypt the data in transit between the ALB and the EC2 instances and the traffic between the EC2 instances
Which combination of activities must the company implement to meet its encryption requirements'? (Select TWO)

A. Configure SSLTLS on the EC2 instances and configure the ALB target group to use HTTPS
B. Ensure that all resources are in the same VPC so the default encryption provided by the VPC is used to encrypt the traffic between the EC2 instances.
C. In the AL
D. select the default encryption to encrypt the traffic between the ALB and the EC2 instances
E. In the code for the application, include a cryptography library and encrypt the data before sending it between the EC2 instances
F. Configure AWS Direct Connect to provide an encrypted tunnel between the EC2 instances

Answer: BC

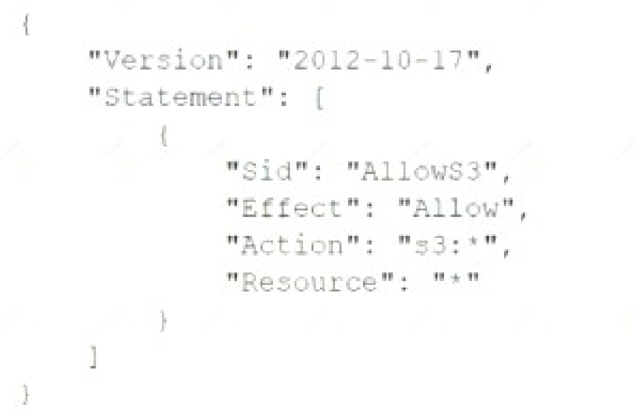
NEW QUESTION 91
- (Exam Topic 1)
A Security Engineer for a large company is managing a data processing application used by 1,500 subsidiary companies. The parent and subsidiary companies all

use AWS. The application uses TCP port 443 and runs on Amazon EC2 behind a Network Load Balancer (NLB). For compliance reasons, the application should only be accessible to the subsidiaries and should not be available on the public internet. To meet the compliance requirements for restricted access, the Engineer has received the public and private CIDR block ranges for each subsidiary
What solution should the Engineer use to implement the appropriate access restrictions for the application?

A. Create a NACL to allow access on TCP port 443 from the 1;500 subsidiary CIDR block ranges.Associate the NACL to both the NLB and EC2 instances
B. Create an AWS security group to allow access on TCP port 443 from the 1,500 subsidiary CIDR block range
C. Associate the security group to the NL
D. Create a second security group for EC2 instances with access on TCP port 443 from the NLB security group.
E. Create an AWS PrivateLink endpoint service in the parent company account attached to the NL
F. Create an AWS security group for the instances to allow access on TCP port 443 from the AWS PrivateLink endpoin
G. Use AWS PrivateLink interface endpoints in the 1,500 subsidiary AWS accounts to connect to the data processing application.
H. Create an AWS security group to allow access on TCP port 443 from the 1,500 subsidiary CIDR block range
I. Associate the security group with EC2 instances.

Answer: D

NEW QUESTION 93
- (Exam Topic 1)
A Security Engineer manages AWS Organizations for a company. The Engineer would like to restrict AWS usage to allow Amazon S3 only in one of the organizational units (OUs). The Engineer adds the following SCP to the OU:



```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowS3",
            "Effect": "Allow",
            "Action": "s3:*",
            "Resource": "*"
        }
    ]
}
```

The next day. API calls to AWS IAM appear in AWS CloudTrail logs In an account under that OU. How should the Security Engineer resolve this issue?

A. Move the account to a new OU and deny IAM:* permissions.
B. Add a Deny policy for all non-S3 services at the account level.
C. Change the policy to:{“Version”: “2012-10-17”,“Statement”: [{“Sid”: “AllowS3”,"Effect": "Allow","Action": "s3:*","Resource": "*/*»}]}
D. Detach the default FullAWSAccess SCP

Answer: C

NEW QUESTION 96
- (Exam Topic 1)
A company is collecting AWS CloudTrail log data from multiple AWS accounts by managing individual trails in each account and forwarding log data to a centralized Amazon S3 bucket residing in a log archive account. After CloudTrail introduced support for AWS Organizations trails, the company decided to further centralize management and automate deployment of the CloudTrail logging capability across all of its AWS accounts.
The company's security engineer created an AWS Organizations trail in the master account, enabled
server-side encryption with AWS KMS managed keys (SSE-KMS) for the log files, and specified the same bucket as the storage location. However, the engineer noticed that logs recorded by the new trail were not delivered to the bucket.
Which factors could cause this issue? (Select TWO.)

A. The CMK key policy does not allow CloudTrail to make encrypt and decrypt API calls against the key.
B. The CMK key policy does not allow CloudTrail to make GenerateDataKey API calls against the key.
C. The IAM role used by the CloudTrail trail does not have permissions to make PutObject API calls against a folder created for the Organizations trail.
D. The S3 bucket policy does not allow CloudTrail to make PutObject API calls against a folder created for the Organizations trail.
E. The CMK key policy does not allow the IAM role used by the CloudTrail trail to use the key for crypto graphical operations.

Answer: AD

NEW QUESTION 100
- (Exam Topic 1)
A company’s security engineer is configuring Amazon S3 permissions to ban all current and future public buckets However, the company hosts several websites directly off S3 buckets with public access enabled
The engineer needs to bock me pubic S3 buckets without causing any outages on me easting websites The
engineer has set up an Amazon CloudFrom distribution (or each website Which set or steps should the security engineer implement next?

A. Configure an S3 bucket as the origin an origin access identity (OAI) for the CloudFront distribution Switch the DNS records from websites to point to the CloudFront distribution Enable Nock public access settings at the account level
B. Configure an S3 bucket as the origin with an origin access identity (OAI) for the CloudFront distribution Switch the ONS records tor the websites to point to the CloudFront disinfection Then, tor each S3 bucket enable block public access settings
C. Configure an S3 bucket as the origin with an origin access identity (OAI) for the CloudFront distribution Enable block public access settings at the account level
D. Configure an S3 bucket as the origin for me CloudFront distribution Configure the S3 bucket policy to accept connections from the CloudFront points of presence only Switch the DNS records for the websites to point to the CloudFront distribution Enable block public access settings at me account level

Answer: A

NEW QUESTION 103

- (Exam Topic 1)
A company has recently recovered from a security incident that required the restoration of Amazon EC2 instances from snapshots.
After performing a gap analysis of its disaster recovery procedures and backup strategies, the company is concerned that, next time, it will not be able to recover the EC2 instances if the AWS account was compromised and Amazon EBS snapshots were deleted.
All EBS snapshots are encrypted using an AWS KMS CMK. Which solution would solve this problem?

A. Create a new Amazon S3 bucket Use EBS lifecycle policies to move EBS snapshots to the new S3 bucke
B. Move snapshots to Amazon S3 Glacier using lifecycle policies, and apply Glacier Vault Lock policies to prevent deletion
C. Use AWS Systems Manager to distribute a configuration that performs local backups of all attached disks to Amazon S3.
D. Create a new AWS account with limited privilege
E. Allow the new account to access the AWS KMS key used to encrypt the EBS snapshots, and copy the encrypted snapshots to the new account on a recuning basis
F. Use AWS Backup to copy EBS snapshots to Amazon S3.

Answer: A

NEW QUESTION 108
- (Exam Topic 1)
A developer is creating an AWS Lambda function that requires environment variables to store connection information and logging settings. The developer is required to use an AWS KMS Customer Master Key (CMK> supplied by the information security department in order to adhere to company standards for securing Lambda environment variables.
Which of the following are required for this configuration to work? (Select TWO.)

A. The developer must configure Lambda access to the VPC using the --vpc-config parameter.
B. The Lambda function execution role must have the kms:Decrypt- permission added in the AWS IAM policy.
C. The KMS key policy must allow permissions for the developer to use the KMS key.
D. The AWS IAM policy assigned to the developer must have the kmseGcnerate-DataKcy permission added.
E. The Lambda execution role must have the kms:Encrypt permission added in the AWS IAM policy.

Answer: BC

NEW QUESTION 111
- (Exam Topic 1)
A security engineer need to ensure their company’s uses of AWS meets AWS security best practices. As part of this, the AWS account root user must not be used for daily work. The root user must be monitored for use, and the Security team must be alerted as quickly as possible if the root user is used. Which solution meets these requirements?

A. Set up an Amazon CloudWatch Events rule that triggers an Amazon SNS notification.
B. Set up an Amazon CloudWatch Events rule that triggers an Amazon SNS notification logs from S3 and generate notifications using Amazon SNS.
C. Set up a rule in AWS config to trigger root user event
D. Trigger an AWS Lambda function and generate notifications using Amazon SNS.
E. Use Amazon Inspector to monitor the usage of the root user and generate notifications using Amazon SNS

Answer: A

NEW QUESTION 112
- (Exam Topic 1)
A security engineer is designing a solution that will provide end-to-end encryption between clients and Docker containers running In Amazon Elastic Container Service (Amazon ECS). This solution will also handle volatile traffic patterns
Which solution would have the MOST scalability and LOWEST latency?

A. Configure a Network Load Balancer to terminate the TLS traffic and then re-encrypt the traffic to the containers
B. Configure an Application Load Balancer to terminate the TLS traffic and then re-encrypt the traffic to the containers
C. Configure a Network Load Balancer with a TCP listener to pass through TLS traffic to the containers
D. Configure Amazon Route 53 to use multivalue answer routing to send traffic to the containers

Answer: A

NEW QUESTION 115
- (Exam Topic 1)
An external Auditor finds that a company's user passwords have no minimum length. The company is currently using two identity providers:
• AWS IAM federated with on-premises Active Directory
• Amazon Cognito user pools to accessing an AWS Cloud application developed by the company Which combination o1 actions should the Security Engineer take to solve this issue? (Select TWO.)

A. Update the password length policy In the on-premises Active Directory configuration.
B. Update the password length policy In the IAM configuration.
C. Enforce an IAM policy In Amazon Cognito and AWS IAM with a minimum password length condition.
D. Update the password length policy in the Amazon Cognito configuration.
E. Create an SCP with AWS Organizations that enforces a minimum password length for AWS IAM and Amazon Cognito.

Answer: AD

NEW QUESTION 116
- (Exam Topic 1)
A company's application runs on Amazon EC2 and stores data in an Amazon S3 bucket The company wants additional security controls in place to limit the likelihood of accidental exposure of data to external parties
Which combination of actions will meet this requirement? (Select THREE.)

A. Encrypt the data in Amazon S3 using server-side encryption with Amazon S3 managed encryption keys (SSE-S3)
B. Encrypt the data in Amazon S3 using server-side encryption with AWS KMS managed encryption keys (SSE-KMS)
C. Create a new Amazon S3 VPC endpoint and modify the VPC's routing tables to use the new endpoint
D. Use the Amazon S3 Block Public Access feature.
E. Configure the bucket policy to allow access from the application instances only
F. Use a NACL to filter traffic to Amazon S3

Answer: BCE

NEW QUESTION 118
- (Exam Topic 1)
A company has a serverless application for internal users deployed on AWS. The application uses AWS Lambda for the front end and for business logic. The Lambda function accesses an Amazon RDS database inside a VPC The company uses AWS Systems Manager Parameter Store for storing database credentials. A recent security review highlighted the following issues

- The Lambda function has internet access.
- The relational database is publicly accessible.
- The database credentials are not stored in an encrypted state.

Which combination of steps should the company take to resolve these security issues? (Select THREE)

A. Disable public access to the RDS database inside the VPC
B. Move all the Lambda functions inside the VPC.
C. Edit the IAM role used by Lambda to restrict internet access.
D. Create a VPC endpoint for Systems Manage
E. Store the credentials as a string paramete
F. Change the parameter type to an advanced parameter.
G. Edit the IAM role used by RDS to restrict internet access.
H. Create a VPC endpoint for Systems Manage
I. Store the credentials as a SecureString parameter.

Answer: ABE

NEW QUESTION 122
- (Exam Topic 1)
A company Is building a data lake on Amazon S3. The data consists of millions of small files containing sensitive information. The security team has the following requirements for the architecture:
• Data must be encrypted in transit.
• Data must be encrypted at rest.
• The bucket must be private, but if the bucket is accidentally made public, the data must remain confidential. Which combination of steps would meet the requirements? (Select THREE.)

A. Enable AES-256 encryption using server-side encryption with Amazon S3-managed encryption keys (SSE-S3) on the S3 bucket
B. Enable default encryption with server-side encryption with AWS KMS-managed keys (SSE-KMS) on the S3 bucket.
C. Add a bucket policy that includes a deny if a PutObject request does not include awsiSecureTcanspoct.
D. Add a bucket policy with ws: Sourcelpto Allow uploads and downloads from the corporate intranet only.
E. Add a bucket policy that includes a deny if a PutObject request does not include s3:x-amz-sairv9r-side-enctyption: "aws: kms".
F. Enable Amazon Macie to monitor and act on changes to the data lake's S3 bucket.

Answer: BDF

NEW QUESTION 123
- (Exam Topic 1)
A company has implemented centralized logging and monitoring of AWS CloudTrail logs from all Regions in
an Amazon S3 bucket. The log Hies are encrypted using AWS KMS. A Security Engineer is attempting to review the log files using a third-party tool hosted on an Amazon EC2 instance The Security Engineer is unable to access the logs in the S3 bucket and receives an access denied error message
What should the Security Engineer do to fix this issue?

A. Check that the role the Security Engineer uses grants permission to decrypt objects using the KMS CMK.
B. Check that the role the Security Engineer uses grants permission to decrypt objects using the KMS CMK and gives access to the S3 bucket and objects
C. Check that the role the EC2 instance profile uses grants permission lo decrypt objects using the KMS CMK and gives access to the S3 bucket and objects
D. Check that the role the EC2 instance profile uses grants permission to decrypt objects using the KMS CMK

Answer: C

NEW QUESTION 127
- (Exam Topic 1)
A company is designing the securely architecture (or a global latency-sensitive web application it plans to deploy to AWS. A Security Engineer needs to configure a highly available and secure two-tier architecture. The security design must include controls to prevent common attacks such as DDoS, cross-site scripting, and SQL injection.
Which solution meets these requirements?

A. Create an Application Load Balancer (ALB) that uses public subnets across multiple Availability Zones within a single Regio
B. Point the ALB to an Auto Scaling group with Amazon EC2 instances in private subnets across multiple Availability Zones within the same Regio
C. Create an AmazonCloudFront distribution that uses the ALB as its origi
D. Create appropriate AWS WAF ACLs and enable them on the CloudFront distribution.
E. Create an Application Load Balancer (ALB) that uses private subnets across multiple Availability Zones within a single Regio
F. Point the ALB to an Auto Scaling group with Amazon EC2 instances in private subnets across multiple Availability Zones within the same Regio
G. Create an Amazon CloudFront distribution that uses the ALB as its origi
H. Create appropriate AWS WAF ACLs and enable them on the CloudFront distribution.

I. Create an Application Load Balancer (ALB) that uses public subnets across multiple Availability Zones within a single Regio
J. Point the ALB to an Auto Scaling group with Amazon EC2 instances in private subnets across multiple Availability Zones within the same Regio
K. Create appropriate AWS WAF ACLs and enable them on the ALB.
L. Create an Application Load Balancer (ALB) that uses private subnets across multiple Availability Zones within a single Regio
M. Point the ALB to an Auto Scaling group with Amazon EC2 instances in private subnets across multiple Availability Zones within the same Regio
N. Create appropriate AWS WAF ACLs and enable them on the ALB.

Answer: A

NEW QUESTION 130
- (Exam Topic 1)
A security engineer has been tasked with implementing a solution that allows the company's development team to have interactive command line access to Amazon EC2 Linux instances using the AWS Management Console.
Which steps should the security engineer take to satisfy this requirement while maintaining least privilege?

A. Enable AWS Systems Manager in the AWS Management Console and configure for access to EC2 instances using the default AmazonEC2RoleforSSM rol
B. Install the Systems Manager Agent on all EC2 Linux instances that need interactive acces
C. Configure IAM user policies to allow development team access to the Systems Manager Session Manager and attach to the team's IAM users.
D. Enable console SSH access in the EC2 consol
E. Configure IAM user policies to allow development team access to the AWS Systems Manager Session Manager and attach to the development team's IAM users.
F. Enable AWS Systems Manager in the AWS Management Console and configure to access EC2 instances using the default AmazonEC2RoleforSSM rol
G. Install the Systems Manager Agent on all EC2 Linux instances that need interactive acces
H. Configure a security group that allows SSH port 22 from all published IP addresse
I. Configure IAM user policies to allow development team access to the AWS Systems Manager Session Manager and attach to the team's IAM users.
J. Enable AWS Systems Manager in the AWS Management Console and configure to access EC2 instances using the default AmazonEC2RoleforSSM role Install the Systems Manager Agent on all EC2 Linux instances that need interactive acces
K. Configure IAM policies to allow development team access to the EC2 console and attach to the teams IAM users.

Answer: A

NEW QUESTION 132
- (Exam Topic 1)
A Developer reported that AWS CloudTrail was disabled on their account. A Security Engineer investigated the account and discovered the event was undetected by the current security solution. The Security Engineer must recommend a solution that will detect future changes to the CloudTrail configuration and send alerts when changes occur.
What should the Security Engineer do to meet these requirements?

A. Use AWS Resource Access Manager (AWS RAM) to monitor the AWS CloudTrail configuratio
B. Send notifications using Amazon SNS.
C. Create an Amazon CloudWatch Events rule to monitor Amazon GuardDuty finding
D. Send email notifications using Amazon SNS.
E. Update security contact details in AWS account settings for AWS Support to send alerts when suspicious activity is detected.
F. Use Amazon Inspector to automatically detect security issue
G. Send alerts using Amazon SNS.

Answer: B

NEW QUESTION 135
- (Exam Topic 1)
A company hosts its public website on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances are in an EC2 Auto Scaling group across multiple Availability Zones. The website is under a DDoS attack by a specific loT device brand that is visible in the user agent A security engineer needs to mitigate the attack without impacting the availability of the public website.
What should the security engineer do to accomplish this?

A. Configure a web ACL rule for AWS WAF to block requests with a string match condition for the user agent of the loT devic
B. Associate the v/eb ACL with the ALB.
C. Configure an Amazon CloudFront distribution to use the ALB as an origi
D. Configure a web ACL rule for AWS WAF to block requests with a string match condition for the user agent of the loT devic
E. Associate the web ACL with the ALB Change the public DNS entry of the website to point to the CloudFront distribution.
F. Configure an Amazon CloudFront distribution to use a new ALB as an origi
G. Configure a web ACL rule for AWS WAF to block requests with a string match condition for the user agent of the loT devic
H. Change the ALB security group to alow access from CloudFront IP address ranges only Change the public DNS entry of the website to point to the CloudFront distribution.
I. Activate AWS Shield Advanced to enable DDoS protectio
J. Apply an AWS WAF ACL to the AL
K. and configure a listener rule on the ALB to block loT devices based on the user agent.

Answer: D

NEW QUESTION 138
- (Exam Topic 1)
A city is implementing an election results reporting website that will use Amazon GoudFront The website runs on a fleet of Amazon EC2 instances behind an Application Load Balancer (ALB) in an Auto Scaling group. Election results are updated hourly and are stored as .pdf tiles in an Amazon S3 bucket. A Security Engineer needs to ensure that all external access to the website goes through CloudFront.
Which solution meets these requirements?

A. Create an IAM role that allows CloudFront to access the specific S3 bucke
B. Modify the S3 bucket policy to allow only the new IAM role to access its content

C. Create an interface VPC endpoint for CloudFront to securely communicate with the ALB.
D. Create an IAM role that allows CloudFront to access the specific S3 bucke
E. Modify the S3 bucket policy to allow only the new IAM role to access its content
F. Associate the ALB with a security group that allows only incoming traffic from the CloudFront service to communicate with the ALB.
G. Create an origin access identity (OAI) in CloudFron
H. Modify the S3 bucket policy to allow only the new OAI to access the bucket content
I. Create an interface VPC endpoint for CloudFront to securely communicate with the ALB.
J. Create an origin access identity (OAI) in CloudFron
K. Modify the S3 bucket policy to allow only the new OAI to access the bucket content
L. Associate the ALB with a security group that allows onlyincoming traffic from the CloudFront service to communicate with the ALB.

Answer: C

NEW QUESTION 141
- (Exam Topic 1)
A company's Developers plan to migrate their on-premises applications to Amazon EC2 instances running Amazon Linux AMIs. The applications are accessed by a group of partner companies The Security Engineer needs to implement the following host-based security measures for these instances:
• Block traffic from documented known bad IP addresses
• Detect known software vulnerabilities and CIS Benchmarks compliance. Which solution addresses these requirements?

A. Launch the EC2 instances with an IAM role attache
B. Include a user data script that uses the AWS CLI to retrieve the list of bad IP addresses from AWS Secrets Manager and uploads it as a threat list in Amazon GuardDuty Use Amazon Inspector to scan the instances for known software vulnerabilities and CIS Benchmarks compliance
C. Launch the EC2 instances with an IAM role attached Include a user data script that uses the AWS CLl to create NACLs blocking ingress traffic from the known bad IP addresses in the EC2 instance's subnets Use AWS Systems Manager to scan the instances for known software vulnerabilities, and AWS Trusted Advisor to check instances for CIS Benchmarks compliance
D. Launch the EC2 instances with an IAM role attached Include a user data script that uses the AWS CLl to create and attach security groups that only allow an allow listed source IP address range inboun
E. Use Amazon Inspector to scan the instances for known software vulnerabilities, and AWS Trusted Advisor to check instances for CIS Benchmarks compliance
F. Launch the EC2 instances with an IAM role attached Include a user data script that creates a cron job to periodically retrieve the list of bad IP addresses from Amazon S3, and configures iptabies on the instances blocking the list of bad IP addresses Use Amazon inspector to scan the instances for known software vulnerabilities and CIS Benchmarks compliance.

Answer: D

NEW QUESTION 145
- (Exam Topic 1)
A Web Administrator for the website example.com has created an Amazon CloudFront distribution for dev.example.com, with a requirement to configure HTTPS using a custom TLS certificate imported to AWS Certificate Manager.
Which combination of steps is required to ensure availability of the certificate in the CloudFront console? (Choose two.)

A. Call UploadServerCertificate with /cloudfront/dev/ in the path parameter.
B. Import the certificate with a 4,096-bit RSA public key.
C. Ensure that the certificate, private key, and certificate chain are PKCS #12-encoded.
D. Import the certificate in the us-east-1 (
E. Virginia) Region.
F. Ensure that the certificate, private key, and certificate chain are PEM-encoded.

Answer: DE

NEW QUESTION 149
- (Exam Topic 1)
A Security Engineer creates an Amazon S3 bucket policy that denies access to all users. A few days later, the Security Engineer adds an additional statement to the bucket policy to allow read-only access to one other employee Even after updating the policy the employee still receives an access denied message.
What is the likely cause of this access denial?

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

Answer: D

NEW QUESTION 150
- (Exam Topic 1)
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. Operating system-native encryption that uses GnuPG

Answer: B

NEW QUESTION 151
- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 152
- (Exam Topic 1)
A company hosts a web-based application that captures and stores sensitive data in an Amazon DynamoDB table. A security audit reveals that the application does not provide end-to-end data protection or the ability to detect unauthorized data changes The software engineering team needs to make changes that will address the audit findings.
Which set of steps should the software engineering team take?

A. Use an AWS Key Management Service (AWS KMS) CM
B. Encrypt the data at rest.
C. Use AWS Certificate Manager (ACM) Private Certificate Authority Encrypt the data in transit.
D. Use a DynamoDB encryption clien
E. Use client-side encryption and sign the table items
F. Use the AWS Encryption SD
G. Use client-side encryption and sign the table items.

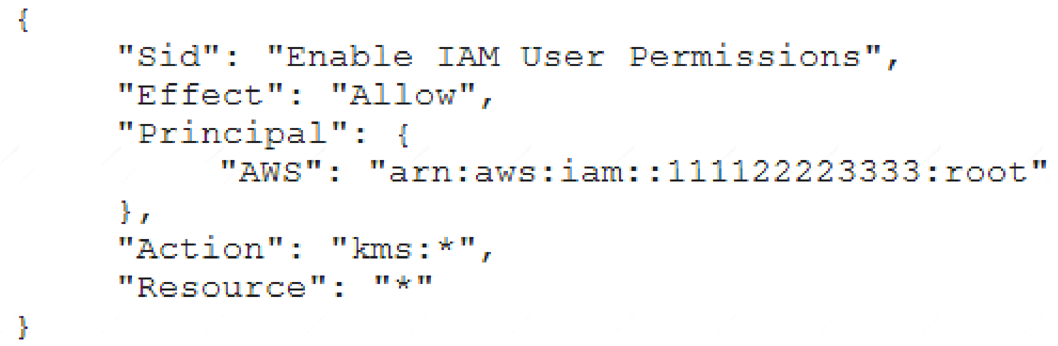
Answer: A

NEW QUESTION 154
- (Exam Topic 1)
A company's security information events management (SIEM) tool receives new AWS CloudTrail logs from an Amazon S3 bucket that is configured to send all object created event notification to an Amazon SNS topic An Amazon SQS queue is subscribed to this SNS topic. The company's SEM tool then ports this SQS queue for new messages using an IAM role and fetches new log events from the S3 bucket based on the SQS messages.
After a recent security review that resulted m restricted permissions, the SEM tool has stopped receiving new CloudTral logs
Which of the following are possible causes of this issue? (Select THREE)

A. The SOS queue does not allow the SQS SendMessage action from the SNS topic
B. The SNS topic does not allow the SNS Publish action from Amazon S3
C. The SNS topic is not delivering raw messages to the SQS queue
D. The S3 bucket policy does not allow CloudTrail to perform the PutObject action
E. The IAM role used by the 5EM tool does not have permission to subscribe to the SNS topic
F. The IAM role used by the SEM tool does not allow the SQS DeleteMessage actio

Answer: ADF

NEW QUESTION 159
- (Exam Topic 2)
A Security Engineer who was reviewing AWS Key Management Service (AWS KMS) key policies found this statement in each key policy in the company AWS account.



```
{
      "Sid": "Enable IAM User Permissions",
      "Effect": "Allow",
      "Principal": {
           "AWS": "arn:aws:iam::111122223333:root"
      },
      "Action": "kms:*",
      "Resource": "*"
}
```

What does the statement allow?

A. All principals from all AWS accounts to use the key.
B. Only the root user from account 111122223333 to use the key.
C. All principals from account 111122223333 to use the key but only on Amazon S3.
D. Only principals from account 111122223333 that have an IAM policy applied that grants access to this key to use the key.

Answer: D

NEW QUESTION 161
- (Exam Topic 2)
A Software Engineer wrote a customized reporting service that will run on a fleet of Amazon EC2 instances. The company security policy states that application logs for the reporting service must be centrally collected.
What is the MOST efficient way to meet these requirements?

A. Write an AWS Lambda function that logs into the EC2 instance to pull the application logs from the EC2 instance and persists them into an Amazon S3 bucket.
B. Enable AWS CloudTrail logging for the AWS account, create a new Amazon S3 bucket, and then configure Amazon CloudWatch Logs to receive the application logs from CloudTrail.
C. Create a simple cron job on the EC2 instances that synchronizes the application logs to an Amazon S3 bucket by using rsync.

D. Install the Amazon CloudWatch Logs Agent on the EC2 instances, and configure it to send the application logs to CloudWatch Logs.

Answer: D

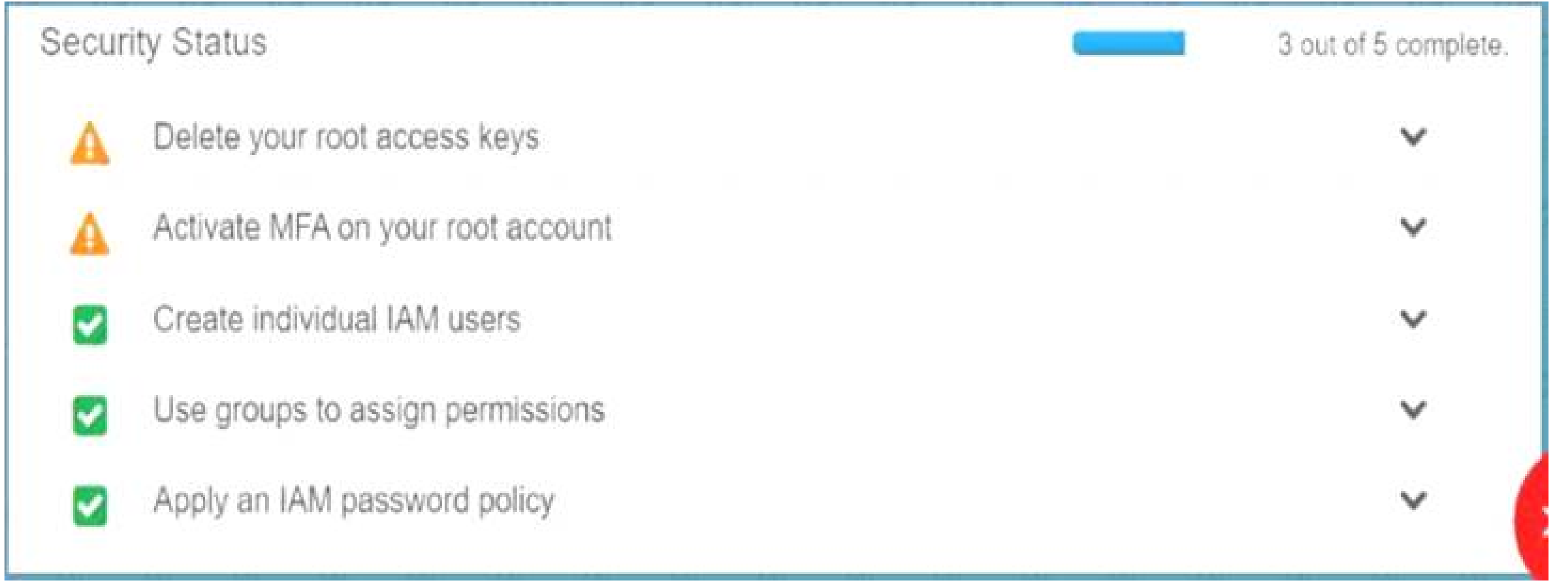
Explanation:
https://aws.amazon.com/blogs/aws/cloudwatch-log-service/

NEW QUESTION 166
- (Exam Topic 2)
Your development team has started using AWS resources for development purposes. The AWS account has just been created. Your IT Security team is worried about possible leakage of AWS keys. What is the first level of measure that should be taken to protect the AWS account.
Please select:

A. Delete the AWS keys for the root account
B. Create IAM Groups
C. Create IAM Roles
D. Restrict access using IAM policies

Answer: A

Explanation:
The first level or measure that should be taken is to delete the keys for the IAM root user
When you log into your account and go to your Security Access dashboard, this is the first step that can be seen
C:\Users\wk\Desktop\mudassar\Untitled.jpg



Security Status

3 out of 5 complete.

- ⚠ Delete your root access keys
- ⚠ Activate MFA on your root account
- ✓ Create individual IAM users
- ✓ Use groups to assign permissions
- ✓ Apply an IAM password policy

Option B and C are wrong because creation of IAM groups and roles will not change the impact of leakage of AWS root access keys
Option D is wrong because the first key aspect is to protect the access keys for the root account For more information on best practises for Security Access keys, please visit the below URL:
https://docs.aws.amazon.com/eeneral/latest/gr/aws-access-keys-best-practices.html
The correct answer is: Delete the AWS keys for the root account Submit your Feedback/Queries to our Experts

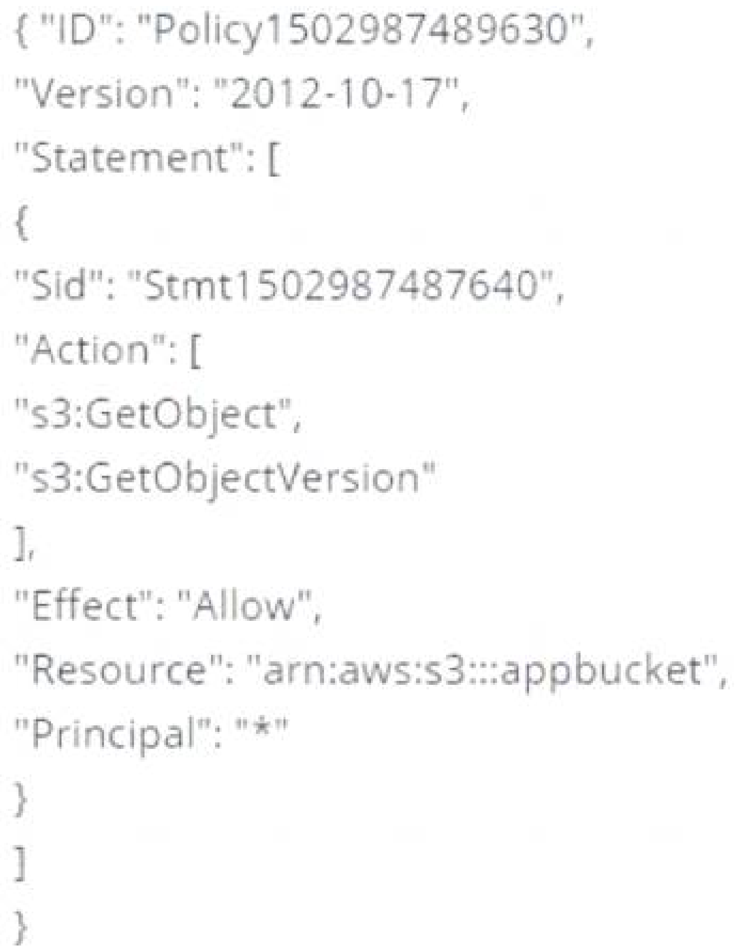
NEW QUESTION 168
- (Exam Topic 2)
You have a web site that is sitting behind AWS Cloudfront. You need to protect the web site against threats such as SQL injection and Cross site scripting attacks. Which of the following service can help in such a scenario
Please select:

A. AWS Trusted Advisor
B. AWS WAF
C. AWS Inspector
D. AWS Config

Answer: B

Explanation:
The AWS Documentation mentions the following
AWS WAF is a web application firewall that helps detect and block malicious web requests targeted at your web applications. AWS WAF allows you to create rules that can help protect against common web exploits like SQL injection and cross-site scripting. With AWS WAF you first identify the resource (either an Amazon CloudFront distribution or an Application Load Balancer) that you need to protect.
Option A is invalid because this will only give advise on how you can better the security in your AWS account but not protect against threats mentioned in the question.
Option C is invalid because this can be used to scan EC2 Instances for vulnerabilities but not protect against threats mentioned in the question.
Option D is invalid because this can be used to check config changes but not protect against threats mentioned in the quest
For more information on AWS WAF, please visit the following URL: https://aws.amazon.com/waf/details;
The correct answer is: AWS WAF
Submit your Feedback/Queries to our Experts

NEW QUESTION 172
- (Exam Topic 2)
You are deivising a policy to allow users to have the ability to access objects in a bucket called appbucket. You define the below custom bucket policy



```
{ "ID": "Policy1502987489630",
"Version": "2012-10-17",
"Statement": [
{
"Sid": "Stmt1502987487640",
"Action": [
"s3:GetObject",
"s3:GetObjectVersion"
],
"Effect": "Allow",
"Resource": "arn:aws:s3:::appbucket",
"Principal": "*"
}
]
}
```

But when you try to apply the policy you get the error "Action does not apply to any resource(s) in statement." What should be done to rectify the error
Please select:

A. Change the IAM permissions by applying PutBucketPolicy permissions.
B. Verify that the policy has the same name as the bucket nam
C. If no
D. make it the same.
E. Change the Resource section to "arn:aws:s3:::appbucket/*'.
F. Create the bucket "appbucket" and then apply the policy.

Answer: C

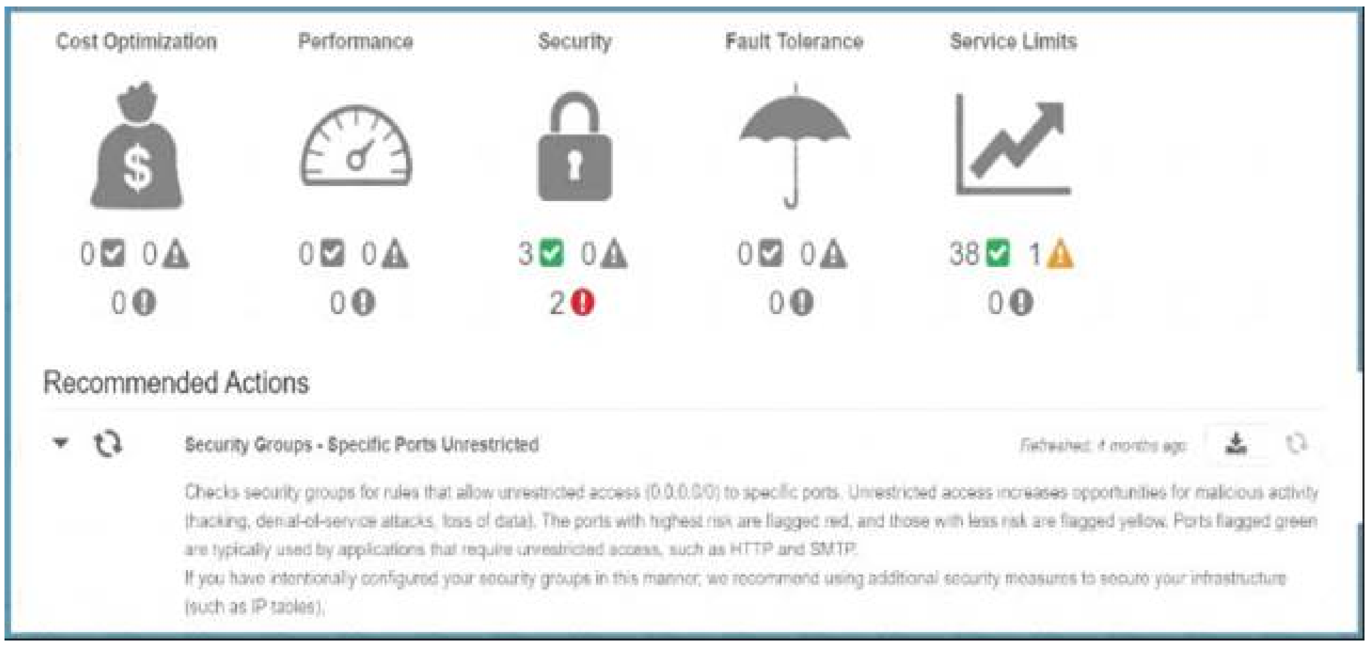
Explanation:
When you define access to objects in a bucket you need to ensure that you specify to which objects in the bucket access needs to be given to. In this case, the * can be used to assign the permission to all objects in the bucket
Option A is invalid because the right permissions are already provided as per the question requirement Option B is invalid because it is not necessary that the policy has the same name as the bucket
Option D is invalid because this should be the default flow for applying the policy For more information on bucket policies please visit the below URL: https://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies.htmll
The correct answer is: Change the Resource section to "arn:aws:s3:::appbucket/" Submit your Feedback/Queries to our Experts

NEW QUESTION 174
- (Exam Topic 2)
Your company has defined a number of EC2 Instances over a period of 6 months. They want to know if any of the security groups allow unrestricted access to a resource. What is the best option to accomplish this requirement?
Please select:

A. Use AWS Inspector to inspect all the security Groups
B. Use the AWS Trusted Advisor to see which security groups have compromised access.
C. Use AWS Config to see which security groups have compromised access.
D. Use the AWS CLI to query the security groups and then filter for the rules which have unrestricted accessd

Answer: B

Explanation:
The AWS Trusted Advisor can check security groups for rules that allow unrestricted access to a resource. Unrestricted access increases opportunities for malicious activity (hacking, denial-of-service attacks, loss of data).
If you go to AWS Trusted Advisor, you can see the details C:\Users\wk\Desktop\mudassar\Untitled.jpg



Recommended Actions

Security Groups - Specific Ports Unrestricted

Refreshed: 4 months ago

Checks security groups for rules that allow unrestricted access (0.0.0.0/0) to specific ports. Unrestricted access increases opportunities for malicious activity (hacking, denial-of-service attacks, loss of data). The ports with highest risk are flagged red, and those with less risk are flagged yellow. Ports flagged green are typically used by applications that require unrestricted access, such as HTTP and SMTP.

If you have intentionally configured your security groups in this manner, we recommend using additional security measures to secure your infrastructure (such as IP tables).

Option A is invalid because AWS Inspector is used to detect security vulnerabilities in instances and not for security groups.
Option C is invalid because this can be used to detect changes in security groups but not show you security groups that have compromised access.
Option Dis partially valid but would just be a maintenance overhead
For more information on the AWS Trusted Advisor, please visit the below URL: https://aws.amazon.com/premiumsupport/trustedadvisor/best-practices;
The correct answer is: Use the AWS Trusted Advisor to see which security groups have compromised access. Submit your Feedback/Queries to our Experts

NEW QUESTION 179
- (Exam Topic 2)
A company's security policy requires that VPC Flow Logs are enabled on all VPCs. A Security Engineer is looking to automate the process of auditing the VPC resources for compliance.
What combination of actions should the Engineer take? (Choose two.)

A. Create an AWS Lambda function that determines whether Flow Logs are enabled for a given VPC.
B. Create an AWS Config configuration item for each VPC in the company AWS account.
C. Create an AWS Config managed rule with a resource type of AWS:: Lambda:: Function.
D. Create an Amazon CloudWatch Event rule that triggers on events emitted by AWS Config.
E. Create an AWS Config custom rule, and associate it with an AWS Lambda function that contains the evaluating logic.

Answer: AE

Explanation:
https://medium.com/mudita-misra/how-to-audit-your-aws-resources-for-security-compliance-by-using-custom-a

NEW QUESTION 181
- (Exam Topic 2)
A company will store sensitive documents in three Amazon S3 buckets based on a data classification scheme of "Sensitive," "Confidential," and "Restricted."
The security solution must meet all of the following requirements:
- Each object must be encrypted using a unique key.
- Items that are stored in the "Restricted" bucket require two-factor authentication for decryption.
- AWS KMS must automatically rotate encryption keys annually.

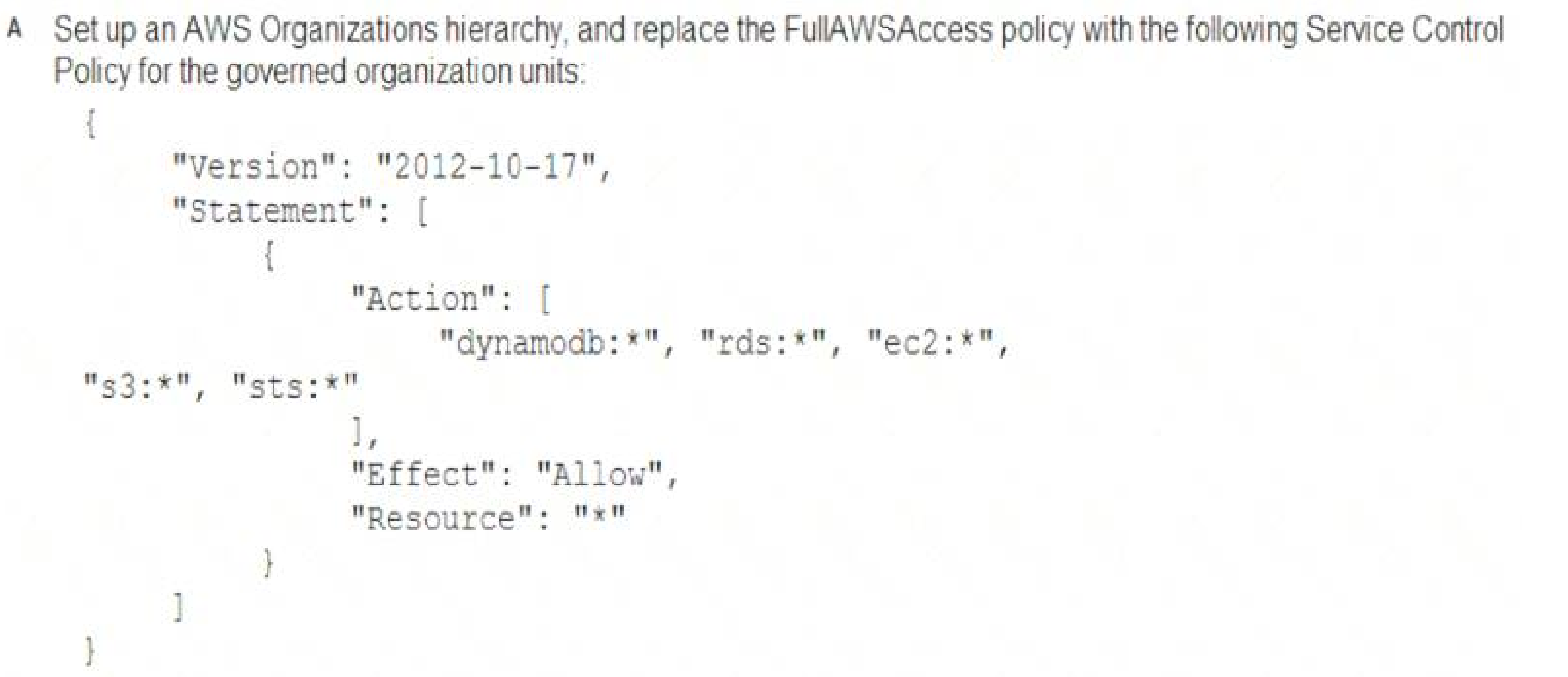
Which of the following meets these requirements?

A. Create a Customer Master Key (CMK) for each data classification type, and enable the rotation of it annuall
B. For the "Restricted" CMK, define the MFA policy within the key polic
C. Use S3 SSE-KMS to encrypt the objects.
D. Create a CMK grant for each data classification type with EnableKeyRotation and MultiFactorAuthPresent set to tru
E. S3 can then use the grants to encrypt each object with a unique CMK.
F. Create a CMK for each data classification type, and within the CMK policy, enable rotation of it annually, and define the MFA polic
G. S3 can then create DEK grants to uniquely encrypt each object within the S3 bucket.
H. Create a CMK with unique imported key material for each data classification type, and rotate them annuall
I. For the "Restricted" key material, define the MFA policy in the key polic
J. Use S3 SSE-KMS to encrypt the objects.

Answer: A

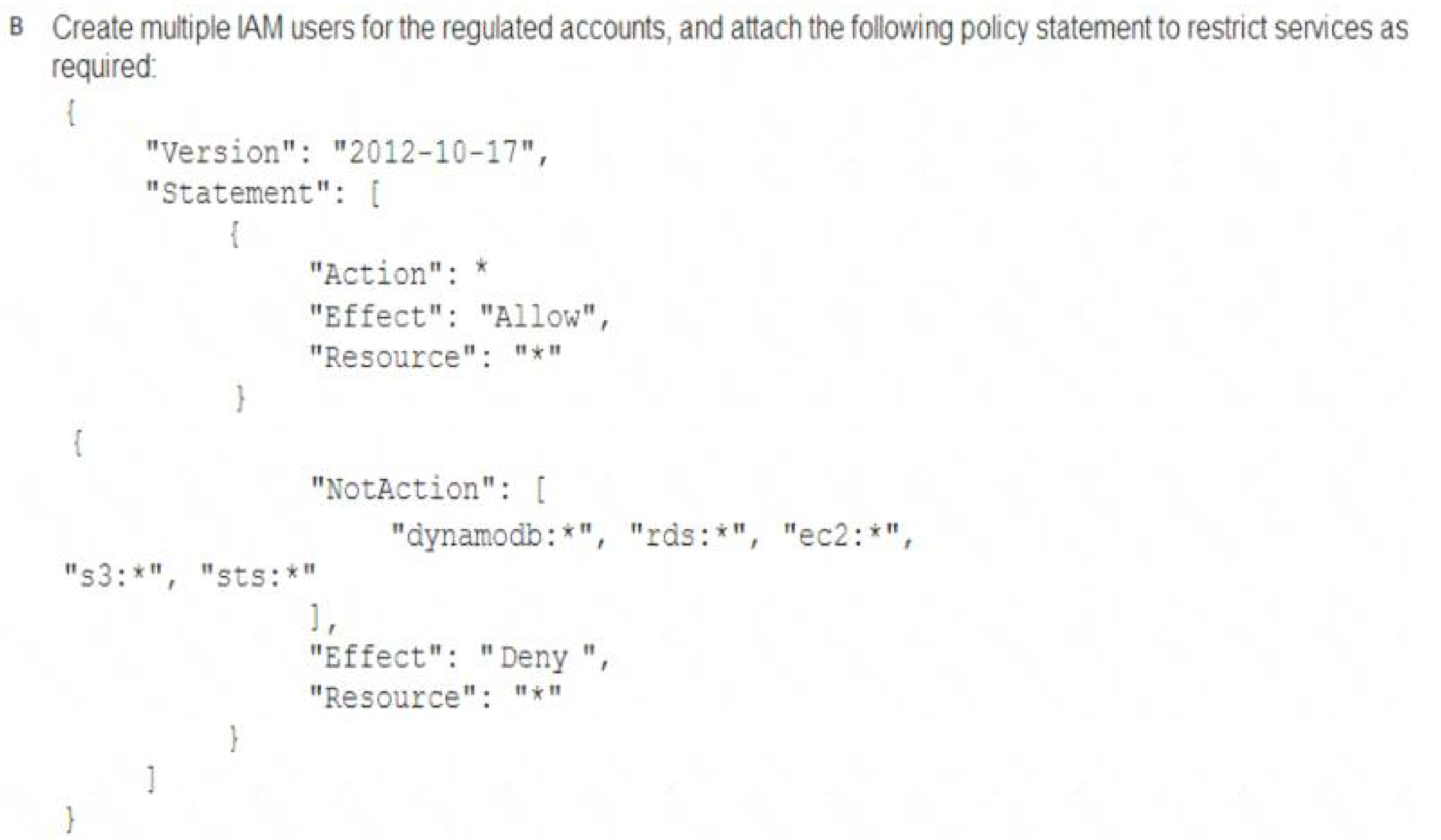
Explanation:
CMKs that are not eligible for automatic key rotation, including asymmetric CMKs, CMKs in custom key stores, and CMKs with imported key material.

NEW QUESTION 186
- (Exam Topic 2)
A Security Engineer must enforce the use of only Amazon EC2, Amazon S3, Amazon RDS, Amazon DynamoDB, and AWS STS in specific accounts.
What is a scalable and efficient approach to meet this requirement?



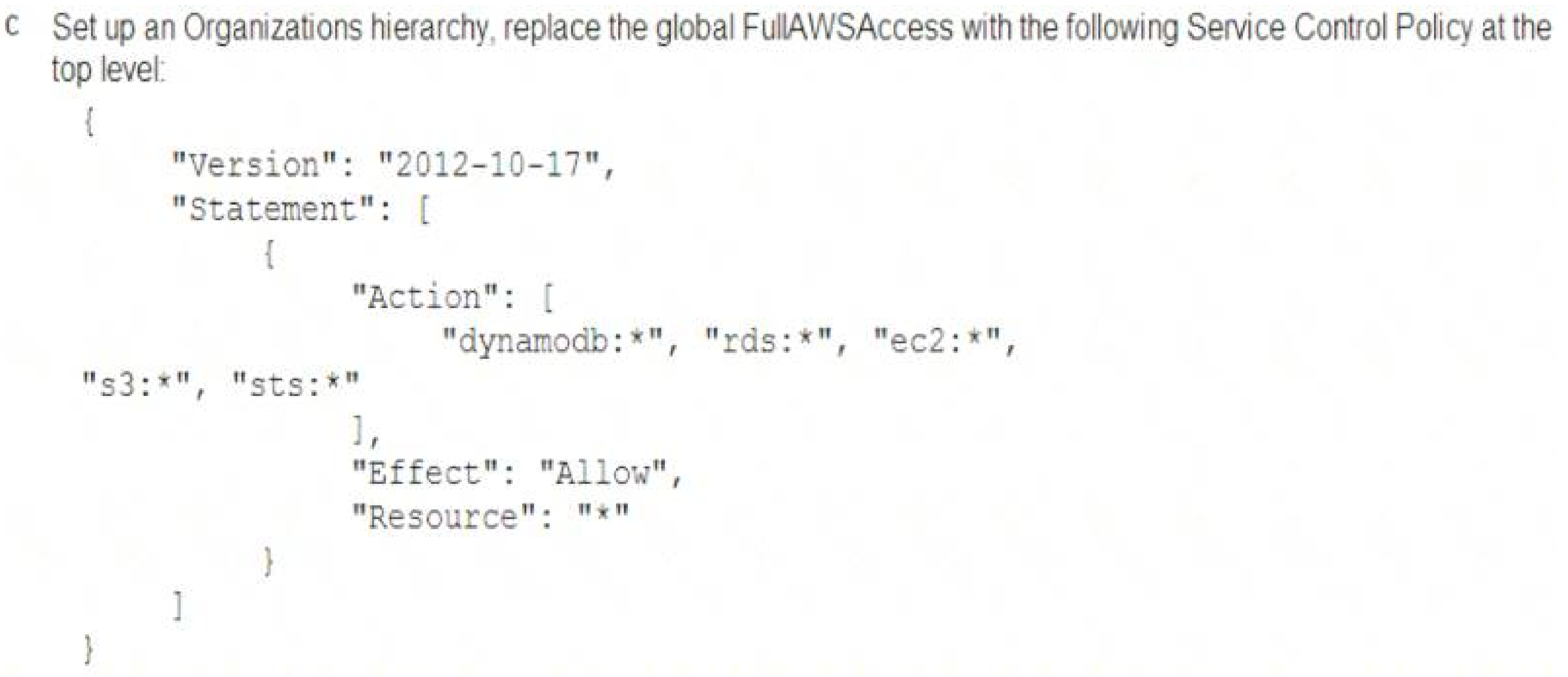
A Set up an AWS Organizations hierarchy, and replace the FullAWSAccess policy with the following Service Control Policy for the governed organization units:

```
{
      "Version": "2012-10-17",
      "Statement": [
           {
                 "Action": [
                      "dynamodb:*", "rds:*", "ec2:*",
"s3:*", "sts:*"
                 ],
                 "Effect": "Allow",
                 "Resource": "*"
           }
      ]
}
```



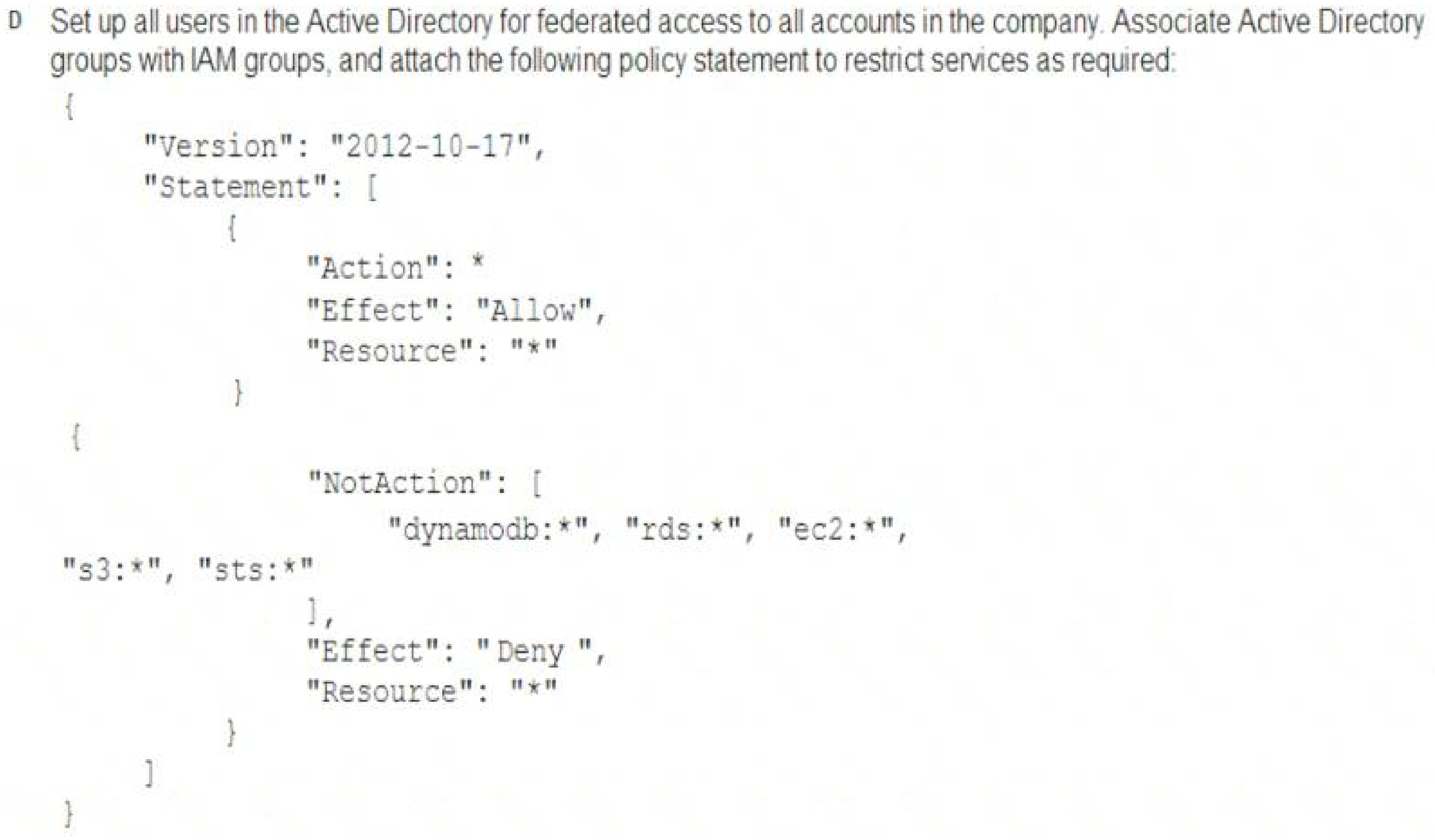
B Create multiple IAM users for the regulated accounts, and attach the following policy statement to restrict services as required:

```
{
      "Version": "2012-10-17",
      "Statement": [
           {
                 "Action": *
                 "Effect": "Allow",
                 "Resource": "*"
           }
{
                 "NotAction": [
                      "dynamodb:*", "rds:*", "ec2:*",
"s3:*", "sts:*"
                 ],
                 "Effect": "Deny ",
                 "Resource": "*"
           }
      ]
}
```



C Set up an Organizations hierarchy, replace the global FullAWSAccess with the following Service Control Policy at the top level:

```
{
      "Version": "2012-10-17",
      "Statement": [
           {
                 "Action": [
                      "dynamodb:*", "rds:*", "ec2:*",
"s3:*", "sts:*"
                 ],
                 "Effect": "Allow",
                 "Resource": "*"
           }
      ]
}
```



D Set up all users in the Active Directory for federated access to all accounts in the company. Associate Active Directory groups with IAM groups, and attach the following policy statement to restrict services as required:

```
{
        "Version": "2012-10-17",
        "Statement": [
                {
                        "Action": *
                        "Effect": "Allow",
                        "Resource": "*"
                }
 {
                        "NotAction": [
                                "dynamodb:*", "rds:*", "ec2:*",
"s3:*", "sts:*"
                        ],
                        "Effect": " Deny ",
                        "Resource": "*"
                }
        ]
}
```

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

Answer: A

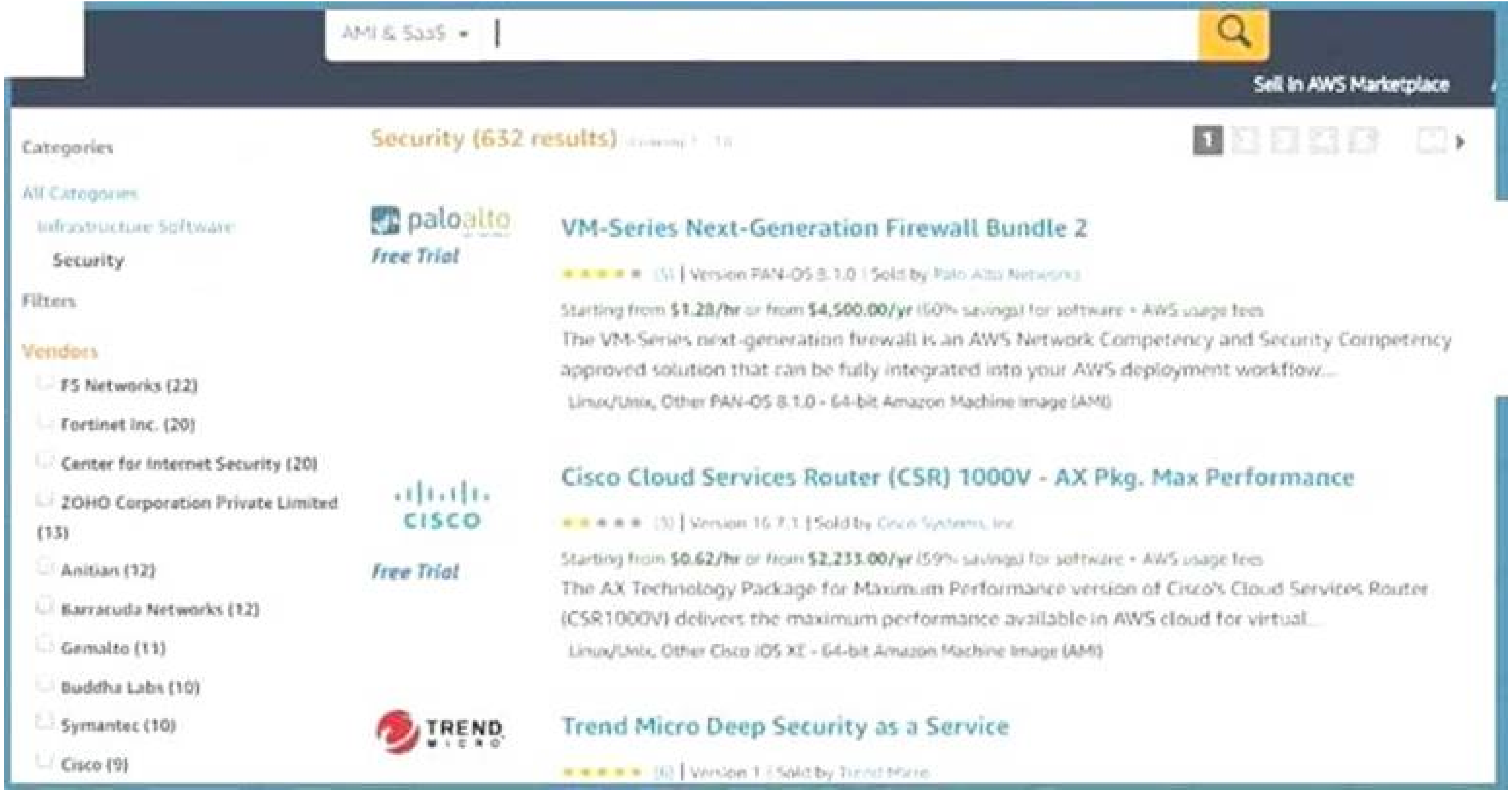
Explanation:
It says specific accounts which mean specific governed OUs under your organization and you apply specific service control policy to these OUs.

NEW QUESTION 191
- (Exam Topic 2)
A company wants to have an Intrusion detection system available for their VPC in AWS. They want to have complete control over the system. Which of the following would be ideal to implement?
Please select:

A. Use AWS WAF to catch all intrusions occurring on the systems in the VPC
B. Use a custom solution available in the AWS Marketplace
C. Use VPC Flow logs to detect the issues and flag them accordingly.
D. Use AWS Cloudwatch to monitor all traffic

Answer: B

Explanation:
Sometimes companies want to have custom solutions in place for monitoring Intrusions to their systems. In such a case, you can use the AWS Marketplace for looking at custom solutions.
C:\Users\wk\Desktop\mudassar\Untitled.jpg



Security (632 results)

VM-Series Next-Generation Firewall Bundle 2
(5) | Version PAN-OS 8.1.0 | Sold by Palo Alto Networks
Starting from **$1.28/hr** or from **$4,500.00/yr** (60% savings) for software + AWS usage fees
The VM-Series next-generation firewall is an AWS Network Competency and Security Competency approved solution that can be fully integrated into your AWS deployment workflow...
Linux/Unix, Other PAN-OS 8.1.0 - 64-bit Amazon Machine Image (AMI)

Cisco Cloud Services Router (CSR) 1000V - AX Pkg. Max Performance
(5) | Version 16.7.1 | Sold by Cisco Systems, Inc.
Starting from **$0.62/hr** or from **$2,233.00/yr** (59% savings) for software + AWS usage fees
The AX Technology Package for Maximum Performance version of Cisco's Cloud Services Router (CSR1000V) delivers the maximum performance available in AWS cloud for virtual...
Linux/Unix, Other Cisco IOS XE - 64-bit Amazon Machine Image (AMI)

Trend Micro Deep Security as a Service
(6) | Version 1 | Sold by Trend Micro

Option A.C and D are all invalid because they cannot be used to conduct intrusion detection or prevention. For more information on using custom security solutions please visit the below URL https://d1.awsstatic.com/Marketplace/security/AWSMP_Security_Solution%200verview.pdf
For more information on using custom security solutions please visit the below URL: https://d1 .awsstatic.com/Marketplace/security/AWSMP Security Solution%20Overview.pd1
The correct answer is: Use a custom solution available in the AWS Marketplace Submit your Feedback/Queries to our Experts

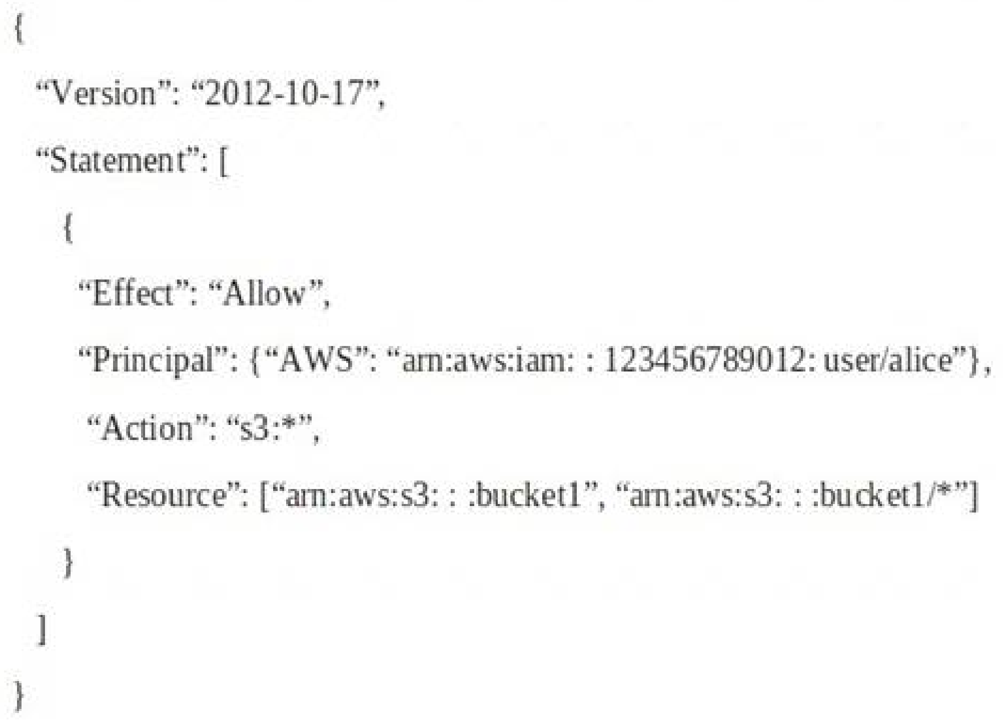
NEW QUESTION 196
- (Exam Topic 2)
An organization is using Amazon CloudWatch Logs with agents deployed on its Linux Amazon EC2 instances. The agent configuration files have been checked and the application log files to be pushed are configured correctly. A review has identified that logging from specific instances is missing.
Which steps should be taken to troubleshoot the issue? (Choose two.)

A. Use an EC2 run command to confirm that the “awslogs” service is running on all instances.
B. Verify that the permissions used by the agent allow creation of log groups/streams and to put log events.
C. Check whether any application log entries were rejected because of invalid time stamps by reviewing/var/cwlogs/rejects.log.
D. Check that the trust relationship grants the service “cwlogs.amazonaws.com” permission to write objects to the Amazon S3 staging bucket.
E. Verify that the time zone on the application servers is in UTC.

Answer: AB

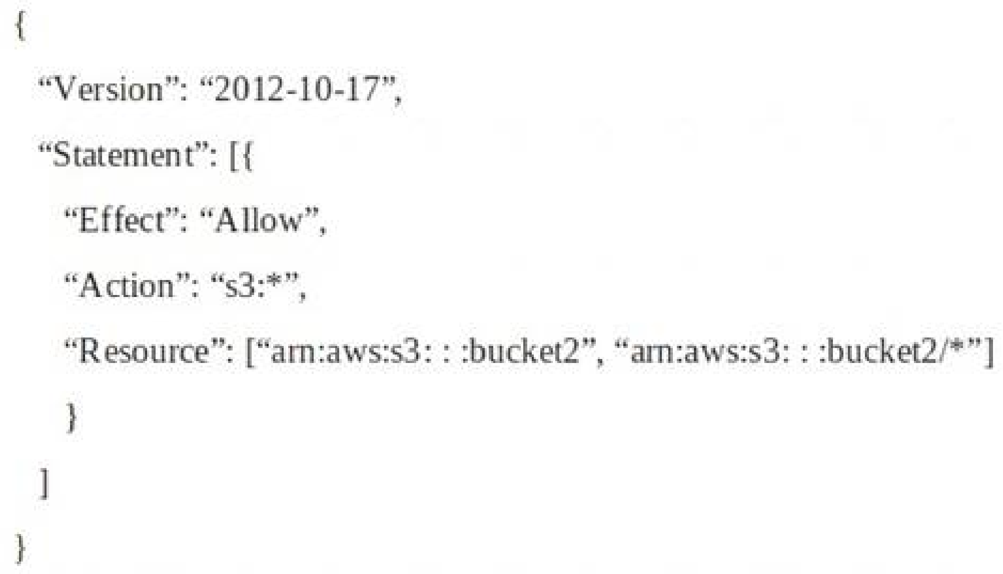
Explanation:
EC2 run command - can run scripts, install software, collect metrics and log files, manage patches and more. Bringing these two services together - can create CloudWatch Events rules that use EC2 Run Command to perform actions on EC2 instances or on-premises servers.

NEW QUESTION 199
- (Exam Topic 2)
An AWS account includes two S3 buckets: bucket1 and bucket2. The bucket2 does not have a policy defined, but bucket1 has the following bucket policy:



```
{
  “Version”: “2012-10-17”,
  “Statement”: [
    {
      “Effect”: “Allow”,
      “Principal”: {“AWS”: “arn:aws:iam: : 123456789012: user/alice”},
       “Action”: “s3:*”,
       “Resource”: [“arn:aws:s3: : :bucket1”, “arn:aws:s3: : :bucket1/*”]
    }
  ]
}
```

In addition, the same account has an IAM User named “alice”, with the following IAM policy.



```
{
  “Version”: “2012-10-17”,
  “Statement”: [{
    “Effect”: “Allow”,
    “Action”: “s3:*”,
    “Resource”: [“arn:aws:s3: : :bucket2”, “arn:aws:s3: : :bucket2/*”]
    }
  ]
}
```

Which buckets can user “alice” access?

A. Bucket1 only
B. Bucket2 only
C. Both bucket1 and bucket2
D. Neither bucket1 nor bucket2

Answer: C

Explanation:
Both S3 policies and IAM policies can be used to grant access to buckets. IAM policies specify what actions are allowed or denied on what AWS resources (e.g. allow ec2:TerminateInstance on the EC2 instance with instance_id=i-8b3620ec). You attach IAM policies to IAM users, groups, or roles, which are then subject to the permissions you’ve defined. In other words, IAM policies define what a principal can do in your AWS environment. S3 bucket policies, on the other hand, are attached only to S3 buckets. S3 bucket policies specify what actions are allowed or denied for which principals on the bucket that the bucket policy is attached to

(e.g. allow user Alice to PUT but not DELETE objects in the bucket).
https://aws.amazon.com/blogs/security/iam-policies-and-bucket-policies-and-acls-oh-my-controlling-access-to-s

NEW QUESTION 204
- (Exam Topic 2)
Which of the following is not a best practice for carrying out a security audit? Please select:

A. Conduct an audit on a yearly basis
B. Conduct an audit if application instances have been added to your account
C. Conduct an audit if you ever suspect that an unauthorized person might have accessed your account
D. Whenever there are changes in your organization

Answer: A

Explanation:
A year's time is generally too long a gap for conducting security audits The AWS Documentation mentions the following
You should audit your security configuration in the following situations: On a periodic basis.
If there are changes in your organization, such as people leaving.
If you have stopped using one or more individual AWS services. This is important for removing permissions that users in your account no longer need.
If you've added or removed software in your accounts, such as applications on Amazon EC2 instances, AWS OpsWor stacks, AWS CloudFormation templates, etc.
If you ever suspect that an unauthorized person might have accessed your account.
Option B, C and D are all the right ways and recommended best practices when it comes to conducting audits For more information on Security Audit guideline, please visit the below URL:
https://docs.aws.amazon.com/eeneral/latest/gr/aws-security-audit-euide.html
The correct answer is: Conduct an audit on a yearly basis Submit your Feedback/Queries to our Experts

NEW QUESTION 209
- (Exam Topic 2)
A company has a few dozen application servers in private subnets behind an Elastic Load Balancer (ELB) in an AWS Auto Scaling group. The application is accessed from the web over HTTPS. The data must always be encrypted in transit. The Security Engineer is worried about potential key exposure due to vulnerabilities in the application software.
Which approach will meet these requirements while protecting the external certificate during a breach?

A. Use a Network Load Balancer (NLB) to pass through traffic on port 443 from the internet to port 443 on the instances.
B. Purchase an external certificate, and upload it to the AWS Certificate Manager (for use with the ELB) and to the instance
C. Have the ELB decrypt traffic, and route and re-encrypt with the same certificate.
D. Generate an internal self-signed certificate and apply it to the instance
E. Use AWS Certificate Manager to generate a new external certificate for the EL
F. Have the ELB decrypt traffic, and route andre-encrypt with the internal certificate.
G. Upload a new external certificate to the load balance
H. Have the ELB decrypt the traffic and forward it on port 80 to the instances.

Answer: C

NEW QUESTION 214
- (Exam Topic 2)
A security alert has been raised for an Amazon EC2 instance in a customer account that is exhibiting strange behavior. The Security Engineer must first isolate the EC2 instance and then use tools for further investigation.
What should the Security Engineer use to isolate and research this event? (Choose three.)

A. AWS CloudTrail
B. Amazon Athena
C. AWS Key Management Service (AWS KMS)
D. VPC Flow Logs
E. AWS Firewall Manager
F. Security groups

Answer: ADF

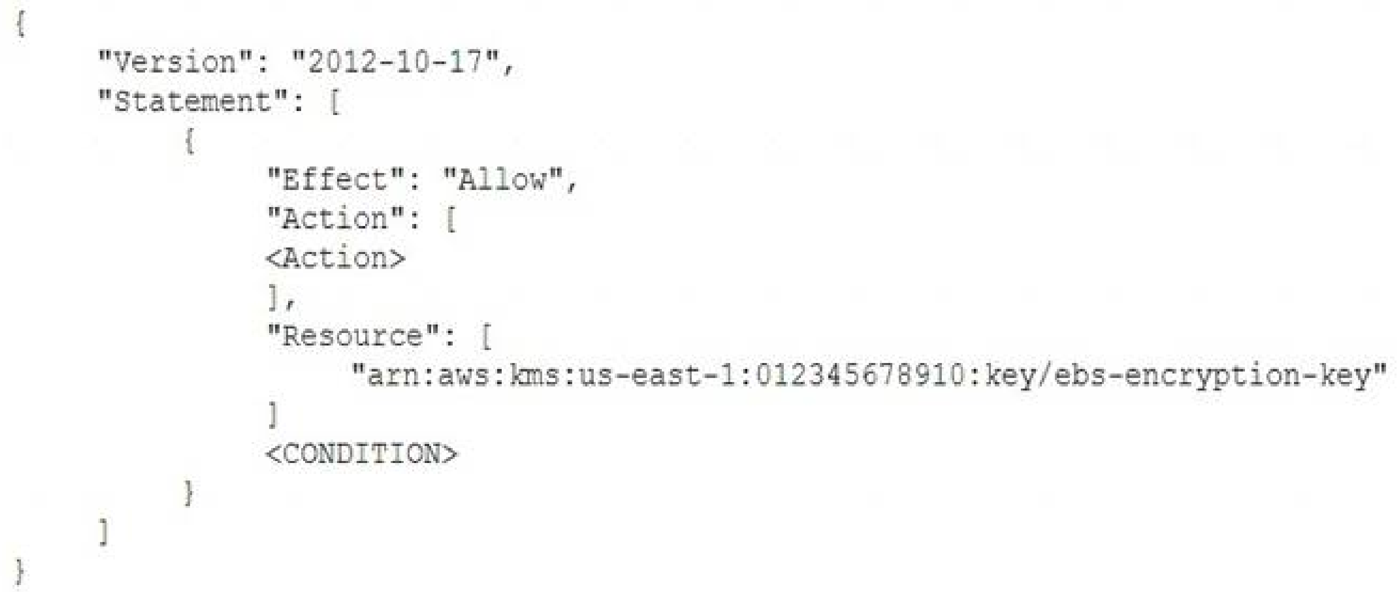
Explanation:
https://github.com/awslabs/aws-well-architected-labs/blob/master/Security/300_Incident_Response_with_AWS

NEW QUESTION 218
- (Exam Topic 2)
An application makes calls to AWS services using the AWS SDK. The application runs on Amazon EC2 instances with an associated IAM role. When the application attempts to access an object within an Amazon S3 bucket; the Administrator receives the following error message: HTTP 403: Access Denied.
Which combination of steps should the Administrator take to troubleshoot this issue? (Select three.)

A. Confirm that the EC2 instance's security group authorizes S3 access.
B. Verify that the KMS key policy allows decrypt access for the KMS key for this IAM principle.
C. Check the S3 bucket policy for statements that deny access to objects.
D. Confirm that the EC2 instance is using the correct key pair.
E. Confirm that the IAM role associated with the EC2 instance has the proper privileges.
F. Confirm that the instance and the S3 bucket are in the same Region.

Answer: BCE

NEW QUESTION 220
- (Exam Topic 2)
An IAM user with fill EC2 permissions could bot start an Amazon EC2 instance after it was stopped for a maintenance task. Upon starting the instance, the instance state would change to “Pending”, but after a few seconds, it would switch back to “Stopped”.
An inspection revealed that the instance has attached Amazon EBS volumes that were encrypted by using a Customer Master Key (CMK). When these encrypted volumes were detached, the IAM user was able to start the EC2 instances.
The IAM user policy is as follows:



```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
            <Action>
            ],
            "Resource": [
                "arn:aws:kms:us-east-1:012345678910:key/ebs-encryption-key"
            ]
            <CONDITION>
        }
    ]
}
```

What additional items need to be added to the IAM user policy? (Choose two.)

A. kms:GenerateDataKey
B. kms:Decrypt
C. kms:CreateGrant
D. “Condition”: {“Bool”: {“kms:ViaService”: “ec2.us-west-2.amazonaws.com”}}
E. “Condition”: {“Bool”: {“kms:GrantIsForAWSResource”: true}}

Answer: CE

Explanation:
The EBS which is AWS resource service is encrypted with CMK and to allow EC2 to decrypt , the IAM user should create a grant (action) and a boolean condition for the AWs resource . This link explains how AWS keys works. https://docs.aws.amazon.com/kms/latest/developerguide/key-policies.html

NEW QUESTION 222
- (Exam Topic 2)
Example.com hosts its internal document repository on Amazon EC2 instances. The application runs on EC2 instances and previously stored the documents on encrypted Amazon EBS volumes. To optimize the application for scale, example.com has moved the files to Amazon S3. The security team has mandated that all the files are securely deleted from the EBS volume, and it must certify that the data is unreadable before releasing the underlying disks.
Which of the following methods will ensure that the data is unreadable by anyone else?

A. Change the volume encryption on the EBS volume to use a different encryption mechanis
B. Then, release the EBS volumes back to AWS.
C. Release the volumes back to AW
D. AWS immediately wipes the disk after it is deprovisioned.
E. Delete the encryption key used to encrypt the EBS volum
F. Then, release the EBS volumes back to AWS.
G. Delete the data by using the operating system delete command
H. Run Quick Format on the drive and then release the EBS volumes back to AWS.

Answer: D

Explanation:
Amazon EBS volumes are presented to you as raw unformatted block devices that have been wiped prior to being made available for use. Wiping occurs immediately before reuse so that you can be assured that the wipe process completed. If you have procedures requiring that all data be wiped via a specific method, such as those detailed in NIST 800-88 (“Guidelines for Media Sanitization”), you have the ability to do so on Amazon EBS. You should conduct a specialized wipe procedure prior to deleting the volume for compliance with your established requirements.
https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

NEW QUESTION 226
- (Exam Topic 2)
While analyzing a company's security solution, a Security Engineer wants to secure the AWS account root user.
What should the Security Engineer do to provide the highest level of security for the account?

A. Create a new IAM user that has administrator permissions in the AWS accoun
B. Delete the password forthe AWS account root user.
C. Create a new IAM user that has administrator permissions in the AWS accoun
D. Modify the permissions for the existing IAM users.
E. Replace the access key for the AWS account root use
F. Delete the password for the AWS account root user.
G. Create a new IAM user that has administrator permissions in the AWS accoun
H. Enable multi-factor authentication for the AWS account root user.

Answer: D

Explanation:

If you continue to use the root user credentials, we recommend that you follow the security best practice to enable multi-factor authentication (MFA) for your account. Because your root user can perform sensitive operations in your account, adding an additional layer of authentication helps you to better secure your account. Multiple types of MFA are available.

NEW QUESTION 229
- (Exam Topic 2)
An organization receives an alert that indicates that an EC2 instance behind an ELB Classic Load Balancer has been compromised.
What techniques will limit lateral movement and allow evidence gathering?

A. Remove the instance from the load balancer and terminate it.
B. Remove the instance from the load balancer, and shut down access to the instance by tightening the security group.
C. Reboot the instance and check for any Amazon CloudWatch alarms.
D. Stop the instance and make a snapshot of the root EBS volume.

Answer: B

Explanation:
https://d1.awsstatic.com/whitepapers/aws_security_incident_response.pdf

NEW QUESTION 233
- (Exam Topic 2)
A company is hosting a website that must be accessible to users for HTTPS traffic. Also port 22 should be open for administrative purposes. The administrator's workstation has a static IP address of 203.0.113.1/32. Which of the following security group configurations are the MOST secure but still functional to support these requirements? Choose 2 answers from the options given below
Please select:

A. Port 443 coming from 0.0.0.0/0
B. Port 443 coming from 10.0.0.0/16
C. Port 22 coming from 0.0.0.0/0
D. Port 22 coming from 203.0.113.1/32

Answer: AD

Explanation:
Since HTTPS traffic is required for all users on the Internet, Port 443 should be open on all IP addresses. For port 22, the traffic should be restricted to an internal subnet.
Option B is invalid, because this only allow traffic from a particular CIDR block and not from the internet Option C is invalid because allowing port 22 from the internet is a security risk
For more information on AWS Security Groups, please visit the following UR https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/usins-network-secunty.htmll
The correct answers are: Port 443 coming from 0.0.0.0/0, Port 22 coming from 203.0.113.1 /32 Submit your Feedback/Queries to our Experts

NEW QUESTION 234
- (Exam Topic 2)
The InfoSec team has mandated that in the future only approved Amazon Machine Images (AMIs) can be used.
How can the InfoSec team ensure compliance with this mandate?

A. Terminate all Amazon EC2 instances and relaunch them with approved AMIs.
B. Patch all running instances by using AWS Systems Manager.
C. Deploy AWS Config rules and check all running instances for compliance.
D. Define a metric filter in Amazon CloudWatch Logs to verify compliance.

Answer: C

Explanation:
https://docs.aws.amazon.com/config/latest/developerguide/approved-amis-by-id.html

NEW QUESTION 236
- (Exam Topic 2)
A security team must present a daily briefing to the CISO that includes a report of which of the company's thousands of EC2 instances and on-premises servers are missing the latest security patches. All instances/servers must be brought into compliance within 24 hours so they do not show up on the next day's report.
How can the security team fulfill these requirements?
Please select:

A. Use Amazon QuickSight and Cloud Trail to generate the report of out of compliance instances/servers.Redeploy all out of compliance instances/servers using an AMI with the latest patches.
B. Use Systems Manger Patch Manger to generate the report of out of compliance instances/ server
C. Use Systems Manager Patch Manger to install the missing patches.
D. Use Systems Manger Patch Manger to generate the report of out of compliance instances/ servers.Redeploy all out of1 compliance instances/servers using an AMI with the latest patches.
E. Use Trusted Advisor to generate the report of out of compliance instances/server
F. Use Systems Manger Patch Manger to install the missing patches.

Answer: B

Explanation:
Use the Systems Manger Patch Manger to generate the report and also install the missing patches The AWS Documentation mentions the following
AWS Systems Manager Patch Manager automates the process of patching managed instances with
security-related updates. For Linux-based instances, you can also install patches for non-security updates. You can patch fleets of Amazon EC2 instances or your on-premises servers and virtual machines (VMs) by operating system type. This includes supported versions of Windows, Ubuntu Server, Red Hat Enterprise

Linux (RHEL), SUSE Linux Enterprise Server (SLES), and Amazon Linux. You can scan instances to see only a report of missing patches, or you can scan and automatically install all missing patches.
Option A is invalid because Amazon QuickSight and Cloud Trail cannot be used to generate the list of servers that don't meet compliance needs.
Option C is wrong because deploying instances via new AMI'S would impact the applications hosted on these servers
Option D is invalid because Amazon Trusted Advisor cannot be used to generate the list of servers that don't meet compliance needs.
For more information on the AWS Patch Manager, please visit the below URL:
https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-patch.html (
The correct answer is: Use Systems Manger Patch Manger to generate the report of out of compliance instances/ servers. Use Systems Manager Patch Manger to install the missing patches.
Submit your Feedback/Queries to our Experts

NEW QUESTION 237
- (Exam Topic 2)
Your company has mandated that all calls to the AWS KMS service be recorded. How can this be achieved? Please select:

A. Enable logging on the KMS service
B. Enable a trail in Cloudtrail
C. Enable Cloudwatch logs
D. Use Cloudwatch metrics

Answer: B

Explanation:
The AWS Documentation states the following
AWS KMS is integrated with CloudTrail, a service that captures API calls made by or on behalf of AWS KMS in your AWS account and delivers the log files to an Amazon S3 bucket that you specify. CloudTrail captures API calls from the AWS KMS console or from the AWS KMS API. Using the information collected by CloudTrail, you can determine what request was made, the source IP address from which the request was made, who made the request when it was made, and so on.
Option A is invalid because logging is not possible in the KMS service
Option C and D are invalid because Cloudwatch cannot be used to monitor API calls For more information on logging using Cloudtrail please visit the below URL https://docs.aws.amazon.com/kms/latest/developerguide/loeeing-usine-cloudtrail.html The correct answer is: Enable a trail in Cloudtrail
Jubmit your Feedback/Queries to our Experts

NEW QUESTION 239
- (Exam Topic 2)
An application has been built with Amazon EC2 instances that retrieve messages from Amazon SQS. Recently, IAM changes were made and the instances can no longer retrieve messages.
What actions should be taken to troubleshoot the issue while maintaining least privilege. (Select two.)

A. Configure and assign an MFA device to the role used by the instances.
B. Verify that the SQS resource policy does not explicitly deny access to the role used by the instances.
C. Verify that the access key attached to the role used by the instances is active.
D. Attach the AmazonSQSFullAccess managed policy to the role used by the instances.
E. Verify that the role attached to the instances contains policies that allow access to the queue.

Answer: BE

NEW QUESTION 242
- (Exam Topic 2)
A Security Administrator is restricting the capabilities of company root user accounts. The company uses AWS Organizations and has enabled it for all feature sets, including consolidated billing. The top-level account is used for billing and administrative purposes, not for operational AWS resource purposes.
How can the Administrator restrict usage of member root user accounts across the organization?

A. Disable the use of the root user account at the organizational roo
B. Enable multi-factor authentication of the root user account for each organizational member account.
C. Configure IAM user policies to restrict root account capabilities for each Organizations member account.
D. Create an organizational unit (OU) in Organizations with a service control policy that controls usage of the root use
E. Add all operational accounts to the new OU.
F. Configure AWS CloudTrail to integrate with Amazon CloudWatch Logs and then create a metric filter for RootAccountUsage.

Answer: C

Explanation:
Applying a "Control Policy" in your organization. A policy applied to: 1) root applies to all accounts in the organization 2) OU applies to all accounts in the OU and to any child OUs 3) account applies to one account only Note- this requires that Acquirements: -all features are enabled for the organization in AWS Organizations -Only service control policy (SCP) are supported https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies.html

NEW QUESTION 245
- (Exam Topic 2)
A Development team has asked for help configuring the IAM roles and policies in a new AWS account. The team using the account expects to have hundreds of master keys and therefore does not want to manage access control for customer master keys (CMKs).
Which of the following will allow the team to manage AWS KMS permissions in IAM without the complexity of editing individual key policies?

A. The account’s CMK key policy must allow the account’s IAM roles to perform KMS EnableKey.
B. Newly created CMKs must have a key policy that allows the root principal to perform all actions.
C. Newly created CMKs must allow the root principal to perform the kms CreateGrant API operation.
D. Newly created CMKs must mirror the IAM policy of the KMS key administrator.

Answer: B

Explanation:
https://docs.aws.amazon.com/kms/latest/developerguide/key-policies.html#key-policy-default-allow-root-enable

NEW QUESTION 249
- (Exam Topic 2)
The AWS Systems Manager Parameter Store is being used to store database passwords used by an AWS Lambda function. Because this is sensitive data, the parameters are stored as type SecureString and protected by an AWS KMS key that allows access through IAM. When the function executes, this parameter cannot be retrieved as the result of an access denied error.
Which of the following actions will resolve the access denied error?

A. Update the ssm.amazonaws.com principal in the KMS key policy to allow kms: Decrypt.
B. Update the Lambda configuration to launch the function in a VPC.
C. Add a policy to the role that the Lambda function uses, allowing kms: Decrypt for the KMS key.
D. Add lambda.amazonaws.com as a trusted entity on the IAM role that the Lambda function uses.

Answer: C

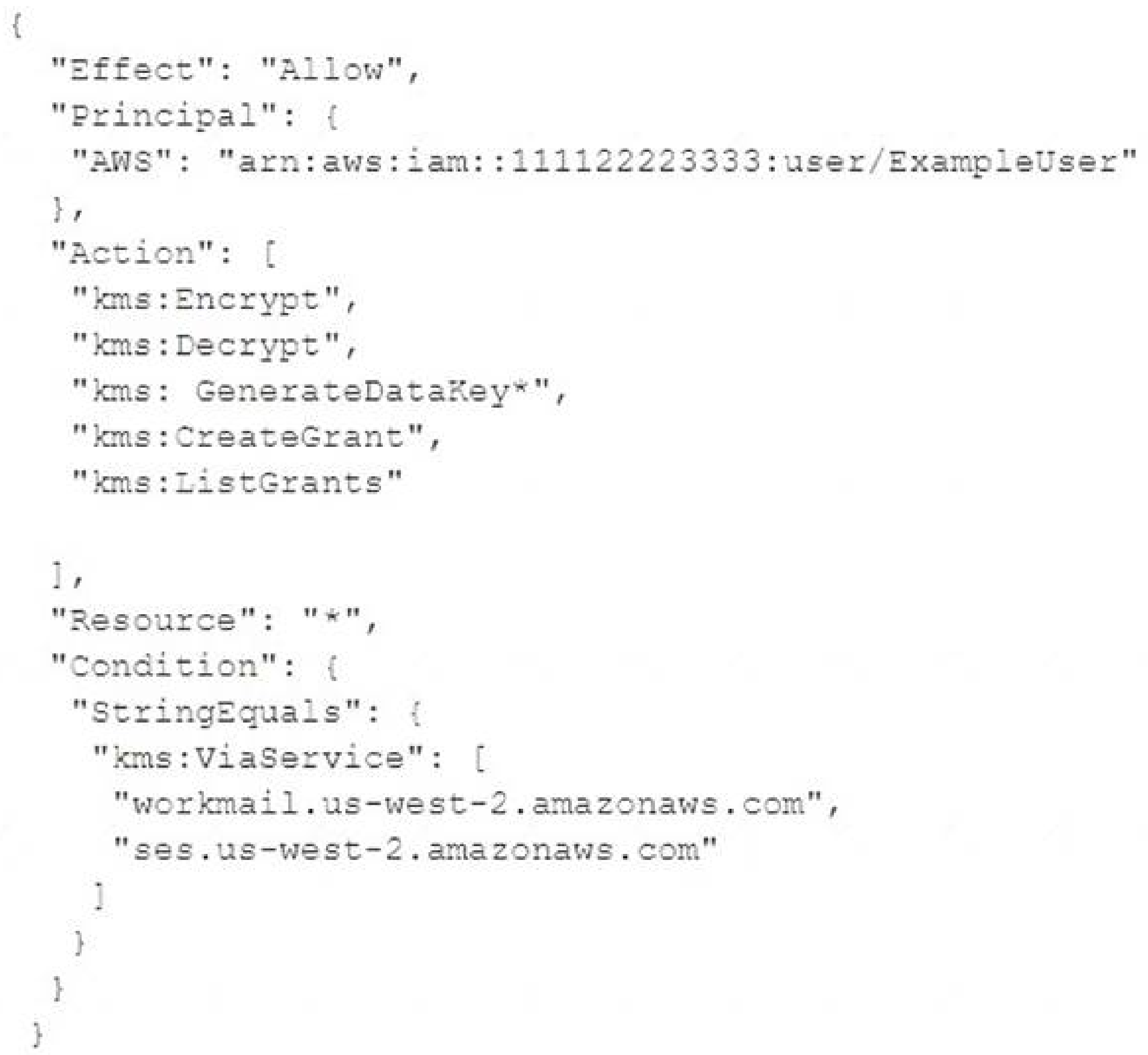
Explanation:
https://docs.amazonaws.cn/en_us/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Integrating.Authorizing

NEW QUESTION 253
- (Exam Topic 2)
A threat assessment has identified a risk whereby an internal employee could exfiltrate sensitive data from production host running inside AWS (Account 1). The threat was documented as follows:
Threat description: A malicious actor could upload sensitive data from Server X by configuring credentials for an AWS account (Account 2) they control and uploading data to an Amazon S3 bucket within their control.
Server X has outbound internet access configured via a proxy server. Legitimate access to S3 is required so that the application can upload encrypted files to an S3 bucket. Server X is currently using an IAM instance role. The proxy server is not able to inspect any of the server communication due to TLS encryption.
Which of the following options will mitigate the threat? (Choose two.)

A. Bypass the proxy and use an S3 VPC endpoint with a policy that whitelists only certain S3 buckets within Account 1.
B. Block outbound access to public S3 endpoints on the proxy server.
C. Configure Network ACLs on Server X to deny access to S3 endpoints.
D. Modify the S3 bucket policy for the legitimate bucket to allow access only from the public IP addresses associated with the application server.
E. Remove the IAM instance role from the application server and save API access keys in a trusted and encrypted application config file.

Answer: AB

NEW QUESTION 254
- (Exam Topic 2)
What is the function of the following AWS Key Management Service (KMS) key policy attached to a customer master key (CMK)?



```
{
  "Effect": "Allow",
  "Principal": {
   "AWS": "arn:aws:iam::111122223333:user/ExampleUser"
  },
  "Action": [
   "kms:Encrypt",
   "kms:Decrypt",
   "kms: GenerateDataKey*",
   "kms:CreateGrant",
   "kms:ListGrants"

  ],
  "Resource": "*",
  "Condition": {
   "StringEquals": {
    "kms:ViaService": [
     "workmail.us-west-2.amazonaws.com",
     "ses.us-west-2.amazonaws.com"
    ]
   }
  }
 }
```

A. The Amazon WorkMail and Amazon SES services have delegated KMS encrypt and decrypt permissions to the ExampleUser principal in the 111122223333 account.
B. The ExampleUser principal can transparently encrypt and decrypt email exchanges specifically between ExampleUser and AWS.

C. The CMK is to be used for encrypting and decrypting only when the principal is ExampleUser and the request comes from WorkMail or SES in the specified region.
D. The key policy allows WorkMail or SES to encrypt or decrypt on behalf of the user for any CMK in the account.

Answer: C

NEW QUESTION 256
- (Exam Topic 2)
A Systems Engineer is troubleshooting the connectivity of a test environment that includes a virtual security appliance deployed inline. In addition to using the virtual security appliance, the Development team wants to use security groups and network ACLs to accomplish various security requirements in the environment.
What configuration is necessary to allow the virtual security appliance to route the traffic?

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

Answer: C

Explanation:
Each EC2 instance performs source/destination checks by default. This means that the instance must be the source or destination of any traffic it sends or receives. In this case virtual security appliance instance must be able to send and receive traffic when the source or destination is not itself. Therefore, you must disable source/destination checks on the NAT instance."

NEW QUESTION 258
- (Exam Topic 2)
Amazon CloudWatch Logs agent is successfully delivering logs to the CloudWatch Logs service. However, logs stop being delivered after the associated log stream has been active for a specific number of hours.
What steps are necessary to identify the cause of this phenomenon? (Choose two.)

A. Ensure that file permissions for monitored files that allow the CloudWatch Logs agent to read the file have not been modified.
B. Verify that the OS Log rotation rules are compatible with the configuration requirements for agent streaming.
C. Configure an Amazon Kinesis producer to first put the logs into Amazon Kinesis Streams.
D. Create a CloudWatch Logs metric to isolate a value that changes at least once during the period before logging stops.
E. Use AWS CloudFormation to dynamically create and maintain the configuration file for the CloudWatch Logs agent.

Answer: AB

Explanation:
https://acloud.guru/forums/aws-certified-security-specialty/discussion/-Lm5A3w6_NybQPhh6tRP/Cloudwatch%

NEW QUESTION 262
- (Exam Topic 2)
A company uses user data scripts that contain sensitive information to bootstrap Amazon EC2 instances. A Security Engineer discovers that this sensitive information is viewable by people who should not have access to it.
What is the MOST secure way to protect the sensitive information used to bootstrap the instances?

A. Store the scripts in the AMI and encrypt the sensitive data using AWS KMS Use the instance role profile to control access to the KMS keys needed to decrypt the data.
B. Store the sensitive data in AWS Systems Manager Parameter Store using the encrypted string parameter and assign the GetParameters permission to the EC2 instance role.
C. Externalize the bootstrap scripts in Amazon S3 and encrypt them using AWS KM
D. Remove the scripts from the instance and clear the logs after the instance is configured.
E. Block user access of the EC2 instance's metadata service using IAM policie
F. Remove all scripts and clear the logs after execution.

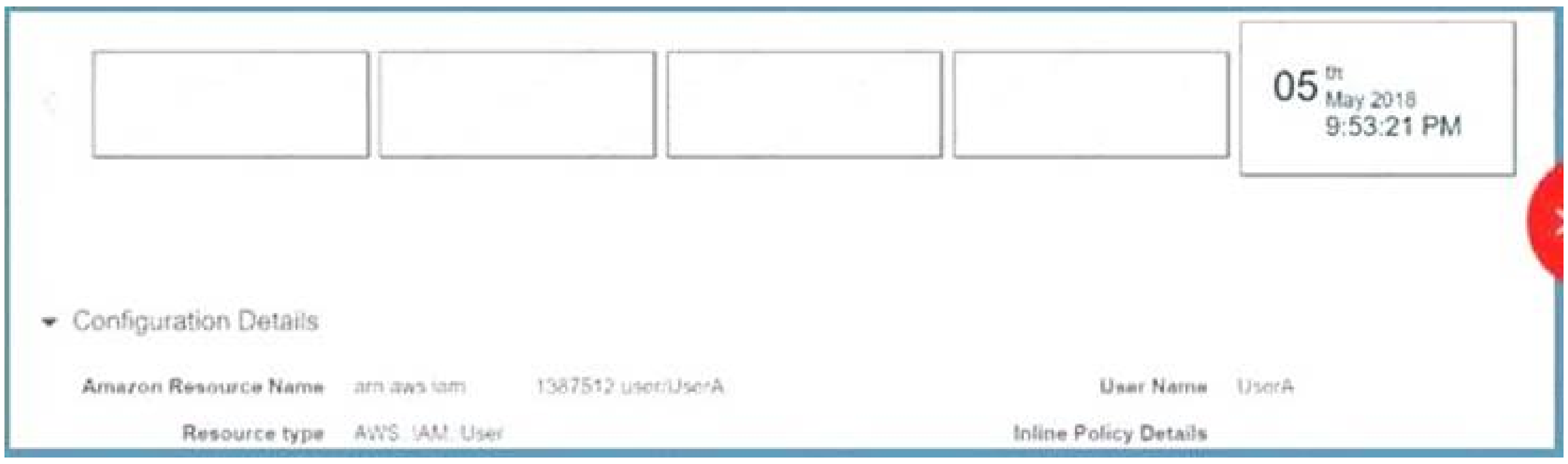
Answer: B

NEW QUESTION 266
- (Exam Topic 2)
A security team is creating a response plan in the event an employee executes unauthorized actions on AWS infrastructure. They want to include steps to determine if the employee's IAM permissions changed as part of the incident.
What steps should the team document in the plan? Please select:

A. Use AWS Config to examine the employee's IAM permissions prior to the incident and compare them to the employee's current IAM permissions.
B. Use Made to examine the employee's IAM permissions prior to the incident and compare them to the employee's A current IAM permissions.
C. Use CloudTrail to examine the employee's IAM permissions prior to the incident and compare them to the employee's current IAM permissions.
D. Use Trusted Advisor to examine the employee's IAM permissions prior to the incident and compare them to the employee's current IAM permissions.

Answer: A

Explanation:
You can use the AWSConfig history to see the history of a particular item.
The below snapshot shows an example configuration for a user in AWS Config C:\Users\wk\Desktop\mudassar\Untitled.jpg



05 th May 2018 9:53:21 PM

Configuration Details

Amazon Resource Name arn aws iam 1387512 user/UserA

User Name UserA

Resource type AWS IAM User

Inline Policy Details

Option B,C and D are all invalid because these services cannot be used to see the history of a particular configuration item. This can only be accomplished by AWS Config.
For more information on tracking changes in AWS Config, please visit the below URL:
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/TrackineChanees.htmll
The correct answer is: Use AWS Config to examine the employee's IAM permissions prior to the incident and compare them the employee's current IAM permissions.
Submit your Feedback/Queries to our Experts

NEW QUESTION 267
- (Exam Topic 2)
The Security Engineer is given the following requirements for an application that is running on Amazon EC2 and managed by using AWS CloudFormation templates with EC2 Auto Scaling groups:
-Have the EC2 instances bootstrapped to connect to a backend database.
-Ensure that the database credentials are handled securely.
-Ensure that retrievals of database credentials are logged.
Which of the following is the MOST efficient way to meet these requirements?

A. Pass databases credentials to EC2 by using CloudFormation stack parameters with the property set to tru
B. Ensure that the instance is configured to log to Amazon CloudWatch Logs.
C. Store database passwords in AWS Systems Manager Parameter Store by using SecureString parameters.Set the IAM role for the EC2 instance profile to allow access to the parameters.
D. Create an AWS Lambda that ingests the database password and persists it to Amazon S3 with server-side encryptio
E. Have the EC2 instances retrieve the S3 object on startup, and log all script invocations to syslog.
F. Write a script that is passed in as UserData so that it is executed upon launch of the EC2 instance.Ensure that the instance is configured to log to Amazon CloudWatch Logs.

Answer: B

NEW QUESTION 268
- (Exam Topic 2)
During a recent security audit, it was discovered that multiple teams in a large organization have placed restricted data in multiple Amazon S3 buckets, and the data may have been exposed. The auditor has requested that the organization identify all possible objects that contain personally identifiable information (PII) and then determine whether this information has been accessed.
What solution will allow the Security team to complete this request?

A. Using Amazon Athena, query the impacted S3 buckets by using the PII query identifier functio
B. Then, create a new Amazon CloudWatch metric for Amazon S3 object access to alert when the objects are accessed.
C. Enable Amazon Macie on the S3 buckets that were impacted, then perform data classificatio
D. For identified objects that contain PII, use the research function for auditing AWS CloudTrail logs and S3 bucket logs for GET operations.
E. Enable Amazon GuardDuty and enable the PII rule set on the S3 buckets that were impacted, then perform data classificatio
F. Using the PII findings report from GuardDuty, query the S3 bucket logs by using Athena for GET operations.
G. Enable Amazon Inspector on the S3 buckets that were impacted, then perform data classificatio
H. For identified objects that contain PII, query the S3 bucket logs by using Athena for GET operations.

Answer: B

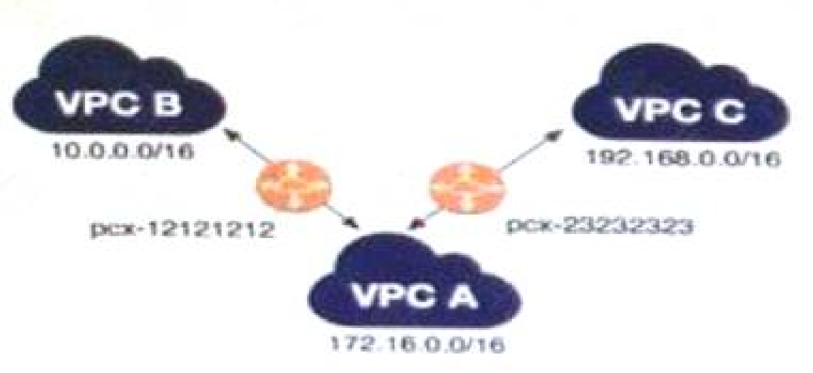
NEW QUESTION 270
- (Exam Topic 2)
The Security Engineer has discovered that a new application that deals with highly sensitive data is storing Amazon S3 objects with the following key pattern, which itself contains highly sensitive data.
Pattern: "randomID_datestamp_PII.csv" Example:
"1234567_12302017_000-00-0000 csv"
The bucket where these objects are being stored is using server-side encryption (SSE). Which solution is the most secure and cost-effective option to protect the sensitive data?

A. Remove the sensitive data from the object name, and store the sensitive data using S3 user-defined metadata.
B. Add an S3 bucket policy that denies the action s3:GetObject
C. Use a random and unique S3 object key, and create an S3 metadata index in Amazon DynamoDB using client-side encrypted attributes.
D. Store all sensitive objects in Binary Large Objects (BLOBS) in an encrypted Amazon RDS instance.

Answer: C

Explanation:
https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingMetadata.html https://aws.amazon.com/blogs/database/best-practices-for-securing-sensitive-data-in-aws-data-stores/

NEW QUESTION 274
- (Exam Topic 2)
A company has multiple VPCs in their account that are peered, as shown in the diagram. A Security Engineer wants to perform penetration tests of the Amazon EC2 instances in all three VPCs.
How can this be accomplished? (Choose two.)



A. Deploy a pre-authorized scanning engine from the AWS Marketplace into VPC B, and use it to scan instances in all three VPC
B. Do not complete the penetration test request form.
C. Deploy a pre-authorized scanning engine from the Marketplace into each VPC, and scan instances in each VPC from the scanning engine in that VP
D. Do not complete the penetration test request form.
E. Create a VPN connection from the data center to VPC
F. Use an on-premises scanning engine to scan the instances in all three VPC
G. Complete the penetration test request form for all three VPCs.
H. Create a VPN connection from the data center to each of the three VPC
I. Use an on-premises scanning engine to scan the instances in each VP
J. Do not complete the penetration test request form.
K. Create a VPN connection from the data center to each of the three VPC
L. Use an on-premises scanning engine to scan the instances in each VP
M. Complete the penetration test request form for all three VPCs.

Answer: BD

Explanation:
https://aws.amazon.com/security/penetration-testing/

NEW QUESTION 279
- (Exam Topic 2)
A Developer who is following AWS best practices for secure code development requires an application to encrypt sensitive data to be stored at rest, locally in the application, using AWS KMS. What is the simplest and MOST secure way to decrypt this data when required?

A. Request KMS to provide the stored unencrypted data key and then use the retrieved data key to decrypt the data.
B. Keep the plaintext data key stored in Amazon DynamoDB protected with IAM policie
C. Query DynamoDB to retrieve the data key to decrypt the data
D. Use the Encrypt API to store an encrypted version of the data key with another customer managed key.Decrypt the data key and use it to decrypt the data when required.
E. Store the encrypted data key alongside the encrypted dat
F. Use the Decrypt API to retrieve the data key to decrypt the data when required.

Answer: D

Explanation:
We recommend that you use the following pattern to locally encrypt data: call the GenerateDataKey API, use the key returned in the Plaintext response field to locally encrypt data, and then erase the plaintext data key from memory. Store the encrypted data key (contained in the CiphertextBlob field) alongside of the locally encrypted data. The Decrypt API returns the plaintext key from the encrypted key.
https://docs.aws.amazon.com/sdkfornet/latest/apidocs/items/MKeyManagementServiceKeyManagementService

NEW QUESTION 283
- (Exam Topic 2)
A Security Engineer is implementing a solution to allow users to seamlessly encrypt Amazon S3 objects without having to touch the keys directly. The solution must be highly scalable without requiring continual management. Additionally, the organization must be able to immediately delete the encryption keys.
Which solution meets these requirements?

A. Use AWS KMS with AWS managed keys and the ScheduleKeyDeletion API with a PendingWindowInDays set to 0 to remove the keys if necessary.
B. Use KMS with AWS imported key material and then use the DeletelmportedKeyMaterial API to remove the key material if necessary.
C. Use AWS CloudHSM to store the keys and then use the CloudHSM API or the PKCS11 library to delete the keys if necessary.
D. Use the Systems Manager Parameter Store to store the keys and then use the service API operations to delete the key if necessary.

Answer: C

Explanation:
https://docs.aws.amazon.com/kms/latest/developerguide/importing-keys-delete-key-material.html

NEW QUESTION 284
- (Exam Topic 2)
In response to the past DDoS attack experiences, a Security Engineer has set up an Amazon CloudFront distribution for an Amazon S3 bucket. There is concern that some users may bypass the CloudFront distribution and access the S3 bucket directly.
What must be done to prevent users from accessing the S3 objects directly by using URLs?

A. Change the S3 bucket/object permission so that only the bucket owner has access.
B. Set up a CloudFront origin access identity (OAI), and change the S3 bucket/object permission so that only the OAI has access.
C. Create IAM roles for CloudFront, and change the S3 bucket/object permission so that only the IAM role has access.
D. Redirect S3 bucket access to the corresponding CloudFront distribution.

Answer: B

Explanation:
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3

NEW QUESTION 285
- (Exam Topic 2)
Which option for the use of the AWS Key Management Service (KMS) supports key management best practices that focus on minimizing the potential scope of data exposed by a possible future key compromise?

A. Use KMS automatic key rotation to replace the master key, and use this new master key for future encryption operations without re-encrypting previously encrypted data.
B. Generate a new Customer Master Key (CMK), re-encrypt all existing data with the new CMK, and use it for all future encryption operations.
C. Change the CMK alias every 90 days, and update key-calling applications with the new key alias.
D. Change the CMK permissions to ensure that individuals who can provision keys are not the same individuals who can use the keys.

Answer: B

Explanation:
"automatic key rotation has no effect on the data that the CMK protects. It does not rotate the data keys that the CMK generated or re-encrypt any data protected by the CMK, and it will not mitigate the effect of a compromised data key. You might decide to create a new CMK and use it in place of the original CMK. This has the same effect as rotating the key material in an existing CMK, so it's often thought of as manually rotating the key."
https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html

NEW QUESTION 286
......