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 Developer is building a serverless application that uses Amazon API Gateway as the front end. The application will not be publicly accessible. Other legacy applications running on Amazon EC2 will make calls to the application A Security Engineer Has been asked to review the security controls for authentication and authorization of the application
Which combination of actions would provide the MOST secure solution? (Select TWO)

A. Configure an IAM policy that allows the least permissive actions to communicate with the API Gateway Attach the policy to the role used by the legacy EC2 instances
B. Enable IAM WAF for API Gateway Configure rules to explicitly allow connections from the legacy EC2 instances
C. Create a VPC endpoint for API Gateway Attach an IAM resource policy that allows the role of the legacy EC2 instances to call specific APIs
D. Create a usage plan Generate a set of API keys for each application that needs to call the API.
E. Configure cross-origin resource sharing (CORS) in each API Share the CORS information with the applications that call the API.

Answer: AE

NEW QUESTION 3
- (Exam Topic 1)
A city is implementing an election results reporting website that will use Amazon GoudFront The website runs on a fleet of Amazon EC2 instances behind an Application Load Balancer (ALB) in an Auto Scaling group. Election results are updated hourly and are stored as .pdf tiles in an Amazon S3 bucket. A Security Engineer needs to ensure that all external access to the website goes through CloudFront.
Which solution meets these requirements?

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

Answer: C

NEW QUESTION 4
- (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 5
- (Exam Topic 1)
A company Is building a data lake on Amazon S3. The data consists of millions of small files containing sensitive information. The security team has the following requirements for the architecture:
• Data must be encrypted in transit.
• Data must be encrypted at rest.
• The bucket must be private, but if the bucket is accidentally made public, the data must remain confidential. Which combination of steps would meet the requirements? (Select THREE.)

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

Answer: BDF

NEW QUESTION 6
- (Exam Topic 1)
A company's architecture requires that its three Amazon EC2 instances run behind an Application Load Balancer (ALB). The EC2 instances transmit sensitive data between each other Developers use SSL certificates to encrypt the traffic between the public users and the ALB However the Developers are unsure of how to encrypt the data in transit between the ALB and the EC2 instances and the traffic between the EC2 instances
Which combination of activities must the company implement to meet its encryption requirements'? (Select TWO)
A. Configure SSLTLS on the EC2 instances and configure the ALB target group to use HTTPS
B. Ensure that all resources are in the same VPC so the default encryption provided by the VPC is used to encrypt the traffic between the EC2 instances.
C. In the AL
D. select the default encryption to encrypt the traffic between the ALB and the EC2 instances
E. In the code for the application, include a cryptography library and encrypt the data before sending it between the EC2 instances
F. Configure IAM Direct Connect to provide an encrypted tunnel between the EC2 instances

Answer: BC

NEW QUESTION 7
- (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 8
- (Exam Topic 1)
A company has implemented centralized logging and monitoring of IAM CloudTrail logs from all Regions in an Amazon S3 bucket. The log Hies are encrypted using IAM KMS. A Security Engineer is attempting to review the log files using a third-party tool hosted on an Amazon EC2 instance The Security Engineer is unable to access the logs in the S3 bucket and receives an access denied error message
What should the Security Engineer do to fix this issue?

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

Answer: C

NEW QUESTION 9
- (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 10
- (Exam Topic 1)
A company’s security engineer is configuring Amazon S3 permissions to ban all current and future public buckets However, the company hosts several websites directly off S3 buckets with public access enabled
The engineer needs to bock me pubic S3 buckets without causing any outages on me easting websites The engineer has set up an Amazon CloudFrom distribution (or each website
Which set or steps should the security engineer implement next?

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

Answer: A

NEW QUESTION 11
- (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 14
- (Exam Topic 1)
After a recent security audit involving Amazon S3, a company has asked assistance reviewing its S3 buckets to determine whether data is properly secured. The first S3 bucket on the list has the following bucket policy.

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

Is this bucket policy sufficient to ensure that the data is not publicity accessible?

A. Yes, the bucket policy makes the whole bucket publicly accessible despite now the S3 bucket ACL or object ACLs are configured.
B. Yes, none of the data in the bucket is publicity accessible, regardless of how the S3 bucket ACL and object ACLs are configured.
C. No, the IAM user policy would need to be examined first to determine whether any data is publicly accessible.

D. No, the S3 bucket ACL and object ACLs need to be examined first to determine whether any data is publicly accessible.

Answer: A

NEW QUESTION 16
- (Exam Topic 1)
A company's on-premises data center forwards DNS logs to a third-party security incident events management (SIEM) solution that alerts on suspicious behavior. The company wants to introduce a similar capability to its IAM accounts that includes automatic remediation. The company expects to double in size within the next few months.
Which solution meets the company's current and future logging requirements?

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

Answer: A

NEW QUESTION 21
- (Exam Topic 1)
A security engineer need to ensure their company’s uses of IAM meets IAM security best practices. As part of this, the IAM account root user must not be used for daily work. The root user must be monitored for use, and the Security team must be alerted as quickly as possible if the root user is used.
Which solution meets these requirements?

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

Answer: A

NEW QUESTION 23
- (Exam Topic 1)
A company has several critical applications running on a large fleet of Amazon EC2 instances. As part of a security operations review, the company needs to apply a critical operating system patch to EC2 instances within 24 hours of the patch becoming available from the operating system vendor. The company does not have a patching solution deployed on IAM, but does have IAM Systems Manager configured. The solution must also minimize administrative overhead.
What should a security engineer recommend to meet these requirements?

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

Answer: B

NEW QUESTION 25
- (Exam Topic 1)
An company is using IAM Secrets Manager to store secrets that are encrypted using a CMK and are stored in the security account 111122223333. One of the company's production accounts. 444455556666, must to retrieve the secret values from the security account 111122223333. A security engineer needs to apply a policy to the secret in the security account based on least privilege access so the production account can retrieve the secret value only.
Which policy should the security engineer apply?

A.
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "secretsmanager:*",
            "Principal": {"AWS": "444455556666"},
            "Resource": "*"
        }
    ]
}
```

B.
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "secretsmanager:*",
            "Principal": {"AWS": "111122223333"},
            "Resource": "*"
        }
    ]
}
```

C.
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "secretsmanager:GetSecretValue",
            "Principal": {"AWS": "111122223333"},
            "Resource": "*"
        }
    ]
}
```

D.
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "secretsmanager:GetSecretValue",
            "Principal": {"AWS": "444455556666"},
            "Resource": "*"
        }
    ]
```

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

Answer: A

NEW QUESTION 28
- (Exam Topic 1)
Users report intermittent availability of a web application hosted on IAM. Monitoring systems report an excess of abnormal network traffic followed by high CPU utilization on the application web tier. Which of the following techniques will improve the availability of the application? (Select TWO.)

A. Deploy IAM WAF to block all unsecured web applications from accessing the internet.
B. Deploy an Intrusion Detection/Prevention System (IDS/IPS) to monitor or block unusual incoming network traffic.
C. Configure security groups to allow outgoing network traffic only from hosts that are protected with up-to-date antivirus software.
D. Create Amazon CloudFront distribution and configure IAM WAF rules to protect the web applications from malicious traffic.
E. Use the default Amazon VPC for externakfacing systems to allow IAM to actively block malicious network traffic affecting Amazon EC2 instances.

Answer: BD

NEW QUESTION 33
- (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 35
- (Exam Topic 1)
To meet regulatory requirements, a Security Engineer needs to implement an IAM policy that restricts the use of IAM services to the us-east-1 Region.
What policy should the Engineer implement?

A

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

B

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

C

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

D

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

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

Answer: B

NEW QUESTION 40
- (Exam Topic 1)
A Security Engineer for a large company is managing a data processing application used by 1,500 subsidiary companies. The parent and subsidiary companies all use IAM. The application uses TCP port 443 and runs on Amazon EC2 behind a Network Load Balancer (NLB). For compliance reasons, the application should only be accessible to the subsidiaries and should not be available on the public internet. To meet the compliance requirements for restricted access, the Engineer has received the public and private CIDR block ranges for each subsidiary
What solution should the Engineer use to implement the appropriate access restrictions for the application?

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

Answer: D

NEW QUESTION 41
- (Exam Topic 1)
A Security Engineer accidentally deleted the imported key material in an IAM KMS CMK. What should the Security Engineer do to restore the deleted key material?

A. Create a new CM
B. Download a new wrapping key and a new import token to import the original key material
C. Create a new CMK Use the original wrapping key and import token to import the original key material.
D. Download a new wrapping key and a new import token Import the original key material into the existing CMK.
E. Use the original wrapping key and import token Import the original key material into the existing CMK

Answer: C

NEW QUESTION 42
- (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 47
- (Exam Topic 1)
A Security Engineer is troubleshooting a connectivity issue between a web server that is writing log files to the logging server in another VPC. The Engineer has confirmed that a peering relationship exists between the two VPCs. VPC flow logs show that requests sent from the web server are accepted by the togging server but the web server never receives a reply
Which of the following actions could fix this issue1?

A. Add an inbound rule to the security group associated with the logging server that allows requests from the web server
B. Add an outbound rule to the security group associated with the web server that allows requests to the logging server.
C. Add a route to the route table associated with the subnet that hosts the logging server that targets the peering connection
D. Add a route to the route table associated with the subnet that hosts the web server that targets the peering connection

Answer: C

NEW QUESTION 49
- (Exam Topic 1)
A company's web application is hosted on Amazon EC2 instances running behind an Application Load Balancer (ALB) in an Auto Scaling group. An IAM WAF web ACL is associated with the ALB. IAM CloudTrail is enabled, and stores logs in Amazon S3 and Amazon CloudWatch Logs.
The operations team has observed some EC2 instances reboot at random. After rebooting, all access logs on the instances have been deleted. During an investigation, the operations team found that each reboot happened just after a PHP error occurred on the new-user-creation.php file. The operations team needs to view log information to determine if the company is being attacked.
Which set of actions will identify the suspect attacker's IP address for future occurrences?

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

Answer: D

Explanation:
You send logs from your web ACL to an Amazon Kinesis Data Firehose with a configured storage destination. After you enable logging, IAM WAF delivers logs to your storage destination through the HTTPS endpoint of Kinesis Data Firehose. https://docs.IAM.amazon.com/waf/latest/developerguide/logging.html

NEW QUESTION 51
- (Exam Topic 1)
A global company that deals with International finance is investing heavily in cryptocurrencies and wants to experiment with mining technologies using IAM. The company's security team has enabled Amazon GuardDuty and is concerned by the number of findings being generated by the accounts. The security team wants to minimize the possibility of GuardDuty finding false negatives for compromised instances that are performing mining
How can the security team continue using GuardDuty while meeting these requirements?

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

Answer: A

NEW QUESTION 53
- (Exam Topic 1)
A company has the software development teams that are creating applications that store sensitive data in Amazon S3 Each team's data must always be separate. The company's security team must design a data encryption strategy for both teams that provides the ability to audit key usage. The solution must also minimize operational overhead
what should me security team recommend?

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

Answer: A

NEW QUESTION 57
- (Exam Topic 1)
A recent security audit identified that a company's application team injects database credentials into the environment variables of an IAM Fargate task. The company's security policy mandates that all sensitive data be encrypted at rest and in transit.

When combination of actions should the security team take to make the application compliant within the security policy? (Select THREE)

A. Store the credentials securely in a file in an Amazon S3 bucket with restricted access to the application team IAM role Ask the application team to read the credentials from the S3 object instead
B. Create an IAM Secrets Manager secret and specify the key/value pairs to be stored in this secret
C. Modify the application to pull credentials from the IAM Secrets Manager secret instead of the environment variables.
D. Add the following statement to the container instance IAM role policy

```
{
    "Effect": "Allow",
    "Action": [
        "ssm:GetParameters",
        "secretsmanager:GetSecretValue",
        "kms:Decrypt"
    ],
    "Resource": [
        "arn:aws:secretsmanager:<region>:<aws_account_id>:secret:secret_name",
        "arn:aws:kms:<region>:<aws_account_id>:key/key_id"
    ]
}
```

E. Add the following statement to the execution role policy.

```
{
"Effect": "Allow",
"Action": [
    "ssm:GetParameters",
    "secretsmanager:GetSecretValue",
    "kms:Decrypt"
],
"Resource": [
    "arn:aws:secretsmanager:<region>:<aws_account_id>:secret:secret_name",
    "arn:aws:kms:<region>:<aws_account_id>:key/key_id"
]
}
```

F. Log in to the IAM Fargate instance, create a script to read the secret value from IAM Secret Manager, and inject the environment variable
G. Ask the application team to redeploy the application.

Answer: BEF

NEW QUESTION 58
- (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 59
- (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 64
- (Exam Topic 1)
A company is running an application on Amazon EC2 instances in an Auto Scaling group. The application stores logs locally A security engineer noticed that logs were lost after a scale-in event. The security engineer needs to recommend a solution to ensure the durability and availability of log data All logs must be kept for a minimum of 1 year for auditing purposes
What should the security engineer recommend?

A. Within the Auto Scaling lifecycle, add a hook to create and attach an Amazon Elastic Block Store (Amazon EBS) log volume each time an EC2 instance is create
B. When the instance is terminated, the EBS volume can be reattached to another instance for log review.
C. Create an Amazon Elastic File System (Amazon EFS) file system and add a command in the user data section of the Auto Scaling launch template to mount the EFS file system during EC2 instance creation Configure a process on the instance to copy the logs once a day from an instance Amazon Elastic Block Store (Amazon EBS) volume to a directory in the EFS file system.
D. Build the Amazon CloudWatch agent into the AMI used in the Auto Scaling grou
E. Configure the CloudWatch agent to send the logs to Amazon CloudWatch Logs for review.

F. Within the Auto Scaling lifecycle, add a lifecycle hook at the terminating state transition and alert the engineering team by using a lifecycle notification to Amazon Simple Notification Service (Amazon SNS). Configure the hook to remain in the Terminating:Wait state for 1 hour to allow manual review of the security logs prior to instance termination.

Answer: B

NEW QUESTION 66
- (Exam Topic 1)
A company is using IAM Organizations to manage multiple IAM accounts. The company has an application that allows users to assume the AppUser IAM role to download files from an Amazon S3 bucket that is encrypted with an IAM KMS CMK However when users try to access the files in the S3 bucket they get an access denied error.
What should a Security Engineer do to troubleshoot this error? (Select THREE)

A. Ensure the KMS policy allows the AppUser role to have permission to decrypt for the CMK
B. Ensure the S3 bucket policy allows the AppUser role to have permission to get objects for the S3 bucket
C. Ensure the CMK was created before the S3 bucket.
D. Ensure the S3 block public access feature is enabled for the S3 bucket.
E. Ensure that automatic key rotation is disabled for the CMK
F. Ensure the SCPs within Organizations allow access to the S3 bucket.

Answer: ABF

NEW QUESTION 70
- (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 71
- (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 74
- (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 77
- (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 82
- (Exam Topic 1)
A Security Engineer creates an Amazon S3 bucket policy that denies access to all users. A few days later, the Security Engineer adds an additional statement to the bucket policy to allow read-only access to one other employee Even after updating the policy the employee still receives an access denied message.
What is the likely cause of this access denial?

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

Answer: D

NEW QUESTION 86
- (Exam Topic 1)
A company's Security Engineer has been asked to monitor and report all IAM account root user activities. Which of the following would enable the Security Engineer to monitor and report all root user activities?
(Select TWO)

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

Answer: BE

NEW QUESTION 89
- (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 94
- (Exam Topic 1)
A security engineer is auditing a production system and discovers several additional IAM roles that are not required and were not previously documented during the last audit 90 days ago. The engineer is trying to find out who created these IAM roles and when they were created. The solution must have the lowest operational overhead.
Which solution will meet this requirement?

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

Answer: A

NEW QUESTION 98
- (Exam Topic 2)
The Security Engineer implemented a new vault lock policy for 10TB of data and called initiate-vault-lock 12 hours ago. The Audit team identified a typo that is allowing incorrect access to the vault.
What is the MOST cost-effective way to correct this?

A. Call the abort-vault-lock operation, fix the typo, and call the initiate-vault-lock again.
B. Copy the vault data to Amazon S3, delete the vault, and create a new vault with the data.

C. Update the policy, keeping the vault lock in place.
D. Update the policy and call initiate-vault-lock again to apply the new policy.

Answer: A

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

NEW QUESTION 100
- (Exam Topic 2)
Your company has an EC2 Instance that is hosted in an IAM VPC. There is a requirement to ensure that logs files from the EC2 Instance are stored accordingly. The access should also be limited for the destination of the log files. How can this be accomplished? Choose 2 answers from the options given below. Each answer forms part of the solution
Please select:

A. Stream the log files to a separate Cloudtrail trail
B. Stream the log files to a separate Cloudwatch Log group
C. Create an IAM policy that gives the desired level of access to the Cloudtrail trail
D. Create an IAM policy that gives the desired level of access to the Cloudwatch Log group

Answer: BD

Explanation:
You can create a Log group and send all logs from the EC2 Instance to that group. You can then limit the access to the Log groups via an IAM policy.
Option A is invalid because Cloudtrail is used to record API activity and not for storing log files Option C is invalid because Cloudtrail is the wrong service to be used for this requirement
For more information on Log Groups and Log Streams, please visit the following URL:
* https://docs.IAM.amazon.com/AmazonCloudWatch/latest/logs/Workinj
For more information on Access to Cloudwatch logs, please visit the following URL:
* https://docs.IAM.amazon.com/AmazonCloudWatch/latest/logs/auth-and-access-control-cwl.html
The correct answers are: Stream the log files to a separate Cloudwatch Log group. Create an IAM policy that gives the desired level of access to the Cloudwatch Log group
Submit your Feedback/Queries to our Experts

NEW QUESTION 102
- (Exam Topic 2)
You have an S3 bucket hosted in IAM. This is used to host promotional videos uploaded by yourself. You need to provide access to users for a limited duration of time. How can this be achieved?
Please select:

A. Use versioning and enable a timestamp for each version
B. Use Pre-signed URL's
C. Use IAM Roles with a timestamp to limit the access
D. Use IAM policies with a timestamp to limit the access

Answer: B

Explanation:
The IAM Documentation mentions the following
All objects by default are private. Only the object owner has permission to access these objects. However, the object owner can optionally share objects with others by creating a pre-signed URL using their own security credentials, to grant time-limited permission to download the objects.
Option A is invalid because this can be used to prevent accidental deletion of objects Option C is invalid because timestamps are not possible for Roles
Option D is invalid because policies is not the right way to limit access based on time For more information on pre-signed URL's, please visit the URL:
https://docs.IAM.ama2on.com/AmazonS3/latest/dev/ShareObiectPreSisnedURL.html
The correct answer is: Use Pre-signed URL's Submit your Feedback/Queries to our Experts

NEW QUESTION 104
- (Exam Topic 2)
Example.com hosts its internal document repository on Amazon EC2 instances. The application runs on EC2 instances and previously stored the documents on encrypted Amazon EBS volumes. To optimize the application for scale, example.com has moved the files to Amazon S3. The security team has mandated that all the files are securely deleted from the EBS volume, and it must certify that the data is unreadable before releasing the underlying disks.
Which of the following methods will ensure that the data is unreadable by anyone else?

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

Answer: D

Explanation:
Amazon EBS volumes are presented to you as raw unformatted block devices that have been wiped prior to being made available for use. Wiping occurs immediately before reuse so that you can be assured that the wipe process completed. If you have procedures requiring that all data be wiped via a specific

method, such as those detailed in NIST 800-88 (“Guidelines for Media Sanitization”), you have the ability to do so on Amazon EBS. You should conduct a specialized wipe procedure prior to deleting the volume for compliance with your established requirements.
https://d0.IAMstatic.com/whitepapers/IAM-security-whitepaper.pdf

NEW QUESTION 106
- (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 111
- (Exam Topic 2)
A Security Administrator is restricting the capabilities of company root user accounts. The company uses IAM Organizations and has enabled it for all feature sets, including consolidated billing. The top-level account is used for billing and administrative purposes, not for operational IAM resource purposes.
How can the Administrator restrict usage of member root user accounts across the organization?

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

Answer: C

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

NEW QUESTION 115
- (Exam Topic 2)
A company plans to move most of its IT infrastructure to IAM. They want to leverage their existing on-premises Active Directory as an identity provider for IAM.
Which combination of steps should a Security Engineer take to federate the company’s on-premises Active Directory with IAM? (Choose two.)

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

Answer: AD

Explanation:
https://IAM.amazon.com/blogs/security/how-to-establish-federated-access-to-your-IAM-resources-by-using-acti

NEW QUESTION 118
- (Exam Topic 2)
A Security Engineer is defining the logging solution for a newly developed product. Systems Administrators and Developers need to have appropriate access to event log files in IAM CloudTrail to support and troubleshoot the product.
Which combination of controls should be used to protect against tampering with and unauthorized access to log files? (Choose two.)

A. Ensure that the log file integrity validation mechanism is enabled.
B. Ensure that all log files are written to at least two separate Amazon S3 buckets in the same account.
C. Ensure that Systems Administrators and Developers can edit log files, but prevent any other access.
D. Ensure that Systems Administrators and Developers with job-related need-to-know requirements only are capable of viewing—but not modifying—the log files.
E. Ensure that all log files are stored on Amazon EC2 instances that allow SSH access from the internal corporate network only.

Answer: AD

NEW QUESTION 119
- (Exam Topic 2)
What is the function of the following IAM Key Management Service (KMS) key policy attached to a customer master key (CMK)?

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

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

A. The Amazon WorkMail and Amazon SES services have delegated KMS encrypt and decrypt permissions to the ExampleUser principal in the 111122223333 account.
B. The ExampleUser principal can transparently encrypt and decrypt email exchanges specifically between ExampleUser and IAM.
C. The CMK is to be used for encrypting and decrypting only when the principal is ExampleUser and the request comes from WorkMail or SES in the specified region.
D. The key policy allows WorkMail or SES to encrypt or decrypt on behalf of the user for any CMK in the account.

Answer: C

NEW QUESTION 121
- (Exam Topic 2)
The Security Engineer is given the following requirements for an application that is running on Amazon EC2 and managed by using IAM CloudFormation templates with EC2 Auto Scaling groups:
-Have the EC2 instances bootstrapped to connect to a backend database.
-Ensure that the database credentials are handled securely.
-Ensure that retrievals of database credentials are logged.
Which of the following is the MOST efficient way to meet these requirements?

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

Answer: B

NEW QUESTION 122
- (Exam Topic 2)
Which option for the use of the IAM Key Management Service (KMS) supports key management best practices that focus on minimizing the potential scope of data exposed by a possible future key compromise?

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

Answer: A

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

NEW QUESTION 127

- (Exam Topic 2)
A company has contracted with a third party to audit several IAM accounts. To enable the audit, cross-account IAM roles have been created in each account targeted for audit. The Auditor is having trouble accessing some of the accounts.
Which of the following may be causing this problem? (Choose three.)

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

Answer: ACF

Explanation:
Using IAM to grant access to a Third-Party Account 1) Create a role to provide access to the require resources 1.1) Create a role policy that specifies the IAM Account ID to be accessed, "sts:AssumeRole" as action, and "sts:ExternalID" as condition 1.2) Create a role using the role policy just created 1.3) Assign a resouce policy to the role. This will provide permission to access resource ARNs to the auditor 2) Repeat steps 1 and 2 on all IAM accounts 3) The auditor connects to the IAM account IAM Security Token Service (STS). The auditor must provide its ExternalID from step 1.2, the ARN of the role he is trying to assume from step 1.3, sts:ExternalID 4) STS provide the auditor with temporary credentials that provides the role access from step 1
https://docs.IAM.amazon.com/IAM/latest/UserGuide/id_roles_create_for-user_externalid.html
https://IAM.amazon.com/blogs/security/how-to-audit-cross-account-roles-using-IAM-cloudtrail-and-amazon-clo

NEW QUESTION 129
- (Exam Topic 2)
A Lambda function reads metadata from an S3 object and stores the metadata in a DynamoDB table. The function is triggered whenever an object is stored within the S3 bucket.
How should the Lambda function be given access to the DynamoDB table? Please select:

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

Answer: D

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

NEW QUESTION 133
- (Exam Topic 2)
A Security Engineer must add additional protection to a legacy web application by adding the following HTTP security headers:
-Content Security-Policy
-X-Frame-Options
-X-XSS-Protection
The Engineer does not have access to the source code of the legacy web application. Which of the following approaches would meet this requirement?

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

Answer: B

NEW QUESTION 138
- (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 141
- (Exam Topic 2)
You have enabled Cloudtrail logs for your company's IAM account. In addition, the IT Security department has mentioned that the logs need to be encrypted. How can this be achieved?
Please select:

A. Enable SSL certificates for the Cloudtrail logs
B. There is no need to do anything since the logs will already be encrypted
C. Enable Server side encryption for the trail
D. Enable Server side encryption for the destination S3 bucket

Answer: B

Explanation:
The IAM Documentation mentions the following.
By default CloudTrail event log files are encrypted using Amazon S3 server-side encryption (SSE). You can also choose to encryption your log files with an IAM Key Management Service (IAM KMS) key. You can store your log files in your bucket for as long as you want. You can also define Amazon S3 lifecycle rules to archive or delete log files automatically. If you want notifications about lo file delivery and validation, you can set up Amazon SNS notifications.
Option A.C and D are not valid since logs will already be encrypted
For more information on how Cloudtrail works, please visit the following URL: https://docs.IAM.amazon.com/IAMcloudtrail/latest/usereuide/how-cloudtrail-works.htmll
The correct answer is: There is no need to do anything since the logs will already be encrypted
Submit your Feedback/Queries to our Experts

NEW QUESTION 143
- (Exam Topic 2)
Your company has a set of resources defined in the IAM Cloud. Their IT audit department has requested to get a list of resources that have been defined across the account. How can this be achieved in the easiest manner?
Please select:

A. Create a powershell script using the IAM CL
B. Query for all resources with the tag of production.
C. Create a bash shell script with the IAM CL
D. Query for all resources in all region
E. Store the results in an S3 bucket.
F. Use Cloud Trail to get the list of all resources
G. Use IAM Config to get the list of all resources

Answer: D

Explanation:
The most feasible option is to use IAM Config. When you turn on IAM Config, you will get a list of resources defined in your IAM Account.
A sample snapshot of the resources dashboard in IAM Config is shown below C:\Users\wk\Desktop\mudassar\Untitled.jpg

Option A is incorrect because this would give the list of production based resources and now all resources Option B is partially correct But this will just add more maintenance overhead.
Option C is incorrect because this can be used to log API activities but not give an account of all resou For more information on IAM Config, please visit the below URL: https://docs.IAM.amazon.com/config/latest/developereuide/how-does-confie-work.html
The correct answer is: Use IAM Config to get the list of all resources
Submit your Feedback/Queries to our Experts

NEW QUESTION 148
- (Exam Topic 2)
A Security Engineer is trying to determine whether the encryption keys used in an IAM service are in compliance with certain regulatory standards.
Which of the following actions should the Engineer perform to get further guidance?

A. Read the IAM Customer Agreement.
B. Use IAM Artifact to access IAM compliance reports.
C. Post the question on the IAM Discussion Forums.
D. Run IAM Config and evaluate the configuration outputs.

Answer: B

Explanation:
https://IAM.amazon.com/artifact/
Third-party auditors assess the security and compliance of IAM Key Management Service as part of multiple IAM compliance programs. These include SOC, PCI, FedRAMP, HIPPA, and others. The compliance document is found in IAM Artifact.

NEW QUESTION 149
- (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 151
- (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 154
- (Exam Topic 2)
You are hosting a web site via website hosting on an S3 bucket - http://demo.s3-website-us-east-l
.a mazonIAM.com. You have some web pages that use Javascript that access resources in another bucket which has web site hosting also enabled. But when users access the web pages , they are getting a blocked Javascript error. How can you rectify this?
Please select:

A. Enable CORS for the bucket
B. Enable versioning for the bucket
C. Enable MFA for the bucket
D. Enable CRR for the bucket

Answer: A

Explanation:
Your answer is incorrect Answer-A
Such a scenario is also given in the IAM Documentation Cross-Origin Resource Sharing: Use-case Scenarios The following are example scenarios for using CORS:
• Scenario 1: Suppose that you are hosting a website in an Amazon S3 bucket named website as described in Hosting a Static Website on Amazon S3. Your users load the website endpoint http://website.s3-website-us-east-1.a mazonIAM.com. Now you want to use JavaScript on the webpages that are stored in this bucket to be able to make authenticated GET and PUT requests against the same bucket by using the Amazon S3 API endpoint for the bucket website.s3.amazonIAM.com. A browser would normally block JavaScript from allowing those requests, but with CORS you can configure your bucket to explicitly enable cross-origin requests from website.s3-website-us-east-1 .amazonIAM.com.
• Scenario 2: Suppose that you want to host a web font from your S3 bucket. Again, browsers require a CORS check (also called a preflight check) for loading web fonts. You would configure the bucket that is hosting the web font to allow any origin to make these requests.
Option Bis invalid because versioning is only to create multiple versions of an object and can help in accidental deletion of objects
Option C is invalid because this is used as an extra measure of caution for deletion of objects Option D is invalid because this is used for Cross region replication of objects
For more information on Cross Origin Resource sharing, please visit the following URL
• ittps://docs.IAM.amazon.com/AmazonS3/latest/dev/cors.html The correct answer is: Enable CORS for the bucket
Submit your Feedback/Queries to our Experts

NEW QUESTION 158
- (Exam Topic 2)
A Systems Engineer has been tasked with configuring outbound mail through Simple Email Service (SES) and requires compliance with current TLS standards.
The mail application should be configured to connect to which of the following endpoints and corresponding ports?

A. email.us-east-1.amazonIAM.com over port 8080
B. email-pop3.us-east-1.amazonIAM.com over port 995
C. email-smtp.us-east-1.amazonIAM.com over port 587
D. email-imap.us-east-1.amazonIAM.com over port 993

Answer: C

Explanation:
https://docs.IAM.amazon.com/ses/latest/DeveloperGuide/smtp-connect.html

NEW QUESTION 161
- (Exam Topic 2)
A Security Engineer who was reviewing IAM Key Management Service (IAM KMS) key policies found this statement in each key policy in the company IAM account.

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

What does the statement allow?

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

Answer: D

NEW QUESTION 164
- (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 168
- (Exam Topic 2)
Which of the following is used as a secure way to log into an EC2 Linux Instance? Please select:

A. IAM User name and password
B. Key pairs
C. IAM Access keys
D. IAM SDK keys

Answer: B

Explanation:
The IAM Documentation mentions the following
Key pairs consist of a public key and a private key. You use the private key to create a digital signature, and then IAM uses the corresponding public key to validate the signature. Key pairs are used only for Amazon EC2 and Amazon CloudFront.
Option A.C and D are all wrong because these are not used to log into EC2 Linux Instances For more information on IAM Security credentials, please visit the below URL: https://docs.IAM.amazon.com/eeneral/latest/er/IAM-sec-cred-types.html
The correct answer is: Key pairs
Submit your Feedback/Queries to our Experts

NEW QUESTION 173
- (Exam Topic 2)
You are designing a custom IAM policy that would allow uses to list buckets in S3 only if they are MFA authenticated. Which of the following would best match this requirement?

A. C:\Users\wk\Desktop\mudassar\Untitled.jpg

```
"Version": "2012-10-17",
"Statement": {
 "Effect": "Allow",
 "Action": [
     "s3:ListAllMyBuckets",
     "s3:GetBucketLocation"
  ],
 "Resource": "Resource": "arn:aws:s3:::*",
 "Condition": {
  "Bool": {"aws:MultiFactorAuthPresent": true}
 }
}
}
```

B. C:\Users\wk\Desktop\mudassar\Untitled.jpg

```
"Version": "2012-10-17",
"Statement": {
 "Effect": "Allow",
 "Action": [
     "s3:ListAllMyBuckets",
     "s3:GetBucketLocation"
  ],
 "Resource": "Resource": "arn:aws:s3:::*",
 "Condition": {
  "Bool": {"aws:MultiFactorAuthPresent":false}
 }
}
```

C. C:\Users\wk\Desktop\mudassar\Untitled.jpg

D. C:\Users\wk\Desktop\mudassar\Untitled.jpg

Answer: A

Explanation:
The Condition clause can be used to ensure users can only work with resources if they are MFA authenticated. Option B and C are wrong since the IAM:MultiFactorAuthPresent clause should be marked as true. Here you are saying that onl if the user has been MFA activated, that means it is true, then allow access.
Option D is invalid because the "boor clause is missing in the evaluation for the condition clause. Boolean conditions let you construct Condition elements that restrict access based on comparing a key to
"true" or "false."
Here in this scenario the boot attribute in the condition element will return a value True for option A which will ensure that access is allowed on S3 resources.
For more information on an example on such a policy, please visit the following URL:

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 179
- (Exam Topic 2)
An application has a requirement to be resilient across not only Availability Zones within the application's primary region but also be available within another region altogether.
Which of the following supports this requirement for IAM resources that are encrypted by IAM KMS?

A. Copy the application's IAM KMS CMK from the source region to the target region so that it can be used to decrypt the resource after it is copied to the target region.
B. Configure IAM KMS to automatically synchronize the CMK between regions so that it can be used to decrypt the resource in the target region.
C. Use IAM services that replicate data across regions, and re-wrap the data encryption key created in the source region by using the CMK in the target region so that the target region's CMK can decrypt the database encryption key.
D. Configure the target region's IAM service to communicate with the source region's IAM KMS so that it can decrypt the resource in the target region.

Answer: C

NEW QUESTION 180
- (Exam Topic 2)
A Security Engineer has created an Amazon CloudWatch event that invokes an IAM Lambda function daily. The Lambda function runs an Amazon Athena query that checks IAM CloudTrail logs in Amazon S3 to detect whether any IAM user accounts or credentials have been created in the past 30 days. The results of the

Athena query are created in the same S3 bucket. The Engineer runs a test execution of the Lambda function via the IAM Console, and the function runs successfully.
After several minutes, the Engineer finds that his Athena query has failed with the error message: “Insufficient Permissions”. The IAM permissions of the Security Engineer and the Lambda function are shown below:
Security Engineer

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:*",
                "iam:*",
                "lambda:*",
                "athena:Get*",
                "athena:List*",
                "cloudwatch:*"

            ],
            "Resource": "*"
        }
    ]
}
```

Lambda function execution role

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

What is causing the error?

A. The Lambda function does not have permissions to start the Athena query execution.
B. The Security Engineer does not have permissions to start the Athena query execution.
C. The Athena service does not support invocation through Lambda.
D. The Lambda function does not have permissions to access the CloudTrail S3 bucket.

Answer: D

NEW QUESTION 182
- (Exam Topic 2)
The InfoSec team has mandated that in the future only approved Amazon Machine Images (AMIs) can be used.
How can the InfoSec team ensure compliance with this mandate?

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

Answer: C

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

NEW QUESTION 184
- (Exam Topic 2)
You have just recently set up a web and database tier in a VPC and hosted the application. When testing the app , you are not able to reach the home page for the app. You have verified the security groups. What can help you diagnose the issue.
Please select:

A. Use the IAM Trusted Advisor to see what can be done.
B. Use VPC Flow logs to diagnose the traffic
C. Use IAM WAF to analyze the traffic
D. Use IAM Guard Duty to analyze the traffic

Answer: B

Explanation:
Option A is invalid because this can be used to check for security issues in your account, but not verify as to why you cannot reach the home page for your application
Option C is invalid because this used to protect your app against application layer attacks, but not verify as to why you cannot reach the home page for your application
Option D is invalid because this used to protect your instance against attacks, but not verify as to why you cannot reach the home page for your application
The IAM Documentation mentions the following
VPC Flow Logs capture network flow information for a VPC, subnet or network interface and stores it in Amazon CloudWatch Logs. Flow log data can help customers troubleshoot network issues; for example, to diagnose why specific traffic is not reaching an instance, which might be a result of overly restrictive security group rules. Customers can also use flow logs as a security toi to monitor the traffic that reaches their instances, to profile network traffic, and to look for abnormal traffic behaviors.
For more information on IAM Security, please visit the following URL: https://IAM.amazon.com/answers/networking/vpc-security-capabilities>
The correct answer is: Use VPC Flow logs to diagnose the traffic Submit your Feedback/Queries to our Experts

NEW QUESTION 185
- (Exam Topic 2)
IAM CloudTrail is being used to monitor API calls in an organization. An audit revealed that CloudTrail is failing to deliver events to Amazon S3 as expected.
What initial actions should be taken to allow delivery of CloudTrail events to S3? (Select two.)

A. Verify that the S3 bucket policy allow CloudTrail to write objects.
B. Verify that the IAM role used by CloudTrail has access to write to Amazon CloudWatch Logs.
C. Remove any lifecycle policies on the S3 bucket that are archiving objects to Amazon Glacier.
D. Verify that the S3 bucket defined in CloudTrail exists.
E. Verify that the log file prefix defined in CloudTrail exists in the S3 bucket.

Answer: BD

Explanation:
https://docs.IAM.amazon.com/IAMcloudtrail/latest/userguide/create-s3-bucket-policy-for-cloudtrail.html

NEW QUESTION 187
- (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 188
- (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 192
- (Exam Topic 2)
An organization is using IAM CloudTrail, Amazon CloudWatch Logs, and Amazon CloudWatch to send alerts when new access keys are created. However, the alerts are no longer appearing in the Security Operations mail box.
Which of the following actions would resolve this issue?

A. In CloudTrail, verify that the trail logging bucket has a log prefix configured.
B. In Amazon SNS, determine whether the “Account spend limit” has been reached for this alert.
C. In SNS, ensure that the subscription used by these alerts has not been deleted.
D. In CloudWatch, verify that the alarm threshold “consecutive periods” value is equal to, or greater than 1.

Answer: C

NEW QUESTION 196
- (Exam Topic 2)
A security team is responsible for reviewing IAM API call activity in the cloud environment for security violations. These events must be recorded and retained in a centralized location for both current and future IAM regions.
What is the SIMPLEST way to meet these requirements?

A. Enable IAM Trusted Advisor security checks in the IAM Console, and report all security incidents for all regions.
B. Enable IAM CloudTrail by creating individual trails for each region, and specify a single Amazon S3 bucket to receive log files for later analysis.
C. Enable IAM CloudTrail by creating a new trail and applying the trail to all region
D. Specify a single Amazon S3 bucket as the storage location.
E. Enable Amazon CloudWatch logging for all IAM services across all regions, and aggregate them to a single Amazon S3 bucket for later analysis.

Answer: C

Explanation:
https://docs.IAM.amazon.com/IAMcloudtrail/latest/userguide/creating-trail-organization.html

NEW QUESTION 200
- (Exam Topic 2)
Which of the following is not a best practice for carrying out a security audit? Please select:

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

Answer: A

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

NEW QUESTION 204
- (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 206
- (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 207
- (Exam Topic 2)
The Security team believes that a former employee may have gained unauthorized access to IAM resources sometime in the past 3 months by using an identified access key.
What approach would enable the Security team to find out what the former employee may have done within IAM?

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

Answer: A

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

NEW QUESTION 208
- (Exam Topic 2)
A company will store sensitive documents in three Amazon S3 buckets based on a data classification scheme of “Sensitive,” “Confidential,” and “Restricted.”
The security solution must meet all of the following
requirements:
- Each object must be encrypted using a unique key.
- Items that are stored in the “Restricted” bucket require two-factor authentication for decryption.
- IAM KMS must automatically rotate encryption keys annually.

Which of the following meets these requirements?

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

Answer: A

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

NEW QUESTION 211
- (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 215
- (Exam Topic 2)
You have a vendor that needs access to an IAM resource. You create an IAM user account. You want to restrict access to the resource using a policy for just that user over a brief period. Which of the following would be an ideal policy to use?
Please select:

A. An IAM Managed Policy
B. An Inline Policy

C. A Bucket Policy
D. A bucket ACL

Answer: B

Explanation:
The IAM Documentation gives an example on such a case
Inline policies are useful if you want to maintain a strict one-to-one relationship between a policy and the principal entity that if s applied to. For example, you want to be sure that the permissions in a policy are not inadvertently assigned to a principal entity other than the one they're intended for. When you use an inline policy, the permissions in the policy cannot be inadvertently attached to the wrong principal entity. In addition, when you use the IAM Management Console to delete that principal entit the policies embedded in the principal entity are deleted as well. That's because they are part of the principal entity.
Option A is invalid because IAM Managed Polices are ok for a group of users, but for individual users, inline policies are better.
Option C and D are invalid because they are specifically meant for access to S3 buckets For more information on policies, please visit the following URL:
https://docs.IAM.amazon.com/IAM/latest/UserGuide/access managed-vs-inline
The correct answer is: An Inline Policy Submit your Feedback/Queries to our Experts

NEW QUESTION 217
- (Exam Topic 3)
When managing permissions for the API gateway, what can be used to ensure that the right level of permissions are given to developers, IT admins and users? These permissions should be easily managed.
Please select:

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

Answer: B

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

NEW QUESTION 219
- (Exam Topic 3)
Your company has a set of EC2 Instances defined in IAM. They need to ensure that all traffic packets are monitored and inspected for any security threats. How can this be achieved? Choose 2 answers from the options given below
Please select:

A. Use a host based intrusion detection system
B. Use a third party firewall installed on a central EC2 instance
C. Use VPC Flow logs
D. Use Network Access control lists logging

Answer: AB

Explanation:
If you want to inspect the packets themselves, then you need to use custom based software A diagram representation of this is given in the IAM Security best practices
Option C is invalid because VPC Flow logs cannot conduct packet inspection. For more information on IAM Security best practices, please refer to below URL:
The correct answers are: Use a host based intrusion detection system. Use a third party firewall installed on a central EC2
Submit your Feedback/Queries to our Experts

NEW QUESTION 223
- (Exam Topic 3)
A company is planning on extending their on-premise IAM Infrastructure to the IAM Cloud. They need to have a solution that would give core benefits of traffic encryption and ensure latency is kept to a minimum. Which of the following would help fulfil this requirement? Choose 2 answers from the options given below
Please select:

A. IAM VPN
B. IAM VPC Peering
C. IAM NAT gateways
D. IAM Direct Connect

Answer: AD

Explanation:
The IAM Document mention the following which supports the requirement Option B is invalid because VPC peering is only used for connection between VPCs and cannot be used to connect On-premise infrastructure to the IAM Cloud.
Option C is invalid because NAT gateways is used to connect instances in a private subnet to the internet For more information on VPN Connections, please visit the following url
https://docs.IAM.amazon.com/AmazonVPC/latest/UserGuideA/pn-connections.html

The correct answers are: IAM VPN, IAM Direct Connect Submit your Feedback/Queries to our Experts

NEW QUESTION 228
- (Exam Topic 3)
Your company has the following setup in IAM
* a. A set of EC2 Instances hosting a web application
* b. An application load balancer placed in front of the EC2 Instances
There seems to be a set of malicious requests coming from a set of IP addresses. Which of the following can be used to protect against these requests?
Please select:

A. Use Security Groups to block the IP addresses
B. Use VPC Flow Logs to block the IP addresses
C. Use IAM inspector to block the IP addresses
D. Use IAM WAF to block the IP addresses

Answer: D

Explanation:
Your answer is incorrect Answer -D
The IAM Documentation mentions the following on IAM WAF which can be used to protect Application Load Balancers and Cloud front
A web access control list (web ACL) gives you fine-grained control over the web requests that your Amazon CloudFront distributions or Application Load Balancers respond to. You can allow or block the following types of requests:
Originate from an IP address or a range of IP addresses Originate from a specific country or countries
Contain a specified string or match a regular expression (regex) pattern in a particular part of requests Exceed a specified length
Appear to contain malicious SQL code (known as SQL injection) Appear to contain malicious scripts (known as cross-site scripting)
Option A is invalid because by default Security Groups have the Deny policy
Options B and C are invalid because these services cannot be used to block IP addresses For information on IAM WAF, please visit the below URL:
https://docs.IAM.amazon.com/waf/latest/developerguide/web-acl.html
The correct answer is: Use IAM WAF to block the IP addresses Submit your Feedback/Queries to our Experts

NEW QUESTION 229
- (Exam Topic 3)
An employee keeps terminating EC2 instances on the production environment. You've determined the best way to ensure this doesn't happen is to add an extra layer of defense against terminating the instances. What is the best method to ensure the employee does not terminate the production instances? Choose the 2 correct answers from the options below
Please select:

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

Answer: AB

Explanation:
Tags enable you to categorize your IAM resources in different ways, for example, by purpose, owner, or environment. This is useful when you have many resources of the same type — you can quickly identify a specific resource based on the tags you've assigned to it. Each tag consists of a key and an optional value, both of which you define
Options C&D are incorrect because it will not ensure that the employee cannot terminate the instance. For more information on tagging answer resources please refer to the below URL:
http://docs.IAM.amazon.com/IAMEC2/latest/UserGuide/Usins_Tags.htmll
The correct answers are: Tag the instance with a production-identifying tag and add resource-level permissions to the employe user with an explicit deny on the terminate API call to instances with the production tag.. Tag the instance with a production-identifying tag and modify the employees group to allow only start stop, and reboot API calls and not the terminate instance
Submit your Feedback/Queries to our Experts

NEW QUESTION 233
- (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 237
- (Exam Topic 3)
Your company has an EC2 Instance hosted in IAM. This EC2 Instance hosts an application. Currently this application is experiencing a number of issues. You need to inspect the network packets to see what the type of error that is occurring? Which one of the below steps can help address this issue?
Please select:

A. Use the VPC Flow Logs.
B. Use a network monitoring tool provided by an IAM partner.
C. Use another instanc
D. Setup a port to "promiscuous mode" and sniff the traffic to analyze the packet
E. Use Cloudwatch metric

Answer: B

NEW QUESTION 239
- (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 240
- (Exam Topic 3)
A company hosts data in S3. There is now a mandate that going forward all data in the S3 bucket needs to encrypt at rest. How can this be achieved?
Please select:

A. Use IAM Access keys to encrypt the data
B. Use SSL certificates to encrypt the data
C. Enable server side encryption on the S3 bucket
D. Enable MFA on the S3 bucket

Answer: C

Explanation:
The IAM Documentation mentions the following
Server-side encryption is about data encryption at rest—that is, Amazon S3 encrypts your data at the object level as it writes it to disks in its data centers and decrypts it for you when you access it. As long as you authenticate your request and you have access permissions, there is no difference in the way you access encrypted or unencrypted objects.
Options A and B are invalid because neither Access Keys nor SSL certificates can be used to encrypt data. Option D is invalid because MFA is just used as an extra level of security for S3 buckets
For more information on S3 server side encryption, please refer to the below Link: https://docs.IAM.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html
Submit your Feedback/Queries to our Experts

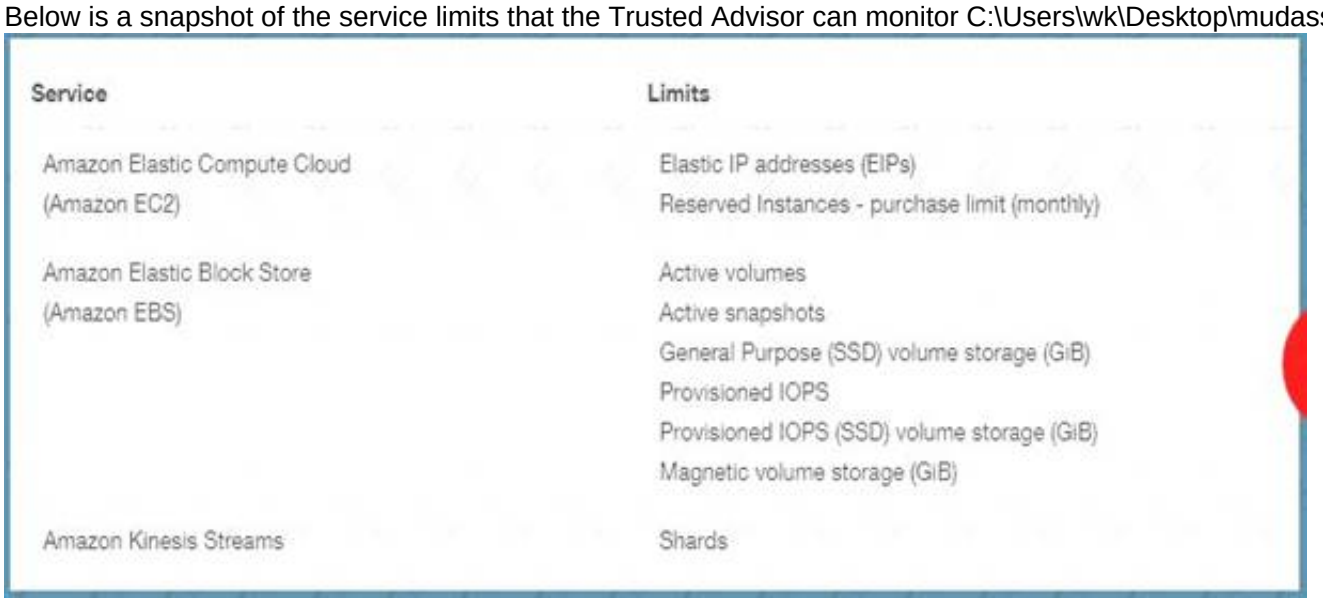
NEW QUESTION 241
- (Exam Topic 3)
You want to ensure that you keep a check on the Active EBS Volumes, Active snapshots and Elastic IP addresses you use so that you don't go beyond the service limit. Which of the below services can help in this regard?
Please select:

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



Service	Limits
Amazon Elastic Compute Cloud (Amazon EC2)	Elastic IP addresses (EIPs)
	Reserved Instances - purchase limit (monthly)
Amazon Elastic Block Store (Amazon EBS)	Active volumes
	Active snapshots
	General Purpose (SSD) volume storage (GiB)
	Provisioned IOPS
	Provisioned IOPS (SSD) volume storage (GiB)
	Magnetic volume storage (GiB)
Amazon Kinesis Streams	Shards

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 243
- (Exam Topic 3)
An application running on EC2 instances in a VPC must call an external web service via TLS (port 443). The instances run in public subnets.
Which configurations below allow the application to function and minimize the exposure of the instances? Select 2 answers from the options given below
Please select:

A. A network ACL with a rule that allows outgoing traffic on port 443.
B. A network ACL with rules that allow outgoing traffic on port 443 and incoming traffic on ephemeral ports
C. A network ACL with rules that allow outgoing traffic on port 443 and incoming traffic on port 443.
D. A security group with a rule that allows outgoing traffic on port 443
E. A security group with rules that allow outgoing traffic on port 443 and incoming traffic on ephemeral ports.
F. A security group with rules that allow outgoing traffic on port 443 and incoming traffic on port 443.

Answer: BD

Explanation:
Since here the traffic needs to flow outbound from the Instance to a web service on Port 443, the outbound rules on both the Network and Security Groups need to allow outbound traffic. The Incoming traffic should be allowed on ephermal ports for the Operating System on the Instance to allow a connection to be established on any desired or available port.
Option A is invalid because this rule alone is not enough. You also need to ensure incoming traffic on ephemeral ports
Option C is invalid because need to ensure incoming traffic on ephemeral ports and not only port 443 Option E and F are invalid since here you are allowing additional ports on Security groups which are not
required
For more information on VPC Security Groups, please visit the below URL:
https://docs.IAM.amazon.com/AmazonVPC/latest/UserGuideA/PC_SecurityGroups.htmll
The correct answers are: A network ACL with rules that allow outgoing traffic on port 443 and incoming traffic on ephemeral ports, A security group with a rule that allows outgoing traffic on port 443
Submit your Feedback/Queries to our Experts

NEW QUESTION 248
- (Exam Topic 3)
You need to ensure that the cloudtrail logs which are being delivered in your IAM account is encrypted. How can this be achieved in the easiest way possible?
Please select:

A. Don't do anything since CloudTrail logs are automatically encrypted.
B. Enable S3-SSE for the underlying bucket which receives the log files
C. Enable S3-KMS for the underlying bucket which receives the log files
D. Enable KMS encryption for the logs which are sent to Cloudwatch

Answer: A

Explanation:
The IAM Documentation mentions the following
By default the log files delivered by CloudTrail to your bucket are encrypted by Amazon server-side encryption with Amazon S3-managed encryption keys (SSE-S3)
Option B,C and D are all invalid because by default all logs are encrypted when they sent by Cloudtrail to S3 buckets
For more information on IAM Cloudtrail log encryption, please visit the following URL: https://docs.IAM.amazon.com/IAMcloudtrail/latest/usereuide/encryptine-cloudtrail-loe-files-with-IAM-kms.htm The correct answer is: Don't do anything since CloudTrail logs are automatically encrypted. Submit your Feedback/Queries to our Experts

NEW QUESTION 249

- (Exam Topic 3)
One of the EC2 Instances in your company has been compromised. What steps would you take to ensure that you could apply digital forensics on the Instance. Select 2 answers from the options given below
Please select:

A. Remove the role applied to the Ec2 Instance
B. Create a separate forensic instance
C. Ensure that the security groups only allow communication to this forensic instance
D. Terminate the instance

Answer: BC

Explanation:
Option A is invalid because removing the role will not help completely in such a situation
Option D is invalid because terminating the instance means that you cannot conduct forensic analysis on the instance
One way to isolate an affected EC2 instance for investigation is to place it in a Security Group that only the forensic investigators can access. Close all ports except to receive inbound SSH or RDP traffic from one single IP address from which the investigators can safely examine the instance.
For more information on security scenarios for your EC2 Instance, please refer to below URL: https://d1.IAMstatic.com/Marketplace/scenarios/security/SEC 11 TSB Final.pd1
The correct answers are: Create a separate forensic instance. Ensure that the security groups only allow communication to this forensic instance
Submit your Feedback/Queries to our Experts

NEW QUESTION 254
- (Exam Topic 3)
You are working for a company and been allocated the task for ensuring that there is a federated authentication mechanism setup between IAM and their On-premise Active Directory. Which of the following are important steps that need to be covered in this process? Choose 2 answers from the options given below.
Please select:

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

Answer: AD

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

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

NEW QUESTION 259
- (Exam Topic 3)
Your company has many IAM accounts defined and all are managed via IAM Organizations. One IAM account has a S3 bucket that has critical data. How can we ensure that all the users in the IAM organisation have access to this bucket?
Please select:

A. Ensure the bucket policy has a condition which involves IAM:PrincipalOrgID
B. Ensure the bucket policy has a condition which involves IAM:AccountNumber
C. Ensure the bucket policy has a condition which involves IAM:PrincipaliD
D. Ensure the bucket policy has a condition which involves IAM:OrgID

Answer: A

Explanation:
The IAM Documentation mentions the following

IAM Identity and Access Management (IAM) now makes it easier for you to control access to your IAM resources by using the IAM organization of IAM principals (users and roles). For some services, you grant permissions using resource-based policies to specify the accounts and principals that can access the resource and what actions they can perform on it. Now, you can use a new condition key, IAM:PrincipalOrgID, in these policies to require all principals accessing the resource to be from an account in the organization
Option B.C and D are invalid because the condition in the bucket policy has to mention IAM:PrincipalOrgID For more information on controlling access via Organizations, please refer to the below Link:
https://IAM.amazon.com/blogs/security/control-access-to-IAM-resources-by-usins-the-IAM-organization-of-iam (
The correct answer is: Ensure the bucket policy has a condition which involves IAM:PrincipalOrgID Submit your Feedback/Queries to our Experts

NEW QUESTION 262
- (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 CloudTrail 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 265
- (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 267
.....

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