Amazon-Web-Services

Exam Questions SCS-C02

AWS Certified Security - Specialty

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

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

Answer: CD

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

NEW QUESTION 2
- (Exam Topic 1)
An application is currently secured using network access control lists and security groups. Web servers are located in public subnets behind an Application Load Balancer (ALB); application servers are located in private subnets.
How can edge security be enhanced to safeguard the Amazon EC2 instances against attack? (Choose two.)

A. Configure the application's EC2 instances to use NAT gateways for all inbound traffic.
B. Move the web servers to private subnets without public IP addresses.
C. Configure IAM WAF to provide DDoS attack protection for the ALB.
D. Require all inbound network traffic to route through a bastion host in the private subnet.
E. Require all inbound and outbound network traffic to route through an IAM Direct Connect connection.

Answer: BC

NEW QUESTION 3
- (Exam Topic 1)
A company has multiple IAM accounts that are part of IAM Organizations. The company's Security team wants to ensure that even those Administrators with full access to the company's IAM accounts are unable to access the company's Amazon S3 buckets
How should this be accomplished?

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

Answer: A

NEW QUESTION 4
- (Exam Topic 1)
A security engineer has created an Amazon Cognito user pool. The engineer needs to manually verify the ID and access token sent by the application for troubleshooting purposes
What is the MOST secure way to accomplish this?

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

Answer: A

NEW QUESTION 5
- (Exam Topic 1)
A Developer is building a serverless application that uses Amazon API Gateway as the front end. The application will not be publicly accessible. Other legacy applications running on Amazon EC2 will make calls to the application A Security Engineer Has been asked to review the security controls for authentication and authorization of the application
Which combination of actions would provide the MOST secure solution? (Select TWO)

A. Configure an IAM policy that allows the least permissive actions to communicate with the API Gateway Attach the policy to the role used by the legacy EC2 instances

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

Answer: AE

NEW QUESTION 6
- (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 7
- (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 8
- (Exam Topic 1)
An external Auditor finds that a company's user passwords have no minimum length. The company is currently using two identity providers:
• IAM IAM federated with on-premises Active Directory
• Amazon Cognito user pools to accessing an IAM Cloud application developed by the company Which combination o1 actions should the Security Engineer take to solve this issue? (Select TWO.)

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

Answer: AD

NEW QUESTION 9
- (Exam Topic 1)
A company Is building a data lake on Amazon S3. The data consists of millions of small files containing sensitive information. The security team has the following requirements for the architecture:
• Data must be encrypted in transit.
• Data must be encrypted at rest.
• The bucket must be private, but if the bucket is accidentally made public, the data must remain confidential. Which combination of steps would meet the requirements? (Select THREE.)

A. Enable AES-256 encryption using server-side encryption with Amazon S3-managed encryption keys (SSE-S3) on the S3 bucket
B. Enable default encryption with server-side encryption with IAM KMS-managed keys (SSE-KMS) on the S3 bucket.
C. Add a bucket policy that includes a deny if a PutObject request does not include IAMiSecureTcanspoct.
D. Add a bucket policy with ws: Sourcelpto Allow uploads and downloads from the corporate intranet only.

E. Add a bucket policy that includes a deny if a PutObject request does not include s3:x-amz-sairv9r-side-enctyption: "IAM: kms".
F. Enable Amazon Macie to monitor and act on changes to the data lake's S3 bucket.

Answer: BDF

NEW QUESTION 10
- (Exam Topic 1)
A company had one of its Amazon EC2 key pairs compromised. A Security Engineer must identify which current Linux EC2 instances were deployed and used the compromised key pair.
How can this task be accomplished?

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

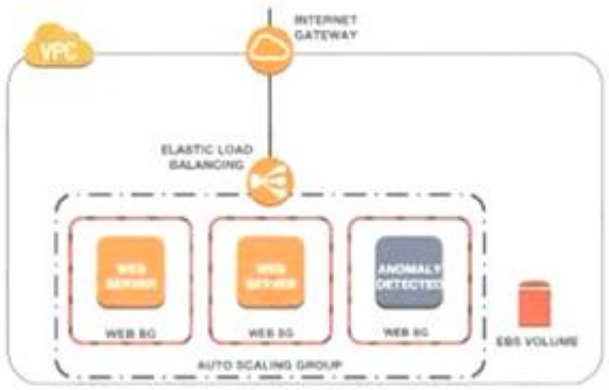
Answer: A

NEW QUESTION 10
- (Exam Topic 1)
A Security Engineer discovered a vulnerability in an application running on Amazon ECS. The vulnerability allowed attackers to install malicious code. Analysis of the code shows it exfiltrates data on port 5353 in batches at random time intervals.
While the code of the containers is being patched, how can Engineers quickly identify all compromised hosts and stop the egress of data on port 5353?

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

Answer: C

NEW QUESTION 13
- (Exam Topic 1)
A Security Engineer noticed an anomaly within a company EC2 instance as shown in the image. The Engineer must now investigate what e causing the anomaly.
What are the MOST effective steps to take lo ensure that the instance is not further manipulated while allowing the Engineer to understand what happened?



A. Remove the instance from the Auto Scaling group Place the instance within an isolation security group, detach the EBS volume launch an EC2 instance with a forensic toolkit and attach the E8S volume to investigate
B. Remove the instance from the Auto Scaling group and the Elastic Load Balancer Place the instance within an isolation security group, launch an EC2 instance with a forensic toolkit, and allow the forensic toolkit image to connect to the suspicious Instance to perform the Investigation.
C. Remove the instance from the Auto Scaling group Place the Instance within an isolation security group, launch an EC2 Instance with a forensic toolkit and use the forensic toolkit imago to deploy an ENI as a network span port to inspect all traffic coming from the suspicious instance.
D. Remove the instance from the Auto Scaling group and the Elastic Load Balancer Place the instance within an isolation security group, make a copy of the EBS volume from a new snapshot, launch an EC2 Instance with a forensic toolkit and attach the copy of the EBS volume to investigate.

Answer: B

NEW QUESTION 17
- (Exam Topic 1)
A security engineer is designing an incident response plan to address the risk of a compromised Amazon EC2 instance. The plan must recommend a solution to meet the following requirements:
• A trusted forensic environment must be provisioned
• Automated response processes must be orchestrated
Which IAM services should be included in the plan? {Select TWO)

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

Answer: AE

NEW QUESTION 19
- (Exam Topic 1)
A company is configuring three Amazon EC2 instances with each instance in a separate Availability Zone. The EC2 instances wilt be used as transparent proxies for outbound internet traffic for ports 80 and 443 so the proxies can block traffic to certain internet destinations as required by the company's security policies. A Security Engineer completed the following:
• Set up the proxy software on the EC2 instances.
• Modified the route tables on the private subnets to use the proxy EC2 instances as the default route.
• Created a security group rule opening inbound port 80 and 443 TCP protocols on the proxy EC2 instance security group.
However, the proxy EC2 instances are not successfully forwarding traffic to the internet.
What should the Security Engineer do to make the proxy EC2 instances route traffic to the internet?

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

Answer: B

NEW QUESTION 20
- (Exam Topic 1)
A security engineer needs to configure monitoring and auditing for IAM Lambda.
Which combination of actions using IAM services should the security engineer take to accomplish this goal? (Select TWO.)

A. Use IAM Config to track configuration changes to Lambda functions, runtime environments, tags, handler names, code sizes, memory allocation, timeout settings, and concurrency settings, along with Lambda IAM execution role, subnet, and security group associations.
B. Use IAM CloudTrail to implement governance, compliance, operational, and risk auditing for Lambda.
C. Use Amazon Inspector to automatically monitor for vulnerabilities and perform governance, compliance, operational, and risk auditing for Lambda.
D. Use IAM Resource Access Manager to track configuration changes to Lambda functions, runtime environments, tags, handler names, code sizes, memory allocation, timeout settings, and concurrency settings, along with Lambda IAM execution role, subnet, and security group associations.
E. Use Amazon Macie to discover, classify, and protect sensitive data being executed inside the Lambda function.

Answer: AB

NEW QUESTION 23
- (Exam Topic 1)
A company's development team is designing an application using IAM Lambda and Amazon Elastic Container Service (Amazon ECS). The development team needs to create IAM roles to support these systems. The company's security team wants to allow the developers to build IAM roles directly, but the security team wants to retain control over the permissions the developers can delegate to those roles. The development team needs access to more permissions than those required for the application's IAM services. The solution must minimize management overhead.
How should the security team prevent privilege escalation for both teams?

A. Enable IAM CloudTrai
B. Create a Lambda function that monitors the event history for privilege escalation events and notifies the security team.
C. Create a managed IAM policy for the permissions require
D. Reference the IAM policy as a permissions boundary within the development team's IAM role.
E. Enable IAM Organizations Create an SCP that allows the IAM CreateUser action but that has a condition that prevents API calls other than those required by the development team
F. Create an IAM policy with a deny on the IAMCreateUser action and assign the policy to the development tea
G. Use a ticket system to allow the developers to request new IAM roles for their application
H. The IAM roles will then be created by the security team.

Answer: A

NEW QUESTION 24
- (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 26
- (Exam Topic 1)
A company has an application hosted in an Amazon EC2 instance and wants the application to access secure strings stored in IAM Systems Manager Parameter Store When the application tries to access the secure string key value, it fails.
Which factors could be the cause of this failure? (Select TWO.)

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

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

Answer: AB

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

NEW QUESTION 31
- (Exam Topic 1)
After multiple compromises of its Amazon EC2 instances, a company's Security Officer is mandating that memory dumps of compromised instances be captured for further analysis. A Security Engineer just received an EC2 abuse notification report from IAM stating that an EC2 instance running the most recent Windows Server 2019 Base AMI is compromised.
How should the Security Engineer collect a memory dump of the EC2 instance for forensic analysis?

A. Give consent to the IAM Security team to dump the memory core on the compromised instance and provide it to IAM Support for analysis.
B. Review memory dump data that the IAM Systems Manager Agent sent to Amazon CloudWatch Logs.
C. Download and run the EC2Rescue for Windows Server utility from IAM.
D. Reboot the EC2 Windows Server, enter safe mode, and select memory dump.

Answer: C

Explanation:
https://docs.IAM.amazon.com/IAMEC2/latest/WindowsGuide/ec2rw-cli.html

NEW QUESTION 32
- (Exam Topic 1)
A large government organization is moving to the cloud and has specific encryption requirements. The first workload to move requires that a customer's data be immediately destroyed when the customer makes that request.
Management has asked the security team to provide a solution that will securely store the data, allow only authorized applications to perform encryption and decryption and allow for immediate destruction of the data
Which solution will meet these requirements?

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

Answer: A

NEW QUESTION 33
- (Exam Topic 1)
After a recent security audit involving Amazon S3, a company has asked assistance reviewing its S3 buckets to determine whether data is properly secured. The first S3 bucket on the list has the following bucket policy.

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

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

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

Answer: A

NEW QUESTION 35
- (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 38
- (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 41
- (Exam Topic 1)
A company uses Microsoft Active Directory for access management for on-premises resources and wants to use the same mechanism for accessing its IAM accounts. Additionally, the development team plans to launch a public-facing application for which they need a separate authentication solution.
When coma nation of the following would satisfy these requirements? (Select TWO)

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

Answer: CD

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

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

Answer: B

NEW QUESTION 47
- (Exam Topic 1)
A company has several critical applications running on a large fleet of Amazon EC2 instances. As part of a security operations review, the company needs to apply a critical operating system patch to EC2 instances within 24 hours of the patch becoming available from the operating system vendor. The company does not have a patching solution deployed on IAM, but does have IAM Systems Manager configured. The solution must also minimize administrative overhead.
What should a security engineer recommend to meet these requirements?

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

Answer: B

NEW QUESTION 51
- (Exam Topic 1)
An company is using IAM Secrets Manager to store secrets that are encrypted using a CMK and are stored in the security account 111122223333. One of the company's production accounts. 444455556666, must to retrieve the secret values from the security account 111122223333. A security engineer needs to apply a policy to the secret in the security account based on least privilege access so the production account can retrieve the secret value only.
Which policy should the security engineer apply?

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

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

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

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

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

Answer: A

NEW QUESTION 54
- (Exam Topic 1)
A company has multiple production IAM accounts. Each account has IAM CloudTrail configured to log to a single Amazon S3 bucket in a central account. Two of the production accounts have trails that are not logging anything to the S3 bucket.
Which steps should be taken to troubleshoot the issue? (Choose three.)

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

Answer: BDF

NEW QUESTION 58
- (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 62
- (Exam Topic 1)
A company's Developers plan to migrate their on-premises applications to Amazon EC2 instances running Amazon Linux AMIs. The applications are accessed by a group of partner companies The Security Engineer needs to implement the following host-based security measures for these instances:
• Block traffic from documented known bad IP addresses
• Detect known software vulnerabilities and CIS Benchmarks compliance. Which solution addresses these requirements?

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

Answer: D

NEW QUESTION 64
- (Exam Topic 1)
A company has decided to migrate sensitive documents from on-premises data centers to Amazon S3. Currently, the hard drives are encrypted to meet a compliance requirement regarding data encryption. The CISO wants to improve security by encrypting each file using a different key instead of a single key. Using a different key would limit the security impact of a single exposed key.
Which of the following requires the LEAST amount of configuration when implementing this approach?

A. Place each file into a different S3 bucke
B. Set the default encryption of each bucket to use a different IAM KMS customer managed key.
C. Put all the files in the same S3 bucke
D. Using S3 events as a trigger, write an IAM Lambda function to encrypt each file as it is added using different IAM KMS data keys.
E. Use the S3 encryption client to encrypt each file individually using S3-generated data keys
F. Place all the files in the same S3 bucke
G. Use server-side encryption with IAM KMS-managed keys (SSE-KMS) to encrypt the data

Answer: D

Explanation:
References:
https://docs.IAM.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html
Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3) When you use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3), each object is encrypted with a unique key. Server-Side Encryption with Customer Master Keys (CMKs) Stored in IAM Key Management Service (SSE-KMS) is similar to SSE-S3, but with some additional benefits and charges for using this service.
When you use SSE-KMS to protect your data without an S3 Bucket Key, Amazon S3 uses an individual IAM KMS data key for every object. It makes a call to IAM KMS every time a request is made against a
KMS-encrypted object. https://docs.IAM.amazon.com/AmazonS3/latest/dev/bucket-key.html
https://docs.IAM.amazon.com/kms/latest/developerguide/symmetric-asymmetric.html

NEW QUESTION 65

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

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

Answer: C

NEW QUESTION 69
- (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 73
- (Exam Topic 1)
While securing the connection between a company's VPC and its on-premises data center, a Security Engineer sent a ping command from an on-premises host (IP address 203.0.113.12) to an Amazon EC2 instance (IP address 172.31.16.139). The ping command did not return a response. The flow log in the VPC showed the following:
2 123456789010 eni-1235b8ca 203.0.113.12 172.31.16.139 0 0 1 4 336 1432917027 1432917142 ACCEPT OK
2 123456789010 eni-1235b8ca 172.31.16.139 203.0.113.12 0 0 1 4 336 1432917094 1432917142 REJECT OK
What action should be performed to allow the ping to work?

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

Answer: D

NEW QUESTION 74
- (Exam Topic 1)
A company is setting up products to deploy in IAM Service Catalog. Management is concerned that when users launch products, elevated IAM privileges will be required to create resources. How should the company mitigate this concern?

A. Add a template constraint to each product in the portfolio.
B. Add a launch constraint to each product in the portfolio.
C. Define resource update constraints for each product in the portfolio.
D. Update the IAM CloudFormalion template backing the product to include a service role configuration.

Answer: B

Explanation:
https://docs.IAM.amazon.com/servicecatalog/latest/adminguide/constraints-launch.html
Launch constraints apply to products in the portfolio (product-portfolio association). Launch constraints do not apply at the portfolio level or to a product across all portfolios. To associate a launch constraint with all products in a portfolio, you must apply the launch constraint to each product individually.

NEW QUESTION 77
- (Exam Topic 1)
A security engineer has been tasked with implementing a solution that allows the company's development team to have interactive command line access to Amazon EC2 Linux instances using the IAM Management Console.
Which steps should the security engineer take to satisfy this requirement while maintaining least privilege?

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

K. Configure IAM policies to allow development team access to the EC2 console and attach to the teams IAM users.

Answer: A

NEW QUESTION 81
- (Exam Topic 1)
A Security Administrator at a university is configuring a fleet of Amazon EC2 instances. The EC2 instances are shared among students, and non-root SSH access is allowed. The Administrator is concerned about students attacking other IAM account resources by using the EC2 instance metadata service.
What can the Administrator do to protect against this potential attack?

A. Disable the EC2 instance metadata service.
B. Log all student SSH interactive session activity.
C. Implement ip tables-based restrictions on the instances.
D. Install the Amazon Inspector agent on the instances.

Answer: A

Explanation:
"To turn off access to instance metadata on an existing instance....." https://docs.IAM.amazon.com/IAMEC2/latest/UserGuide/configuring-instance-metadata-service.html You can disable the service for existing (running or stopped) ec2 instances. https://docs.IAM.amazon.com/cli/latest/reference/ec2/modify-instance-metadata-options.html

NEW QUESTION 82
- (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 87
- (Exam Topic 1)
A global company that deals with International finance is investing heavily in cryptocurrencies and wants to experiment with mining technologies using IAM. The company's security team has enabled Amazon GuardDuty and is concerned by the number of findings being generated by the accounts. The security team wants to minimize the possibility of GuardDuty finding false negatives for compromised instances that are performing mining
How can the security team continue using GuardDuty while meeting these requirements?

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

Answer: A

NEW QUESTION 92
- (Exam Topic 1)
A company has several workloads running on IAM. Employees are required to authenticate using on-premises ADFS and SSO to access the IAM Management Console. Developers migrated an existing legacy web application to an Amazon EC2 instance. Employees need to access this application from anywhere on the internet, but currently, there is no authentication system built into the application.
How should the Security Engineer implement employee-only access to this system without changing the application?

A. Place the application behind an Application Load Balancer (ALB). Use Amazon Cognito as authentication for the AL
B. Define a SAML-based Amazon Cognito user pool and connect it to ADFS.
C. Implement IAM SSO in the master account and link it to ADFS as an identity provide
D. Define the EC2 instance as a managed resource, then apply an IAM policy on the resource.
E. Define an Amazon Cognito identity pool, then install the connector on the Active Directory serve

F. Use the Amazon Cognito SDK on the application instance to authenticate the employees using their Active Directory user names and passwords.
G. Create an IAM Lambda custom authorizer as the authenticator for a reverse proxy on Amazon EC2.Ensure the security group on Amazon EC2 only allows access from the Lambda function.

Answer: A

Explanation:
https://docs.IAM.amazon.com/elasticloadbalancing/latest/application/listener-authenticate-users.html
- Authenticate users through social IdPs, such as Amazon, Facebook, or Google, through the user pools supported by Amazon Cognito.
- Authenticate users through corporate identities, using SAML, LDAP, or Microsoft AD, through the user pools supported by Amazon Cognito.

NEW QUESTION 97
- (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 102
- (Exam Topic 1)
A company uses HTTP Live Streaming (HLS) to stream live video content to paying subscribers by using
Amazon CloudFront. HLS splits the video content into chunks so that the user can request the right chunk based on different conditions Because the video events last for several hours, the total video is made up of thousands of chunks
The origin URL is not disclosed and every user is forced to access the CloudFront URL The company has a web application that authenticates the paying users against an internal repository and a CloudFront key pair that is already issued.
What is the simplest and MOST effective way to protect the content?

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

Answer: B

NEW QUESTION 106
- (Exam Topic 1)
A Developer signed in to a new account within an IAM Organizations organizations unit (OU) containing multiple accounts. Access to the Amazon S3 service is restricted with the following SCP:

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

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

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

Answer: C

NEW QUESTION 107
- (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 110
- (Exam Topic 1)
A company is using IAM Organizations to manage multiple IAM member accounts. All of these accounts have Amazon GuardDuty enabled in all Regions. The company's IAM Security Operations Center has a centralized security account for logging and monitoring. One of the member accounts has received an excessively high bill A security engineer discovers that a compromised Amazon EC2 instance is being used to mine crypto currency. The Security Operations Center did not receive a GuardDuty finding in the central security account.
but there was a GuardDuty finding in the account containing the compromised EC2 instance. The security engineer needs to ensure an GuardDuty finding are available in the security account.
What should the security engineer do to resolve this issue?

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

Answer: D

NEW QUESTION 114
- (Exam Topic 1)
A Security Engineer manages IAM Organizations for a company. The Engineer would like to restrict IAM usage to allow Amazon S3 only in one of the organizational units (OUs). The Engineer adds the following SCP to the OU:

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

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

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

Answer: D

Explanation:
https://docs.IAM.amazon.com/organizations/latest/APIReference/API_DetachPolicy.html
Every root, OU, and account must have at least one SCP attached. If you want to replace the default FullIAMAccess policy with an SCP that limits the permissions that can be delegated, you must attach the replacement SCP before you can remove the default SCP. This is the authorization strategy of an "allow list". If you instead attach a second SCP and leave the FullIAMAccess SCP still attached, and specify "Effect": "Deny" in the second SCP to override the "Effect": "Allow" in the FullIAMAccess policy (or any other attached SCP), you're using the authorization strategy of a "deny list".

NEW QUESTION 115
- (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 118

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

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

Answer: D

NEW QUESTION 121
- (Exam Topic 1)
A company needs its Amazon Elastic Block Store (Amazon EBS) volumes to be encrypted at all times. During a security incident. EBS snapshots of suspicious instances are shared to a forensics account for analysis A security engineer attempting to share a suspicious EBS snapshot to the forensics account receives the following error
"Unable to share snapshot: An error occurred (OperationNotPermitted) when calling the ModifySnapshotAttribute operation: Encrypted snapshots with EBS default key cannot be shared.
Which combination of steps should the security engineer take in the incident account to complete the sharing operation? (Select THREE)

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

Answer: ABF

NEW QUESTION 123
- (Exam Topic 1)
A Solutions Architect is designing a web application that uses Amazon CloudFront, an Elastic Load Balancing Application Load Balancer, and an Auto Scaling group of Amazon EC2 instances. The load balancer and EC2 instances are in the US West (Oregon) region. It has been decided that encryption in transit is necessary by using a customer-branded domain name from the client to CloudFront and from CloudFront to the load balancer.
Assuming that IAM Certificate Manager is used, how many certificates will need to be generated?

A. One in the US West (Oregon) region and one in the US East (Virginia) region.
B. Two in the US West (Oregon) region and none in the US East (Virginia) region.
C. One in the US West (Oregon) region and none in the US East (Virginia) region.
D. Two in the US East (Virginia) region and none in the US West (Oregon) region.

Answer: A

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

NEW QUESTION 128
- (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 133
- (Exam Topic 1)
A developer is creating an IAM Lambda function that requires environment variables to store connection information and logging settings. The developer is required to use an IAM KMS Customer Master Key (CMK> supplied by the information security department in order to adhere to company standards for securing Lambda environment variables.
Which of the following are required for this configuration to work? (Select TWO.)

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

Answer: BC

NEW QUESTION 138
- (Exam Topic 1)
A company has decided to use encryption in its IAM account to secure the objects in Amazon S3 using server-side encryption. Object sizes range from 16.000 B to 5 MB. The requirements are as follows:
• The key material must be generated and stored in a certified Federal Information Processing Standard (FIPS) 140-2 Level 3 machine.
• The key material must be available in multiple Regions. Which option meets these requirements?

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

Answer: D

NEW QUESTION 143
- (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 145
- (Exam Topic 1)
A Security Engineer creates an Amazon S3 bucket policy that denies access to all users. A few days later, the Security Engineer adds an additional statement to the bucket policy to allow read-only access to one other employee Even after updating the policy the employee still receives an access denied message.
What is the likely cause of this access denial?
A. The ACL in the bucket needs to be updated.
B. The IAM policy does not allow the user to access the bucket
C. It takes a few minutes for a bucket policy to take effect
D. The allow permission is being overridden by the deny.

Answer: D

NEW QUESTION 146
- (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 151
- (Exam Topic 1)
A Security Engineer launches two Amazon EC2 instances in the same Amazon VPC but in separate Availability Zones. Each instance has a public IP address and is able to connect to external hosts on the internet. The two instances are able to communicate with each other by using their private IP addresses, but they are not able to communicate with each other when using their public IP addresses.
Which action should the Security Engineer take to allow communication over the public IP addresses?

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

Answer: D

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

NEW QUESTION 156
- (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 160
- (Exam Topic 2)
Your company has an EC2 Instance that is hosted in an IAM VPC. There is a requirement to ensure that logs files from the EC2 Instance are stored accordingly. The access should also be limited for the destination of the log files. How can this be accomplished? Choose 2 answers from the options given below. Each answer forms part of the solution
Please select:

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

Answer: BD

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

NEW QUESTION 163
- (Exam Topic 2)
An application running on EC2 instances must use a username and password to access a database. The developer has stored those secrets in the SSM Parameter Store with type SecureString using the default KMS CMK. Which combination of configuration steps will allow the application to access the secrets via the API? Select 2 answers from the options below
Please select:

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

E. Add permission to use the KMS key to decrypt to the EC2 instance role
F. Add the SSM service role as a trusted service to the EC2 instance role.

Answer: CD

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

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

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

NEW QUESTION 167
- (Exam Topic 2)
During a recent internal investigation, it was discovered that all API logging was disabled in a production account, and the root user had created new API keys that appear to have been used several times.
What could have been done to detect and automatically remediate the incident?

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

Answer: B

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

NEW QUESTION 168
- (Exam Topic 2)
Example.com hosts its internal document repository on Amazon EC2 instances. The application runs on EC2 instances and previously stored the documents on encrypted Amazon EBS volumes. To optimize the application for scale, example.com has moved the files to Amazon S3. The security team has mandated that all the files are securely deleted from the EBS volume, and it must certify that the data is unreadable before releasing the underlying disks.
Which of the following methods will ensure that the data is unreadable by anyone else?

A. Change the volume encryption on the EBS volume to use a different encryption mechanis
B. Then, release the EBS volumes back to IAM.
C. Release the volumes back to IA
D. IAM immediately wipes the disk after it is deprovisioned.
E. Delete the encryption key used to encrypt the EBS volum
F. Then, release the EBS volumes back to IAM.

G. Delete the data by using the operating system delete command
H. Run Quick Format on the drive and then release the EBS volumes back to IAM.

Answer: D

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

NEW QUESTION 171
- (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 174
- (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 178
- (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 182
- (Exam Topic 2)
An organization wants to deploy a three-tier web application whereby the application servers run on Amazon EC2 instances. These EC2 instances need access to credentials that they will use to authenticate their SQL connections to an Amazon RDS DB instance. Also, IAM Lambda functions must issue queries to the RDS database by using the same database credentials.
The credentials must be stored so that the EC2 instances and the Lambda functions can access them. No other access is allowed. The access logs must record when the credentials were accessed and by whom.
What should the Security Engineer do to meet these requirements?

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

Answer: D

NEW QUESTION 184
- (Exam Topic 2)
Which of the following is the most efficient way to automate the encryption of IAM CloudTrail logs using a Customer Master Key (CMK) in IAM KMS?

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

Answer: C

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

NEW QUESTION 187
- (Exam Topic 2)
A Security Engineer is working with a Product team building a web application on IAM. The application uses Amazon S3 to host the static content, Amazon API Gateway to provide RESTful services; and Amazon DynamoDB as the backend data store. The users already exist in a directory that is exposed through a SAML identity provider.
Which combination of the following actions should the Engineer take to enable users to be authenticated into the web application and call APIs? (Choose three.)

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

Answer: BDE

NEW QUESTION 191
- (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 192
- (Exam Topic 2)
A company plans to move most of its IT infrastructure to IAM. They want to leverage their existing on-premises Active Directory as an identity provider for IAM.

Which combination of steps should a Security Engineer take to federate the company's on-premises Active Directory with IAM? (Choose two.)

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

Answer: AD

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

NEW QUESTION 195
- (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 196
- (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 200
- (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 202
- (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 205
- (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 208
- (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 210
- (Exam Topic 2)
The Security Engineer is given the following requirements for an application that is running on Amazon EC2 and managed by using IAM CloudFormation templates with EC2 Auto Scaling groups:
-Have the EC2 instances bootstrapped to connect to a backend database.
-Ensure that the database credentials are handled securely.
-Ensure that retrievals of database credentials are logged.
Which of the following is the MOST efficient way to meet these requirements?

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

Answer: B

NEW QUESTION 214
- (Exam Topic 2)
Which option for the use of the IAM Key Management Service (KMS) supports key management best practices that focus on minimizing the potential scope of data exposed by a possible future key compromise?

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

Answer: A

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

NEW QUESTION 217
- (Exam Topic 2)
The Accounting department at Example Corp. has made a decision to hire a third-party firm, AnyCompany, to monitor Example Corp.'s IAM account to help optimize costs.
The Security Engineer for Example Corp. has been tasked with providing AnyCompany with access to the required Example Corp. IAM resources. The Engineer has created an IAM role and granted permission to AnyCompany's IAM account to assume this role.
When customers contact AnyCompany, they provide their role ARN for validation. The Engineer is concerned that one of AnyCompany's other customers might deduce Example Corp.'s role ARN and potentially compromise the company's account.
What steps should the Engineer perform to prevent this outcome?

A. Create an IAM user and generate a set of long-term credential
B. Provide the credentials to AnyCompany.Monitor access in IAM access advisor and plan to rotate credentials on a recurring basis.
C. Request an external ID from AnyCompany and add a condition with sts:Externald to the role's trust policy.
D. Require two-factor authentication by adding a condition to the role's trust policy with IAM:MultiFactorAuthPresent.
E. Request an IP range from AnyCompany and add a condition with IAM:SourceIp to the role's trust policy.

Answer: B

NEW QUESTION 222

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

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

Answer: C

NEW QUESTION 225
- (Exam Topic 2)
An application has been written that publishes custom metrics to Amazon CloudWatch. Recently, IAM changes have been made on the account and the metrics are no longer being reported.
Which of the following is the LEAST permissive solution that will allow the metrics to be delivered?

A. Add a statement to the IAM policy used by the application to allow logs:putLogEvents and logs:createLogStream
B. Modify the IAM role used by the application by adding the CloudWatchFullAccess managed policy.
C. Add a statement to the IAM policy used by the application to allow cloudwatch:putMetricData.
D. Add a trust relationship to the IAM role used by the application for cloudwatch.amazonIAM.com.

Answer: C

Explanation:
https://docs.IAM.amazon.com/AmazonCloudWatch/latest/monitoring/permissions-reference-cw.html

NEW QUESTION 230
- (Exam Topic 2)
A Lambda function reads metadata from an S3 object and stores the metadata in a DynamoDB table. The function is triggered whenever an object is stored within the S3 bucket.
How should the Lambda function be given access to the DynamoDB table? Please select:

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

Answer: D

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

NEW QUESTION 232
- (Exam Topic 2)
A Security Engineer is building a Java application that is running on Amazon EC2. The application communicates with an Amazon RDS instance and authenticates with a user name and password.
Which combination of steps can the Engineer take to protect the credentials and minimize downtime when the credentials are rotated? (Choose two.)

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

Answer: CE

NEW QUESTION 235
- (Exam Topic 2)
A Security Engineer is implementing a solution to allow users to seamlessly encrypt Amazon S3 objects without having to touch the keys directly. The solution must be highly scalable without requiring continual management. Additionally, the organization must be able to immediately delete the encryption keys.
Which solution meets these requirements?

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

Answer: B

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

NEW QUESTION 240
- (Exam Topic 2)
An Amazon EC2 instance is denied access to a newly created IAM KMS CMK used for decrypt actions. The environment has the following configuration:
- The instance is allowed the kms:Decrypt action in its IAM role for all resources
- The IAM KMS CMK status is set to enabled
- The instance can communicate with the KMS API using a configured VPC endpoint What is causing the issue?

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

Answer: D

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

NEW QUESTION 245
- (Exam Topic 2)
Which of the following minimizes the potential attack surface for applications?

A. Use security groups to provide stateful firewalls for Amazon EC2 instances at the hypervisor level.
B. Use network ACLs to provide stateful firewalls at the VPC level to prevent access to any specific IAM resource.
C. Use IAM Direct Connect for secure trusted connections between EC2 instances within private subnets.
D. Design network security in a single layer within the perimeter network (also known as DMZ, demilitarized zone, and screened subnet) to facilitate quicker responses to threats.

Answer: A

Explanation:
https://IAM.amazon.com/answers/networking/vpc-security-capabilities/ Security Group is stateful and hypervisor level.

NEW QUESTION 247
- (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 249
- (Exam Topic 2)
An organization wants to be alerted when an unauthorized Amazon EC2 instance in its VPC performs a network port scan against other instances in the VPC. When the Security team performs its own internal tests in a separate account by using pre-approved third-party scanners from the IAM Marketplace, the Security team also then receives multiple Amazon GuardDuty events from Amazon CloudWatch alerting on its test activities.
How can the Security team suppress alerts about authorized security tests while still receiving alerts about the unauthorized activity?

A. Use a filter in IAM CloudTrail to exclude the IP addresses of the Security team's EC2 instances.
B. Add the Elastic IP addresses of the Security team's EC2 instances to a trusted IP list in Amazon GuardDuty.
C. Install the Amazon Inspector agent on the EC2 instances that the Security team uses.
D. Grant the Security team's EC2 instances a role with permissions to call Amazon GuardDuty API operations.

Answer: B

Explanation:
Trusted IP lists consist of IP addresses that you have whitelisted for secure communication with your IAM infrastructure and applications. GuardDuty does not generate findings for IP addresses on trusted IP lists. At any given time, you can have only one uploaded trusted IP list per IAM account per region. Threat lists consist of known malicious IP addresses. GuardDuty generates findings based on threat lists. At any given time, you can have up to six uploaded threat lists per IAM account per region. https://docs.IAM.amazon.com/guardduty/latest/ug/guardduty_upload_lists.html

NEW QUESTION 252
- (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 254
- (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 256
- (Exam Topic 2)
Your company has a set of resources defined in the IAM Cloud. Their IT audit department has requested to get a list of resources that have been defined across the account. How can this be achieved in the easiest manner?
Please select:

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

Answer: D

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

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

NEW QUESTION 261
- (Exam Topic 2)
A Security Administrator has a website hosted in Amazon S3. The Administrator has been given the following requirements:
- Users may access the website by using an Amazon CloudFront distribution.
- Users may not access the website directly by using an Amazon S3 URL.

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

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

Answer: AC

NEW QUESTION 264
- (Exam Topic 2)
A company uses user data scripts that contain sensitive information to bootstrap Amazon EC2 instances. A Security Engineer discovers that this sensitive information is viewable by people who should not have access to it.
What is the MOST secure way to protect the sensitive information used to bootstrap the instances?

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

Answer: B

NEW QUESTION 265
- (Exam Topic 2)
You are deivising a policy to allow users to have the ability to access objects in a bucket called appbucket. You define the below custom bucket policy

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

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

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

Answer: C

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

NEW QUESTION 269
- (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 271
- (Exam Topic 2)
Your company has defined a number of EC2 Instances over a period of 6 months. They want to know if any of the security groups allow unrestricted access to a resource. What is the best option to accomplish this requirement?
Please select:

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

Answer: B

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

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

NEW QUESTION 273
- (Exam Topic 2)
An organization is moving non-business-critical applications to IAM while maintaining a mission-critical application in an on-premises data center. An on-premises application must share limited confidential information with the applications in IAM. The internet performance is unpredictable.
Which configuration will ensure continued connectivity between sites MOST securely?

A. VPN and a cached storage gateway
B. IAM Snowball Edge
C. VPN Gateway over IAM Direct Connect
D. IAM Direct Connect

Answer: C

Explanation:
https://docs.IAM.amazon.com/whitepapers/latest/IAM-vpc-connectivity-options/IAM-direct-connect-plus-vpn-n

NEW QUESTION 277
- (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 282
- (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 283
- (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 286
- (Exam Topic 2)
A Security Engineer received an IAM Abuse Notice listing EC2 instance IDs that are reportedly abusing other hosts.
Which action should the Engineer take based on this situation? (Choose three.)

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

Answer: BEF

NEW QUESTION 287
- (Exam Topic 2)
A Developer's laptop was stolen. The laptop was not encrypted, and it contained the SSH key used to access multiple Amazon EC2 instances. A Security Engineer has verified that the key has not been used, and has blocked port 22 to all EC2 instances while developing a response plan.
How can the Security Engineer further protect currently running instances?

A. Delete the key-pair key from the EC2 console, then create a new key pair.
B. Use the modify-instance-attribute API to change the key on any EC2 instance that is using the key.
C. Use the EC2 RunCommand to modify the authorized_keys file on any EC2 instance that is using the key.
D. Update the key pair in any AMI used to launch the EC2 instances, then restart the EC2 instances.

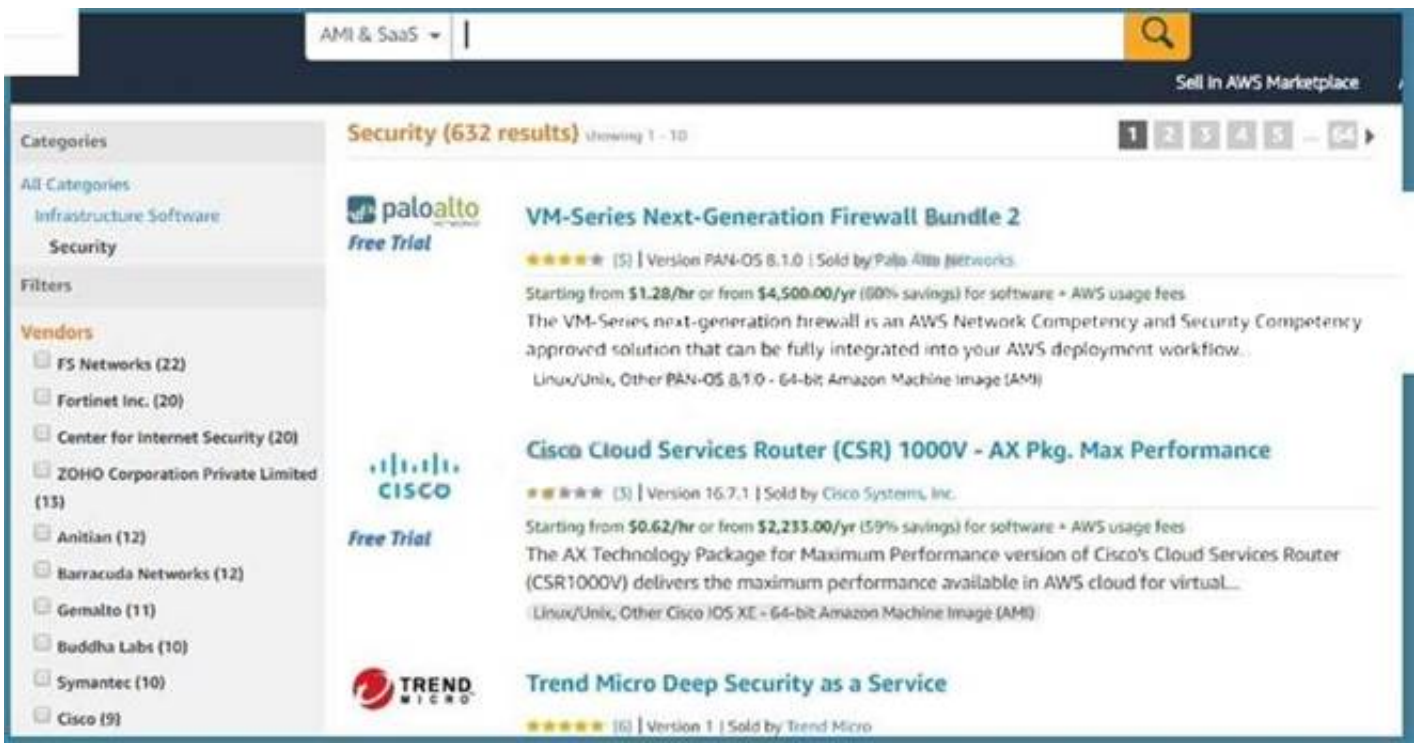
Answer: C

NEW QUESTION 289
- (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%200verview.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 294
.....

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