Exam Questions SCS-C02

AWS Certified Security - Specialty

https://www.2passeasy.com/dumps/SCS-C02/

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

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

Answer: CD

Explanation:
https://docs.IAM.amazon.com/IAMEC2/latest/UserGuide/using-eni.html

NEW QUESTION 2
- (Exam Topic 1)
A company has multiple IAM accounts that are part of IAM Organizations. The company's Security team wants to ensure that even those Administrators with full access to the company's IAM accounts are unable to access the company's Amazon S3 buckets
How should this be accomplished?

A. UseSCPs
B. Add a permissions boundary to deny access to Amazon S3 and attach it to all roles
C. Use an S3 bucket policy
D. Create a VPC endpoint for Amazon S3 and deny statements for access to Amazon S3

Answer: A

NEW QUESTION 3
- (Exam Topic 1)
A security engineer has created an Amazon Cognito user pool. The engineer needs to manually verify the ID and access token sent by the application for troubleshooting purposes
What is the MOST secure way to accomplish this?

A. Extract the subject (sub), audience (aud), and cognito:username from the ID token payload Manually check the subject and audience for the user name In the user pool
B. Search for the public key with a key ID that matches the key ID In the header of the toke
C. Then use a JSON Web Token (JWT) library to validate the signature of the token and extract values, such as the expiry date
D. Verify that the token is not expire
E. Then use the token_use claim function In Amazon Cognito to validate the key IDs
F. Copy the JSON Web Token (JWT) as a JSON document Obtain the public JSON Web Key (JWK) and convert It to a pem fil
G. Then use the file to validate the original JWT.

Answer: A

NEW QUESTION 4
- (Exam Topic 1)
An application running on Amazon EC2 instances generates log files in a folder on a Linux file system. The instances block access to the console and file transfer utilities, such as Secure Copy Protocol (SCP) and Secure File Transfer Protocol (SFTP). The Application Support team wants to automatically monitor the application log files so the team can set up notifications in the future.
A Security Engineer must design a solution that meets the following requirements:
• Make the log files available through an IAM managed service.
• Allow for automatic monitoring of the logs.
• Provide an Interlace for analyzing logs.
• Minimize effort.
Which approach meets these requirements^

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

Answer: D

NEW QUESTION 5

- (Exam Topic 1)
Which of the following are valid configurations for using SSL certificates with Amazon CloudFront? (Select THREE)

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

Answer: ACD

NEW QUESTION 6
- (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:
• IAM IAM federated with on-premises Active Directory
• Amazon Cognito user pools to accessing an IAM 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 IAM IAM with a minimum password length condition.
D. Update the password length policy in the Amazon Cognito configuration.
E. Create an SCP with IAM Organizations that enforces a minimum password length for IAM IAM and Amazon Cognito.

Answer: AD

NEW QUESTION 7
- (Exam Topic 1)
A company had one of its Amazon EC2 key pairs compromised. A Security Engineer must identify which current Linux EC2 instances were deployed and used the compromised key pair.
How can this task be accomplished?

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

Answer: A

NEW QUESTION 8
- (Exam Topic 1)
A Security Engineer discovered a vulnerability in an application running on Amazon ECS. The vulnerability allowed attackers to install malicious code. Analysis of the code shows it exfiltrates data on port 5353 in batches at random time intervals.
While the code of the containers is being patched, how can Engineers quickly identify all compromised hosts and stop the egress of data on port 5353?

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

Answer: C

NEW QUESTION 9
- (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 IAM 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 IAM 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 10
- (Exam Topic 1)
A company requires that SSH commands used to access its IAM instance be traceable to the user who executed each command.
How should a Security Engineer accomplish this?

A. Allow inbound access on port 22 at the security group attached to the instance Use IAM Systems Manager Session Manager for shell access to Amazon EC2

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

Answer: C

NEW QUESTION 10
- (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 14
- (Exam Topic 1)
A company recently performed an annual security assessment of its IAM environment. The assessment showed that audit logs are not available beyond 90 days and that unauthorized changes to IAM policies are made without detection.
How should a security engineer resolve these issues?

A. Create an Amazon S3 lifecycle policy that archives IAM CloudTrail trail logs to Amazon S3 Glacier after 90 day
B. Configure Amazon Inspector to provide a notification when a policy change is made to resources.
C. Configure IAM Artifact to archive IAM CloudTrail logs Configure IAM Trusted Advisor to provide a notification when a policy change is made to resources.
D. Configure Amazon CloudWatch to export log groups to Amazon S3. Configure IAM CloudTrail to provide a notification when a policy change is made to resources.
E. Create an IAM CloudTrail trail that stores audit logs in Amazon S3. Configure an IAM Config rule to provide a notification when a policy change is made to resources.

Answer: D

Explanation:
https://docs.IAM.amazon.com/IAMcloudtrail/latest/userguide/best-practices-security.html
"For an ongoing record of events in your IAM account, you must create a trail. Although CloudTrail provides 90 days of event history information for management events in the CloudTrail console without creating a trail, it is not a permanent record, and it does not provide information about all possible types of events. For an ongoing record, and for a record that contains all the event types you specify, you must create a trail, which delivers log files to an Amazon S3 bucket that you specify."
https://IAM.amazon.com/blogs/security/how-to-record-and-govern-your-iam-resource-configurations-using-IAM

NEW QUESTION 19
- (Exam Topic 1)
A security engineer is responsible for providing secure access to IAM resources for thousands of developer in a company’s corporate identity provider (idp). The developers access a set of IAM services from the corporate premises using IAM credential. Due to the velum of require for provisioning new IAM users, it is taking a long time to grant access permissions. The security engineer receives reports that developer are sharing their IAM credentials with others to avoid provisioning delays. The causes concern about overall security for the security engineer.
Which actions will meet the program requirements that address security?

A. Create an Amazon CloudWatch alarm for IAM CloudTrail Events Create a metric filter to send a notification when me same set of IAM credentials is used by multiple developer
B. Create a federation between IAM and the existing corporate IdP Leverage IAM roles to provide federated access to IAM resources
C. Create a VPN tunnel between the corporate premises and the VPC Allow permissions to all IAM services only if it originates from corporate premises.
D. Create multiple IAM rotes for each IAM user Ensure that users who use the same IAM credentials cannot assume the same IAM role at the same time.

Answer: B

NEW QUESTION 23
- (Exam Topic 1)
A company has an application hosted in an Amazon EC2 instance and wants the application to access secure strings stored in IAM 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 IAM Key Management Sen/ice (IAM 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 IAM Key Management Service (IAM KMS) to decrypt the parameter
D. The EC2 instance role does not have encrypt permissions on the IAM Key Management Service (IAM KMS) key associated with the secret

E. The EC2 instance does not have any tags associated.

Answer: AB

Explanation:
https://docs.IAM.amazon.com/systems-manager/latest/userguide/sysman-paramstore-access.html

NEW QUESTION 28
- (Exam Topic 1)
A large government organization is moving to the cloud and has specific encryption requirements. The first workload to move requires that a customer's data be immediately destroyed when the customer makes that request.
Management has asked the security team to provide a solution that will securely store the data, allow only authorized applications to perform encryption and decryption and allow for immediate destruction of the data
Which solution will meet these requirements?

A. Use IAM Secrets Manager and an IAM SDK to create a unique secret for the customer-specific data
B. Use IAM Key Management Service (IAM KMS) and the IAM Encryption SDK to generate and store a data encryption key for each customer.
C. Use IAM Key Management Service (IAM KMS) with service-managed keys to generate and store customer-specific data encryption keys
D. Use IAM Key Management Service (IAM KMS) and create an IAM CloudHSM custom key store Use CloudHSM to generate and store a new CMK for each customer.

Answer: A

NEW QUESTION 30
- (Exam Topic 1)
A Security Engineer is looking for a way to control access to data that is being encrypted under a CMK. The Engineer is also looking to use additional authenticated data (AAD) to prevent tampering with ciphertext.
Which action would provide the required functionality?

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

Answer: C

Explanation:
https://IAM.amazon.com/blogs/security/how-to-protect-the-integrity-of-your-encrypted-data-by-using-IAM-key One of the most important and critical concepts in IAM Key Management Service (KMS) for advanced and secure data usage is EncryptionContext. Using EncryptionContext properly can help significantly improve the security of your applications. EncryptionContext is a key-value map (both strings) that is provided to KMS with each encryption and decryption request. EncryptionContext provides three benefits: Additional authenticated data (AAD), Audit trail, Authorization context

NEW QUESTION 35
- (Exam Topic 1)
A company is collecting IAM CloudTrail log data from multiple IAM 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 IAM Organizations trails, the company decided to further centralize management and automate deployment of the CloudTrail logging capability across all of its IAM accounts.
The company's security engineer created an IAM Organizations trail in the master account, enabled server-side encryption with IAM 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 39
- (Exam Topic 1)
A company has multiple production IAM accounts. Each account has IAM CloudTrail configured to log to a single Amazon S3 bucket in a central account. Two of the production accounts have trails that are not logging anything to the S3 bucket.
Which steps should be taken to troubleshoot the issue? (Choose three.)

A. Verify that the log file prefix is set to the name of the S3 bucket where the logs should go.
B. Verify that the S3 bucket policy allows access for CloudTrail from the production IAM account IDs.
C. Create a new CloudTrail configuration in the account, and configure it to log to the account’s S3 bucket.
D. Confirm in the CloudTrail Console that each trail is active and healthy.
E. Open the global CloudTrail configuration in the master account, and verify that the storage location is set to the correct S3 bucket.
F. Confirm in the CloudTrail Console that the S3 bucket name is set correctly.

Answer: BDF

NEW QUESTION 40
- (Exam Topic 1)
A Security Engineer is setting up an IAM CloudTrail trail for all regions in an IAM account. For added security, the logs are stored using server-side encryption with

IAM 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: B

Explanation:
Enabling server-side encryption encrypts the log files but not the digest files with SSE-KMS. Digest files are encrypted with Amazon S3-managed encryption keys (SSE-S3). https://docs.IAM.amazon.com/IAMcloudtrail/latest/userguide/encrypting-cloudtrail-log-files-with-IAM-kms.htm

NEW QUESTION 41
- (Exam Topic 1)
While securing the connection between a company's VPC and its on-premises data center, a Security Engineer sent a ping command from an on-premises host (IP address 203.0.113.12) to an Amazon EC2 instance (IP address 172.31.16.139). The ping command did not return a response. The flow log in the VPC showed the following:
2 123456789010 eni-1235b8ca 203.0.113.12 172.31.16.139 0 0 1 4 336 1432917027 1432917142 ACCEPT OK
2 123456789010 eni-1235b8ca 172.31.16.139 203.0.113.12 0 0 1 4 336 1432917094 1432917142 REJECT OK
What action should be performed to allow the ping to work?

A. In the security group of the EC2 instance, allow inbound ICMP traffic.
B. In the security group of the EC2 instance, allow outbound ICMP traffic.
C. In the VPC's NACL, allow inbound ICMP traffic.
D. In the VPC's NACL, allow outbound ICMP traffic.

Answer: D

NEW QUESTION 43
- (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 47
- (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 IAM Management Console.
Which steps should the security engineer take to satisfy this requirement while maintaining least privilege?

A. Enable IAM Systems Manager in the IAM 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 IAM Systems Manager Session Manager and attach to the development team's IAM users.
F. Enable IAM Systems Manager in the IAM 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 IAM Systems Manager Session Manager and attach to the team's IAM users.
J. Enable IAM Systems Manager in the IAM 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 51
- (Exam Topic 1)
A company wants to encrypt data locally while meeting regulatory requirements related to key exhaustion. The encryption key can be no more than 10 days old or encrypt more than 2" 16 objects Any encryption key must be generated on a FIPS-validated hardware security module (HSM). The company is cost-conscious, as plans to upload an average of 100 objects to Amazon S3 each second for sustained operations across 5 data producers
When approach MOST efficiently meets the company's needs?

A. Use the IAM Encryption SDK and set the maximum age to 10 days and the minimum number of messages encrypted to 3" 16. Use IAM Key Management Service (IAM KMS) to generate the master key and data key Use data key caching with the Encryption SDk during the encryption process.
B. Use IAM Key Management Service (IAM KMS) to generate an IAM managed CM
C. Then use Amazon S3 client-side encryption configured to automatically rotate with every object

D. Use IAM CloudHSM to generate the master key and data key
E. Then use Boto 3 and Python to locally encrypt data before uploading the object Rotate the data key every 10 days or after 2" 16 objects have been Uploaded to Amazon 33
F. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3) and set the master key to automatically rotate.

Answer: A

NEW QUESTION 54
- (Exam Topic 1)
A company has an IAM account and allows a third-party contractor who uses another IAM account, to assume certain IAM roles. The company wants to ensure that IAM roles can be assumed by the contractor only if the contractor has multi-factor authentication enabled on their IAM user accounts
What should the company do to accomplish this?
A)

```
Add the following condition to the IAM policy attached to all IAM roles.
"Effect" : "Deny",
"Condition" : { "BoolIfExists" : { "aws:MultiFactorAuthPresent" : false } }
```

B)

```
Add the following condition to the IAM policy attached to all IAM roles.
"Effect" : "Deny",
"Condition" : { "Bool" : { "aws:MultiFactorAuthPresent" : false } }
```

C)

```
Add the following condition to the IAM policy attached to all IAM roles.
"Effect" : "Allow",
"Condition" : { "Null" : { "aws:MultiFactorAuthPresent" : false } }
```

D)

```
Add the following condition to the IAM policy attached to all IAM roles
"Effect" : "Allow",
"Condition" : { "BoolIfExists" : { "aws:MultiFactorAuthPresent" : false } }
```

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

Answer: A

NEW QUESTION 57
- (Exam Topic 1)
A company has a VPC with an IPv6 address range and a public subnet with an IPv6 address block. The VPC currently hosts some public Amazon EC2 instances but a Security Engineer needs to migrate a second application into the VPC that also requires IPv6 connectivity.
This new application will occasionally make API requests to an external, internet-accessible endpoint to receive updates However, the Security team does not want the application's EC2 instance exposed directly to the internet The Security Engineer intends to create a private subnet with a custom route table and to associate the route table with the private subnet
What else does the Security Engineer need to do to ensure the application will not be exposed directly to the internet, but can still communicate as required"

A. Launch a NAT instance in the public subnet Update the custom route table with a new route to the NAT instance
B. Remove the internet gateway, and add IAM PrivateLink to the VPC Then update the custom route table with a new route to IAM PrivateLink
C. Add a managed NAT gateway to the VPC Update the custom route table with a new route to the gateway
D. Add an egress-only internet gateway to the VP
E. Update the custom route table with a new route to thegateway

Answer: D

NEW QUESTION 61
- (Exam Topic 1)
A company has several production IAM accounts and a central security IAM account. The security account is used for centralized monitoring and has IAM privileges to all resources in every corporate account. All of the company's Amazon S3 buckets are tagged with a value denoting the data classification of their contents.
A Security Engineer is deploying a monitoring solution in the security account that will enforce bucket policy compliance. The system must monitor S3 buckets in all production accounts and confirm that any policy change is in accordance with the bucket's data classification. If any change is out of compliance; the Security team must be notified quickly.
Which combination of actions would build the required solution? (Choose three.)

A. Configure Amazon CloudWatch Events in the production accounts to send all S3 events to the security account event bus.
B. Enable Amazon GuardDuty in the security accoun
C. and join the production accounts as members.
D. Configure an Amazon CloudWatch Events rule in the security account to detect S3 bucket creation or modification events.
E. Enable IAM Trusted Advisor and activate email notifications for an email address assigned to the security contact.
F. Invoke an IAM Lambda function in the security account to analyze S3 bucket settings in response to S3 events, and send non-compliance notifications to the Security team.
G. Configure event notifications on S3 buckets for PUT; POST, and DELETE events.

Answer: DEF

NEW QUESTION 65

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

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

Answer: D

NEW QUESTION 70
- (Exam Topic 1)
A company is operating an open-source software platform that is internet facing. The legacy software platform no longer receives security updates. The software platform operates using Amazon route 53 weighted load balancing to send traffic to two Amazon EC2 instances that connect to an Amazon POS cluster a recent report suggests this software platform is vulnerable to SQL injection attacks. with samples of attacks provided. The company's security engineer must secure this system against SQL injection attacks within 24 hours. The secure, engineer's solution involve the least amount of effort and maintain normal operations during implementation.
What should the security engineer do to meet these requirements?

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

Answer: A

NEW QUESTION 72
- (Exam Topic 1)
An employee accidentally exposed an IAM access key and secret access key during a public presentation. The company Security Engineer immediately disabled the key.
How can the Engineer assess the impact of the key exposure and ensure that the credentials were not misused? (Choose two.)

A. Analyze IAM CloudTrail for activity.
B. Analyze Amazon CloudWatch Logs for activity.
C. Download and analyze the IAM Use report from IAM Trusted Advisor.
D. Analyze the resource inventory in IAM Config for IAM user activity.
E. Download and analyze a credential report from IAM.

Answer: AD

Explanation:
https://docs.IAM.amazon.com/IAM/latest/UserGuide/id_credentials_getting-report.html

NEW QUESTION 75
- (Exam Topic 1)
A company's security information events management (SIEM) tool receives new IAM 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 action.

Answer: ADF

NEW QUESTION 79

- (Exam Topic 1)
A developer is creating an IAM Lambda function that requires environment variables to store connection information and logging settings. The developer is required to use an IAM 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 IAM IAM policy.
C. The KMS key policy must allow permissions for the developer to use the KMS key.
D. The IAM 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 IAM IAM policy.

Answer: BC

NEW QUESTION 81
- (Exam Topic 1)
A company has decided to use encryption in its IAM account to secure the objects in Amazon S3 using server-side encryption. Object sizes range from 16.000 B to 5 MB. The requirements are as follows:
• The key material must be generated and stored in a certified Federal Information Processing Standard (FIPS) 140-2 Level 3 machine.
• The key material must be available in multiple Regions. Which option meets these requirements?

A. Use an IAM KMS customer managed key and store the key material in IAM with replication across Regions
B. Use an IAM customer managed key, import the key material into IAM KMS using in-house IAM CloudHS
C. and store the key material securely in Amazon S3.
D. Use an IAM KMS custom key store backed by IAM CloudHSM clusters, and copy backups across Regions
E. Use IAM CloudHSM to generate the key material and backup keys across Regions Use the Java Cryptography Extension (JCE) and Public Key Cryptography Standards #11 (PKCS #11) encryption libraries to encrypt and decrypt the data.

Answer: D

NEW QUESTION 84
- (Exam Topic 1)
A security engineer has noticed that VPC Flow Logs are getting a lot REJECT traffic originating from a single Amazon EC2 instance in an Auto Scaling group. The security engineer is concerned that this EC2 instance may be compromised.
What immediate action should the security engineer take? What immediate action should the security engineer take?

A. Remove me instance from the Auto Seating group Close me security group mm ingress only from a single forensic P address to perform an analysis.
B. Remove me instance from the Auto Seating group Change me network ACL rules to allow traffic only from a single forensic IP address to perform en analysis Add a rule to deny all other traffic.
C. Remove the instance from the Auto Scaling group Enable Amazon GuardDuty in that IAM account Install the Amazon Inspector agent cm the suspicious EC 2 instance to perform a scan.
D. Take a snapshot of the suspicious EC2 instanc
E. Create a new EC2 instance from me snapshot in a closed security group with ingress only from a single forensic IP address to perform an analysis

Answer: B

NEW QUESTION 89
- (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 IAM X-Ray to trace the end-to-end application flow

Answer: C

NEW QUESTION 94
- (Exam Topic 1)
An application developer is using an IAM Lambda function that must use IAM KMS to perform encrypt and decrypt operations for API keys that are less than 2 KB
Which key policy would allow the application to do this while granting least privilege?

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

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

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

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

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

Answer: C

NEW QUESTION 96
- (Exam Topic 1)
A company has a compliance requirement to rotate its encryption keys on an annual basis. A Security Engineer needs a process to rotate the KMS Customer Master Keys (CMKs) that were created using imported key material.
How can the Engineer perform the key rotation process MOST efficiently?

A. Create a new CMK, and redirect the existing Key Alias to the new CMK
B. Select the option to auto-rotate the key
C. Upload new key material into the existing CMK.
D. Create a new CMK, and change the application to point to the new CMK

Answer: A

NEW QUESTION 101
- (Exam Topic 1)
A Security Engineer launches two Amazon EC2 instances in the same Amazon VPC but in separate Availability Zones. Each instance has a public IP address and is able to connect to external hosts on the internet. The two instances are able to communicate with each other by using their private IP addresses, but they are not able to communicate with each other when using their public IP addresses.
Which action should the Security Engineer take to allow communication over the public IP addresses?

A. Associate the instances to the same security groups.
B. Add 0.0.0.0/0 to the egress rules of the instance security groups.
C. Add the instance IDs to the ingress rules of the instance security groups.
D. Add the public IP addresses to the ingress rules of the instance security groups.

Answer: D

Explanation:
https://docs.IAM.amazon.com/IAMEC2/latest/UserGuide/security-group-rules-reference.html#sg-rules-other-in

NEW QUESTION 102
- (Exam Topic 2)

You have a web site that is sitting behind IAM Cloudfront. You need to protect the web site against threats such as SQL injection and Cross site scripting attacks. Which of the following service can help in such a scenario Please select:

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

Answer: B

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

NEW QUESTION 104
- (Exam Topic 2)
An application running on EC2 instances must use a username and password to access a database. The developer has stored those secrets in the SSM Parameter Store with type SecureString using the default KMS CMK. Which combination of configuration steps will allow the application to access the secrets via the API? Select 2 answers from the options below
Please select:

A. Add the EC2 instance role as a trusted service to the SSM service role.
B. Add permission to use the KMS key to decrypt to the SSM service role.
C. Add permission to read the SSM parameter to the EC2 instance rol
D. .
E. Add permission to use the KMS key to decrypt to the EC2 instance role
F. Add the SSM service role as a trusted service to the EC2 instance role.

Answer: CD

Explanation:
The below example policy from the IAM Documentation is required to be given to the EC2 Instance in order to read a secure string from IAM KMS. Permissions need to be given to the Get Parameter API and the KMS API call to decrypt the secret.
C:\Users\wk\Desktop\mudassar\Untitled.jpg

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:GetParameter**
      ],
      "Resource": "arn:aws:ssm:us-west-2:111122223333:/parameter/ReadableParameters/*"
    },
    {
      "Effect": "Allow",
      "Action": [
      ], "kms:Decrypt"
      ],
      "Resource": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    }
  ]
}
```

Option A is invalid because roles can be attached to EC2 and not EC2 roles to SSM Option B is invalid because the KMS key does not need to decrypt the SSM service role.
Option E is invalid because this configuration is valid For more information on the parameter store, please visit the below URL: https://docs.IAM.amazon.com/kms/latest/developerguide/services-parameter-store.htmll
The correct answers are: Add permission to read the SSM parameter to the EC2 instance role., Add permission to use the KMS key to decrypt to the EC2 instance role
Submit your Feedback/Queries to our Experts

NEW QUESTION 107
- (Exam Topic 2)

During a recent internal investigation, it was discovered that all API logging was disabled in a production account, and the root user had created new API keys that appear to have been used several times.
What could have been done to detect and automatically remediate the incident?

A. Using Amazon Inspector, review all of the API calls and configure the inspector agent to leverage SNS topics to notify security of the change to IAM CloudTrail, and revoke the new API keys for the root user.
B. Using IAM Config, create a config rule that detects when IAM CloudTrail is disabled, as well as any calls to the root user create-api-ke
C. Then use a Lambda function to re-enable CloudTrail logs and deactivate the root API keys.
D. Using Amazon CloudWatch, create a CloudWatch event that detects IAM CloudTrail deactivation and a separate Amazon Trusted Advisor check to automatically detect the creation of root API key
E. Then use a Lambda function to enable IAM CloudTrail and deactivate the root API keys.
F. Using Amazon CloudTrail, create a new CloudTrail event that detects the deactivation of CloudTrail logs, and a separate CloudTrail event that detects the creation of root API key
G. Then use a Lambda function to enable CloudTrail and deactivate the root API keys.

Answer: B

Explanation:
https://docs.IAM.amazon.com/config/latest/developerguide/cloudtrail-enabled.html https://docs.IAM.amazon.com/config/latest/developerguide/iam-root-access-key-check.html

NEW QUESTION 108
- (Exam Topic 2)
During a recent security audit, it was discovered that multiple teams in a large organization have placed restricted data in multiple Amazon S3 buckets, and the data may have been exposed. The auditor has requested that the organization identify all possible objects that contain personally identifiable information (PII) and then determine whether this information has been accessed.
What solution will allow the Security team to complete this request?

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

Answer: B

NEW QUESTION 112
- (Exam Topic 2)
An organization has three applications running on IAM, each accessing the same data on Amazon S3. The data on Amazon S3 is server-side encrypted by using an IAM KMS Customer Master Key (CMK).
What is the recommended method to ensure that each application has its own programmatic access control permissions on the KMS CMK?

A. Change the key policy permissions associated with the KMS CMK for each application when it must access the data in Amazon S3.
B. Have each application assume an IAM role that provides permissions to use the IAM Certificate Manager CMK.
C. Have each application use a grant on the KMS CMK to add or remove specific access controls on the KMS CMK.
D. Have each application use an IAM policy in a user context to have specific access permissions on the KMS CMK.

Answer: C

NEW QUESTION 117
- (Exam Topic 2)
An organization wants to deploy a three-tier web application whereby the application servers run on Amazon EC2 instances. These EC2 instances need access to credentials that they will use to authenticate their SQL connections to an Amazon RDS DB instance. Also, IAM Lambda functions must issue queries to the RDS database by using the same database credentials.
The credentials must be stored so that the EC2 instances and the Lambda functions can access them. No other access is allowed. The access logs must record when the credentials were accessed and by whom.
What should the Security Engineer do to meet these requirements?

A. Store the database credentials in IAM Key Management Service (IAM KMS). Create an IAM role with access to IAM KMS by using the EC2 and Lambda service principals in the role’s trust polic
B. Add the role to an EC2 instance profil
C. Attach the instance profile to the EC2 instance
D. Set up Lambda to use the new role for execution.
E. Store the database credentials in IAM KM
F. Create an IAM role with access to KMS by using the EC2 and Lambda service principals in the role’s trust polic
G. Add the role to an EC2 instance profil
H. Attach the instance profile to the EC2 instances and the Lambda function.
I. Store the database credentials in IAM Secrets Manage
J. Create an IAM role with access to Secrets Manager by using the EC2 and Lambda service principals in the role’s trust polic
K. Add the role to an EC2 instance profil
L. Attach the instance profile to the EC2 instances and the Lambda function.
M. Store the database credentials in IAM Secrets Manage
N. Create an IAM role with access to Secrets Manager by using the EC2 and Lambda service principals in the role’s trust polic
O. Add the role to an EC2 instance profil
P. Attach the instance profile to the EC2 instance
Q. Set up Lambda to use the new role for execution.

Answer: D

NEW QUESTION 120
- (Exam Topic 2)
Which of the following is the most efficient way to automate the encryption of IAM CloudTrail logs using a Customer Master Key (CMK) in IAM KMS?

A. Use the KMS direct encrypt function on the log data every time a CloudTrail log is generated.
B. Use the default Amazon S3 server-side encryption with S3-managed keys to encrypt and decrypt the CloudTrail logs.
C. Configure CloudTrail to use server-side encryption using KMS-managed keys to encrypt and decrypt CloudTrail logs.
D. Use encrypted API endpoints so that all IAM API calls generate encrypted CloudTrail log entries using the TLS certificate from the encrypted API call.

Answer: C

Explanation:
https://docs.IAM.amazon.com/AmazonS3/latest/dev/UsingKMSEncryption.html

NEW QUESTION 121
- (Exam Topic 2)
A Security Engineer is working with a Product team building a web application on IAM. The application uses Amazon S3 to host the static content, Amazon API Gateway to provide RESTful services; and Amazon DynamoDB as the backend data store. The users already exist in a directory that is exposed through a SAML identity provider.
Which combination of the following actions should the Engineer take to enable users to be authenticated into the web application and call APIs? (Choose three.)

A. Create a custom authorization service using IAM Lambda.
B. Configure a SAML identity provider in Amazon Cognito to map attributes to the Amazon Cognito user pool attributes.
C. Configure the SAML identity provider to add the Amazon Cognito user pool as a relying party.
D. Configure an Amazon Cognito identity pool to integrate with social login providers.
E. Update DynamoDB to store the user email addresses and passwords.
F. Update API Gateway to use a COGNITO_USER_POOLS authorizer.

Answer: BDE

NEW QUESTION 122
- (Exam Topic 2)
A company is using CloudTrail to log all IAM API activity for all regions in all of its accounts. The CISO has asked that additional steps be taken to protect the integrity of the log files.
What combination of steps will protect the log files from intentional or unintentional alteration? Choose 2 answers from the options given below
Please select:

A. Create an S3 bucket in a dedicated log account and grant the other accounts write only acces
B. Deliver all log files from every account to this S3 bucket.
C. Write a Lambda function that queries the Trusted Advisor Cloud Trail check
D. Run the function every 10 minutes.
E. Enable CloudTrail log file integrity validation
F. Use Systems Manager Configuration Compliance to continually monitor the access policies of S3 buckets containing Cloud Trail logs.
G. Create a Security Group that blocks all traffic except calls from the CloudTrail servic
H. Associate the security group with) all the Cloud Trail destination S3 buckets.

Answer: AC

Explanation:
The IAM Documentation mentions the following
To determine whether a log file was modified, deleted, or unchanged after CloudTrail delivered it you can use CloudTrail log fill integrity validation. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.
Option B is invalid because there is no such thing as Trusted Advisor Cloud Trail checks Option D is invalid because Systems Manager cannot be used for this purpose.
Option E is invalid because Security Groups cannot be used to block calls from other services For more information on Cloudtrail log file validation, please visit the below URL:
https://docs.IAM.amazon.com/IAMcloudtrail/latest/userguide/cloudtrail-loe-file-validation-intro.htmll For more information on delivering Cloudtrail logs from multiple accounts, please visit the below URL:
https://docs.IAM.amazon.com/IAMcloudtrail/latest/userguide/cloudtrail-receive-logs-from-multiple-accounts.ht
The correct answers are: Create an S3 bucket in a dedicated log account and grant the other accounts write only access. Deliver all log files from every account to this S3 bucket, Enable Cloud Trail log file integrity validation
Submit your Feedback/Queries to our Experts

NEW QUESTION 126
- (Exam Topic 2)
An application outputs logs to a text file. The logs must be continuously monitored for security incidents. Which design will meet the requirements with MINIMUM effort?

A. Create a scheduled process to copy the component’s logs into Amazon S3. Use S3 events to trigger a Lambda function that updates Amazon CloudWatch metrics with the log dat
B. Set up CloudWatch alerts based on the metrics.
C. Install and configure the Amazon CloudWatch Logs agent on the application’s EC2 instanc
D. Create a CloudWatch metric filter to monitor the application log
E. Set up CloudWatch alerts based on the metrics.
F. Create a scheduled process to copy the application log files to IAM CloudTrai
G. Use S3 events to trigger Lambda functions that update CloudWatch metrics with the log dat

H. Set up CloudWatch alerts based on the metrics.
I. Create a file watcher that copies data to Amazon Kinesis when the application writes to the log file.Have Kinesis trigger a Lambda function to update Amazon CloudWatch metrics with the log dat
J. Set up CloudWatch alerts based on the metrics.

Answer: B

Explanation:
https://docs.IAM.amazon.com/AmazonCloudWatch/latest/logs/QuickStartEC2Instance.html

NEW QUESTION 128
- (Exam Topic 2)
A company wants to have a secure way of generating, storing and managing cryptographic exclusive access for the keys. Which of the following can be used for this purpose?
Please select:

A. Use KMS and the normal KMS encryption keys
B. Use KMS and use an external key material
C. Use S3 Server Side encryption
D. Use Cloud HSM

Answer: D

Explanation:
The IAM Documentation mentions the following
The IAM CloudHSM service helps you meet corporate, contractual and regulatory compliance requirements for data security by using dedicated Hardware Security Module (HSM) instances within the IAM cloud. IAM and IAM Marketplace partners offer a variety of solutions for protecting sensitive data within the IAM platform, but for some applications and data subject to contractual or regulatory mandates for managing cryptographic keys, additional protection may be necessary.
CloudHSM complements existing data protection solutions and allows you to protect your encryption keys within HSMs that are desigr and validated to government standards for secure key management. CloudHSM allows you to securely generate, store and manage cryptographic keys used for data encryption in a way that keys are accessible only by you.
Option A.B and Care invalid because in all of these cases, the management of the key will be with IAM. Here the question specifically mentions that you want to have exclusive access over the keys. This can be achieved with Cloud HSM
For more information on CloudHSM, please visit the following URL: https://IAM.amazon.com/cloudhsm/faq:
The correct answer is: Use Cloud HSM Submit your Feedback/Queries to our Experts

NEW QUESTION 129
- (Exam Topic 2)
An organization has tens of applications deployed on thousands of Amazon EC2 instances. During testing, the Application team needs information to let them know whether the network access control lists (network ACLs) and security groups are working as expected.
How can the Application team’s requirements be met?

A. Turn on VPC Flow Logs, send the logs to Amazon S3, and use Amazon Athena to query the logs.
B. Install an Amazon Inspector agent on each EC2 instance, send the logs to Amazon S3, and use Amazon EMR to query the logs.
C. Create an IAM Config rule for each network ACL and security group configuration, send the logs to Amazon S3, and use Amazon Athena to query the logs.
D. Turn on IAM CloudTrail, send the trails to Amazon S3, and use IAM Lambda to query the trails.

Answer: A

NEW QUESTION 134
- (Exam Topic 2)
A Security Administrator is performing a log analysis as a result of a suspected IAM account compromise. The Administrator wants to analyze suspicious IAM CloudTrail log files but is overwhelmed by the volume of audit logs being generated.
What approach enables the Administrator to search through the logs MOST efficiently?

A. Implement a “write-only” CloudTrail event filter to detect any modifications to the IAM account resources.
B. Configure Amazon Macie to classify and discover sensitive data in the Amazon S3 bucket that contains the CloudTrail audit logs.
C. Configure Amazon Athena to read from the CloudTrail S3 bucket and query the logs to examine account activities.
D. Enable Amazon S3 event notifications to trigger an IAM Lambda function that sends an email alarm when there are new CloudTrail API entries.

Answer: C

NEW QUESTION 136
- (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 IAM Systems Manager Parameter Store and notifies the Engineer that the application needs to be restarted.
C. Configure automatic rotation of credentials in IAM Secrets Manager.
D. Store the credential in an encrypted string parameter in IAM Systems Manager Parameter Stor
E. Grant permission to the instance role associated with the EC2 instance to access the parameter and the IAM KMS key that is used to encrypt it.
F. Configure the Java application to catch a connection failure and make a call to IAM 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 140
- (Exam Topic 2)
A company uses IAM Organization to manage 50 IAM accounts. The finance staff members log in as IAM IAM users in the FinanceDept IAM account. The staff members need to read the consolidated billing information in the MasterPayer IAM account. They should not be able to view any other resources in the MasterPayer IAM account. IAM access to billing has been enabled in the MasterPayer account.
Which of the following approaches grants the finance staff the permissions they require without granting any unnecessary permissions?

A. Create an IAM group for the finance users in the FinanceDept account, then attach the IAM managed ReadOnlyAccess IAM policy to the group.
B. Create an IAM group for the finance users in the MasterPayer account, then attach the IAM managed ReadOnlyAccess IAM policy to the group.
C. Create an IAM IAM role in the FinanceDept account with the ViewBilling permission, then grant the finance users in the MasterPayer account the permission to assume that role.
D. Create an IAM IAM role in the MasterPayer account with the ViewBilling permission, then grant the finance users in the FinanceDept account the permission to assume that role.

Answer: D

Explanation:
IAM Region that You Request a Certificate In (for IAM Certificate Manager) If you want to require HTTPS between viewers and CloudFront, you must change the IAM region to US East (N. Virginia) in the IAM Certificate Manager console before you request or import a certificate. If you want to require HTTPS between CloudFront and your origin, and you're using an ELB load balancer as your origin, you can request or import a certificate in any region.
https://docs.IAM.amazon.com/AmazonCloudFront/latest/DeveloperGuide/cnames-and-https-requirements.html

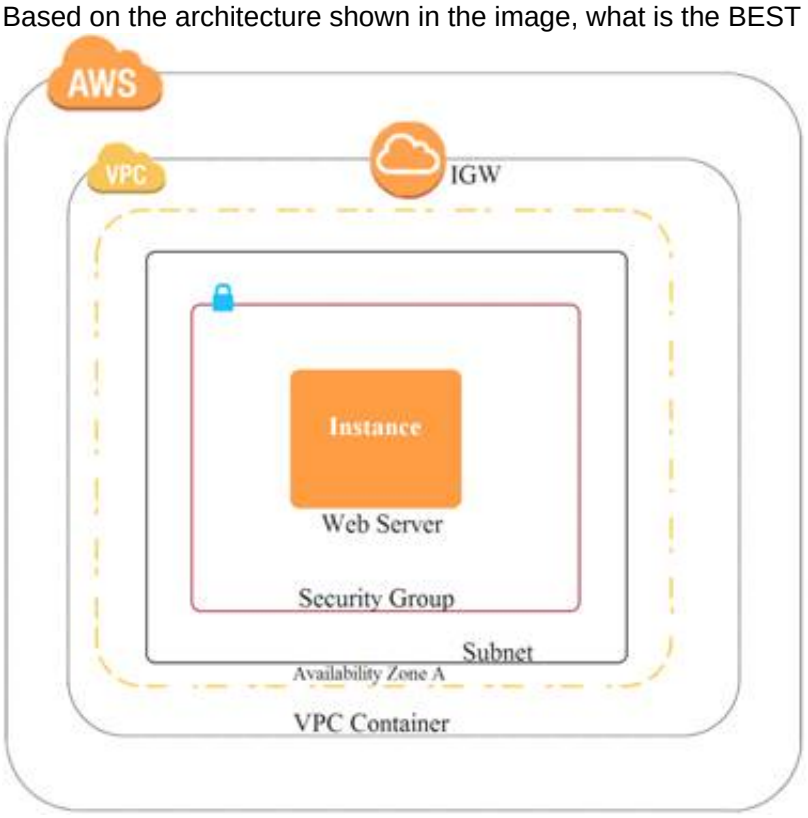
NEW QUESTION 142
- (Exam Topic 2)
During a security event, it is discovered that some Amazon EC2 instances have not been sending Amazon CloudWatch logs.
Which steps can the Security Engineer take to troubleshoot this issue? (Select two.)

A. Connect to the EC2 instances that are not sending the appropriate logs and verify that the CloudWatch Logs agent is running.
B. Log in to the IAM account and select CloudWatch Log
C. Check for any monitored EC2 instances that are in the “Alerting” state and restart them using the EC2 console.
D. Verify that the EC2 instances have a route to the public IAM API endpoints.
E. Connect to the EC2 instances that are not sending log
F. Use the command prompt to verify that the right permissions have been set for the Amazon SNS topic.
G. Verify that the network access control lists and security groups of the EC2 instances have the access to send logs over SNMP.

Answer: AC

Explanation:
https://docs.IAM.amazon.com/AmazonCloudWatch/latest/monitoring/cloudwatch-and-interface-VPC.html

NEW QUESTION 144
- (Exam Topic 2)
A company recently experienced a DDoS attack that prevented its web server from serving content. The website is static and hosts only HTML, CSS, and PDF files that users download.
Based on the architecture shown in the image, what is the BEST way to protect the site against future attacks while minimizing the ongoing operational overhead?



A. Move all the files to an Amazon S3 bucke
B. Have the web server serve the files from the S3 bucket.
C. Launch a second Amazon EC2 instance in a new subne
D. Launch an Application Load Balancer in front of both instances.
E. Launch an Application Load Balancer in front of the EC2 instanc
F. Create an Amazon CloudFront distribution in front of the Application Load Balancer.
G. Move all the files to an Amazon S3 bucke
H. Create a CloudFront distribution in front of the bucket and terminate the web server.

Answer: D

Explanation:
https://docs.IAM.amazon.com/AmazonS3/latest/dev/WebsiteHosting.html

NEW QUESTION 146
- (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 IAM 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/IAM-overview/analytics.html#amazon-athena

NEW QUESTION 150
- (Exam Topic 2)
A threat assessment has identified a risk whereby an internal employee could exfiltrate sensitive data from production host running inside IAM (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 IAM 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 addressesassociated 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 155
- (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 IAM Documentation mentions the following
You can connect directly to IAM 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 IAM KMS is conducted entirely within the IAM 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 IAM.
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.IAM.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 156
- (Exam Topic 2)
A company maintains sensitive data in an Amazon S3 bucket that must be protected using an IAM KMS
CMK. The company requires that keys be rotated automatically every year. How should the bucket be configured?

A. Select server-side encryption with Amazon S3-managed keys (SSE-S3) and select an IAM-managed CMK.
B. Select Amazon S3-IAM KMS managed encryption keys (S3-KMS) and select a customer-managed CMK with key rotation enabled.
C. Select server-side encryption with Amazon S3-managed keys (SSE-S3) and select a customer-managed CMK that has imported key material.
D. Select server-side encryption with IAM KMS-managed keys (SSE-KMS) and select an alias to an IAM-managed CMK.

Answer: B

NEW QUESTION 157
- (Exam Topic 2)

A Security Administrator has a website hosted in Amazon S3. The Administrator has been given the following requirements:
- Users may access the website by using an Amazon CloudFront distribution.
- Users may not access the website directly by using an Amazon S3 URL.

Which configurations will support these requirements? (Choose two.)

A. Associate an origin access identity with the CloudFront distribution.
B. Implement a “Principal”: “cloudfront.amazonIAM.com” condition in the S3 bucket policy.
C. Modify the S3 bucket permissions so that only the origin access identity can access the bucket contents.
D. Implement security groups so that the S3 bucket can be accessed only by using the intended CloudFront distribution.
E. Configure the S3 bucket policy so that it is accessible only through VPC endpoints, and place the CloudFront distribution into the specified VPC.

Answer: AC

NEW QUESTION 158
- (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 IAM KMS Use the instance role profile to control access to the KMS keys needed to decrypt the data.
B. Store the sensitive data in IAM 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 IAM 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 162
- (Exam Topic 2)
A Security Architect is evaluating managed solutions for storage of encryption keys. The requirements are:
-Storage is accessible by using only VPCs.
-Service has tamper-evident controls.
-Access logging is enabled.
-Storage has high availability.
Which of the following services meets these requirements?

A. Amazon S3 with default encryption
B. IAM CloudHSM
C. Amazon DynamoDB with server-side encryption
D. IAM Systems Manager Parameter Store

Answer: B

NEW QUESTION 167
- (Exam Topic 2)
A company stores data on an Amazon EBS volume attached to an Amazon EC2 instance. The data is asynchronously replicated to an Amazon S3 bucket. Both the EBS volume and the S3 bucket are encrypted
with the same IAM KMS Customer Master Key (CMK). A former employee scheduled a deletion of that CMK before leaving the company.
The company’s Developer Operations department learns about this only after the CMK has been deleted. Which steps must be taken to address this situation?

A. Copy the data directly from the EBS encrypted volume before the volume is detached from the EC2 instance.
B. Recover the data from the EBS encrypted volume using an earlier version of the KMS backing key.
C. Make a request to IAM Support to recover the S3 encrypted data.
D. Make a request to IAM Support to restore the deleted CMK, and use it to recover the data.

Answer: A

Explanation:
https://docs.IAM.amazon.com/kms/latest/developerguide/deleting-keys.html#deleting-keys-how-it-works

NEW QUESTION 168
- (Exam Topic 2)
An IAM Lambda function was misused to alter data, and a Security Engineer must identify who invoked the function and what output was produced. The Engineer cannot find any logs created by the Lambda function in Amazon CloudWatch Logs.
Which of the following explains why the logs are not available?

A. The execution role for the Lambda function did not grant permissions to write log data to CloudWatch Logs.
B. The Lambda function was executed by using Amazon API Gateway, so the logs are not stored in CloudWatch Logs.
C. The execution role for the Lambda function did not grant permissions to write to the Amazon S3 bucket where CloudWatch Logs stores the logs.
D. The version of the Lambda function that was executed was not current.

Answer: A

NEW QUESTION 169

- (Exam Topic 2)
A company runs an application on IAM that needs to be accessed only by employees. Most employees work from the office, but others work remotely or travel.
How can the Security Engineer protect this workload so that only employees can access it?

A. Add each employee's home IP address to the security group for the application so that only those users can access the workload.
B. Create a virtual gateway for VPN connectivity for each employee, and restrict access to the workload from within the VPC.
C. Use a VPN appliance from the IAM Marketplace for users to connect to, and restrict workload access to traffic from that appliance.
D. Route all traffic to the workload through IAM WA
E. Add each employee's home IP address into an IAM WAF rule, and block all other traffic.

Answer: C

Explanation:
https://docs.IAM.amazon.com/vpn/latest/clientvpn-admin/what-is.html

NEW QUESTION 171
- (Exam Topic 2)
An organization is using Amazon CloudWatch Logs with agents deployed on its Linux Amazon EC2 instances. The agent configuration files have been checked and the application log files to be pushed are configured correctly. A review has identified that logging from specific instances is missing.
Which steps should be taken to troubleshoot the issue? (Choose two.)

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

Answer: AB

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

NEW QUESTION 175
- (Exam Topic 2)
An Amazon EC2 instance is part of an EC2 Auto Scaling group that is behind an Application Load Balancer (ALB). It is suspected that the EC2 instance has been compromised.
Which steps should be taken to investigate the suspected compromise? (Choose three.)

A. Detach the elastic network interface from the EC2 instance.
B. Initiate an Amazon Elastic Block Store volume snapshot of all volumes on the EC2 instance.
C. Disable any Amazon Route 53 health checks associated with the EC2 instance.
D. De-register the EC2 instance from the ALB and detach it from the Auto Scaling group.
E. Attach a security group that has restrictive ingress and egress rules to the EC2 instance.
F. Add a rule to an IAM WAF to block access to the EC2 instance.

Answer: BDE

Explanation:
https://d1.IAMstatic.com/whitepapers/IAM_security_incident_response.pdf

NEW QUESTION 178
- (Exam Topic 2)
An Amazon S3 bucket is encrypted using an IAM KMS CMK. An IAM user is unable to download objects from the S3 bucket using the IAM Management Console; however, other users can download objects from the S3 bucket.
Which policies should the Security Engineer review and modify to resolve this issue? (Select three.)

A. The CMK policy
B. The VPC endpoint policy
C. The S3 bucket policy
D. The S3 ACL
E. The IAM policy

Answer: ACE

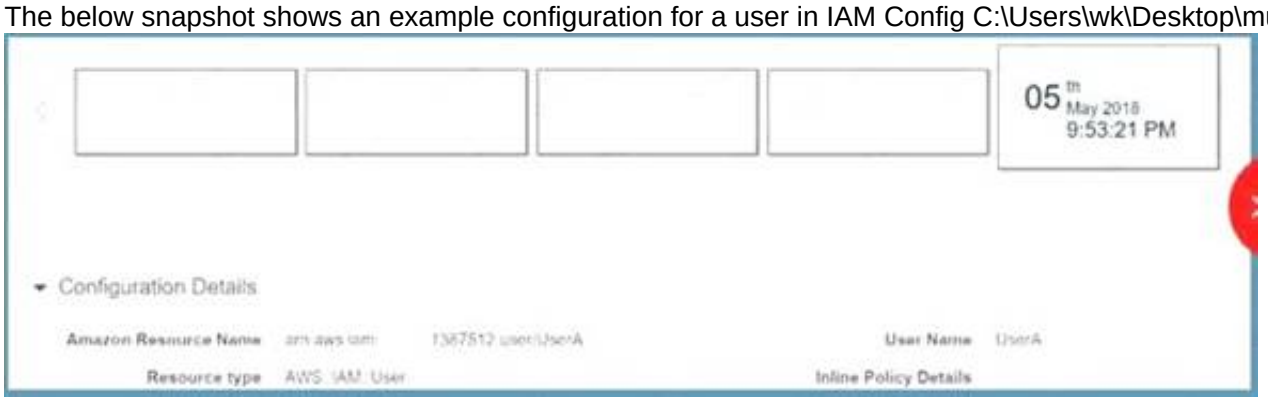
Explanation:
https://IAM.amazon.com/premiumsupport/knowledge-center/decrypt-kms-encrypted-objects-s3/

NEW QUESTION 181
- (Exam Topic 2)
A security team is creating a response plan in the event an employee executes unauthorized actions on IAM infrastructure. They want to include steps to determine if the employee's IAM permissions changed as part of the incident.
What steps should the team document in the plan? Please select:

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

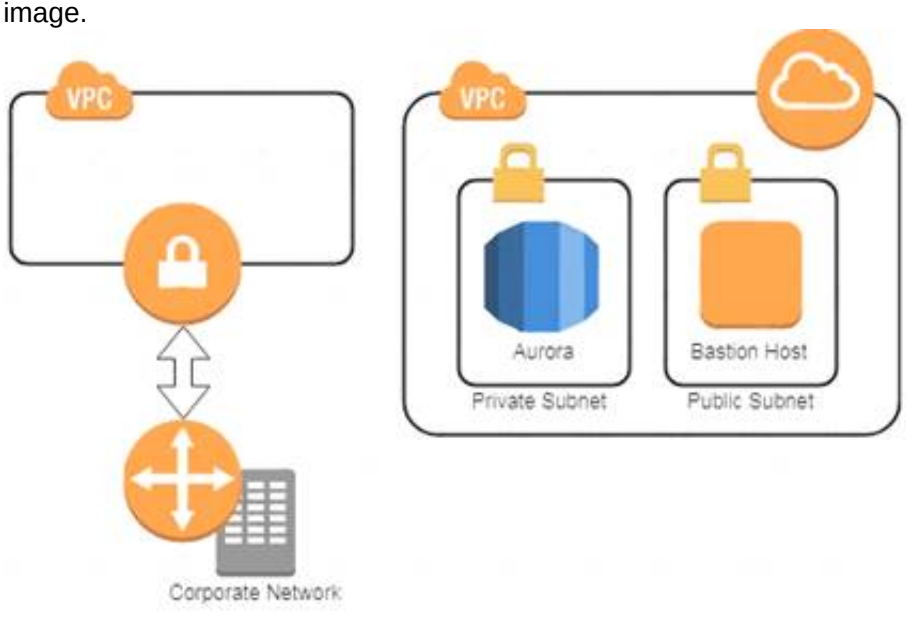
Answer: A

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



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

NEW QUESTION 184
- (Exam Topic 2)
A company has two IAM accounts, each containing one VPC. The first VPC has a VPN connection with its corporate network. The second VPC, without a VPN, hosts an Amazon Aurora database cluster in private subnets. Developers manage the Aurora database from a bastion host in a public subnet as shown in the image.



A security review has flagged this architecture as vulnerable, and a Security Engineer has been asked to make this design more secure. The company has a short deadline and a second VPN connection to the Aurora account is not possible.
How can a Security Engineer securely set up the bastion host?

A. Move the bastion host to the VPC with VPN connectivit
B. Create a VPC peering relationship between the bastion host VPC and Aurora VPC.
C. Create a SSH port forwarding tunnel on the Developer's workstation to the bastion host to ensure that only authorized SSH clients can access the bastion host.
D. Move the bastion host to the VPC with VPN connectivit
E. Create a cross-account trust relationship between the bastion VPC and Aurora VPC, and update the Aurora security group for the relationship.
F. Create an IAM Direct Connect connection between the corporate network and the Aurora account, and adjust the Aurora security group for this connection.

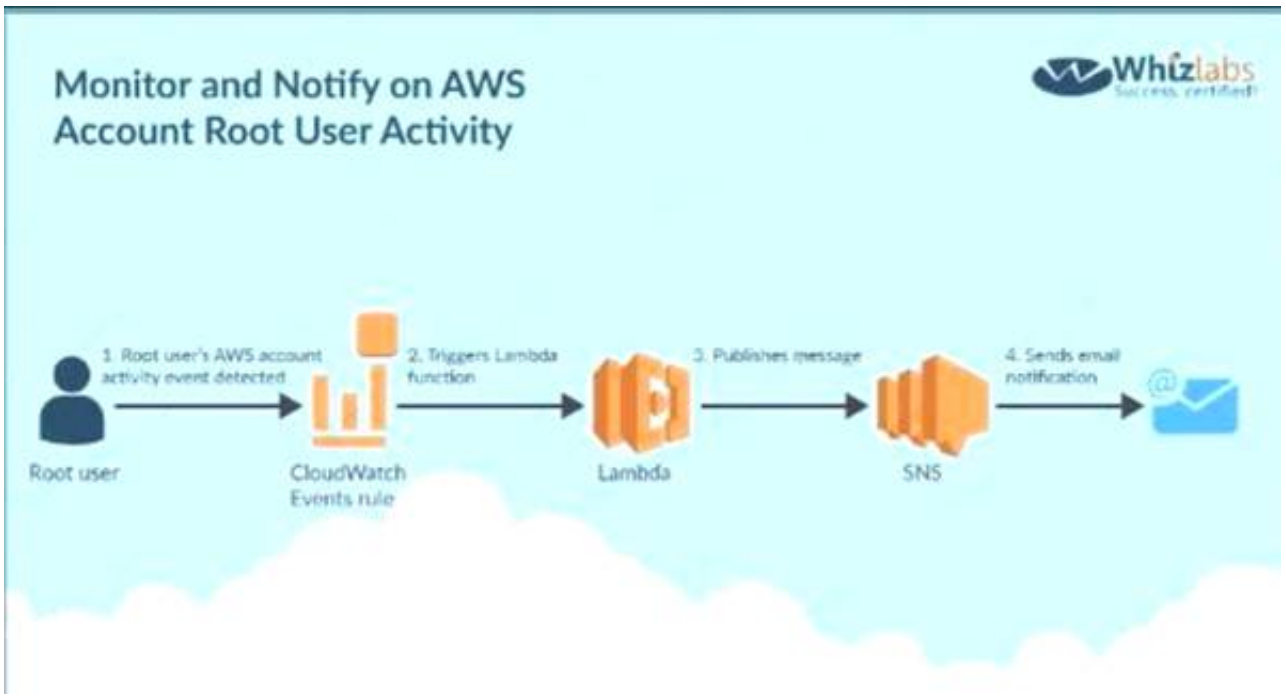
Answer: A

NEW QUESTION 187
- (Exam Topic 2)
Your company has a requirement to monitor all root user activity by notification. How can this best be achieved? Choose 2 answers from the options given below. Each answer forms part of the solution
Please select:

A. Create a Cloudwatch Events Rule s
B. Create a Cloudwatch Logs Rule
C. Use a Lambda function
D. Use Cloudtrail API call

Answer: AC

Explanation:
Below is a snippet from the IAM blogs on a solution C:\Users\wk\Desktop\mudassar\Untitled.jpg



Option B is invalid because you need to create a Cloudwatch Events Rule and there is such thing as a Cloudwatch Logs Rule Option D is invalid because Cloud Trail API calls can be recorded but cannot be used to send across notifications For more information on this blog article, please visit the following URL:
https://IAM.amazon.com/blogs/mt/monitor-and-notify-on-IAM-account-root-user-activityy The correct answers are: Create a Cloudwatch Events Rule, Use a Lambda function
Submit your Feedback/Queries to our Experts

NEW QUESTION 192
- (Exam Topic 2)
A company's database developer has just migrated an Amazon RDS database credential to be stored and managed by IAM Secrets Manager. The developer has also enabled rotation of the credential within the Secrets Manager console and set the rotation to change every 30 days.
After a short period of time, a number of existing applications have failed with authentication errors. What is the MOST likely cause of the authentication errors?

A. Migrating the credential to RDS requires that all access come through requests to the Secrets Manager.
B. Enabling rotation in Secrets Manager causes the secret to rotate immediately, and the applications are using the earlier credential.
C. The Secrets Manager IAM policy does not allow access to the RDS database.
D. The Secrets Manager IAM policy does not allow access for the applications.

Answer: B

Explanation:
https://docs.IAM.amazon.com/secretsmanager/latest/userguide/enable-rotation-rds.html

NEW QUESTION 195
- (Exam Topic 2)
Your IT Security team has advised to carry out a penetration test on the resources in their company's IAM Account. This is as part of their capability to analyze the security of the Infrastructure. What should be done first in this regard?
Please select:

A. Turn on Cloud trail and carry out the penetration test
B. Turn on VPC Flow Logs and carry out the penetration test
C. Submit a request to IAM Support
D. Use a custom IAM Marketplace solution for conducting the penetration test

Answer: C

Explanation:
This concept is given in the IAM Documentation
How do I submit a penetration testing request for my IAM resources? Issue
I want to run a penetration test or other simulated event on my IAM architecture. How do I get permission from IAM to do that?
Resolution
Before performing security testing on IAM resources, you must obtain approval from IAM. After you submit your request IAM will reply in about two business days. IAM might have additional questions about your test which can extend the approval process, so plan accordingly and be sure that your initial request is as detailed as possible.
If your request is approved, you'll receive an authorization number.
Option A.B and D are all invalid because the first step is to get prior authorization from IAM for penetration tests
For more information on penetration testing, please visit the below URL
* https://IAM.amazon.com/security/penetration-testing/
* https://IAM.amazon.com/premiumsupport/knowledge-center/penetration-testing/ (
The correct answer is: Submit a request to IAM Support Submit your Feedback/Queries to our Experts

NEW QUESTION 196
- (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://IAM.amazon.com/blogs/compute/maintaining-transport-layer-security-all-the-way-to-your-container-usin

NEW QUESTION 201
- (Exam Topic 2)
A Security Engineer discovers that developers have been adding rules to security groups that allow SSH and RDP traffic from 0.0.0.0/0 instead of the organization firewall IP.
What is the most efficient way to remediate the risk of this activity?

A. Delete the internet gateway associated with the VPC.
B. Use network access control lists to block source IP addresses matching 0.0.0.0/0.
C. Use a host-based firewall to prevent access from all but the organization's firewall IP.
D. Use IAM Config rules to detect 0.0.0.0/0 and invoke an IAM Lambda function to update the security group with the organization's firewall IP.

Answer: D

NEW QUESTION 205
- (Exam Topic 2)
A company hosts a critical web application on the IAM Cloud. This is a key revenue generating application for the company. The IT Security team is worried about potential DDos attacks against the web site. The senior management has also specified that immediate action needs to be taken in case of a potential DDos attack. What should be done in this regard?
Please select:

A. Consider using the IAM Shield Service
B. Consider using VPC Flow logs to monitor traffic for DDos attack and quickly take actions on a trigger of a potential attack.
C. Consider using the IAM Shield Advanced Service
D. Consider using Cloudwatch logs to monitor traffic for DDos attack and quickly take actions on a trigger of a potential attack.

Answer: C

Explanation:
Option A is invalid because the normal IAM Shield Service will not help in immediate action against a DDos attack. This can be done via the IAM Shield Advanced Service
Option B is invalid because this is a logging service for VPCs traffic flow but cannot specifically protect against DDos attacks.
Option D is invalid because this is a logging service for IAM Services but cannot specifically protect against DDos attacks.
The IAM Documentation mentions the following
IAM Shield Advanced provides enhanced protections for your applications running on Amazon EC2. Elastic Load Balancing (ELB), Amazon CloudFront and Route 53 against larger and more sophisticated attacks. IAM Shield Advanced is available to IAM Business Support and IAM Enterprise Support customers. IAM Shield Advanced protection provides always-on, flow-based monitoring of network traffic and active application monitoring to provide near real-time notifications of DDoS attacks. IAM Shield Advanced also gives customers highly flexible controls over attack mitigations to take actions instantly. Customers can also engage the DDoS Response Team (DRT) 24X7 to manage and mitigate their application layer DDoS attacks.
For more information on IAM Shield, please visit the below URL: https://IAM.amazon.com/shield/faqs;
The correct answer is: Consider using the IAM Shield Advanced Service Submit your Feedback/Queries to our Experts

NEW QUESTION 206
- (Exam Topic 2)
An application makes calls to IAM services using the IAM SDK. The application runs on Amazon EC2 instances with an associated IAM role. When the application attempts to access an object within an Amazon S3 bucket; the Administrator receives the following error message: HTTP 403: Access Denied.
Which combination of steps should the Administrator take to troubleshoot this issue? (Select three.)

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

Answer: BCE

NEW QUESTION 208
- (Exam Topic 2)
A Systems Administrator has written the following Amazon S3 bucket policy designed to allow access to an S3 bucket for only an authorized IAM IAM user from the IP address range 10.10.10.0/24:

```
{
  "Version": "2012-10-17",
  "Id": "S3Policy1",
  "Statement": [
  {
   "Sid": ["OfficeAllowIP"],
   "Effect": ["Allow"],
   "Principal": ["*"],
   "Action": ["s3:*"],
   "Resource": ["arn:aws:s3:::Bucket"],
   "Condition": {
     "IpAddress": [
       {"aws: SourceIp": "10.10.10.0/24"}
      ]
     }
   }]
}
```

When trying to download an object from the S3 bucket from 10.10.10.40, the IAM user receives an access denied message.
What does the Administrator need to change to grant access to the user?

A. Change the "Resource" from "arn: IAM:s3:::Bucket" to "arn:IAM:s3:::Bucket/*".
B. Change the "Principal" from "*" to {IAM:"arn:IAM:iam: : account-number: user/username"}
C. Change the "Version" from "2012-10-17" to the last revised date of the policy
D. Change the "Action" from ["s3:*"] to ["s3:GetObject", "s3:ListBucket"]

Answer: A

NEW QUESTION 210
- (Exam Topic 2)
Which approach will generate automated security alerts should too many unauthorized IAM 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 IAM CloudTrail to stream event data to Amazon Kinesi
C. Configure an IAM 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 IAM services, and raise an alert if service error rates increase.

Answer: A

Explanation:
https://docs.IAM.amazon.com/IAMcloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail.html#cloudwatc Open the CloudWatch console at https://console.IAM.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 214
- (Exam Topic 2)
A company has a few dozen application servers in private subnets behind an Elastic Load Balancer (ELB) in an IAM Auto Scaling group. The application is accessed from the web over HTTPS. The data must always be encrypted in transit. The Security Engineer is worried about potential key exposure due to vulnerabilities in the application software.
Which approach will meet these requirements while protecting the external certificate during a breach?

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

Answer: C

NEW QUESTION 215
- (Exam Topic 2)
A company requires that IP packet data be inspected for invalid or malicious content. Which of the following approaches achieve this requirement? (Choose two.)

A. Configure a proxy solution on Amazon EC2 and route all outbound VPC traffic through i
B. Perform inspection within proxy software on the EC2 instance.

C. Configure the host-based agent on each EC2 instance within the VP
D. Perform inspection within the host-based agent.
E. Enable VPC Flow Logs for all subnets in the VP
F. Perform inspection from the Flow Log data within Amazon CloudWatch Logs.
G. Configure Elastic Load Balancing (ELB) access log
H. Perform inspection from the log data within the ELB access log files.
I. Configure the CloudWatch Logs agent on each EC2 instance within the VP
J. Perform inspection from the log data within CloudWatch Logs.

Answer: AB

Explanation:
"EC2 Instance IDS/IPS solutions offer key features to help protect your EC2 instances. This includes alerting administrators of malicious activity and policy violations, as well as identifying and taking action against attacks. You can use IAM services and third party IDS/IPS solutions offered in IAM Marketplace to stay one step ahead of potential attackers."

NEW QUESTION 219
- (Exam Topic 2)
A Security Analyst attempted to troubleshoot the monitoring of suspicious security group changes. The Analyst was told that there is an Amazon CloudWatch alarm in place for these IAM CloudTrail log events.
The Analyst tested the monitoring setup by making a configuration change to the security group but did not receive any alerts.
Which of the following troubleshooting steps should the Analyst perform?

A. Ensure that CloudTrail and S3 bucket access logging is enabled for the Analyst's IAM account.
B. Verify that a metric filter was created and then mapped to an alar
C. Check the alarm notification action.
D. Check the CloudWatch dashboards to ensure that there is a metric configured with an appropriate dimension for security group changes.
E. Verify that the Analyst's account is mapped to an IAM policy that includes permissions for cloudwatch: GetMetricStatistics and Cloudwatch: ListMetrics.

Answer: B

Explanation:
MetricFilter:
Type: 'IAM::Logs::MetricFilter' Properties:
LogGroupName: '' FilterPattern: >{ ($.eventName = AuthorizeSecurityGroupIngress) || ($.eventName = AuthorizeSecurityGroupEgress) || ($.eventName = RevokeSecurityGroupIngress) || ($.eventName = RevokeSecurityGroupEgress)
|| ($.eventName = CreateSecurityGroup) || ($.eventName = DeleteSecurityGroup) }
MetricTransformations:
- MetricValue: '1'
MetricNamespace: CloudTrailMetrics MetricName: SecurityGroupEventCount

NEW QUESTION 224
- (Exam Topic 2)
The IAM Systems Manager Parameter Store is being used to store database passwords used by an IAM Lambda function. Because this is sensitive data, the parameters are stored as type SecureString and protected by an IAM KMS key that allows access through IAM. When the function executes, this parameter cannot be retrieved as the result of an access denied error.
Which of the following actions will resolve the access denied error?

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

Answer: C

Explanation:
https://docs.amazonIAM.cn/en_us/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Integrating.Authorizin

NEW QUESTION 227
- (Exam Topic 2)
A company has complex connectivity rules governing ingress, egress, and communications between Amazon EC2 instances. The rules are so complex that they cannot be implemented within the limits of the maximum number of security groups and network access control lists (network ACLs).
What mechanism will allow the company to implement all required network rules without incurring additional cost?

A. Configure IAM WAF rules to implement the required rules.
B. Use the operating system built-in, host-based firewall to implement the required rules.
C. Use a NAT gateway to control ingress and egress according to the requirements.
D. Launch an EC2-based firewall product from the IAM Marketplace, and implement the required rules in that product.

Answer: B

NEW QUESTION 231
- (Exam Topic 2)
A Security Engineer must design a system that can detect whether a file on an Amazon EC2 host has been modified. The system must then alert the Security Engineer of the modification.
What is the MOST efficient way to meet these requirements?

A. Install antivirus software and ensure that signatures are up-to-dat
B. Configure Amazon CloudWatch alarms to send alerts for security events.

C. Install host-based IDS software to check for file integrit
D. Export the logs to Amazon CloudWatch Logs for monitoring and alerting.
E. Export system log files to Amazon S3. Parse the log files using an IAM Lambda function that will send alerts of any unauthorized system login attempts through Amazon SNS.
F. Use Amazon CloudWatch Logs to detect file system change
G. If a change is detected, automaticallyterminate and recreate the instance from the most recent AM
H. Use Amazon SNS to send notification of the event.

Answer: B

NEW QUESTION 233
- (Exam Topic 2)
Your company is planning on hosting an internal network in IAM. They want machines in the VPC to authenticate using private certificates. They want to minimize the work and maintenance in working with certificates. What is the ideal way to fulfil this requirement.
Please select:

A. Consider using Windows Server 2016 Certificate Manager
B. Consider using IAM Certificate Manager
C. Consider using IAM Access keys to generate the certificates
D. Consider using IAM Trusted Advisor for managing the certificates

Answer: B

Explanation:
The IAM Documentation mentions the following
ACM is tightly linked with IAM Certificate Manager Private Certificate Authority. You can use ACM PCA to create a private certificate authority (CA) and then use ACM to issue private certificates. These are SSL/TLS X.509 certificates that identify users, computers, applications, services, servers, and other devices internally. Private certificates cannot be publicly trusted
Option A is partially invalid. Windows Server 2016 Certificate Manager can be used but since there is a requirement to "minimize the work and maintenance", IAM Certificate Manager should be used
Option C and D are invalid because these cannot be used for managing certificates. For more information on ACM, please visit the below URL: https://docs.IAM.amazon.com/acm/latest/userguide/acm-overview.html
The correct answer is: Consider using IAM Certificate Manager Submit your Feedback/Queries to our Experts

NEW QUESTION 236
- (Exam Topic 3)
You company has mandated that all data in IAM be encrypted at rest. How can you achieve this for EBS volumes? Choose 2 answers from the options given below
Please select:

A. Use Windows bit locker for EBS volumes on Windows instances
B. Use TrueEncrypt for EBS volumes on Linux instances
C. Use IAM Systems Manager to encrypt the existing EBS volumes
D. Boot EBS volume can be encrypted during launch without using custom AMI

Answer: AB

Explanation:
EBS encryption can also be enabled when the volume is created and not for existing volumes. One can use existing tools for OS level encryption.
Option C is incorrect.
IAM Systems Manager is a management service that helps you automatically collect software inventory, apply OS patches, create system images, and configure Windows and Linux operating systems.
Option D is incorrect
You cannot choose to encrypt a non-encrypted boot volume on instance launch. To have encrypted boot volumes during launch , your custom AMI must have it's boot volume encrypted before launch.
For more information on the Security Best practices, please visit the following URL: com/whit Security Practices.
The correct answers are: Use Windows bit locker for EBS volumes on Windows instances. Use TrueEncrypt for EBS volumes on Linux instances
Submit your Feedback/Queries to our Experts

NEW QUESTION 239
- (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 IAM KMS Customer Default master key
C. Use SSL/TLS for encrypting the data
D. Use S3 Encryption

Answer: B

Explanation:
The IAM Documentation mentions the following
Amazon Redshift uses a hierarchy of encryption keys to encrypt the database. You can use either IAM Key Management Servic (IAM 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.IAM.amazon.com/redshift/latest/memt/workine-with-db-encryption.htmll

The correct answer is: Use IAM KMS Customer Default master key Submit your Feedback/Queries to our Experts

NEW QUESTION 240
- (Exam Topic 3)
A company hosts data in S3. There is a requirement to control access to the S3 buckets. Which are the 2 ways in which this can be achieved?
Please select:

A. Use Bucket policies
B. Use the Secure Token service
C. Use IAM user policies
D. Use IAM Access Keys

Answer: AC

Explanation:
The IAM Documentation mentions the following
Amazon S3 offers access policy options broadly categorized as resource-based policies and user policies. Access policies you attach to your resources (buckets and objects) are referred to as resource-based policies. For example, bucket policies and access control lists (ACLs) are resource-based policies. You can also attach access policies to users in your account. These are called user policies. You may choose to use resource-based policies, user policies, or some combination of these to manage permissions to your Amazon S3 resources.
Option B and D are invalid because these cannot be used to control access to S3 buckets For more information on S3 access control, please refer to the below Link: https://docs.IAM.amazon.com/AmazonS3/latest/dev/s3-access-control.htmll
The correct answers are: Use Bucket policies. Use IAM user policies Submit your Feedback/Queries to our Experts

NEW QUESTION 242
- (Exam Topic 3)
Your company has a set of 1000 EC2 Instances defined in an IAM Account. They want to effectively automate several administrative tasks on these instances. Which of the following would be an effective way to achieve this?
Please select:

A. Use the IAM Systems Manager Parameter Store
B. Use the IAM Systems Manager Run Command
C. Use the IAM Inspector
D. Use IAM Config

Answer: B

Explanation:
The IAM Documentation mentions the following
IAM Systems Manager Run Command lets you remotely and securely manage the configuration of your managed instances. A managed instance is any Amazon EC2 instance or on-premises machine in your hybrid environment that has been configured for Systems Manager. Run Command enables you to automate common administrative tasks and perform ad hoc configuration changes at scale. You can use Run Command from the IAM console, the IAM Command Line Interface, IAM Tools for Windows PowerShell, or the IAM SDKs. Run Command is offered at no additional cost.
Option A is invalid because this service is used to store parameter Option C is invalid because this service is used to scan vulnerabilities in an EC2 Instance.
Option D is invalid because this service is used to check for configuration changes For more information on executing remote commands, please visit the below U https://docs.IAM.amazon.com/systems-manaEer/latest/usereuide/execute-remote-commands.htmll (
The correct answer is: Use the IAM Systems Manager Run Command Submit your Feedback/Queries to our Experts

NEW QUESTION 244
- (Exam Topic 3)
A company has a set of EC2 instances hosted in IAM. These instances have EBS volumes for storing critical information. There is a business continuity requirement and in order to boost the agility of the business and to ensure data durability which of the following options are not required.
Please select:

A. Use lifecycle policies for the EBS volumes
B. Use EBS Snapshots
C. Use EBS volume replication
D. Use EBS volume encryption

Answer: CD

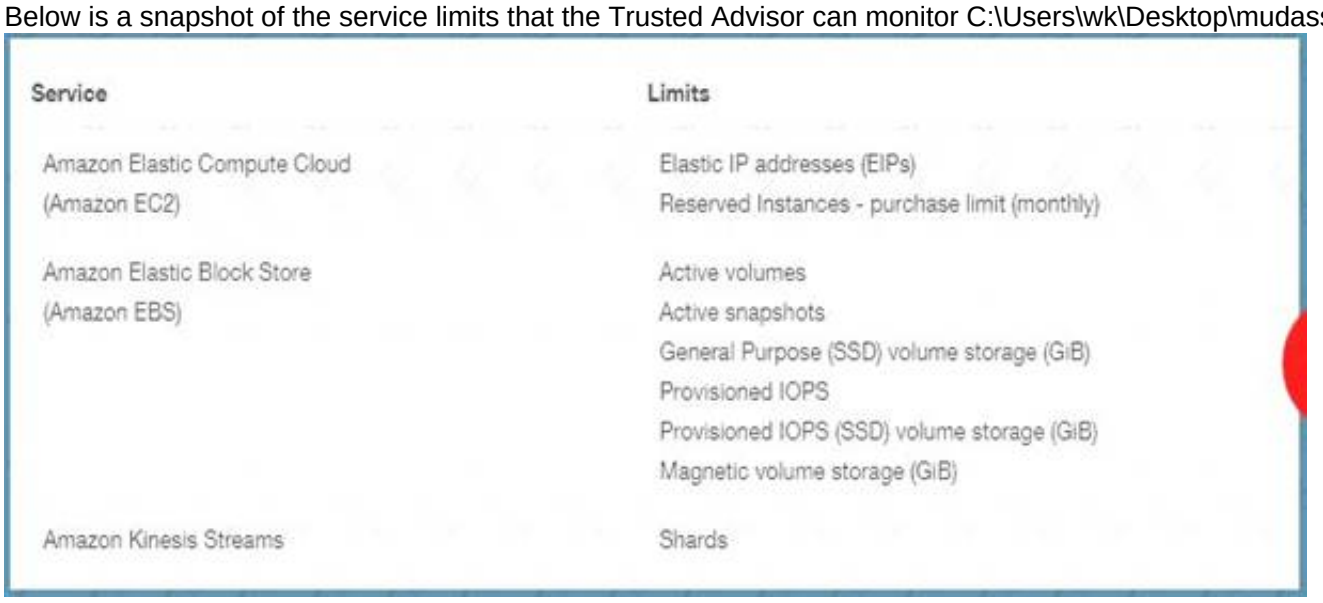
Explanation:
Data stored in Amazon EBS volumes is redundantly stored in multiple physical locations as part of normal operation of those services and at no additional charge. However, Amazon EBS replication is stored within the same availability zone, not across multiple zones; therefore, it is highly recommended that you conduct regular snapshots to Amazon S3 for long-term data durability.
You can use Amazon Data Lifecycle Manager (Amazon DLM) to automate the creation, retention, and deletion of snapshots
taken to back up your Amazon EBS volumes.
With lifecycle management, you can be sure that snapshots are cleaned up regularly and keep costs under control.
EBS Lifecycle Policies
A lifecycle policy consists of these core settings:
• Resource type—The IAM resource managed by the policy, in this case, EBS volumes.
• Target tag—The tag that must be associated with an EBS volume for it to be managed by the policy.
• Schedule—Defines how often to create snapshots and the maximum number of snapshots to keep. Snapshot creation starts within an hour of the specified start time. If creating a new snapshot exceeds the maximum number of snapshots to keep for the volume, the oldest snapshot is deleted.
Option C is correct. Each Amazon EBS volume is automatically replicated within its Availability Zone to protect you from component failure, offering high availability and durability. But it does not have an explicit feature like that.
Option D is correct Encryption does not ensure data durability
For information on security for Compute Resources, please visit the below URL https://d1.IAMstatic.com/whitepapers/Security/Security Compute Services Whitepaper.pdl
The correct answers are: Use EBS volume replication. Use EBS volume encryption Submit your Feedback/Queries to our Experts

NEW QUESTION 248
- (Exam Topic 3)
You want to ensure that you keep a check on the Active EBS Volumes, Active snapshots and Elastic IP addresses you use so that you don't go beyond the service limit. Which of the below services can help in this regard?
Please select:

A. IAM Cloudwatch
B. IAM EC2
C. IAM Trusted Advisor
D. IAM SNS

Answer: C

Explanation:
Below is a snapshot of the service limits that the Trusted Advisor can monitor C:\Users\wk\Desktop\mudassar\Untitled.jpg



Option A is invalid because even though you can monitor resources, it cannot be checked against the service limit.
Option B is invalid because this is the Elastic Compute cloud service Option D is invalid because it can be send notification but not check on service limit For more information on the Trusted Advisor monitoring, please visit the below URL:
https://IAM.amazon.com/premiumsupport/ta-faqs> The correct answer is: IAM Trusted Advisor Submit your Feedback/Queries to our Experts

NEW QUESTION 251
- (Exam Topic 3)
Which of the below services can be integrated with the IAM Web application firewall service. Choose 2 answers from the options given below
Please select:

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

Answer: AC

Explanation:
The IAM documentation mentions the following on the Application Load Balancer
IAM 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 IAM WAF.
For more information on the web application firewall please refer to the below URL: https://IAM.amazon.com/waf/faq;
The correct answers are: IAM Cloudfront IAM Application Load Balancer Submit your Feedback/Queries to our Experts

NEW QUESTION 254
- (Exam Topic 3)
Your company has been using IAM for the past 2 years. They have separate S3 buckets for logging the various IAM services that have been used. They have hired an external vendor for analyzing their log files. They have their own IAM account. What is the best way to ensure that the partner account can access the log files in the company account for analysis. Choose 2 answers from the options given below
Please select:

A. Create an IAM user in the company account
B. Create an IAM Role in the company account
C. Ensure the IAM user has access for read-only to the S3 buckets
D. Ensure the IAM Role has access for read-only to the S3 buckets

Answer: BD

Explanation:
The IAM Documentation mentions the following
To share log files between multiple IAM accounts, you must perform the following general steps. These steps are explained in detail later in this section.
Create an IAM role for each account that you want to share log files with.
For each of these IAM roles, create an access policy that grants read-only access to the account you want to share the log files with.
Have an IAM user in each account programmatically assume the appropriate role and retrieve the log files. Options A and C are invalid because creating an IAM user and then sharing the IAM user credentials with the vendor is a direct 'NO' practise from a security perspective.
For more information on sharing cloudtrail logs files, please visit the following URL https://docs.IAM.amazon.com/IAMcloudtrail/latest/userguide/cloudtrail-sharine-

loes.htmll
The correct answers are: Create an IAM Role in the company account Ensure the IAM Role has access for read-only to the S3 buckets
Submit your Feedback/Queries to our Experts

NEW QUESTION 255
- (Exam Topic 3)
A company has hired a third-party security auditor, and the auditor needs read-only access to all IAM resources and logs of all VPC records and events that have occurred on IAM. How can the company meet the auditor's requirements without comprising security in the IAM environment? Choose the correct answer from the options below
Please select:

A. Create a role that has the required permissions for the auditor.
B. Create an SNS notification that sends the CloudTrail log files to the auditor's email when CIoudTrail delivers the logs to S3, but do not allow the auditor access to the IAM environment.
C. The company should contact IAM as part of the shared responsibility model, and IAM will grant required access to th^ third-party auditor.
D. Enable CloudTrail logging and create an IAM user who has read-only permissions to the required IAM resources, including the bucket containing the CloudTrail logs.

Answer: D

Explanation:
IAM CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your IAM account. With CloudTrail, you can log, continuously monitor, and retain events related to API calls across your IAM infrastructure. CloudTrail provides a history of IAM API calls for your account including API calls made through the IAM Management Console, IAM SDKs, command line tools, and other IAM services. This history simplifies security analysis, resource change tracking, and troubleshooting.
Option A and C are incorrect since Cloudtrail needs to be used as part of the solution Option B is incorrect since the auditor needs to have access to Cloudtrail
For more information on cloudtrail, please visit the below URL: https://IAM.amazon.com/cloudtraiL
The correct answer is: Enable CloudTrail logging and create an IAM user who has read-only permissions to the required IAM resources, including the bucket containing the CloudTrail logs.
Submit your Feedback/Queries to our Experts

NEW QUESTION 260
- (Exam Topic 3)
A company has several Customer Master Keys (CMK), some of which have imported key material. Each CMK must be rotated annually.
What two methods can the security team use to rotate each key? Select 2 answers from the options given below Please select:

A. Enable automatic key rotation for a CMK
B. Import new key material to an existing CMK
C. Use the CLI or console to explicitly rotate an existing CMK
D. Import new key material to a new CMK; Point the key alias to the new CMK.
E. Delete an existing CMK and a new default CMK will be created.

Answer: AD

Explanation:
The IAM Documentation mentions the following
Automatic key rotation is available for all customer managed CMKs with KMS-generated key material. It is not available for CMKs that have imported key material (the value of the Origin field is External), but you can rotate these CMKs manually.
Rotating Keys Manually
You might want to create a newCMKand use it in place of a current CMK instead of enabling automatic key rotation. When the new CMK has different cryptographic material than the current CMK, using the new CMK has the same effect as changing the backing key in an existing CMK. The process of replacing one CMK with another is known as manual key rotation.
When you begin using the new CMK, be sure to keep the original CMK enabled so that IAM KMS can decrypt data that the original CMK encrypted. When decrypting data, KMS identifies the CMK that was used to encrypt the data, and it uses the sam CMK to decrypt the data. As long as you keep both the original and new CMKs enabled, IAM KMS can decrypt any data that was encrypted by either CMK.
Option B is invalid because you also need to point the key alias to the new key Option C is invalid because existing CMK keys cannot be rotated as they are
Option E is invalid because deleting existing keys will not guarantee the creation of a new default CMK key For more information on Key rotation please see the below Link: https://docs.IAM.amazon.com/kms/latest/developereuide/rotate-keys.html
The correct answers are: Enable automatic key rotation for a CMK, Import new key material to a new CMK; Point the key alias to the new CMK.
Submit your Feedback/Queries to our Experts

NEW QUESTION 263
- (Exam Topic 3)
A customer has an instance hosted in the IAM 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'sWorkstation
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 268
- (Exam Topic 3)
A company requires that data stored in IAM be encrypted at rest. Which of the following approaches achieve this requirement? Select 2 answers from the options given below.
Please select:

A. When storing data in Amazon EBS, use only EBS-optimized Amazon EC2 instances.
B. When storing data in EBS, encrypt the volume by using IAM KMS.
C. When storing data in Amazon S3, use object versioning and MFA Delete.
D. When storing data in Amazon EC2 Instance Store, encrypt the volume by using KMS.
E. When storing data in S3, enable server-side encryption.

Answer: BE

Explanation:
The IAM Documentation mentions the following
To create an encrypted Amazon EBS volume, select the appropriate box in the Amazon EBS section of the Amazon EC2 console. You can use a custom customer master key (CMK) by choosing one from the list that appears below the encryption box. If you do not specify a custom CMK, Amazon EBS uses the IAM-managed CMK for Amazon EBS in your account. If there is no IAM-managed CMK for Amazon EBS in your account, Amazon EBS creates one.
Data protection refers to protecting data while in-transit (as it travels to and from Amazon S3) and at rest (while it is stored on disks in Amazon S3 data centers). You can protect data in transit by using SSL or by using client-side encryption. You have the following options of protecting data at rest in Amazon S3.
• Use Server-Side Encryption - You request Amazon S3 to encrypt your object before saving it on disks in its data centers and decrypt it when you download the objects.
• Use Client-Side Encryption - You can encrypt data client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, the encryption keys, and related tools.
Option A is invalid because using EBS-optimized Amazon EC2 instances alone will not guarantee protection of instances at rest. Option C is invalid because this will not encrypt data at rest for S3 objects. Option D is invalid because you don't store data in Instance store. For more information on EBS encryption, please visit the below URL:
https://docs.IAM.amazon.com/kms/latest/developerguide/services-ebs.html For more information on S3 encryption, please visit the below URL:
https://docs.IAM.amazon.com/AmazonS3/latest/dev/UsinEEncryption.html
The correct answers are: When storing data in EBS, encrypt the volume by using IAM KMS. When storing data in S3, enable server-side encryption.
Submit your Feedback/Queries to our Experts

NEW QUESTION 271
- (Exam Topic 3)
Your company has a set of EC2 Instances that are placed behind an ELB. Some of the applications hosted on these instances communicate via a legacy protocol. There is a security mandate that all traffic between the client and the EC2 Instances need to be secure. How would you accomplish this?
Please select:

A. Use an Application Load balancer and terminate the SSL connection at the ELB
B. Use a Classic Load balancer and terminate the SSL connection at the ELB
C. Use an Application Load balancer and terminate the SSL connection at the EC2 Instances
D. Use a Classic Load balancer and terminate the SSL connection at the EC2 Instances

Answer: D

Explanation:
Since there are applications which work on legacy protocols, you need to ensure that the ELB can be used at the network layer as well and hence you should choose the Classic ELB. Since the traffic needs to be secure till the EC2 Instances, the SSL termination should occur on the Ec2 Instances.
Option A and C are invalid because you need to use a Classic Load balancer since this is a legacy application. Option B is incorrect since encryption is required until the EC2 Instance
For more information on HTTPS listeners for classic load balancers, please refer to below URL
https://docs.IAM.ama20n.com/elasticloadbalancing/latest/classic/elb-https-load-balancers.htmll
The correct answer is: Use a Classic Load balancer and terminate the SSL connection at the EC2 Instances Submit your Feedback/Queries to our Experts

NEW QUESTION 276
- (Exam Topic 3)
An EC2 Instance hosts a Java based application that access a DynamoDB table. This EC2 Instance is currently serving production based users. Which of the following is a secure way of ensuring that the EC2 Instance access the Dynamo table
Please select:

A. Use IAM Roles with permissions to interact with DynamoDB and assign it to the EC2 Instance
B. Use KMS keys with the right permissions to interact with DynamoDB and assign it to the EC2 Instance
C. Use IAM Access Keys with the right permissions to interact with DynamoDB and assign it to the EC2 Instance
D. Use IAM Access Groups with the right permissions to interact with DynamoDB and assign it to the EC2 Instance

Answer: A

Explanation:
To always ensure secure access to IAM resources from EC2 Instances, always ensure to assign a Role to the EC2 Instance Option B is invalid because KMS keys are not used as a mechanism for providing EC2 Instances access to IAM services. Option C is invalid Access keys is not a safe mechanism for providing EC2 Instances access to IAM services. Option D is invalid because there is no way access groups can be assigned to EC2 Instances. For more information on IAM Roles, please refer to the below URL:
https://docs.IAM.amazon.com/IAM/latest/UserGuide/id roles.html
The correct answer is: Use IAM Roles with permissions to interact with DynamoDB and assign it to the EC2 Instance Submit your Feedback/Queries to our Experts

NEW QUESTION 280
- (Exam Topic 3)
You are responsible to deploying a critical application onto IAM. Part of the requirements for this application is to ensure that the controls set for this application met PCI compliance. Also there is a need to monitor web application logs to identify any malicious activity. Which of the following services can be used to fulfil this requirement. Choose 2 answers from the options given below
Please select:

A. Amazon Cloudwatch Logs
B. Amazon VPC Flow Logs
C. Amazon IAM Config
D. Amazon Cloudtrail

Answer: AD

Explanation:
The IAM Documentation mentions the following about these services
IAM CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your IAM account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your IAM infrastructure. CloudTrail provides event history of your IAM account activity, including actions taken through the IAM Management Console, IAM SDKs, command line tools, and other IAM services. This event history simplifies security analysis, resource change tracking, and troubleshooting.
Option B is incorrect because VPC flow logs can only check for flow to instances in a VPC Option C is incorrect because this can check for configuration changes only
For more information on Cloudtrail, please refer to below URL: https://IAM.amazon.com/cloudtrail;
You can use Amazon CloudWatch Logs to monitor, store, and access your log files from Amazon Elastic Compute Cloud (Amazon EC2) instances, IAM CloudTrail, Amazon Route 53, and other sources. You can then retrieve the associated log data from CloudWatch Logs.
For more information on Cloudwatch logs, please refer to below URL: http://docs.IAM.amazon.com/AmazonCloudWatch/latest/loes/WhatisCloudWatchLoES.htmll
The correct answers are: Amazon Cloudwatch Logs, Amazon Cloudtrail

NEW QUESTION 281
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SCS-C02 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SCS-C02 Product From:

https://www.2passeasy.com/dumps/SCS-C02/

Money Back Guarantee

SCS-C02 Practice Exam Features:

* SCS-C02 Questions and Answers Updated Frequently

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

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

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