Amazon-Web-Services

Exam Questions SCS-C01

AWS Certified Security- Specialty

NEW QUESTION 1
- (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 2
- (Exam Topic 1)
A company is configuring three Amazon EC2 instances with each instance in a separate Availability Zone. The EC2 instances wilt be used as transparent proxies for outbound internet traffic for ports 80 and 443 so the proxies can block traffic to certain internet destinations as required by the company's security policies. A Security Engineer completed the following:
• Set up the proxy software on the EC2 instances.
• Modified the route tables on the private subnets to use the proxy EC2 instances as the default route.
• Created a security group rule opening inbound port 80 and 443 TCP protocols on the proxy EC2 instance security group.
However, the proxy EC2 instances are not successfully forwarding traffic to the internet.
What should the Security Engineer do to make the proxy EC2 instances route traffic to the internet?

A. Put all the proxy EC2 instances in a cluster placement group.
B. Disable source and destination checks on the proxy EC2 instances.
C. Open all inbound ports on the proxy EC2 instance security group.
D. Change the VPC's DHCP domain-name-servers options set to the IP addresses of proxy EC2 instances.

Answer: B

NEW QUESTION 3
- (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 4
- (Exam Topic 1)
A company has a VPC with several Amazon EC2 instances behind a NAT gateway. The company's security policy states that all network traffic must be logged and must include the original source and destination IP addresses. The existing VPC Flow Logs do not include this information. A security engineer needs to recommend a solution.
Which combination of steps should the security engineer recommend? (Select TWO)

A. Edit the existing VPC Flow Log
B. Change the log format of the VPC Flow Logs from the Amazon default format to a custom format.
C. Delete and recreate the existing VPC Flow Log
D. Change the log format of the VPC Flow Logs from the Amazon default format to a custom format.
E. Change the destination to Amazon CloudWatch Logs.
F. Include the pkt-srcaddr and pkt-dstaddr fields in the log format.
G. Include the subnet-id and instance-id fields in the log format.

Answer: AE

NEW QUESTION 5
- (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 6
- (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 7
- (Exam Topic 1)
A Security Engineer is setting up an AWS CloudTrail trail for all regions in an AWS account. For added security, the logs are stored using server-side encryption with AWS KMS-managed keys (SSE-KMS) and have log integrity validation enabled.
While testing the solution, the Security Engineer discovers that the digest files are readable, but the log files are not. What is the MOST likely cause?

A. The log files fail integrity validation and automatically are marked as unavailable.
B. The KMS key policy does not grant the Security Engineer's IAM user or role permissions to decrypt with it.
C. The bucket is set up to use server-side encryption with Amazon S3-managed keys (SSE-S3) as the default and does not allow SSE-KMS-encrypted files.
D. An IAM policy applicable to the Security Engineer's IAM user or role denies access to the "CloudTrail/" prefix in the Amazon S3 bucket

Answer: D

NEW QUESTION 8
- (Exam Topic 1)
A Security Engineer has launched multiple Amazon EC2 instances from a private AMI using an AWS CloudFormation template. The Engineer notices instances terminating right after they are launched.
What could be causing these terminations?

A. The IAM user launching those instances is missing ec2:Runinstances permission.
B. The AMI used as encrypted and the IAM does not have the required AWS KMS permissions.
C. The instance profile used with the EC2 instances in unable to query instance metadata.
D. AWS currently does not have sufficient capacity in the Region.

Answer: C

NEW QUESTION 9
- (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 10
- (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 10
- (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 11
- (Exam Topic 1)
A company needs its Amazon Elastic Block Store (Amazon EBS) volumes to be encrypted at all times. During a security incident. EBS snapshots of suspicious instances are shared to a forensics account for analysis A security engineer attempting to share a suspicious EBS snapshot to the forensics account receives the following error
"Unable to share snapshot: An error occurred (OperationNotPermitted) when calling the ModifySnapshotAttribute operation: Encrypted snapshots with EBS default key cannot be shared.
Which combination of steps should the security engineer take in the incident account to complete the sharing operation? (Select THREE)

A. Create a customer managed CMK Copy the EBS snapshot encrypting the destination snapshot using the new CMK.
B. Allow forensics accounting principals to use the CMK by modifying its policy.
C. Create an Amazon EC2 instanc
D. Attach the encrypted and suspicious EBS volum
E. Copy data from the suspicious volume to an unencrypted volum
F. Snapshot the unencrypted volume
G. Copy the EBS snapshot to the new decrypted snapshot
H. Restore a volume from the suspicious EBS snapsho
I. Create an unencrypted EBS volume of the samesize.
J. Share the target EBS snapshot with the forensics account.

Answer: ABF

NEW QUESTION 14
- (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 15
- (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 19
- (Exam Topic 1)
The Development team receives an error message each time the team members attempt to encrypt or decrypt a Secure String parameter from the SSM Parameter Store by using an AWS KMS customer managed key (CMK).
Which CMK-related issues could be responsible? (Choose two.)

A. The CMK specified in the application does not exist.
B. The CMK specified in the application is currently in use.
C. The CMK specified in the application is using the CMK KeyID instead of CMK Amazon Resource Name.
D. The CMK specified in the application is not enabled.
E. The CMK specified in the application is using an alias.

Answer: AD

Explanation:
https://docs.amazonaws.cn/en_us/kms/latest/developerguide/services-parameter-store.html

NEW QUESTION 20
- (Exam Topic 1)
A company's Security Engineer has been asked to monitor and report all AWS account root user activities. Which of the following would enable the Security Engineer to monitor and report all root user activities?
(Select TWO)

A. Configuring AWS Organizations to monitor root user API calls on the paying account
B. Creating an Amazon CloudWatch Events rule that will trigger when any API call from the root user isreported
C. Configuring Amazon Inspector to scan the AWS account for any root user activity
D. Configuring AWS Trusted Advisor to send an email to the Security team when the root user logs in to the console
E. Using Amazon SNS to notify the target group

Answer: BE

NEW QUESTION 21
- (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 26
- (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 28
- (Exam Topic 1)

A Developer signed in to a new account within an AWS Organizations organizations unit (OU) containing multiple accounts. Access to the Amazon S3 service is restricted with the following SCP:

How can the Security Engineer provide the Developer with Amazon S3 access without affecting other accounts?

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

Answer: B

NEW QUESTION 31
- (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 33
- (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 34
- (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 37
- (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 42
- (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 44
- (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 CLI 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 CLI 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 48
- (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 52
- (Exam Topic 1)
A company's security team has defined a set of AWS Config rules that must be enforced globally in all AWS accounts the company owns. What should be done to provide a consolidated compliance overview for the security team?

A. Use AWS Organizations to limit AWS Config rules to the appropriate Regions, and then consolidate the Amazon CloudWatch dashboard into one AWS account.
B. Use AWS Config aggregation to consolidate the views into one AWS account, and provide role access to the security team.
C. Consolidate AWS Config rule results with an AWS Lambda function and push data to Amazon SQ
D. Use Amazon SNS to consolidate and alert when some metrics are triggered.
E. Use Amazon GuardDuty to load data results from the AWS Config rules compliance status, aggregate GuardDuty findings of all AWS accounts into one AWS account, and provide role access to the security team.

Answer: B

NEW QUESTION 56
- (Exam Topic 1)
A security engineer has noticed an unusually high amount of traffic coming from a single IP address. This was discovered by analyzing the Application Load Balancer's access logs. How can the security engineer limit the number of requests from a specific IP address without blocking the IP address?

A. Add a rule to the Application Load Balancer to route the traffic originating from the IP address in question and show a static webpage.
B. Implement a rate-based rule with AWS WAF
C. Use AWS Shield to limit the originating traffic hit rate.
D. Implement the GeoLocation feature in Amazon Route 53.

Answer: C

NEW QUESTION 59
- (Exam Topic 1)
A company has a website with an Amazon CloudFront HTTPS distribution, an Application Load Balancer (ALB) with multiple web instances for dynamic website content, and an Amazon S3 bucket for static website content. The company's security engineer recently updated the website security requirements:
• HTTPS needs to be enforced for all data in transit with specific ciphers.
• The CloudFront distribution needs to be accessible from the internet only. Which solution will meet these requirements?

A. Set up an S3 bucket policy with the awssecuretransport key Configure the CloudFront origin access identity (OAI) with the S3 bucket Configure CloudFront to use specific cipher
B. Enforce the ALB with an HTTPS listener only and select the appropriate security policy for the ciphers Link the ALB with AWS WAF to allow access from the CloudFront IP ranges.
C. Set up an S3 bucket policy with the aws:securetransport ke
D. Configure the CloudFront origin access identity (OAI) with the S3 bucke
E. Enforce the ALB with an HTTPS listener only and select the appropriate security policy for the ciphers.
F. Modify the CloudFront distribution to use AWS WA
G. Force HTTPS on the S3 bucket with specific ciphers in the bucket polic
H. Configure an HTTPS listener only for the AL
I. Set up a security group to limit access to the ALB from the CloudFront IP ranges
J. Modify the CloudFront distribution to use the ALB as the origi
K. Enforce an HTTPS listener on the AL
L. Create a path-based routing rule on the ALB with proxies that connect lo Amazon S3. Create a bucket policy to allow access from these proxies only.A company Is trying to replace its on-premises bastion hosts used to access on-premises Linux servers with AWS Systems Manager Session Manage
M. A security engineer has installed the Systems Manager Agent on all server
N. The security engineer verifies that the agent is running on all the servers, but Session Manager cannot connect to the
O. The security engineer needs to perform verification steps before Session Manager will work on the servers.Which combination of steps should the security engineer perform? (Select THREE.)
P. Open inbound port 22 to 0 0.0.0/0 on all Linux servers.
Q. Enable the advanced-instances tier in Systems Manager.
R. Create a managed-instance activation for the on-premises servers.
S. Reconfigure the Systems Manager Agent with the activation code and ID.
T. Assign an IAM role to all of the on-premises servers.
. Initiate an inventory collection with Systems Manager on the on-premises servers

Answer: CEF

NEW QUESTION 64
- (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 66
- (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 70
- (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

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 74
- (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. 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 77
- (Exam Topic 2)
A Security Engineer received an AWS Abuse Notice listing EC2 instance IDs that are reportedly abusing other hosts.
Which action should the Engineer take based on this situation? (Choose three.)

A. Use AWS Artifact to capture an exact image of the state of each instance.
B. Create EBS Snapshots of each of the volumes attached to the compromised instances.
C. Capture a memory dump.
D. Log in to each instance with administrative credentials to restart the instance.
E. Revoke all network ingress and egress except for to/from a forensics workstation.
F. Run Auto Recovery for Amazon EC2.

Answer: BEF

NEW QUESTION 80
- (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:

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

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 84
- (Exam Topic 2)
A company has Windows Amazon EC2 instances in a VPC that are joined to on-premises Active Directory servers for domain services. The security team has enabled Amazon GuardDuty on the AWS account to alert on issues with the instances.
During a weekly audit of network traffic, the Security Engineer notices that one of the EC2 instances is attempting to communicate with a known command-and-control server but failing. This alert does not show up in GuardDuty.
Why did GuardDuty fail to alert to this behavior?

A. GuardDuty did not have the appropriate alerts activated.
B. GuardDuty does not see these DNS requests.
C. GuardDuty only monitors active network traffic flow for command-and-control activity.
D. GuardDuty does not report on command-and-control activity.

Answer: B

Explanation:
https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_data-sources.html https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_backdoor.html

NEW QUESTION 87
- (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:

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 91
- (Exam Topic 2)
The Security Engineer implemented a new vault lock policy for 10TB of data and called initiate-vault-lock 12 hours ago. The Audit team identified a typo that is allowing incorrect access to the vault.
What is the MOST cost-effective way to correct this?

A. Call the abort-vault-lock operation, fix the typo, and call the initiate-vault-lock again.
B. Copy the vault data to Amazon S3, delete the vault, and create a new vault with the data.
C. Update the policy, keeping the vault lock in place.
D. Update the policy and call initiate-vault-lock again to apply the new policy.

Answer: A

Explanation:
Initiate the lock by attaching a vault lock policy to your vault, which sets the lock to an in-progress state and returns a lock ID. While in the in-progress state, you have 24 hours to validate your vault lock policy before the lock ID expires. Use the lock ID to complete the lock process. If the vault lock policy doesn't work as expected, you can abort the lock and restart from the beginning. For information on how to use the S3 Glacier API to lock a vault, see Locking a Vault by Using the Amazon S3 Glacier API. https://docs.aws.amazon.com/amazonglacier/latest/dev/vault-lock-policy.html

NEW QUESTION 95
- (Exam Topic 2)
A Security Engineer is building a Java application that is running on Amazon EC2. The application communicates with an Amazon RDS instance and authenticates with a user name and password.
Which combination of steps can the Engineer take to protect the credentials and minimize downtime when the credentials are rotated? (Choose two.)

A. Have a Database Administrator encrypt the credentials and store the ciphertext in Amazon S3. Grant permission to the instance role associated with the EC2 instance to read the object and decrypt the ciphertext.
B. Configure a scheduled job that updates the credential in AWS Systems Manager Parameter Store and notifies the Engineer that the application needs to be restarted.
C. Configure automatic rotation of credentials in AWS Secrets Manager.
D. Store the credential in an encrypted string parameter in AWS Systems Manager Parameter Stor
E. Grant permission to the instance role associated with the EC2 instance to access the parameter and the AWS KMS key that is used to encrypt it.
F. Configure the Java application to catch a connection failure and make a call to AWS Secrets Manager to retrieve updated credentials when the password is rotate
G. Grant permission to the instance role associated with the EC2 instance to access Secrets Manager.

Answer: CE

NEW QUESTION 96
- (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 99
- (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 104
- (Exam Topic 2)
You want to get a list of vulnerabilities for an EC2 Instance as per the guidelines set by the Center of Internet Security. How can you go about doing this?
Please select:

A. Enable AWS Guard Duty for the Instance
B. Use AWS Trusted Advisor
C. Use AWS inspector
D. UseAWSMacie

Answer: C

Explanation:
The AWS Inspector service can inspect EC2 Instances based on specific Rules. One of the rules packages is based on the guidelines set by the Center of Internet Security
Center for Internet security (CIS) Benchmarks
The CIS Security Benchmarks program provides well-defined, un-biased and consensus-based industry best practices to help organizations assess and improve their security. Amazon Web Services is a CIS Security Benchmarks Member company and the list of Amazon Inspector certifications can be viewed nere.
Option A is invalid because this can be used to protect an instance but not give the list of vulnerabilities Options B and D are invalid because these services cannot give a list of vulnerabilities For more information
on the guidelines, please visit the below URL:
* https://docs.aws.amazon.com/inspector/latest/userguide/inspector_cis.html The correct answer is: Use AWS Inspector
Submit your Feedback/Queries to our Experts

NEW QUESTION 105
- (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 108
- (Exam Topic 2)
A Security Engineer must add additional protection to a legacy web application by adding the following HTTP security headers:
-Content Security-Policy
-X-Frame-Options
-X-XSS-Protection
The Engineer does not have access to the source code of the legacy web application. Which of the following approaches would meet this requirement?

A. Configure an Amazon Route 53 routing policy to send all web traffic that does not include the required headers to a black hole.
B. Implement an AWS Lambda@Edge origin response function that inserts the required headers.
C. Migrate the legacy application to an Amazon S3 static website and front it with an Amazon CloudFront distribution.
D. Construct an AWS WAF rule to replace existing HTTP headers with the required security headers by using regular expressions.

Answer: B

NEW QUESTION 111
- (Exam Topic 2)
A company plans to move most of its IT infrastructure to AWS. They want to leverage their existing on-premises Active Directory as an identity provider for AWS.
Which combination of steps should a Security Engineer take to federate the company's on-premises Active Directory with AWS? (Choose two.)

A. Create IAM roles with permissions corresponding to each Active Directory group.
B. Create IAM groups with permissions corresponding to each Active Directory group.
C. Configure Amazon Cloud Directory to support a SAML provider.
D. Configure Active Directory to add relying party trust between Active Directory and AWS.
E. Configure Amazon Cognito to add relying party trust between Active Directory and AWS.

Answer: AD

Explanation:

https://aws.amazon.com/blogs/security/how-to-establish-federated-access-to-your-aws-resources-by-using-activ

NEW QUESTION 112
- (Exam Topic 2)
Which approach will generate automated security alerts should too many unauthorized AWS API requests be identified?

A. Create an Amazon CloudWatch metric filter that looks for API call error codes and then implement an alarm based on that metric's rate.
B. Configure AWS CloudTrail to stream event data to Amazon Kinesi
C. Configure an AWS Lambda function on the stream to alarm when the threshold has been exceeded.
D. Run an Amazon Athena SQL query against CloudTrail log file
E. Use Amazon QuickSight to create an operational dashboard.
F. Use the Amazon Personal Health Dashboard to monitor the account's use of AWS services, and raise an alert if service error rates increase.

Answer: A

Explanation:
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail.html#cloudwatch- Open the CloudWatch console at https://console.aws.amazon.com/cloudwatch/. In the navigation pane, choose Logs. In the list of log groups, select the check box next to the log group that you created for CloudTrail log events. Choose Create Metric Filter. On the Define Logs Metric Filter screen, choose Filter Pattern and then type the following: { ($.errorCode = "*UnauthorizedOperation") || ($.errorCode = "AccessDenied*") } Choose Assign Metric. For Filter Name, type AuthorizationFailures. For Metric Namespace, type CloudTrailMetrics. For Metric Name, type AuthorizationFailureCount.

NEW QUESTION 114
- (Exam Topic 2)
A Security Engineer has been asked to create an automated process to disable IAM user access keys that are more than three months old.
Which of the following options should the Security Engineer use?

A. In the AWS Console, choose the IAM service and select "Users". Review the "Access Key Age" column.
B. Define an IAM policy that denies access if the key age is more than three months and apply to all users.
C. Write a script that uses the GenerateCredentialReport, GetCredentialReport, and UpdateAccessKey APIs.
D. Create an Amazon CloudWatch alarm to detect aged access keys and use an AWS Lambda function to disable the keys older than 90 days.

Answer: C

Explanation:
https://docs.aws.amazon.com/IAM/latest/APIReference/API_UpdateAccessKey.html
https://docs.aws.amazon.com/IAM/latest/APIReference/API_GenerateCredentialReport.html
https://docs.aws.amazon.com/IAM/latest/APIReference/API_GetCredentialReport.html

NEW QUESTION 115
- (Exam Topic 2)
You have a 2 tier application hosted in AWS. It consists of a web server and database server (SQL Server) hosted on separate EC2 Instances. You are devising the security groups for these EC2 Instances. The Web tier needs to be accessed by users across the Internet. You have created a web security group(wg-123) and database security group(db-345). Which combination of the following security group rules will allow the application to be secure and functional. Choose 2 answers from the options given below.
Please select:

A. wg-123 -Allow ports 80 and 443 from 0.0.0.0/0
B. db-345 - Allow port 1433 from wg-123
C. wg-123 - Allow port 1433 from wg-123
D. db-345 -Allow ports 1433 from 0.0.0.0/0

Answer: AB

Explanation:
The Web security groups should allow access for ports 80 and 443 for HTTP and HTTPS traffic to all users from the internet.
The database security group should just allow access from the web security group from port 1433. Option C is invalid because this is not a valid configuration
Option D is invalid because database security should not be allowed on the internet For more information on Security Groups please visit the below URL:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/usins-network-security.htmll
The correct answers are: wg-123 - Allow ports 80 and 443 from 0.0.0.0/0, db-345 - Allow port 1433 from wg-123
Submit your Feedback/Queries to our Experts

NEW QUESTION 118
- (Exam Topic 2)
An organization has a system in AWS that allows a large number of remote workers to submit data files. File sizes vary from a few kilobytes to several megabytes.
A recent audit highlighted a concern that data files are not encrypted while in transit over untrusted networks.
Which solution would remediate the audit finding while minimizing the effort required?

A. Upload an SSL certificate to IAM, and configure Amazon CloudFront with the passphrase for the private key.
B. Call KMS.Encrypt() in the client, passing in the data file contents, and call KMS.Decrypt() server-side.
C. Use AWS Certificate Manager to provision a certificate on an Elastic Load Balancing in front of the web service's servers.
D. Create a new VPC with an Amazon VPC VPN endpoint, and update the web service's DNS record.

Answer: C

NEW QUESTION 122
- (Exam Topic 2)
Compliance requirements state that all communications between company on-premises hosts and EC2 instances be encrypted in transit. Hosts use custom

proprietary protocols for their communication, and EC2 instances need to be fronted by a load balancer for increased availability.
Which of the following solutions will meet these requirements?

A. Offload SSL termination onto an SSL listener on a Classic Load Balancer, and use a TCP connection between the load balancer and the EC2 instances.
B. Route all traffic through a TCP listener on a Classic Load Balancer, and terminate the TLS connection on the EC2 instances.
C. Create an HTTPS listener using an Application Load Balancer, and route all of the communication through that load balancer.
D. Offload SSL termination onto an SSL listener using an Application Load Balancer, and re-spawn and SSL connection between the load balancer and the EC2 instances.

Answer: B

Explanation:
https://aws.amazon.com/blogs/compute/maintaining-transport-layer-security-all-the-way-to-your-container-usin

NEW QUESTION 127
- (Exam Topic 2)
A water utility company uses a number of Amazon EC2 instances to manage updates to a fleet of 2,000 Internet of Things (IoT) field devices that monitor water quality. These devices each have unique access credentials.
An operational safety policy requires that access to specific credentials is independently auditable. What is the MOST cost-effective way to manage the storage of credentials?

A. Use AWS Systems Manager to store the credentials as Secure Strings Parameter
B. Secure by using an AWS KMS key.
C. Use AWS Key Management System to store a master key, which is used to encrypt the credential
D. The encrypted credentials are stored in an Amazon RDS instance.
E. Use AWS Secrets Manager to store the credentials.
F. Store the credentials in a JSON file on Amazon S3 with server-side encryption.

Answer: A

Explanation:
https://docs.aws.amazon.com/systems-manager/latest/userguide/parameter-store-advanced-parameters.html

NEW QUESTION 129
- (Exam Topic 2)
A company has a forensic logging use case whereby several hundred applications running on Docker on EC2 need to send logs to a central location. The Security Engineer must create a logging solution that is able to perform real-time analytics on the log files, grants the ability to replay events, and persists data.
Which AWS Services, together, can satisfy this use case? (Select two.)

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

Answer: AB

Explanation:
https://docs.aws.amazon.com/whitepapers/latest/aws-overview/analytics.html#amazon-athena

NEW QUESTION 131
- (Exam Topic 2)
A company has deployed a custom DNS server in AWS. The Security Engineer wants to ensure that Amazon EC2 instances cannot use the Amazon-provided DNS.
How can the Security Engineer block access to the Amazon-provided DNS in the VPC?

A. Deny access to the Amazon DNS IP within all security groups.
B. Add a rule to all network access control lists that deny access to the Amazon DNS IP.
C. Add a route to all route tables that black holes traffic to the Amazon DNS IP.
D. Disable DNS resolution within the VPC configuration.

Answer: D

Explanation:
https://docs.aws.amazon.com/vpc/latest/userguide/vpc-dns.html

NEW QUESTION 136
- (Exam Topic 2)
A Security Engineer is working with the development team to design a supply chain application that stores sensitive inventory data in an Amazon S3 bucket. The application will use an AWS KMS customer master key (CMK) to encrypt the data on Amazon S3. The inventory data on Amazon S3 will be shared of vendors. All vendors will use AWS principals from their own AWS accounts to access the data on Amazon S3. The vendor list may change weekly, and the solution must support cross-account access.
What is the MOST efficient way to manage access control for the KMS CMK7?

A. Use KMS grants to manage key acces
B. Programmatically create and revoke grants to manage vendor access.
C. Use an IAM role to manage key acces
D. Programmatically update the IAM role policies to manage vendor access.
E. Use KMS key policies to manage key acces

F. Programmatically update the KMS key policies to manage vendor access.
G. Use delegated access across AWS accounts by using IAM roles to manage key access.Programmatically update the IAM trust policy to manage cross-account vendor access.

Answer: A

NEW QUESTION 138
- (Exam Topic 2)
An Amazon EC2 instance is denied access to a newly created AWS KMS CMK used for decrypt actions. The environment has the following configuration:

The instance is allowed the kms:Decrypt action in its IAM role for all resources
The AWS KMS CMK status is set to enabled
The instance can communicate with the KMS API using a configured VPC endpoint What is causing the issue?

A. The kms:GenerateDataKey permission is missing from the EC2 instance's IAM role
B. The ARN tag on the CMK contains the EC2 instance's ID instead of the instance's ARN
C. The kms:Encrypt permission is missing from the EC2 IAM role
D. The KMS CMK key policy that enables IAM user permissions is missing

Answer: A

Explanation:
In a key policy, you use "*" for the resource, which means "this CMK." A key policy applies only to the CMK it is attached to
References:

NEW QUESTION 139
- (Exam Topic 2)
A Lambda function reads metadata from an S3 object and stores the metadata in a DynamoDB table. The function is triggered whenever an object is stored within the S3 bucket.
How should the Lambda function be given access to the DynamoDB table? Please select:

A. Create a VPC endpoint for DynamoDB within a VP
B. Configure the Lambda function to access resources in the VPC.
C. Create a resource policy that grants the Lambda function permissions to write to the DynamoDB table.Attach the poll to the DynamoDB table.
D. Create an IAM user with permissions to write to the DynamoDB tabl
E. Store an access key for that user in the Lambda environment variables.
F. Create an IAM service role with permissions to write to the DynamoDB tabl
G. Associate that role with the Lambda function.

Answer: D

Explanation:
The ideal way is to create an IAM role which has the required permissions and then associate it with the Lambda function
The AWS Documentation additionally mentions the following
Each Lambda function has an IAM role (execution role) associated with it. You specify the IAM role when you create your Lambda function. Permissions you grant to this role determine what AWS Lambda can do when it assumes the role. There are two types of permissions that you grant to the IAM role:
If your Lambda function code accesses other AWS resources, such as to read an object from an S3 bucket or write logs to CloudWatch Logs, you need to grant permissions for relevant Amazon S3 and CloudWatch actions to the role.
If the event source is stream-based (Amazon Kinesis Data Streams and DynamoDB streams), AWS Lambda polls these streams on your behalf. AWS Lambda needs permissions to poll the stream and read new records on the stream so you need to grant the relevant permissions to this role.
Option A is invalid because the VPC endpoint allows access instances in a private subnet to access DynamoDB
Option B is invalid because resources policies are present for resources such as S3 and KMS, but not AWS Lambda
Option C is invalid because AWS Roles should be used and not IAM Users
For more information on the Lambda permission model, please visit the below URL: https://docs.aws.amazon.com/lambda/latest/dg/intro-permission-model.html
The correct answer is: Create an IAM service role with permissions to write to the DynamoDB table. Associate that role with the Lambda function.
Submit your Feedback/Queries to our Exp

NEW QUESTION 141
- (Exam Topic 2)
The Security team believes that a former employee may have gained unauthorized access to AWS resources sometime in the past 3 months by using an identified access key.
What approach would enable the Security team to find out what the former employee may have done within AWS?

A. Use the AWS CloudTrail console to search for user activity.
B. Use the Amazon CloudWatch Logs console to filter CloudTrail data by user.
C. Use AWS Config to see what actions were taken by the user.
D. Use Amazon Athena to query CloudTrail logs stored in Amazon S3.

Answer: A

Explanation:
You can use CloudTrail to search event history for the last 90 days. You can use CloudWatch queries to search API history beyond the last 90 days. You can use Athena to query CloudTrail logs over the last 90 days. https://aws.amazon.com/premiumsupport/knowledge-center/view-iam-history/

NEW QUESTION 145
- (Exam Topic 2)
You have an Ec2 Instance in a private subnet which needs to access the KMS service. Which of the following methods can help fulfil this requirement, keeping security in perspective
Please select:

A. Use a VPC endpoint
B. Attach an Internet gateway to the subnet
C. Attach a VPN connection to the VPC
D. Use VPC Peering

Answer: A

Explanation:
The AWS Documentation mentions the following
You can connect directly to AWS KMS through a private endpoint in your VPC instead of connecting over the internet. When you use a VPC endpoint communication between your VPC and AWS KMS is conducted entirely within the AWS network.
Option B is invalid because this could open threats from the internet
Option C is invalid because this is normally used for communication between on-premise environments and AWS.
Option D is invalid because this is normally used for communication between VPCs
For more information on accessing KMS via an endpoint, please visit the following URL https://docs.aws.amazon.com/kms/latest/developerguide/kms-vpc-endpoint.htmll
The correct answer is: Use a VPC endpoint Submit your Feedback/Queries to our Experts

NEW QUESTION 146
- (Exam Topic 2)
An organization operates a web application that serves users globally. The application runs on Amazon EC2 instances behind an Application Load Balancer. There is an Amazon CloudFront distribution in front of the load balancer, and the organization uses AWS WAF. The application is currently experiencing a volumetric attack whereby the attacker is exploiting a bug in a popular mobile game.
The application is being flooded with HTTP requests from all over the world with the User-Agent set to the following string: Mozilla/5.0 (compatible; ExampleCorp; ExampleGame/1.22; Mobile/1.0)
What mitigation can be applied to block attacks resulting from this bug while continuing to service legitimate requests?

A. Create a rule in AWS WAF rules with conditions that block requests based on the presence of ExampleGame/1.22 in the User-Agent header
B. Create a geographic restriction on the CloudFront distribution to prevent access to the application from most geographic regions
C. Create a rate-based rule in AWS WAF to limit the total number of requests that the web application services.
D. Create an IP-based blacklist in AWS WAF to block the IP addresses that are originating from requests that contain ExampleGame/1.22 in the User-Agent header.

Answer: A

Explanation:
Since all the attack has http header- User-Agent set to string: Mozilla/5.0 (compatible; ExampleCorp;) it would be much more easier to block these attack by simply denying traffic with the header match . HTH ExampleGame/1.22; Mobile/1.0)

NEW QUESTION 150
- (Exam Topic 3)
A company has an existing AWS account and a set of critical resources hosted in that account. The employee who was in-charge of the root account has left the company. What must be now done to secure the account. Choose 3 answers from the options given below.
Please select:

A. Change the access keys for all IAM users.
B. Delete all custom created IAM policies
C. Delete the access keys for the root account
D. Confirm MFAtoa secure device
E. Change the password for the root account
F. Change the password for all IAM users

Answer: CDE

Explanation:
Now if the root account has a chance to be compromised, then you have to carry out the below steps

* 1. Delete the access keys for the root account
* 2. Confirm MFA to a secure device
* 3. Change the password for the root account
This will ensure the employee who has left has no change to compromise the resources in AWS. Option A is invalid because this would hamper the working of the current IAM users
Option B is invalid because this could hamper the current working of services in your AWS account Option F is invalid because this would hamper the working of the current IAM users
For more information on IAM root user, please visit the following URL: https://docs.aws.amazon.com/IAM/latest/UserGuide/id root-user.html
The correct answers are: Delete the access keys for the root account Confirm MFA to a secure device. Change the password for the root account
Submit Your Feedback/Queries to our Experts

NEW QUESTION 154
- (Exam Topic 3)
A company has a web-based application using Amazon CloudFront and running on Amazon Elastic Container Service (Amazon ECS) behind an Application Load Balancer (ALB). The ALB is terminating TLS and balancing load across ECS service tasks A security engineer needs to design a solution to ensure that application content is accessible only through CloudFront and that I is never accessible directly.
How should the security engineer build the MOST secure solution?

A. Add an origin custom header Set the viewer protocol policy to HTTP and HTTPS Set the origin protocol pokey to HTTPS only Update the application to validate the CloudFront custom header
B. Add an origin custom header Set the viewer protocol policy to HTTPS only Set the origin protocol policy to match viewer Update the application to validate the CloudFront custom header.
C. Add an origin custom header Set the viewer protocol policy to redirect HTTP to HTTPS Set the origin protocol policy to HTTP only Update the application to validate the CloudFront custom header.
D. Add an origin custom header Set the viewer protocol policy to redirect HTTP to HTTP
E. Set the origin protocol policy to HTTPS only Update the application to validate the CloudFront custom header

Answer: D

NEW QUESTION 157
- (Exam Topic 3)
You are trying to use the Systems Manager to patch a set of EC2 systems. Some of the systems are not getting covered in the patching process. Which of the following can be used to troubleshoot the issue? Choose 3 answers from the options given below.
Please select:

A. Check to see if the right role has been assigned to the EC2 instances
B. Check to see if the IAM user has the right permissions for EC2
C. Ensure that agent is running on the instances.
D. Check the Instance status by using the Health API.

Answer: ACD

Explanation:
For ensuring that the instances are configured properly you need to ensure the followi .
1) You installed the latest version of the SSM Agent on your instance
2) Your instance is configured with an AWS Identity and Access Management (IAM) role that enables the instance to communicate with the Systems Manager API
3) You can use the Amazon EC2 Health API to quickly determine the following information about Amazon EC2 instances The status of one or more instances
The last time the instance sent a heartbeat value The version of the SSM Agent
The operating system
The version of the EC2Config service (Windows) The status of the EC2Config service (Windows)
Option B is invalid because IAM users are not supposed to be directly granted permissions to EC2 Instances For more information on troubleshooting AWS SSM, please visit the following URL:
https://docs.aws.amazon.com/systems-manager/latest/userguide/troubleshooting-remote-commands.html The correct answers are: Check to see if the right role has been assigned to the EC2 Instances, Ensure that
agent is running on the Instances., Check the Instance status by using the Health API.
Submit your Feedback/Queries to our Experts

NEW QUESTION 158
- (Exam Topic 3)
A customer has an instance hosted in the AWS Public Cloud. The VPC and subnet used to host the Instance have been created with the default settings for the Network Access Control Lists. They need to provide an IT Administrator secure access to the underlying instance. How can this be accomplished.
Please select:

A. Ensure the Network Access Control Lists allow Inbound SSH traffic from the IT Administrator's Workstation
B. Ensure the Network Access Control Lists allow Outbound SSH traffic from the IT Administrator's Workstation
C. Ensure that the security group allows Inbound SSH traffic from the IT Administrator's Workstation
D. Ensure that the security group allows Outbound SSH traffic from the IT Administrator's Workstation

Answer: C

Explanation:
Options A & B are invalid as default NACL rule will allow all inbound and outbound traffic.
The requirement is that the IT administrator should be able to access this EC2 instance from his workstation. For that we need to enable the Security Group of EC2 instance to allow traffic from the IT administrator's workstation. Hence option C is correct.
Option D is incorrect as we need to enable the Inbound SSH traffic on the EC2 instance Security Group since the traffic originate' , from the IT admin's workstation.
The correct answer is: Ensure that the security group allows Inbound SSH traffic from the IT Administrator's Workstation Submit your Feedback/Queries to our Experts

NEW QUESTION 163

- (Exam Topic 3)
You have an Amazon VPC that has a private subnet and a public subnet in which you have a NAT instance server. You have created a group of EC2 instances that configure themselves at startup by downloading a bootstrapping script from S3 that deploys an application via GIT.
Which one of the following setups would give us the highest level of security? Choose the correct answer from the options given below.
Please select:

A. EC2 instances in our public subnet, no EIPs, route outgoing traffic via the IGW
B. EC2 instances in our public subnet, assigned EIPs, and route outgoing traffic via the NAT
C. EC2 instance in our private subnet, assigned EIPs, and route our outgoing traffic via our IGW
D. EC2 instances in our private subnet, no EIPs, route outgoing traffic via the NAT

Answer: D

Explanation:
The below diagram shows how the NAT instance works. To make EC2 instances very secure, they need to be in a private sub such as the database server shown below with no EIP and all traffic routed via the NAT.
C:\Users\wk\Desktop\mudassar\Untitled.jpg

Options A and B are invalid because the instances need to be in the private subnet
Option C is invalid because since the instance needs to be in the private subnet, you should not attach an EIP to the instance
For more information on NAT instance, please refer to the below Link: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuideA/PC Instance.html!
The correct answer is: EC2 instances in our private subnet no EIPs, route outgoing traffic via the NAT Submit your Feedback/Queries to our Experts

NEW QUESTION 165
- (Exam Topic 3)
An employee keeps terminating EC2 instances on the production environment. You've determined the best way to ensure this doesn't happen is to add an extra layer of defense against terminating the instances. What is the best method to ensure the employee does not terminate the production instances? Choose the 2 correct answers from the options below
Please select:

A. Tag the instance with a production-identifying tag and add resource-level permissions to the employee user with an explicit deny on the terminate API call to instances with the production ta
B. <
C. Tag the instance with a production-identifying tag and modify the employees group to allow only start stop, and reboot API calls and not the terminate instance call.
D. Modify the IAM policy on the user to require MFA before deleting EC2 instances and disable MFA access to the employee
E. Modify the IAM policy on the user to require MFA before deleting EC2 instances

Answer: AB

Explanation:
Tags enable you to categorize your AWS resources in different ways, for example, by purpose, owner, or environment. This is useful when you have many resources of the same type — you can quickly identify a specific resource based on the tags you've assigned to it. Each tag consists of a key and an optional value, both of which you define
Options C&D are incorrect because it will not ensure that the employee cannot terminate the instance. For more information on tagging answer resources please refer to the below URL: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Usins_Tags.htmll
The correct answers are: Tag the instance with a production-identifying tag and add resource-level permissions to the employe user with an explicit deny on the terminate API call to instances with the production tag.. Tag the instance with a production-identifying tag and modify the employees group to allow only start stop, and reboot API calls and not the terminate instance
Submit your Feedback/Queries to our Experts

NEW QUESTION 166
- (Exam Topic 3)
You currently have an S3 bucket hosted in an AWS Account. It holds information that needs be accessed by a partner account. Which is the MOST secure way to allow the partner account to access the S3 bucket in your account? Select 3 options.
Please select:

A. Ensure an IAM role is created which can be assumed by the partner account.
B. Ensure an IAM user is created which can be assumed by the partner account.
C. Ensure the partner uses an external id when making the request
D. Provide the ARN for the role to the partner account
E. Provide the Account Id to the partner account
F. Provide access keys for your account to the partner account

Answer: ACD

Explanation:
Option B is invalid because Roles are assumed and not IAM users
Option E is invalid because you should not give the account ID to the partner Option F is invalid because you should not give the access keys to the partner
The below diagram from the AWS documentation showcases an example on this wherein an IAM role and external ID is us> access an AWS account resources
C:\Users\wk\Desktop\mudassar\Untitled.jpg

For more information on creating roles for external ID'S please visit the following URL:
The correct answers are: Ensure an IAM role is created which can be assumed by the partner account. Ensure the partner uses an external id when making the request Provide the ARN for the role to the partner account
Submit your Feedback/Queries to our Experts

NEW QUESTION 169
- (Exam Topic 3)
A security engineer needs to build a solution to turn AWS CloudTrail back on in multiple AWS Regions in case it is ever turned off.
What is the MOST efficient way to implement this solution?

A. Use AWS Config with a managed rule to trigger the AWS-EnableCloudTrail remediation.
B. Create an Amazon EventBridge (Amazon CloudWatch Events) event with a cloudtrail.amazonaws.com event source and a StartLogging event name to trigger an AWS Lambda function to call the StartLogging API.
C. Create an Amazon CloudWatch alarm with a cloudtrail.amazonaws.com event source and a StopLogging event name to trigger an AWS Lambda function to call the StartLogging API.
D. Monitor AWS Trusted Advisor to ensure CloudTrail logging is enabled.

Answer: B

NEW QUESTION 174
- (Exam Topic 3)
You need to ensure that objects in an S3 bucket are available in another region. This is because of the criticality of the data that is hosted in the S3 bucket. How can you achieve this in the easiest way possible?
Please select:

A. Enable cross region replication for the bucket
B. Write a script to copy the objects to another bucket in the destination region
C. Create an S3 snapshot in the destination region
D. Enable versioning which will copy the objects to the destination region

Answer: A

Explanation:
Option B is partially correct but a big maintenance over head to create and maintain a script when the functionality is already available in S3
Option C is invalid because snapshots are not available in S3 Option D is invalid because versioning will not replicate objects The AWS Documentation mentions the following
Cross-region replication is a bucket-level configuration that enables automatic, asynchronous copying of objects across buck in different AWS Regions.
For more information on Cross region replication in the Simple Storage Service, please visit the below URL:
https://docs.aws.amazon.com/AmazonS3/latest/dev/crr.html
The correct answer is: Enable cross region replication for the bucket Submit your Feedback/Queries to our Experts

NEW QUESTION 179
- (Exam Topic 3)
A company uses Amazon RDS for MySQL as a database engine for its applications. A recent security audit revealed an RDS instance that is not compliant with company policy for encrypting data at rest. A security engineer at the company needs to ensure that all existing RDS databases are encrypted using server-side

encryption and that any future deviations from the policy are detected.
Which combination of steps should the security engineer take to accomplish this? (Select TWO.)

A. Create an AWS Config rule to detect the creation of unencrypted RDS database
B. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to trigger on the AWS Config rules compliance state change and use Amazon Simple Notification Service (Amazon SNS) to notify the security operations team.
C. Use AWS System Manager State Manager to detect RDS database encryption configuration drif
D. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to track state changes and use Amazon Simple Notification Service (Amazon SNS) to notify the security operations team.
E. Create a read replica for the existing unencrypted RDS database and enable replica encryption in the proces
F. Once the replica becomes active, promote it into a standalone database instance and terminate the unencrypted database instance.
G. Take a snapshot of the unencrypted RDS databas
H. Copy the snapshot and enable snapshot encryption in the proces
I. Restore the database instance from the newly created encrypted snapsho
J. Terminate the unencrypted database instance.
K. Enable encryption for the identified unencrypted RDS instance by changing the configurations of the existing database

Answer: AD

NEW QUESTION 184
- (Exam Topic 3)
A company wants to ensure that its AWS resources can be launched only in the us-east-1 and us-west-2 Regions.
What is the MOST operationally efficient solution that will prevent developers from launching Amazon EC2 instances in other Regions?

A. Enable Amazon GuardDuty in all Region
B. Create alerts to detect unauthorized activity outside us-east-1 and us-west-2.
C. Use an organization in AWS Organization
D. Attach an SCP that allows all actions when the aws: Requested Region condition key is either us-east-1 or us-west-2. Delete the FullAWSAccess policy.
E. Provision EC2 resources by using AWS Cloud Formation templates through AWS CodePipelin
F. Allow only the values of us-east-1 and us-west-2 in the AWS CloudFormation template's parameters.
G. Create an AWS Config rule to prevent unauthorized activity outside us-east-1 and us-west-2.

Answer: C

NEW QUESTION 187
- (Exam Topic 3)
Your current setup in AWS consists of the following architecture. 2 public subnets, one subnet which has the web servers accessed by users across the internet and the other subnet for the database server. Which of the following changes to the architecture would add a better security boundary to the resources hosted in your setup
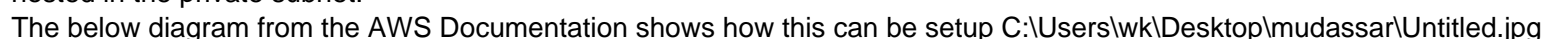Please select:

A. Consider moving the web server to a private subnet
B. Consider moving the database server to a private subnet
C. Consider moving both the web and database server to a private subnet
D. Consider creating a private subnet and adding a NAT instance to that subnet

Answer: B

Explanation:
The ideal setup is to ensure that the web server is hosted in the public subnet so that it can be accessed by users on the internet. The database server can be hosted in the private subnet.
The below diagram from the AWS Documentation shows how this can be setup C:\Users\wk\Desktop\mudassar\Untitled.jpg

Option A and C are invalid because if you move the web server to a private subnet, then it cannot be accessed by users Option D is invalid because NAT instances should be present in the public subnet
For more information on public and private subnets in AWS, please visit the following url com/AmazonVPC/latest/UserGuide/VPC Scenario2.
The correct answer is: Consider moving the database server to a private subnet Submit your Feedback/Queries to our Experts

NEW QUESTION 189
- (Exam Topic 3)
A company wants to monitor the deletion of customer managed CMKs A security engineer must create an alarm that will notify the company before a CMK is deleted The security engineer has configured the integration of AWS CloudTrail with Amazon CloudWatch
What should the security engineer do next to meet this requirement?
Within AWS Key Management Service (AWS KMS} specify the deletion time of the key material during CMK creation AWS KMS will automatically create a CloudWatch.
Create an amazon Eventbridge (Amazon CloudWatch Events) rule to look for API calls of DeleteAlias Create an AWS Lamabda function to send an Amazon Simple Notification Service (Amazon SNS) messages to the company Add the Lambda functions as the target of the Eventbridge (CloudWatch Events) rule.
Create an Amazon EventBridge (Amazon CloudWath Events) rule to look for API calls of DisableKey and ScheduleKeyDeletion. Create an AWS Lambda function to generate the alarm and send the notification to the company. Add the lambda function as the target of the SNS policy.

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

Answer: A

NEW QUESTION 192
- (Exam Topic 3)
A company is using a Redshift cluster to store their data warehouse. There is a requirement from the Internal IT Security team to ensure that data gets encrypted for the Redshift database. How can this be achieved?
Please select:

A. Encrypt the EBS volumes of the underlying EC2 Instances
B. Use AWS KMS Customer Default master key
C. Use SSL/TLS for encrypting the data
D. Use S3 Encryption

Answer: B

Explanation:
The AWS Documentation mentions the following
Amazon Redshift uses a hierarchy of encryption keys to encrypt the database. You can use either AWS Key Management Servic (AWS KMS) or a hardware security module (HSM) to manage the top-level encryption keys in this hierarchy. The process that Amazon Redshift uses for encryption differs depending on how you manage keys.
Option A is invalid because its the cluster that needs to be encrypted
Option C is invalid because this encrypts objects in transit and not objects at rest Option D is invalid because this is used only for objects in S3 buckets
For more information on Redshift encryption, please visit the following URL: https://docs.aws.amazon.com/redshift/latest/memt/workine-with-db-encryption.htmll
The correct answer is: Use AWS KMS Customer Default master key Submit your Feedback/Queries to our Experts

NEW QUESTION 196
- (Exam Topic 3)
A company has multiple Amazon S3 buckets encrypted with customer-managed CMKs Due to regulatory requirements the keys must be rotated every year. The company's Security Engineer has enabled automatic key rotation for the CMKs; however the company wants to verity that the rotation has occurred.
What should the Security Engineer do to accomplish this?

A. Filter AWS CloudTrail logs for KeyRotaton events
B. Monitor Amazon CloudWatcn Events for any AWS KMS CMK rotation events
C. Using the AWS CL
D. run the aws kms gel-key-relation-status operation with the --key-id parameter to check the CMK rotation date
E. Use Amazon Athena to query AWS CloudTrail logs saved in an S3 bucket to filter Generate New Key events

Answer: C

NEW QUESTION 200
- (Exam Topic 3)
Company policy requires that all insecure server protocols, such as FTP, Telnet, HTTP, etc be disabled on all servers. The security team would like to regularly check all servers to ensure compliance with this requirement by using a scheduled CloudWatch event to trigger a review of the current infrastructure. What process will check compliance of the company's EC2 instances?
Please select:

A. Trigger an AWS Config Rules evaluation of the restricted-common-ports rule against every EC2 instance.
B. Query the Trusted Advisor API for all best practice security checks and check for "action recommened" status.
C. Enable a GuardDuty threat detection analysis targeting the port configuration on every EC2 instance.
D. Run an Amazon inspector assessment using the Runtime Behavior Analysis rules package against every EC2 instance.

Answer: D

Explanation:
Option B is incorrect because querying Trusted Advisor API's are not possible
Option C is incorrect because GuardDuty should be used to detect threats and not check the compliance of security protocols.
Option D states that Run Amazon Inspector using runtime behavior analysis rules which will analyze the behavior of your instances during an assessment run, and provide guidance about how to make your EC2 instances more secure.
Insecure Server Protocols
This rule helps determine whether your EC2 instances allow support for insecure and unencrypted ports/services such as FTP, Telnet HTTP, IMAP, POP version 3, SMTP, SNMP versions 1 and 2, rsh, and rlogin.
For more information, please refer to below URL: https://docs.aws.amazon.eom/mspector/latest/userguide/inspector_runtime-behavior-analysis.html#insecure-prot (
The correct answer is: Run an Amazon Inspector assessment using the Runtime Behavior Analysis rules package against every EC2 instance.
Submit your Feedback/Queries to our Experts

NEW QUESTION 204
- (Exam Topic 3)
Your company has been using AWS for hosting EC2 Instances for their web and database applications. They want to have a compliance check to see the following
Whether any ports are left open other than admin ones like SSH and RDP
Whether any ports to the database server other than ones from the web server security group are open Which of the following can help achieve this in the easiest way possible. You don't want to carry out an extra configuration changes?
Please select:

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

Answer: B

Explanation:
Trusted Advisor checks for compliance with the following security recommendations:
Limited access to common administrative ports to only a small subset of addresses. This includes ports 22 (SSH), 23 (Telnet) 3389 (RDP), and 5500 (VNQ.
Limited access to common database ports. This includes ports 1433 (MSSQL Server), 1434 (MSSQL Monitor), 3306 (MySQL), Oracle (1521) and 5432 (PostgreSQL).
Option A is partially correct but then you would need to write custom rules for this. The AWS trusted advisor can give you all o these checks on its dashboard
Option C is incorrect. Amazon Inspector needs a software agent to be installed on all EC2 instances that are included in th.
assessment target, the security of which you want to evaluate with Amazon Inspector. It monitors the behavior of the EC2 instance on which it is installed, including network, file system, and process activity, and collects a wide set of behavior and configuration data (telemetry), which it then passes to the Amazon Inspector service.
Our question's requirement is to choose a choice that is easy to implement. Hence Trusted Advisor is more appropriate for this question.
Options D is invalid because this service dont provide these details.
For more information on the Trusted Advisor, please visit the following URL https://aws.amazon.com/premiumsupport/trustedadvisor>
The correct answer is: AWS Trusted Advisor Submit your Feedback/Queries to our Experts

NEW QUESTION 205
- (Exam Topic 3)
During a manual review of system logs from an Amazon Linux EC2 instance, a Security Engineer noticed that there are sudo commands that were never properly alerted or reported on the Amazon CloudWatch Logs agent
Why were there no alerts on the sudo commands?

A. There is a security group blocking outbound port 80 traffic that is preventing the agent from sending the logs
B. The IAM instance profile on the EC2 instance was not properly configured to allow the CloudWatch Logs agent to push the logs to CloudWatch
C. CloudWatch Logs status is set to ON versus SECURE, which prevents it from pulling in OS security event logs
D. The VPC requires that all traffic go through a proxy, and the CloudWatch Logs agent does not support a proxy configuration.

Answer: B

NEW QUESTION 207
- (Exam Topic 3)
Which of the below services can be integrated with the AWS Web application firewall service. Choose 2 answers from the options given below
Please select:

A. AWS Cloudfront
B. AWS Lambda
C. AWS Application Load Balancer
D. AWS Classic Load Balancer

Answer: AC

Explanation:
The AWS documentation mentions the following on the Application Load Balancer
AWS WAF can be deployed on Amazon CloudFront and the Application Load Balancer (ALB). As part of Amazon CloudFront it car be part of your Content Distribution Network (CDN) protecting your resources and content at the Edge locations and as part of the Application Load Balancer it can protect your origin web servers running behind the ALBs.
Options B and D are invalid because only Cloudfront and the Application Load Balancer services are supported by AWS WAF.
For more information on the web application firewall please refer to the below URL: https://aws.amazon.com/waf/faq;
The correct answers are: AWS Cloudfront AWS Application Load Balancer Submit your Feedback/Queries to our Experts

NEW QUESTION 212
- (Exam Topic 3)
In your LAMP application, you have some developers that say they would like access to your logs. However, since you are using an AWS Auto Scaling group, your instances are constantly being re-created. What would you do to make sure that these developers can access these log files? Choose the correct answer from the options below
Please select:

A. Give only the necessary access to the Apache servers so that the developers can gain access to the log files.
B. Give root access to your Apache servers to the developers.
C. Give read-only access to your developers to the Apache servers.
D. Set up a central logging server that you can use to archive your logs; archive these logs to an S3 bucket for developer-access.

Answer: D

Explanation:
One important security aspect is to never give access to actual servers, hence Option A.B and C are just totally wrong from a security perspective.
The best option is to have a central logging server that can be used to archive logs. These logs can then be stored in S3.
Options A,B and C are all invalid because you should not give access to the developers on the Apache se For more information on S3, please refer to the below link
https://aws.amazon.com/documentation/s3j
The correct answer is: Set up a central logging server that you can use to archive your logs; archive these logs to an S3 bucket for developer-access.
Submit vour Feedback/Queries to our Experts

NEW QUESTION 217
- (Exam Topic 3)
A Security Architect has been asked to review an existing security architecture and identify why the application servers cannot successfully initiate a connection to the database servers. The following summary describes the architecture:
* 1 An Application Load Balancer, an internet gateway, and a NAT gateway are configured in the public subnet
* 2. Database, application, and web servers are configured on three different private subnets.
* 3 The VPC has two route tables: one for the public subnet and one for all other subnets The route table for the public subnet has a 0 0 0 0/0 route to the internet

gateway The route table for all other subnets has a 0 0.0.0/0 route to the NAT gateway. All private subnets can route to each other
* 4 Each subnet has a network ACL implemented that limits all inbound and outbound connectivity to only the required ports and protocols
* 5 There are 3 Security Groups (SGs) database application and web Each group limits all inbound and outbound connectivity to the minimum required
Which of the following accurately reflects the access control mechanisms the Architect should verify1?

A. Outbound SG configuration on database servers Inbound SG configuration on application servers inbound and outbound network ACL configuration on the database subnet Inbound and outbound network ACL configuration on the application server subnet
B. Inbound SG configuration on database servers Outbound SG configuration on application serversInbound and outbound network ACL configuration on the database subnetInbound and outbound network ACL configuration on the application server subnet
C. Inbound and outbound SG configuration on database servers Inbound and outbound SG configuration on application servers Inbound network ACL configuration on the database subnet Outbound network ACL configuration on the application server subnet
D. Inbound SG configuration on database servers Outbound SG configuration on application servers Inbound network ACL configuration on the database subnet Outbound network ACL configuration on the application server subnet.

Answer: A

NEW QUESTION 222
- (Exam Topic 3)
You have a set of 100 EC2 Instances in an AWS account. You need to ensure that all of these instances are patched and kept to date. All of the instances are in a private subnet. How can you achieve this. Choose 2 answers from the options given below
Please select:

A. Ensure a NAT gateway is present to download the updates
B. Use the Systems Manager to patch the instances
C. Ensure an internet gateway is present to download the updates
D. Use the AWS inspector to patch the updates

Answer: AB

Explanation:
Option C is invalid because the instances need to remain in the private: Option D is invalid because AWS inspector can only detect the patches
One of the AWS Blogs mentions how patching of Linux servers can be accomplished. Below is the diagram representation of the architecture setup
C:\Users\wk\Desktop\mudassar\Untitled.jpg

For more information on patching Linux workloads in AWS, please refer to the Lin. https://aws.amazon.com/blogs/security/how-to-patch-linux-workloads-on-awsj
The correct answers are: Ensure a NAT gateway is present to download the updates. Use the Systems Manager to patch the instances
Submit your Feedback/Queries to our Experts

NEW QUESTION 224
- (Exam Topic 3)
A company's application team needs to host a MySQL database on AWS. According to the company's security policy, all data that is stored on AWS must be encrypted at rest. In addition, all cryptographic material must be compliant with FIPS 140-2 Level 3 validation.
The application team needs a solution that satisfies the company's security requirements and minimizes operational overhead.
Which solution will meet these requirements?

A. Host the database on Amazon RD
B. Use Amazon Elastic Block Store (Amazon EBS) for encryption.Use an AWS Key Management Service (AWS KMS) custom key store that is backed by AWS CloudHSM for key management.
C. Host the database on Amazon RD
D. Use Amazon Elastic Block Store (Amazon EBS) for encryption.Use an AWS managed CMK in AWS Key Management Service (AWS KMS) for key management.
E. Host the database on an Amazon EC2 instanc
F. Use Amazon Elastic Block Store (Amazon EBS) for encryptio
G. Use a customer managed CMK in AWS Key Management Service (AWS KMS) for key management.
H. Host the database on an Amazon EC2 instanc
I. Use Transparent Data Encryption (TDE) for encryption and key management.

Answer: B

NEW QUESTION 227
- (Exam Topic 3)
Your developer is using the KMS service and an assigned key in their Java program. They get the below error when running the code
arn:aws:iam::113745388712:user/UserB is not authorized to perform: kms:DescribeKey Which of the following could help resolve the issue?
Please select:

A. Ensure that UserB is given the right IAM role to access the key
B. Ensure that UserB is given the right permissions in the IAM policy
C. Ensure that UserB is given the right permissions in the Key policy
D. Ensure that UserB is given the right permissions in the Bucket policy

Answer: C

Explanation:
You need to ensure that UserB is given access via the Key policy for the Key C:\Users\wk\Desktop\mudassar\Untitled.jpg

Option is invalid because you don't assign roles to IAM users
For more information on Key policies please visit the below Link: https://docs.aws.amazon.com/kms/latest/developerguide/key-poli
The correct answer is: Ensure that UserB is given the right permissions in the Key policy

NEW QUESTION 231
- (Exam Topic 3)
You are working for a company and been allocated the task for ensuring that there is a federated authentication mechanism setup between AWS and their On-premise Active Directory. Which of the following are important steps that need to be covered in this process? Choose 2 answers from the options given below.
Please select:

A. Ensure the right match is in place for On-premise AD Groups and IAM Roles.
B. Ensure the right match is in place for On-premise AD Groups and IAM Groups.
C. Configure AWS as the relying party in Active Directory
D. Configure AWS as the relying party in Active Directory Federation services

Answer: AD

Explanation:
The AWS Documentation mentions some key aspects with regards to the configuration of On-premise AD with AWS
One is the Groups configuration in AD Active Directory Configuration
Determining how you will create and delineate your AD groups and IAM roles in AWS is crucial to how you secure access to your account and manage resources. SAML assertions to the AWS environment and the respective IAM role access will be managed through regular expression (regex) matching between your on-premises AD group name to an AWS IAM role.
One approach for creating the AD groups that uniquely identify the AWS IAM role mapping is by selecting a common group naming convention. For example, your AD groups would start with an identifier, for example, AWS-, as this will distinguish your AWS groups from others within the organization. Next include the 12- digitAWS account number. Finally, add the matching role name within the AWS account. Here is an example:
C:\Users\wk\Desktop\mudassar\Untitled.jpg

And next is the configuration of the relying party which is AWS
ADFS federation occurs with the participation of two parties; the identity or claims provider (in this case the owner of the identity repository - Active Directory) and the relying party, which is another application that wishes to outsource authentication to the identity provider; in this case Amazon Secure Token Service (STS). The relying party is a federation partner that is represented by a claims provider trust in the federation service.
Option B is invalid because AD groups should not be matched to IAM Groups
Option C is invalid because the relying party should be configured in Active Directory Federation services For more information on the federated access, please visit the following URL:
1
https://aws.amazon.com/blogs/security/aws-federated-authentication-with-active-directory-federation-services-a
The correct answers are: Ensure the right match is in place for On-premise AD Groups and IAM Roles., Configure AWS as the relying party in Active Directory Federation services
Submit your Feedback/Queries to our Experts

NEW QUESTION 232
- (Exam Topic 3)
You work as an administrator for a company. The company hosts a number of resources using AWS. There is an incident of a suspicious API activity which occurred 11 days ago. The Security Admin has asked to get the API activity from that point in time. How can this be achieved?
Please select:

A. Search the Cloud Watch logs to find for the suspicious activity which occurred 11 days ago
B. Search the Cloudtrail event history on the API events which occurred 11 days ago.
C. Search the Cloud Watch metrics to find for the suspicious activity which occurred 11 days ago
D. Use AWS Config to get the API calls which were made 11 days ago.

Answer: B

Explanation:
The Cloud Trail event history allows to view events which are recorded for 90 days. So one can use a metric filter to gather the API calls from 11 days ago.
Option A and C is invalid because Cloudwatch is used for logging and not for monitoring API activity Option D is invalid because AWSConfig is a configuration service and not for monitoring API activity For more information on AWS Cloudtrail, please visit the following URL:
https://docs.aws.amazon.com/awscloudtrail/latest/usereuide/how-cloudtrail-works.html
Note:
In this question we assume that the customer has enabled cloud trail service.
AWS CloudTrail is enabled by default for ALL CUSTOMERS and will provide visibility into the past seven days of account activity without the need for you to configure a trail in the service to get started. So for an activity that happened 11 days ago to be stored in the cloud trail we need to configure the trail manually to ensure that it is stored in the events history.
• https://aws.amazon.com/blogs/aws/new-amazon-web-services-extends-cloudtrail-to-all-aws-customers/ The correct answer is: Search the Cloudtrail event history on the API events which occurred 11 days ago.

NEW QUESTION 234
- (Exam Topic 3)
A company has a set of EC2 Instances hosted in AWS. The EC2 Instances have EBS volumes which is used to store critical information. There is a business continuity requirement to ensure high availability for the EBS volumes. How can you achieve this?

A. Use lifecycle policies for the EBS volumes
B. Use EBS Snapshots

C. Use EBS volume replication
D. Use EBS volume encryption

Answer: B

Explanation:
Data stored in Amazon EBS volumes is redundantly stored in multiple physical locations as part of normal operation of those services and at no additional charge. However, Amazon EBS replication is stored within the same availability zone, not across multiple zones; therefore, it is highly recommended that you conduct regular snapshots to Amazon S3 for long-term data durability Option A is invalid because there is no lifecycle policy for EBS volumes Option C is invalid because there is no EBS volume replication Option D is invalid because EBS volume encryption will not ensure business continuity For information on security for Compute Resources, please visit the below URL: https://d1.awsstatic.com/whitepapers/Security/Security_Compute_Services_Whitepaper.pdf

NEW QUESTION 237
- (Exam Topic 3)
A company is deploying a new web application on AWS. Based on their other web applications, they anticipate being the target of frequent DDoS attacks. Which steps can the company use to protect their application? Select 2 answers from the options given below.
Please select:

A. Associate the EC2 instances with a security group that blocks traffic from blacklisted IP addresses.
B. Use an ELB Application Load Balancer and Auto Scaling group to scale to absorb application layer traffic.
C. Use Amazon Inspector on the EC2 instances to examine incoming traffic and discard malicious traffic.
D. Use CloudFront and AWS WAF to prevent malicious traffic from reaching the application
E. Enable GuardDuty to block malicious traffic from reaching the application

Answer: BD

Explanation:
The below diagram from AWS shows the best case scenario for avoiding DDos attacks using services such as AWS Cloudfro WAF, ELB and Autoscaling
C:\Users\wk\Desktop\mudassar\Untitled.jpg

Option A is invalid because by default security groups don't allow access Option C is invalid because AWS Inspector cannot be used to examine traffic
Option E is invalid because this can be used for attacks on EC2 Instances but not against DDos attacks on the entire application For more information on DDos mitigation from AWS, please visit the below URL:
https://aws.amazon.com/answers/networking/aws-ddos-attack-mitieationi
The correct answers are: Use an ELB Application Load Balancer and Auto Scaling group to scale to absorb application layer traffic., Use CloudFront and AWS WAF to prevent malicious traffic from reaching the application
Submit your Feedback/Queries to our Experts

NEW QUESTION 241
- (Exam Topic 3)
Your company has confidential documents stored in the simple storage service. Due to compliance requirements, you have to ensure that the data in the S3 bucket is available in a different geographical location. As an architect what is the change you would make to comply with this requirement.
Please select:

A. Apply Multi-AZ for the underlying 53 bucket
B. Copy the data to an EBS Volume in another Region
C. Create a snapshot of the S3 bucket and copy it to another region
D. Enable Cross region replication for the S3 bucket

Answer: D

Explanation:
This is mentioned clearly as a use case for S3 cross-region replication
You might configure cross-region replication on a bucket for various reasons, including the following:
• Compliance requirements - Although, by default Amazon S3 stores your data across multiple geographically distant Availability Zones, compliance requirements might dictate that you store data at even further distances. Cross-region replication allows you to replicate data between distant AWS Regions to satisfy these compliance requirements.
Option A is invalid because Multi-AZ cannot be used to S3 buckets
Option B is invalid because copying it to an EBS volume is not a recommended practice Option C is invalid because creating snapshots is not possible in S3
For more information on S3 cross-region replication, please visit the following URL: https://docs.aws.amazon.com/AmazonS3/latest/dev/crr.htmll
The correct answer is: Enable Cross region replication for the S3 bucket Submit your Feedback/Queries to our Experts

NEW QUESTION 246
- (Exam Topic 3)
When managing permissions for the API gateway, what can be used to ensure that the right level of permissions are given to developers, IT admins and users? These permissions should be easily managed.
Please select:

A. Use the secure token service to manage the permissions for the different users
B. Use IAM Policies to create different policies for the different types of users.
C. Use the AWS Config tool to manage the permissions for the different users
D. Use IAM Access Keys to create sets of keys for the different types of users.

Answer: B

Explanation:

The AWS Documentation mentions the following
You control access to Amazon API Gateway with IAM permissions by controlling access to the following two API Gateway component processes:
* To create, deploy, and manage an API in API Gateway, you must grant the API developer permissions to perform the required actions supported by the API management component of API Gateway.
* To call a deployed API or to refresh the API caching, you must grant the API caller permissions to perform required IAM actions supported by the API execution component of API Gateway.
Option A, C and D are invalid because these cannot be used to control access to AWS services. This needs to be done via policies. For more information on permissions with the API gateway, please visit the following URL:
https://docs.aws.amazon.com/apisateway/latest/developerguide/permissions.html
The correct answer is: Use IAM Policies to create different policies for the different types of users. Submit your Feedback/Queries to our Experts

NEW QUESTION 249
- (Exam Topic 3)
A company wants to deploy a distributed web application on a fleet of EC2 instances. The fleet will be fronted by a Classic Load Balancer that will be configured to terminate the TLS connection The company wants to make sure that all past and current TLS traffic to the Classic Load Balancer stays secure even if the certificate private key is leaked.
To ensure the company meets these requirements, a Security Engineer can configure a Classic Load Balancer with:

A. An HTTPS listener that uses a certificate that is managed by Amazon Certification Manager.
B. An HTTPS listener that uses a custom security policy that allows only perfect forward secrecy cipher suites
C. An HTTPS listener that uses the latest AWS predefined ELBSecuntyPolicy-TLS-1 -2-2017-01 security policy
D. A TCP listener that uses a custom security policy that allows only perfect forward secrecy cipher suites.

Answer: C

NEW QUESTION 250
- (Exam Topic 3)
A developer 15 building a serverless application hosted on AWS that uses Amazon Redshift in a data store. The application has separate modules for read/write and read-only functionality. The modules need their own database users tor compliance reasons.
Which combination of steps should a security engineer implement to grant appropriate access' (Select TWO)

A. Configure cluster security groups for each application module to control access to database users that are required for read-only and read/write.
B. Configure a VPC endpoint for Amazon Redshift Configure an endpoint policy that maps database users to each application module, and allow access to the tables that are required for read-only and read/write
C. Configure an 1AM poky for each module Specify the ARN of an Amazon Redshift database user that allows the GetClusterCredentials API call
D. Create focal database users for each module
E. Configure an 1AM policy for each module Specify the ARN of an 1AM user that allows the GetClusterCredentials API call

Answer: AE

NEW QUESTION 255
- (Exam Topic 3)
A company's Chief Security Officer has requested that a Security Analyst review and improve the security posture of each company AWS account The Security Analyst decides to do this by Improving AWS account root user security.
Which actions should the Security Analyst take to meet these requirements? (Select THREE.)

A. Delete the access keys for the account root user in every account.
B. Create an admin IAM user with administrative privileges and delete the account root user in every account.
C. Implement a strong password to help protect account-level access to the AWS Management Console by the account root user.
D. Enable multi-factor authentication (MFA) on every account root user in all accounts.
E. Create a custom IAM policy to limit permissions to required actions for the account root user and attach the policy to the account root user.
F. Attach an IAM role to the account root user to make use of the automated credential rotation in AWS STS.

Answer: ADE

NEW QUESTION 258
- (Exam Topic 3)
An Incident Response team is investigating an AWS access key leak that resulted in Amazon EC2 instances being launched. The company did not discover the incident until many months later The Director of Information Security wants to implement new controls that will alert when similar incidents happen in the future
Which controls should the company implement to achieve this? {Select TWO.)

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

Answer: AE

NEW QUESTION 263
- (Exam Topic 3)
A company has been using the AW5 KMS service for managing its keys. They are planning on carrying out housekeeping activities and deleting keys which are no longer in use. What are the ways that can be incorporated to see which keys are in use? Choose 2 answers from the options given below

Please select:

A. Determine the age of the master key
B. See who is assigned permissions to the master key
C. See Cloudtrail for usage of the key
D. Use AWS cloudwatch events for events generated for the key

Answer: BC

Explanation:
The direct ways that can be used to see how the key is being used is to see the current access permissions and cloudtrail logs
Option A is invalid because seeing how long ago the key was created would not determine the usage of the key
Option D is invalid because Cloudtrail Event is better for seeing for events generated by the key This is also mentioned in the AWS Documentation
Examining CMK Permissions to Determine the Scope of Potential Usage
Determining who or what currently has access to a customer master key (CMK) might help you determine how widely the CM was used and whether it is still needed. To learn how to determine who or what currently has access to a CMK, go to Determining Access to an AWS KMS Customer Master Key.
Examining AWS CloudTrail Logs to Determine Actual Usage
AWS KMS is integrated with AWS CloudTrail, so all AWS KMS API activity is recorded in CloudTrail log files. If you have CloudTrail turned on in the region where your customer master key (CMK) is located, you can examine your CloudTrail log files to view a history of all AWS KMS API activity for a particular CMK, and thus its usage history. You might be able to use a CMK's usage history to help you determine whether or not you still need it
For more information on determining the usage of CMK keys, please visit the following URL:

https://docs.aws.amazon.com/kms/latest/developerguide/deleting-keys-determining-usage.html
The correct answers are: See who is assigned permissions to the master key. See Cloudtrail for usage of the key Submit your Feedback/Queries to our Experts

NEW QUESTION 267
- (Exam Topic 3)
An organization has setup multiple IAM users. The organization wants that each IAM user accesses the IAM console only within the organization and not from outside. How can it achieve this?
Please select:

A. Create an IAM policy with the security group and use that security group for AWS console login
B. Create an IAM policy with a condition which denies access when the IP address range is not from the organization
C. Configure the EC2 instance security group which allows traffic only from the organization's IP range
D. Create an IAM policy with VPC and allow a secure gateway between the organization and AWS Console

Answer: B

Explanation:
You can actually use a Deny condition which will not allow the person to log in from outside. The below example shows the Deny condition to ensure that any address specified in the source address is not allowed to access the resources in aws.
Option A is invalid because you don't mention the security group in the IAM policy Option C is invalid because security groups by default don't allow traffic
Option D is invalid because the IAM policy does not have such an option For more information on IAM policy conditions, please visit the URL:
http://docs.aws.amazon.com/IAM/latest/UserGuide/access
pol examples.htm l#iam-policy-example-ec2-two-condition!
The correct answer is: Create an IAM policy with a condition which denies access when the IP address range is not from the organization
Submit your Feedback/Queries to our Experts

NEW QUESTION 268
......

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

SCS-C01 Practice Exam Features:

* SCS-C01 Questions and Answers Updated Frequently

* SCS-C01 Practice Questions Verified by Expert Senior Certified Staff

* SCS-C01 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SCS-C01 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The SCS-C01 Practice Test Here