Amazon-Web-Services

Exam Questions SCS-C02

AWS Certified Security - Specialty

NEW QUESTION 1
- (Exam Topic 1)
A Security Engineer has several thousand Amazon EC2 instances split across production and development environments. Each instance is tagged with its environment. The Engineer needs to analyze and patch all the development EC2 instances to ensure they are not currently exposed to any common vulnerabilities or exposures (CVEs)
Which combination of steps is the MOST efficient way for the Engineer to meet these requirements? (Select TWO.)

A. Log on to each EC2 instance, check and export the different software versions installed, and verify this against a list of current CVEs.
B. Install the Amazon Inspector agent on all development instances Build a custom rule package, and configure Inspector to perform a scan using this custom rule on all instances tagged as being in the development environment.
C. Install the Amazon Inspector agent on all development instances Configure Inspector to perform a scan using the CVE rule package on all instances tagged as being in the development environment.
D. Install the Amazon EC2 System Manager agent on all development instances Issue the Run command to EC2 System Manager to update all instances
E. Use IAM Trusted Advisor to check that all EC2 instances have been patched to the most recent version of operating system and installed software.

Answer: CD

NEW QUESTION 2
- (Exam Topic 1)
A Developer reported that IAM CloudTrail was disabled on their account. A Security Engineer investigated the account and discovered the event was undetected by the current security solution. The Security Engineer must recommend a solution that will detect future changes to the CloudTrail configuration and send alerts when changes occur.
What should the Security Engineer do to meet these requirements?

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

Answer: B

NEW QUESTION 3
- (Exam Topic 1)
A company has a serverless application for internal users deployed on IAM. The application uses IAM Lambda for the front end and for business logic. The Lambda function accesses an Amazon RDS database inside a VPC The company uses IAM Systems Manager Parameter Store for storing database credentials.
A recent security review highlighted the following issues
> The Lambda function has internet access.
> The relational database is publicly accessible.
> The database credentials are not stored in an encrypted state.
Which combination of steps should the company take to resolve these security issues? (Select THREE)

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

Answer: ABE

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

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

Answer: D

NEW QUESTION 5
- (Exam Topic 1)
A company has a website with an Amazon CloudFront HTTPS distribution, an Application Load Balancer (ALB) with multiple web instances for dynamic website content, and an Amazon S3 bucket for static website content. The company's security engineer recently updated the website security requirements:
• HTTPS needs to be enforced for all data in transit with specific ciphers.
• The CloudFront distribution needs to be accessible from the internet only. Which solution will meet these requirements?

A. Set up an S3 bucket policy with the IAMsecuretransport key Configure the CloudFront origin access identity (OAI) with the S3 bucket Configure CloudFront to use specific cipher
B. Enforce the ALB with an HTTPS listener only and select the appropriate security policy for the ciphers Link the ALB with IAM WAF to allow access from the CloudFront IP ranges.
C. Set up an S3 bucket policy with the IAM:securetransport ke
D. Configure the CloudFront origin access identity (OAI) with the S3 bucke
E. Enforce the ALB with an HTTPS listener only and select the appropriate security policy for the ciphers.
F. Modify the CloudFront distribution to use IAM WA
G. Force HTTPS on the S3 bucket with specific ciphers in the bucket polic
H. Configure an HTTPS listener only for the AL
I. Set up a security group to limit access to the ALB from the CloudFront IP ranges
J. Modify the CloudFront distribution to use the ALB as the origi
K. Enforce an HTTPS listener on the AL
L. Create a path-based routing rule on the ALB with proxies that connect lo Amazon S3. Create a bucket policy to allow access from these proxies only.

Answer: A

Explanation:
https://IAM.amazon.com/blogs/security/automatically-update-IAM-waf-ip-sets-with-IAM-ip-ranges/ to update CF ip range.

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

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

Answer: DE

NEW QUESTION 8
- (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 9
- (Exam Topic 1)
A security engineer is designing a solution that will provide end-to-end encryption between clients and Docker containers running In Amazon Elastic Container Service (Amazon ECS). This solution will also handle volatile traffic patterns

Which solution would have the MOST scalability and LOWEST latency?

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

Answer: A

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

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

Answer: C

NEW QUESTION 10
- (Exam Topic 1)
A company'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 12
- (Exam Topic 1)
A company wants to encrypt the private network between its orvpremises environment and IAM. The company also wants a consistent network experience for its employees.
What should the company do to meet these requirements?

A. Establish an IAM Direct Connect connection with IAM and set up a Direct Connect gatewa
B. In the Direct Connect gateway configuration, enable IPsec and BGP, and then leverage native IAM network encryption between Availability Zones and Regions,
C. Establish an IAM Direct Connect connection with IAM and set up a Direct Connect gatewa
D. Using the Direct Connect gateway, create a private virtual interface and advertise the customer gateway private IP addresse
E. Create a VPN connection using the customer gateway and the virtual private gateway
F. Establish a VPN connection with the IAM virtual private cloud over the internet
G. Establish an IAM Direct Connect connection with IAM and establish a public virtual interfac
H. For prefixes that need to be advertised, enter the customer gateway public IP addresse
I. Create a VPN connection over Direct Connect using the customer gateway and the virtual private gateway.

Answer: D

NEW QUESTION 15
- (Exam Topic 1)
A global company must mitigate and respond to DDoS attacks at Layers 3, 4 and 7 All of the company's IAM applications are serverless with static content hosted on Amazon S3 using Amazon CloudFront and Amazon Route 53
Which solution will meet these requirements?

A. Use IAM WAF with an upgrade to the IAM Business support plan
B. Use IAM Certificate Manager with an Application Load Balancer configured with an origin access identity
C. Use IAM Shield Advanced
D. Use IAM WAF to protect IAM Lambda functions encrypted with IAM KMS and a NACL restricting all Ingress traffic

Answer: C

NEW QUESTION 20
- (Exam Topic 1)

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

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

Answer: BCE

NEW QUESTION 24
- (Exam Topic 1)
A Security Engineer is looking for a way to control access to data that is being encrypted under a CMK. The Engineer is also looking to use additional authenticated data (AAD) to prevent tampering with ciphertext.
Which action would provide the required functionality?

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

Answer: C

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

NEW QUESTION 26
- (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 28
- (Exam Topic 1)
A security engineer is asked to update an AW3 CoudTrail log file prefix for an existing trail. When attempting to save the change in the CloudTrail console, the security engineer receives the following error message. "There is a problem with the bucket policy''
What will enable the security engineer to saw the change?

A. Create a new trail with the updated log file prefix, and then delete the original nail Update the existing bucket policy in the Amazon S3 console with the new log the prefix, and then update the log file prefix in the CloudTrail console
B. Update the existing bucket policy in the Amazon S3 console to allow the security engineers principal to perform PutBucketPolic
C. and then update the log file prefix in the CloudTrail console
D. Update the existing bucket policy in the Amazon S3 console with the new log file prefix, and then update the log file prefix in the CloudTrail console.
E. Update the existing bucket policy in the Amazon S3 console to allow the security engineers principal to perform GetBucketPolicy, and then update the log file prefix in the CloudTrail console

Answer: C

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

NEW QUESTION 32
- (Exam Topic 1)
A company Is trying to replace its on-premises bastion hosts used to access on-premises Linux servers with IAM Systems Manager Session Manager. A security engineer has installed the Systems Manager Agent on all servers. The security engineer verifies that the agent is running on all the servers, but Session Manager cannot connect to them. The security engineer needs to perform verification steps before Session Manager will work on the servers.
Which combination of steps should the security engineer perform? (Select THREE.)

A. Open inbound port 22 to 0 0.0.0/0 on all Linux servers.
B. Enable the advanced-instances tier in Systems Manager.
C. Create a managed-instance activation for the on-premises servers.
D. Reconfigure the Systems Manager Agent with the activation code and ID.
E. Assign an IAM role to all of the on-premises servers.
F. Initiate an inventory collection with Systems Manager on the on-premises servers

Answer: CEF

NEW QUESTION 34
- (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 36
- (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 38
- (Exam Topic 1)
A company is designing the securely architecture (or a global latency-sensitive web application it plans to deploy to IAM. A Security Engineer needs to configure a highly available and secure two-tier architecture. The security design must include controls to prevent common attacks such as DDoS, cross-site scripting, and SQL injection.
Which solution meets these requirements?

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

Answer: A

NEW QUESTION 39
- (Exam Topic 1)
A Security Engineer has launched multiple Amazon EC2 instances from a private AMI using an IAM CloudFormation template. The Engineer notices instances terminating right after they are launched.
What could be causing these terminations?

A. The IAM user launching those instances is missing ec2:Runinstances permission.

B. The AMI used as encrypted and the IAM does not have the required IAM KMS permissions.
C. The instance profile used with the EC2 instances in unable to query instance metadata.
D. IAM currently does not have sufficient capacity in the Region.

Answer: B

Explanation:
https://docs.IAM.amazon.com/IAMEC2/latest/UserGuide/troubleshooting-launch.html

NEW QUESTION 43
- (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 45
- (Exam Topic 1)
A company's information security team want to do near-real-time anomaly detection on Amazon EC2 performance and usage statistics. Log aggregation is the responsibility of a security engineer. To do the study, the Engineer needs gather logs from all of the company's IAM accounts in a single place.
How should the Security Engineer go about doing this?

A. Log in to each account four times a day and filter the IAM CloudTrail log data, then copy and paste the logs in to the Amazon S3 bucket in the destination account.
B. Set up Amazon CloudWatch to stream data to an Amazon S3 bucket in each source accoun
C. Set up bucket replication for each source account into a centralized bucket owned by the Security Engineer.
D. Set up an IAM Config aggregator to collect IAM configuration data from multiple sources.
E. Set up Amazon CloudWatch cross-account log data sharing with subscriptions in each accoun
F. Send the logs to Amazon Kinesis Data Firehose in the Security Engineer's account.

Answer: D

Explanation:
Read the prerequisites in the question carefully. The solution must support "near real time" analysis of the log data. Cloudwatch doesn't stream logs to S3; it supports exporting them to S3 with an up to 12 hour expected delay:
https://docs.IAM.amazon.com/AmazonCloudWatch/latest/logs/S3Export.html
"Log data can take up to 12 hours to become available for export. For near real-time analysis of log data, see Analyzing log data with CloudWatch Logs Insights or Real-time processing of log data with subscriptions instead."
https://docs.IAM.amazon.com/AmazonCloudWatch/latest/logs/Subscriptions.html
"You can use subscriptions to get access to a real-time feed of log events from CloudWatch Logs and have it delivered to other services such as an Amazon Kinesis stream, an Amazon Kinesis Data Firehose stream, or IAM Lambda for custom processing, analysis, or loading to other systems. When log events are sent to the receiving service, they are Base64 encoded and compressed with the gzip format."
https://docs.IAM.amazon.com/AmazonCloudWatch/latest/logs/CrossAccountSubscriptions.html

NEW QUESTION 46
- (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 49
- (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 52
- (Exam Topic 1)
A security engineer has noticed an unusually high amount of traffic coming from a single IP address. This was discovered by analyzing the Application Load Balancer's access logs. How can the security engineer limit the number of requests from a specific IP address without blocking the IP address?

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

Answer: C

NEW QUESTION 54
- (Exam Topic 1)
A convoys data lake uses Amazon S3 and Amazon Athena. The company's security engineer has been asked to design an encryption solution that meets the company's data protection requirements. The encryption solution must work with Amazon S3 and keys managed by the company. The encryption solution must be protected in a hardware security module that is validated id Federal information Processing Standards (FPS) 140-2 Level 3.
Which solution meets these requirements?

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

Answer: B

NEW QUESTION 55
- (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 59
- (Exam Topic 1)
A company has several production IAM accounts and a central security IAM account. The security account is used for centralized monitoring and has IAM privileges to all resources in every corporate account. All of the company's Amazon S3 buckets are tagged with a value denoting the data classification of their contents.
A Security Engineer is deploying a monitoring solution in the security account that will enforce bucket policy compliance. The system must monitor S3 buckets in all production accounts and confirm that any policy change is in accordance with the bucket's data classification. If any change is out of compliance; the Security team must be notified quickly.
Which combination of actions would build the required solution? (Choose three.)

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

Answer: DEF

NEW QUESTION 60
- (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 63
- (Exam Topic 1)
An employee accidentally exposed an IAM access key and secret access key during a public presentation. The company Security Engineer immediately disabled the key.
How can the Engineer assess the impact of the key exposure and ensure that the credentials were not misused? (Choose two.)

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

Answer: AD

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

NEW QUESTION 66
- (Exam Topic 1)
A company's security information events management (SIEM) tool receives new IAM CloudTrail logs from an Amazon S3 bucket that is configured to send all object created event notification to an Amazon SNS topic An Amazon SQS queue is subscribed to this SNS topic. The company's SEM tool then ports this SQS queue for new messages using an IAM role and fetches new log events from the S3 bucket based on the SQS messages.
After a recent security review that resulted m restricted permissions, the SEM tool has stopped receiving new CloudTral logs
Which of the following are possible causes of this issue? (Select THREE)

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

Answer: ADF

NEW QUESTION 71
- (Exam Topic 1)
An IAM account administrator created an IAM group and applied the following managed policy to require that each individual user authenticate using multi-factor authentication:

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

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

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

Answer: B

NEW QUESTION 76
- (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 81
- (Exam Topic 1)
A company plans to use custom AMIs to launch Amazon EC2 instances across multiple IAM accounts in a single Region to perform security monitoring and analytics tasks. The EC2 instances are launched in EC2 Auto Scaling groups. To increase the security of the solution, a Security Engineer will manage the lifecycle of the custom AMIs in a centralized account and will encrypt them with a centrally managed IAM KMS CMK. The Security Engineer configured the KMS key policy to allow cross-account access. However, the EC2 instances are still not being properly launched by the EC2 Auto Scaling groups.
Which combination of configuration steps should the Security Engineer take to ensure the EC2 Auto Scaling groups have been granted the proper permissions to execute tasks?

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

Answer: B

NEW QUESTION 84
- (Exam Topic 1)

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

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

Answer: A

Explanation:
https://docs.IAM.amazon.com/securityhub/latest/userguide/securityhub-standards-cis-config-resources.html

NEW QUESTION 85
- (Exam Topic 1)
A financial institution has the following security requirements:
⮞ Cloud-based users must be contained in a separate authentication domain.
⮞ Cloud-based users cannot access on-premises systems.
As part of standing up a cloud environment, the financial institution is creating a number of Amazon managed databases and Amazon EC2 instances. An Active Directory service exists on-premises that has all the administrator accounts, and these must be able to access the databases and instances.
How would the organization manage its resources in the MOST secure manner? (Choose two.)

A. Configure an IAM Managed Microsoft AD to manage the cloud resources.
B. Configure an additional on-premises Active Directory service to manage the cloud resources.
C. Establish a one-way trust relationship from the existing Active Directory to the new Active Directory service.
D. Establish a one-way trust relationship from the new Active Directory to the existing Active Directoryservice.
E. Establish a two-way trust between the new and existing Active Directory services.

Answer: AD

Explanation:
Deploy a new forest/domain on IAM with one-way trust. If you are planning on leveraging credentials from an on-premises AD on IAM member servers, you must establish at least a one-way trust to the Active Directory running on IAM. In this model, the IAM domain becomes the resource domain where computer objects are located and on-premises domain becomes the account domain. Ref: https://d1.IAMstatic.com/whitepapers/adds-on-IAM.pdf
https://docs.IAM.amazon.com/directoryservice/latest/admin-guide/directory_microsoft_ad.html

NEW QUESTION 89
- (Exam Topic 2)
The Security Engineer created a new IAM Key Management Service (IAM KMS) key with the following key policy:

```
{
    "Effect": "Allow",
    "Principal": {"AWS": "arn:aws:iam::111122223333:root"),
    "Action": "kms:*";
    "Resource": "*"
}
```

What are the effects of the key policy? (Choose two.)

A. The policy allows access for the IAM account 111122223333 to manage key access though IAM policies.
B. The policy allows all IAM users in account 111122223333 to have full access to the KMS key.
C. The policy allows the root user in account 111122223333 to have full access to the KMS key.
D. The policy allows the KMS service-linked role in account 111122223333 to have full access to the KMS key.
E. The policy allows all IAM roles in account 111122223333 to have full access to the KMS key.

Answer: AC

Explanation:
Giving the IAM account full access to the CMK does this; it enables you to use IAM policies to give IAM users and roles in the account access to the CMK. It does not by itself give any IAM users or roles access to the CMK, but it enables you to use IAM policies to do so.
https://docs.IAM.amazon.com/kms/latest/developerguide/key-policies.html#key-policy-default-allow-root-enabl

NEW QUESTION 90
- (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 93
- (Exam Topic 2)
A company plans to migrate a sensitive dataset to Amazon S3. A Security Engineer must ensure that the data is encrypted at rest. The encryption solution must enable the company to generate its own keys without needing to manage key storage or the encryption process.
What should the Security Engineer use to accomplish this?

A. Server-side encryption with Amazon S3-managed keys (SSE-S3)
B. Server-side encryption with IAM KMS-managed keys (SSE-KMS)
C. Server-side encryption with customer-provided keys (SSE-C)
D. Client-side encryption with an IAM KMS-managed CMK

Answer: B

Explanation:
Reference https://IAM.amazon.com/s3/faqs/

NEW QUESTION 96
- (Exam Topic 2)
You have an instance setup in a test environment in IAM. You installed the required application and the promoted the server to a production environment. Your IT Security team has advised that there maybe traffic flowing in from an unknown IP address to port 22. How can this be mitigated immediately?
Please select:

A. Shutdown the instance
B. Remove the rule for incoming traffic on port 22 for the Security Group
C. Change the AMI for the instance
D. Change the Instance type for the instance

Answer: B

Explanation:
In the test environment the security groups might have been opened to all IP addresses for testing purpose. Always to ensure to remove this rule once all testing is completed.
Option A, C and D are all invalid because this would affect the application running on the server. The easiest way is just to remove the rule for access on port 22.
For more information on authorizing access to an instance, please visit the below URL: https://docs.IAM.amazon.com/IAMEC2/latest/UserGuide/authorizing-access-to-an-instance.htmll
The correct answer is: Remove the rule for incoming traffic on port 22 for the Security Group Submit your Feedback/Queries to our Experts

NEW QUESTION 99
- (Exam Topic 2)
In response to the past DDoS attack experiences, a Security Engineer has set up an Amazon CloudFront distribution for an Amazon S3 bucket. There is concern that some users may bypass the CloudFront distribution and access the S3 bucket directly.
What must be done to prevent users from accessing the S3 objects directly by using URLs?

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

Answer: B

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

NEW QUESTION 101
- (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 105
- (Exam Topic 2)
A security team must present a daily briefing to the CISO that includes a report of which of the company's thousands of EC2 instances and on-premises servers are missing the latest security patches. All instances/servers must be brought into compliance within 24 hours so they do not show up on the next day's report.
How can the security team fulfill these requirements?
Please select:

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

Answer: B

Explanation:
Use the Systems Manger Patch Manger to generate the report and also install the missing patches The IAM Documentation mentions the following
IAM Systems Manager Patch Manager automates the process of patching managed instances with
security-related updates. For Linux-based instances, you can also install patches for non-security updates. You can patch fleets of Amazon EC2 instances or your on-premises servers and virtual machines (VMs) by operating system type. This includes supported versions of Windows, Ubuntu Server, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), and Amazon Linux. You can scan instances to see only a report of missing patches, or you can scan and automatically install all missing patches.
Option A is invalid because Amazon QuickSight and Cloud Trail cannot be used to generate the list of servers that don't meet compliance needs.
Option C is wrong because deploying instances via new AMI'S would impact the applications hosted on these servers
Option D is invalid because Amazon Trusted Advisor cannot be used to generate the list of servers that don't meet compliance needs.
For more information on the IAM Patch Manager, please visit the below URL: https://docs.IAM.amazon.com/systems-manager/latest/userguide/systems-manager-patch.html (
The correct answer is: Use Systems Manger Patch Manger to generate the report of out of compliance instances/ servers. Use Systems Manager Patch Manger to install the missing patches.
Submit your Feedback/Queries to our Experts

NEW QUESTION 106
- (Exam Topic 2)
An organization operates a web application that serves users globally. The application runs on Amazon EC2 instances behind an Application Load Balancer. There is an Amazon CloudFront distribution in front of the load balancer, and the organization uses IAM WAF. The application is currently experiencing a volumetric attack whereby the attacker is exploiting a bug in a popular mobile game.
The application is being flooded with HTTP requests from all over the world with the User-Agent set to the following string: Mozilla/5.0 (compatible; ExampleCorp; ExampleGame/1.22; Mobile/1.0)
What mitigation can be applied to block attacks resulting from this bug while continuing to service legitimate requests?

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

Answer: A

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

NEW QUESTION 109
- (Exam Topic 2)
For compliance reasons, an organization limits the use of resources to three specific IAM regions. It wants to be alerted when any resources are launched in unapproved regions.
Which of the following approaches will provide alerts on any resources launched in an unapproved region?

A. Develop an alerting mechanism based on processing IAM CloudTrail logs.
B. Monitor Amazon S3 Event Notifications for objects stored in buckets in unapproved regions.
C. Analyze Amazon CloudWatch Logs for activities in unapproved regions.
D. Use IAM Trusted Advisor to alert on all resources being created.

Answer: A

Explanation:
https://stackoverflow.com/questions/45449053/cloudwatch-alert-on-any-instance-creation

NEW QUESTION 111
- (Exam Topic 2)
A company is using CloudTrail to log all IAM API activity for all regions in all of its accounts. The CISO has asked that additional steps be taken to protect the integrity of the log files.
What combination of steps will protect the log files from intentional or unintentional alteration? Choose 2 answers from the options given below
Please select:

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

Answer: AC

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

NEW QUESTION 114
- (Exam Topic 2)
What are the MOST secure ways to protect the IAM account root user of a recently opened IAM account? (Choose two.)

A. Use the IAM account root user access keys instead of the IAM Management Console
B. Enable multi-factor authentication for the IAM IAM users with the AdministratorAccess managed policy attached to them
C. Enable multi-factor authentication for the IAM account root user
D. Use IAM KMS to encrypt all IAM account root user and IAM IAM access keys and set automatic rotation to 30 days
E. Do not create access keys for the IAM account root user; instead, create IAM IAM users

Answer: CE

NEW QUESTION 119
- (Exam Topic 2)
A company has multiple VPCs in their account that are peered, as shown in the diagram. A Security Engineer wants to perform penetration tests of the Amazon EC2 instances in all three VPCs.
How can this be accomplished? (Choose two.)

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

Answer: BD

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

NEW QUESTION 120
- (Exam Topic 2)
A company's security policy requires that VPC Flow Logs are enabled on all VPCs. A Security Engineer is looking to automate the process of auditing the VPC resources for compliance.
What combination of actions should the Engineer take? (Choose two.)

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

Answer: AE

Explanation:

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

NEW QUESTION 121
- (Exam Topic 2)
An IAM user with fill EC2 permissions could bot start an Amazon EC2 instance after it was stopped for a maintenance task. Upon starting the instance, the instance state would change to "Pending", but after a few seconds, it would switch back to "Stopped".
An inspection revealed that the instance has attached Amazon EBS volumes that were encrypted by using a Customer Master Key (CMK). When these encrypted volumes were detached, the IAM user was able to start the EC2 instances.
The IAM user policy is as follows:

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

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

A. kms:GenerateDataKey
B. kms:Decrypt
C. kms:CreateGrant
D. "Condition": {"Bool": {"kms:ViaService": "ec2.us-west-2.amazonIAM.com"}}
E. "Condition": {"Bool": {"kms:GrantIsForIAMResource": true}}

Answer: CE

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

NEW QUESTION 124
- (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 128
- (Exam Topic 2)
A company wants to have a secure way of generating, storing and managing cryptographic exclusive access for the keys. Which of the following can be used for this purpose?
Please select:

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

Answer: D

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

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

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

Answer: A

NEW QUESTION 132
- (Exam Topic 2)
A Software Engineer wrote a customized reporting service that will run on a fleet of Amazon EC2 instances. The company security policy states that application logs for the reporting service must be centrally collected.
What is the MOST efficient way to meet these requirements?

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

Answer: D

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

NEW QUESTION 137
- (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
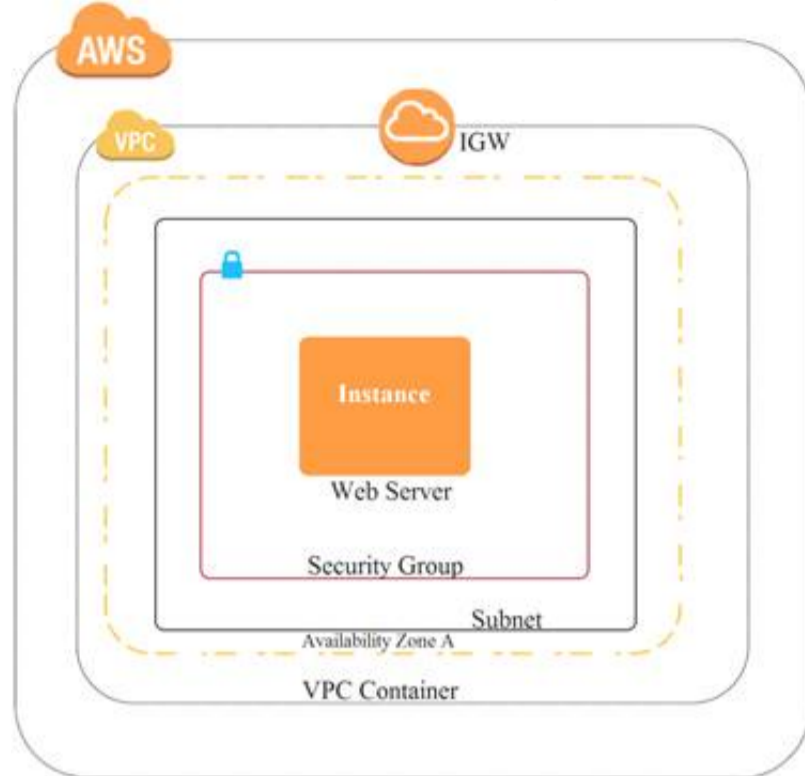Submit your Feedback/Queries to our Experts

NEW QUESTION 138
- (Exam Topic 2)
A company recently experienced a DDoS attack that prevented its web server from serving content. The website is static and hosts only HTML, CSS, and PDF files that users download.
Based on the architecture shown in the image, what is the BEST way to protect the site against future attacks while minimizing the ongoing operational overhead?

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

Answer: D

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

NEW QUESTION 143
- (Exam Topic 2)
A company has a forensic logging use case whereby several hundred applications running on Docker on EC2 need to send logs to a central location. The Security Engineer must create a logging solution that is able to perform real-time analytics on the log files, grants the ability to replay events, and persists data.
Which IAM Services, together, can satisfy this use case? (Select two.)

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

Answer: AB

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

NEW QUESTION 144
- (Exam Topic 2)
Your company has mandated that all calls to the IAM KMS service be recorded. How can this be achieved? Please select:

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

Answer: B

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

Jubmit your Feedback/Queries to our Experts

NEW QUESTION 149
- (Exam Topic 2)
A corporate cloud security policy states that communications between the company's VPC and KMS must travel entirely within the IAM network and not use public service endpoints.
Which combination of the following actions MOST satisfies this requirement? (Choose two.)

A. Add the IAM:sourceVpce condition to the IAM KMS key policy referencing the company's VPC endpoint ID.
B. Remove the VPC internet gateway from the VPC and add a virtual private gateway to the VPC to prevent direct, public internet connectivity.
C. Create a VPC endpoint for IAM KMS with private DNS enabled.
D. Use the KMS Import Key feature to securely transfer the IAM KMS key over a VPN.
E. Add the following condition to the IAM KMS key policy: "IAM:SourceIp": "10.0.0.0/16".

Answer: AC

Explanation:

An IAM policy can deny access to KMS except through your VPC endpoint with the following condition statement:
"Condition": { "StringNotEquals": {
"IAM:sourceVpce": "vpce-0295a3caf8414c94a"
}
}
If you select the Enable Private DNS Name option, the standard IAM KMS DNS hostname (https://kms.<region>.amazonIAM.com) resolves to your VPC endpoint.

NEW QUESTION 150
- (Exam Topic 2)
Due to new compliance requirements, a Security Engineer must enable encryption with customer-provided keys on corporate data that is stored in DynamoDB.
The company wants to retain full control of the encryption keys.
Which DynamoDB feature should the Engineer use to achieve compliance'?

A. Use IAM Certificate Manager to request a certificat
B. Use that certificate to encrypt data prior to uploading it to DynamoDB.
C. Enable S3 server-side encryption with the customer-provided key
D. Upload the data to Amazon S3, and then use S3Copy to move all data to DynamoDB
E. Create a KMS master ke
F. Generate per-record data keys and use them to encrypt data prior to uploading it to DynamoD
G. Dispose of the cleartext and encrypted data keys after encryption without storing.
H. Use the DynamoDB Java encryption client to encrypt data prior to uploading it to DynamoDB.

Answer: D

Explanation:
Follow the link:
https://docs.IAM.amazon.com/dynamodb-encryption-client/latest/devguide/what-is-ddb-encrypt.html

NEW QUESTION 152
- (Exam Topic 2)
You have an Ec2 Instance in a private subnet which needs to access the KMS service. Which of the following methods can help fulfil this requirement, keeping security in perspective
Please select:

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

Answer: A

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

NEW QUESTION 157
- (Exam Topic 2)
You are hosting a web site via website hosting on an S3 bucket - http://demo.s3-website-us-east-I
.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 162
- (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 163
- (Exam Topic 2)
A company has five IAM accounts and wants to use IAM CloudTrail to log API calls. The log files must be stored in an Amazon S3 bucket that resides in a new account specifically built for centralized services with a unique top-level prefix for each trail. The configuration must also enable detection of any modification to the logs.
Which of the following steps will implement these requirements? (Choose three.)

A. Create a new S3 bucket in a separate IAM account for centralized storage of CloudTrail logs, and enable "Log File Validation" on all trails.
B. Use an existing S3 bucket in one of the accounts, apply a bucket policy to the new centralized S3 bucket that permits the CloudTrail service to use the "s3: PutObject" action and the "s3 GetBucketACL" action, and specify the appropriate resource ARNs for the CloudTrail trails.
C. Apply a bucket policy to the new centralized S3 bucket that permits the CloudTrail service to use the "s3 PutObject" action and the "s3 GelBucketACL" action, and specify the appropriate resource ARNs for the CloudTrail trails.
D. Use unique log file prefixes for trails in each IAM account.
E. Configure CloudTrail in the centralized account to log all accounts to the new centralized S3 bucket.
F. Enable encryption of the log files by using IAM Key Management Service

Answer: ACE

Explanation:
https://docs.IAM.amazon.com/IAMcloudtrail/latest/userguide/best-practices-security.html
If you have created an organization in IAM Organizations, you can create a trail that will log all events for all IAM accounts in that organization. This is sometimes referred to as an organization trail. You can also choose to edit an existing trail in the master account and apply it to an organization, making it an organization trail. Organization trails log events for the master account and all member accounts in the organization. For more information about IAM Organizations, see Organizations Terminology and Concepts. Note Reference: https://docs.IAM.amazon.com/IAMcloudtrail/latest/userguide/creating-trail-organization.html You must be logged in with the master account for the organization in order to create an organization trail. You must also have sufficient permissions for the IAM user or role in the master account in order to successfully create an organization trail. If you do not have sufficient permissions, you will not see the option to apply a trail to an organization.

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

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

Answer: A

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

NEW QUESTION 172
- (Exam Topic 2)
A security alert has been raised for an Amazon EC2 instance in a customer account that is exhibiting strange behavior. The Security Engineer must first isolate the EC2 instance and then use tools for further investigation.
What should the Security Engineer use to isolate and research this event? (Choose three.)

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

Answer: ADF

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

NEW QUESTION 174
- (Exam Topic 2)
An IAM Lambda function was misused to alter data, and a Security Engineer must identify who invoked the function and what output was produced. The Engineer cannot find any logs created by the Lambda function in Amazon CloudWatch Logs.
Which of the following explains why the logs are not available?

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

Answer: A

NEW QUESTION 179
- (Exam Topic 2)
A water utility company uses a number of Amazon EC2 instances to manage updates to a fleet of 2,000 Internet of Things (IoT) field devices that monitor water quality. These devices each have unique access credentials.
An operational safety policy requires that access to specific credentials is independently auditable. What is the MOST cost-effective way to manage the storage of credentials?

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

Answer: A

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

NEW QUESTION 180
- (Exam Topic 2)
A company runs an application on IAM that needs to be accessed only by employees. Most employees work from the office, but others work remotely or travel.
How can the Security Engineer protect this workload so that only employees can access it?

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

Answer: C

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

NEW QUESTION 183
- (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 188
- (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 190
- (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 191
- (Exam Topic 2)
Your development team has started using IAM resources for development purposes. The IAM account has just been created. Your IT Security team is worried about possible leakage of IAM keys. What is the first level of measure that should be taken to protect the IAM account.
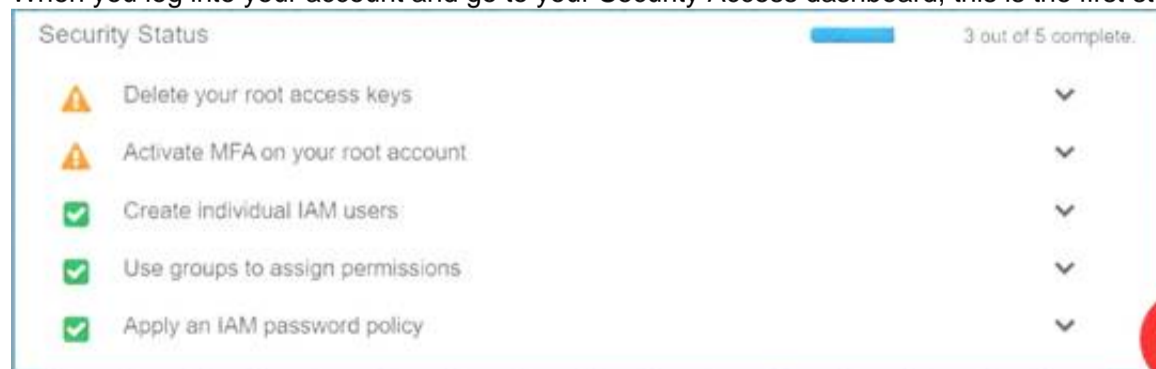Please select:

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

Answer: A

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

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

NEW QUESTION 194
- (Exam Topic 2)
A Development team has asked for help configuring the IAM roles and policies in a new IAM account. The team using the account expects to have hundreds of master keys and therefore does not want to manage access control for customer master keys (CMKs).
Which of the following will allow the team to manage IAM KMS permissions in IAM without the complexity of editing individual key policies?

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

Answer: B

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

NEW QUESTION 196
- (Exam Topic 2)
A company wants to have an Intrusion detection system available for their VPC in IAM. They want to have complete control over the system. Which of the following would be ideal to implement?
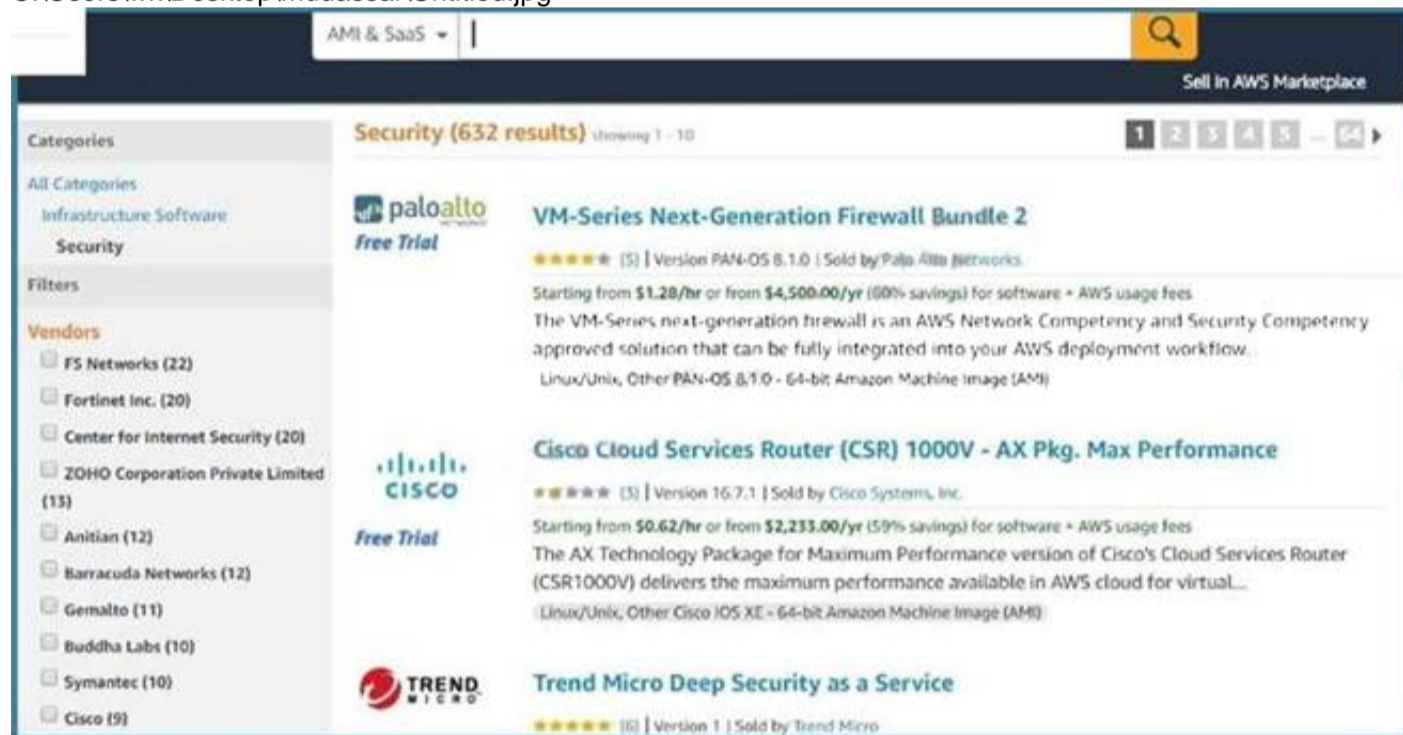Please select:

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

Answer: B

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

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

NEW QUESTION 199
- (Exam Topic 2)
A Security Engineer is working with the development team to design a supply chain application that stores sensitive inventory data in an Amazon S3 bucket. The application will use an IAM KMS customer master key (CMK) to encrypt the data on Amazon S3. The inventory data on Amazon S3 will be shared of vendors. All vendors will use IAM principals from their own IAM accounts to access the data on Amazon S3. The vendor list may change weekly, and the solution must support cross-account access.
What is the MOST efficient way to manage access control for the KMS CMK7?

A. Use KMS grants to manage key acces
B. Programmatically create and revoke grants to manage vendor access.
C. Use an IAM role to manage key acces
D. Programmatically update the IAM role policies to manage vendor access.
E. Use KMS key policies to manage key acces
F. Programmatically update the KMS key policies to manage vendor access.
G. Use delegated access across IAM accounts by using IAM roles to manage key acces
H. Programmatically update the IAM trust policy to manage cross-account vendor access.

Answer: A

NEW QUESTION 200
- (Exam Topic 2)
A company uses identity federation to authenticate users into an identity account (987654321987) where the users assume an IAM role named IdentityRole. The users then assume an IAM role named JobFunctionRole in the target IAM account (123456789123) to perform their job functions.
A user is unable to assume the IAM role in the target account. The policy attached to the role in the identity account is:

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

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

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

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

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

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

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

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

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

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

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

Answer: A

NEW QUESTION 203
- (Exam Topic 2)
The Security Engineer is managing a web application that processes highly sensitive personal information. The application runs on Amazon EC2. The application has strict compliance requirements, which instruct that all incoming traffic to the application is protected from common web exploits and that all outgoing traffic from the EC2 instances is restricted to specific whitelisted URLs.
Which architecture should the Security Engineer use to meet these requirements?

A. Use IAM Shield to scan inbound traffic for web exploit
B. Use VPC Flow Logs and IAM Lambda to restrict egress traffic to specific whitelisted URLs.
C. Use IAM Shield to scan inbound traffic for web exploit
D. Use a third-party IAM Marketplace solution to restrict egress traffic to specific whitelisted URLs.
E. Use IAM WAF to scan inbound traffic for web exploit
F. Use VPC Flow Logs and IAM Lambda to restrict egress traffic to specific whitelisted URLs.
G. Use IAM WAF to scan inbound traffic for web exploit
H. Use a third-party IAM Marketplace solution to restrict egress traffic to specific whitelisted URLs.

Answer: D

Explanation:
IAM Shield is mainly for DDos Attacks.IAM WAF is mainly for some other types of attacks like Injection and XSS etcIn this scenario, It seems it is WAF functionality that is needed.VPC logs do show the source and destination IP and Port , they never show any URL .. because URL are level 7 while VPC are concerned about lover network levels.
https://docs.IAM.amazon.com/vpc/latest/userguide/flow-logs.html

NEW QUESTION 207
- (Exam Topic 2)
Your company has a requirement to monitor all root user activity by notification. How can this best be achieved? Choose 2 answers from the options given below.
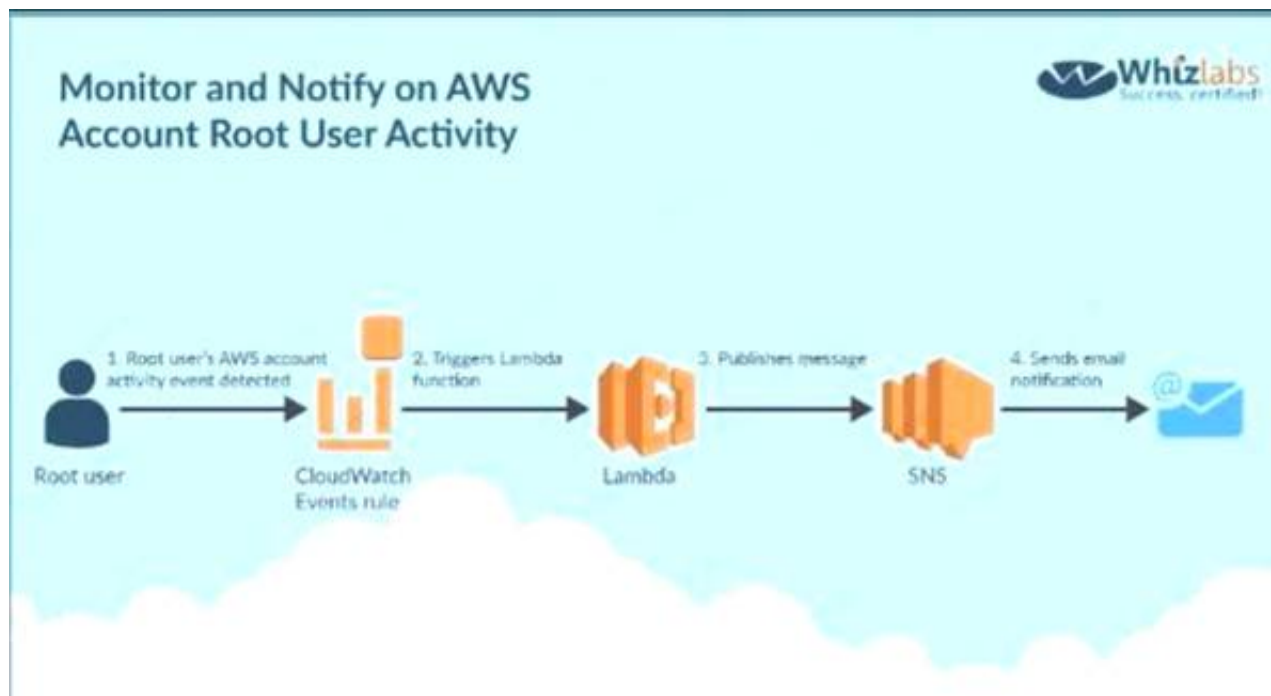Each answer forms part of the solution
Please select:

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

Answer: AC

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

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

NEW QUESTION 210
- (Exam Topic 2)
Your IT Security team has advised to carry out a penetration test on the resources in their company's IAM Account. This is as part of their capability to analyze the security of the Infrastructure. What should be done first in this regard?
Please select:

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

Answer: C

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

NEW QUESTION 211
- (Exam Topic 2)
Compliance requirements state that all communications between company on-premises hosts and EC2 instances be encrypted in transit. Hosts use custom proprietary protocols for their communication, and EC2 instances need to be fronted by a load balancer for increased availability.
Which of the following solutions will meet these requirements?

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

Answer: B

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

NEW QUESTION 214
- (Exam Topic 2)
An organization receives an alert that indicates that an EC2 instance behind an ELB Classic Load Balancer has been compromised.
What techniques will limit lateral movement and allow evidence gathering?

A. Remove the instance from the load balancer and terminate it.
B. Remove the instance from the load balancer, and shut down access to the instance by tightening the security group.
C. Reboot the instance and check for any Amazon CloudWatch alarms.

D. Stop the instance and make a snapshot of the root EBS volume.

Answer: B

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

NEW QUESTION 216
- (Exam Topic 2)
A company requires that IP packet data be inspected for invalid or malicious content. Which of the following approaches achieve this requirement? (Choose two.)

A. Configure a proxy solution on Amazon EC2 and route all outbound VPC traffic through i
B. Perform inspection within proxy software on the EC2 instance.
C. Configure the host-based agent on each EC2 instance within the VP
D. Perform inspection within the host-based agent.
E. Enable VPC Flow Logs for all subnets in the VP
F. Perform inspection from the Flow Log data within Amazon CloudWatch Logs.
G. Configure Elastic Load Balancing (ELB) access log
H. Perform inspection from the log data within the ELB access log files.
I. Configure the CloudWatch Logs agent on each EC2 instance within the VP
J. Perform inspection from the log data within CloudWatch Logs.

Answer: AB

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

NEW QUESTION 221
- (Exam Topic 2)
A pharmaceutical company has digitized versions of historical prescriptions stored on premises. The company would like to move these prescriptions to IAM and perform analytics on the data in them. Any operation with this data requires that the data be encrypted in transit and at rest.
Which application flow would meet the data protection requirements on IAM?

A. Digitized files -> Amazon Kinesis Data Analytics
B. Digitized files -> Amazon Kinesis Data Firehose -> Amazon S3 -> Amazon Athena
C. Digitized files -> Amazon Kinesis Data Streams -> Kinesis Client Library consumer -> Amazon S3 -> Athena
D. Digitized files -> Amazon Kinesis Data Firehose -> Amazon Elasticsearch

Answer: A

Explanation:
(Amazon Kinesis Data Analytics is the easiest way to analyze streaming data, also provide encryption at rest and in-transit)
-https://docs.IAM.amazon.com/kinesisanalytics/latest/dev/data-protection.html

NEW QUESTION 222
- (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 225
- (Exam Topic 2)
A Systems Engineer is troubleshooting the connectivity of a test environment that includes a virtual security appliance deployed inline. In addition to using the virtual security appliance, the Development team wants to use security groups and network ACLs to accomplish various security requirements in the environment.
What configuration is necessary to allow the virtual security appliance to route the traffic?

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

Answer: C

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

NEW QUESTION 228

- (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 230
- (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 232
- (Exam Topic 3)
Your company makes use of S3 buckets for storing data. There is a company policy that all services should have logging enabled. How can you ensure that logging is always enabled for created S3 buckets in the IAM Account?
Please select:

A. Use IAM Inspector to inspect all S3 buckets and enable logging for those where it is not enabled
B. Use IAM Config Rules to check whether logging is enabled for buckets
C. Use IAM Cloudwatch metrics to check whether logging is enabled for buckets
D. Use IAM Cloudwatch logs to check whether logging is enabled for buckets

Answer: B

Explanation:
This is given in the IAM Documentation as an example rule in IAM Config Example rules with triggers Example rule with configuration change trigger
* 1. You add the IAM Config managed rule, S3_BUCKET_LOGGING_ENABLED, to your account to check whether your Amazon S3 buckets have logging enabled.
* 2. The trigger type for the rule is configuration changes. IAM Config runs the evaluations for the rule when an Amazon S3 bucket is created, changed, or deleted.
* 3. When a bucket is updated, the configuration change triggers the rule and IAM Config evaluates whether the bucket is compliant against the rule.
Option A is invalid because IAM Inspector cannot be used to scan all buckets
Option C and D are invalid because Cloudwatch cannot be used to check for logging enablement for buckets. For more information on Config Rules please see the below Link:
➤ https://docs.IAM.amazon.com/config/latest/developerguide/evaluate-config-rules.html
The correct answer is: Use IAM Config Rules to check whether logging is enabled for buckets Submit your Feedback/Queries to our Experts

NEW QUESTION 233
- (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 236
- (Exam Topic 3)
There is a set of Ec2 Instances in a private subnet. The application hosted on these EC2 Instances need to access a DynamoDB table. It needs to be ensured that traffic does not flow out to the internet. How can this be achieved?
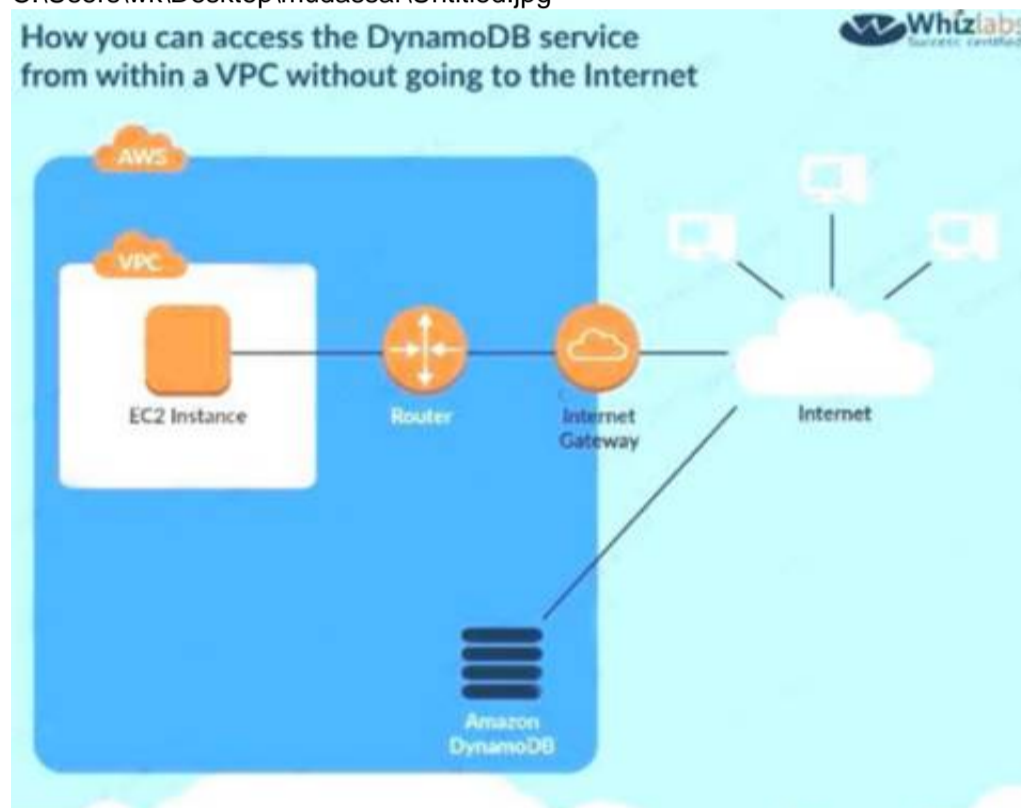Please select:

A. Use a VPC endpoint to the DynamoDB table
B. Use a VPN connection from the VPC
C. Use a VPC gateway from the VPC
D. Use a VPC Peering connection to the DynamoDB table

Answer: A

Explanation:
The following diagram from the IAM Documentation shows how you can access the DynamoDB service from within a V without going to the Internet This can be done with the help of a VPC endpoint
C:\Users\wk\Desktop\mudassar\Untitled.jpg

Option B is invalid because this is used for connection between an on-premise solution and IAM Option C is invalid because there is no such option
Option D is invalid because this is used to connect 2 VPCs
For more information on VPC endpointsfor DynamoDB, please visit the URL:
The correct answer is: Use a VPC endpoint to the DynamoDB table Submit your Feedback/Queries to our Experts

NEW QUESTION 237
- (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 241
- (Exam Topic 3)
You need to have a requirement to store objects in an S3 bucket with a key that is automatically managed and rotated. Which of the following can be used for this purpose?
Please select:

A. IAM KMS
B. IAM S3 Server side encryption
C. IAM Customer Keys
D. IAM Cloud HSM

Answer: B

Explanation:
The IAM Documentation mentions the following
Server-side encryption protects data at rest. Server-side encryption with Amazon S3-managed encryption keys (SSE-S3) uses strong multi-factor encryption. Amazon S3 encrypts each object with a unique key. As an additional safeguard, it encrypts the key itself with a master key that it rotates regularly. Amazon S3 server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt your data.
All other options are invalid since here you need to ensure the keys are manually rotated since you manage the entire key set Using IAM S3 Server side encryption, IAM will manage the rotation of keys automatically.
For more information on Server side encryption, please visit the following URL:
https://docs.IAM.amazon.com/AmazonS3/latest/dev/UsineServerSideEncryption.html
The correct answer is: IAM S3 Server side encryption Submit your Feedback/Queries to our Experts

NEW QUESTION 245
- (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.html
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 247
- (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.html
The correct answer is: Use IAM KMS Customer Default master key Submit your Feedback/Queries to our Experts

NEW QUESTION 249
- (Exam Topic 3)
Your company is planning on developing an application in IAM. This is a web based application. The application user will use their facebook or google identities for

authentication. You want to have the ability to manage user profiles without having to add extra coding to manage this. Which of the below would assist in this.
Please select:

A. Create an OIDC identity provider in IAM
B. Create a SAML provider in IAM
C. Use IAM Cognito to manage the user profiles
D. Use IAM users to manage the user profiles

Answer: C

Explanation:
The IAM Documentation mentions the following
A user pool is a user directory in Amazon Cognito. With a user pool, your users can sign in to your web or mobile app through Amazon Cognito. Your users can also sign in through social identity providers like Facebook or Amazon, and through SAML identity providers. Whether your users sign in directly or through a third party, all members of the user pool have a directory profile that you can access through an SDK.
User pools provide:
Sign-up and sign-in services.
A built-in, customizable web UI to sign in users.
Social sign-in with Facebook, Google, and Login with Amazon, as well as sign-in with SAML identity providers from your user
pool.
User directory management and user profiles.
Security features such as multi-factor authentication (MFA), checks for compromised credentials, account takeover protection, and phone and email verification.
Customized workflows and user migration through IAM Lambda triggers. Options A and B are invalid because these are not used to manage users Option D is invalid because this would be a maintenance overhead
For more information on Cognito User Identity pools, please refer to the below Link: https://docs.IAM.amazon.com/coenito/latest/developerguide/cognito-user-identity-pools.html
The correct answer is: Use IAM Cognito to manage the user profiles Submit your Feedback/Queries to our Experts

NEW QUESTION 252
- (Exam Topic 3)
You are planning on using the IAM KMS service for managing keys for your application. For which of the following can the KMS CMK keys be used for encrypting? Choose 2 answers from the options given below
Please select:

A. Image Objects
B. Large files
C. Password
D. RSA Keys

Answer: CD

Explanation:
The CMK keys themselves can only be used for encrypting data that is maximum 4KB in size. Hence it can be used for encryptii information such as passwords and RSA keys.
Option A and B are invalid because the actual CMK key can only be used to encrypt small amounts of data and not large amoui of data. You have to generate the data key from the CMK key in order to encrypt high amounts of data
For more information on the concepts for KMS, please visit the following URL: https://docs.IAM.amazon.com/kms/latest/developereuide/concepts.htmll
The correct answers are: Password, RSA Keys Submit your Feedback/Queries to our Experts

NEW QUESTION 256
- (Exam Topic 3)
You need to establish a secure backup and archiving solution for your company, using IAM. Documents should be immediately accessible for three months and available for five years for compliance reasons. Which IAM service fulfills these requirements in the most cost-effective way? Choose the correct Answer
Please select:

A. Upload data to S3 and use lifecycle policies to move the data into Glacier for long-term archiving.
B. Upload the data on EBS, use lifecycle policies to move EBS snapshots into S3 and later into Glacier for long-term archiving.
C. Use Direct Connect to upload data to S3 and use IAM policies to move the data into Glacier for long-term archiving.
D. Use Storage Gateway to store data to S3 and use lifecycle policies to move the data into Redshift for long-term archiving.

Answer: A

Explanation:
amazon Glacier is a secure, durable, and extremely low-cost cloud storage service for data archiving and long-term backup. Customers can reliably store large or small amounts of data for as little as $0,004 per gigabyte per month, a significant savings compared to on-premises solutions.
With Amazon lifecycle policies you can create transition actions in which you define when objects transition to another Amazon S3 storage class. For example, you may choose to transition objects to the STANDARDJA (IA, for infrequent access) storage class 30 days after creation, or archive objects to the GLACIER storage class one year after creation.
Option B is invalid because lifecycle policies are not available for EBS volumes Option C is invalid because IAM policies cannot be used to move data to Glacier
Option D is invalid because lifecycle policies is not used to move data to Redshif For more information on S3 lifecycle policies, please visit the URL:
http://docs.IAM.amazon.com/AmazonS3/latest/dev/obiect-lifecycle-mgmt.html
The correct answer is: Upload data to S3 and use lifecycle policies to move the data into Glacier for long-term archiving.
Submit your Feedback/Queries to our Experts

NEW QUESTION 259
......

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

SCS-C02 Practice Exam Features:

* SCS-C02 Questions and Answers Updated Frequently

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

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

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

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