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

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

Answer: A

NEW QUESTION 3
- (Exam Topic 1)
A Security Engineer has several thousand Amazon EC2 instances split across production and development environments. Each instance is tagged with its environment. The Engineer needs to analyze and patch all the development EC2 instances to ensure they are not currently exposed to any common vulnerabilities or exposures (CVEs)
Which combination of steps is the MOST efficient way for the Engineer to meet these requirements? (Select TWO.)

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

Answer: CD

NEW QUESTION 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 company has a serverless application for internal users deployed on IAM. The application uses IAM Lambda for the front end and for business logic. The Lambda function accesses an Amazon RDS database inside a VPC The company uses IAM Systems Manager Parameter Store for storing database credentials.
A recent security review highlighted the following issues
>

The Lambda function has internet access.
> The relational database is publicly accessible.
> The database credentials are not stored in an encrypted state.
Which combination of steps should the company take to resolve these security issues? (Select THREE)

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

Answer: ABE

NEW QUESTION 6
- (Exam Topic 1)
Which of the following are valid configurations for using SSL certificates with Amazon CloudFront? (Select THREE)

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

Answer: ACD

NEW QUESTION 7
- (Exam Topic 1)
A company's architecture requires that its three Amazon EC2 instances run behind an Application Load Balancer (ALB). The EC2 instances transmit sensitive data between each other Developers use SSL certificates to encrypt the traffic between the public users and the ALB However the Developers are unsure of how to encrypt the data in transit between the ALB and the EC2 instances and the traffic between the EC2 instances
Which combination of activities must the company implement to meet its encryption requirements'? (Select TWO)

A. Configure SSLTLS on the EC2 instances and configure the ALB target group to use HTTPS
B. Ensure that all resources are in the same VPC so the default encryption provided by the VPC is used to encrypt the traffic between the EC2 instances.
C. In the AL
D. select the default encryption to encrypt the traffic between the ALB and the EC2 instances
E. In the code for the application, include a cryptography library and encrypt the data before sending it between the EC2 instances
F. Configure IAM Direct Connect to provide an encrypted tunnel between the EC2 instances

Answer: BC

NEW QUESTION 8
- (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 9
- (Exam Topic 1)
A company is outsourcing its operational support 1o an external company. The company's security officer must implement an access solution fen delegating operational support that minimizes overhead.
Which approach should the security officer take to meet these requirements?

A. implement Amazon Cognito identity pools with a role that uses a policy that denies the actions related to Amazon Cognito API management Allow the external company to federate through its identity provider
B. Federate IAM identity and Access Management (IAM) with the external company's identity provider Create an IAM role and attach a policy with the necessary permissions
C. Create an IAM group for me external company Add a policy to the group that denies IAM modifications Securely provide the credentials to the eternal company.
D. Use IAM SSO with the external company's identity provide
E. Create an IAM group to map to the identity provider user group, and attach a policy with the necessary permissions.

Answer: B

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

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

Answer: D

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

NEW QUESTION 10
- (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 11
- (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 15
- (Exam Topic 1)
A company is collecting IAM CloudTrail log data from multiple IAM accounts by managing individual trails in each account and forwarding log data to a centralized Amazon S3 bucket residing in a log archive account. After CloudTrail introduced support for IAM Organizations trails, the company decided to further centralize management and automate deployment of the CloudTrail logging capability across all of its IAM accounts.
The company's security engineer created an IAM Organizations trail in the master account, enabled server-side encryption with IAM KMS managed keys (SSE-KMS) for the log files, and specified the same bucket as the storage location. However, the engineer noticed that logs recorded by the new trail were not delivered to the bucket.
Which factors could cause this issue? (Select TWO.)

A. The CMK key policy does not allow CloudTrail to make encrypt and decrypt API calls against the key.
B. The CMK key policy does not allow CloudTrail to make GenerateDataKey API calls against the key.
C. The IAM role used by the CloudTrail trail does not have permissions to make PutObject API calls against a folder created for the Organizations trail.
D. The S3 bucket policy does not allow CloudTrail to make PutObject API calls against a folder created for the Organizations trail.
E. The CMK key policy does not allow the IAM role used by the CloudTrail trail to use the key for crypto graphical operations.

Answer: AD

NEW QUESTION 16
- (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 19
- (Exam Topic 1)
A company is developing a new mobile app for social media sharing. The company's development team has decided to use Amazon S3 to store at media files generated by mobile app users The company wants to allow users to control whether their own tiles are public, private, of shared with other users in their social network what should the development team do to implement the type of access control with the LEAST administrative effort?

A. Use individual ACLs on each S3 object.
B. Use IAM groups tor sharing files between application social network users
C. Store each user's files in a separate S3 bucket and apery a bucket policy based on the user's sharing settings
D. Generate presigned UPLs for each file access

Answer: A

NEW QUESTION 22
- (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 26
- (Exam Topic 1)
A security engineer must use IAM Key Management Service (IAM KMS) to design a key management solution for a set of Amazon Elastic Block Store (Amazon EBS) volumes that contain sensitive data. The solution needs to ensure that the key material automatically expires in 90 days.
Which solution meets these criteria?

A. A customer managed CMK that uses customer provided key material
B. A customer managed CMK that uses IAM provided key material
C. An IAM managed CMK
D. Operating system-native encryption that uses GnuPG

Answer: B

NEW QUESTION 30
- (Exam Topic 1)
A company has an IAM account and allows a third-party contractor who uses another IAM account, to assume certain IAM roles. The company wants to ensure that IAM roles can be assumed by the contractor only if the contractor has multi-factor authentication enabled on their IAM user accounts
What should the company do to accomplish this?
A)

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

B)

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

C)

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

D)

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

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

Answer: A

NEW QUESTION 33
- (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 36
- (Exam Topic 1)
An IAM account administrator created an IAM group and applied the following managed policy to require that each individual user authenticate using multi-factor authentication:

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

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

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

Answer: B

NEW QUESTION 39
- (Exam Topic 1)
A financial institution has the following security requirements:
⯈ Cloud-based users must be contained in a separate authentication domain.
⯈ Cloud-based users cannot access on-premises systems.
As part of standing up a cloud environment, the financial institution is creating a number of Amazon managed databases and Amazon EC2 instances. An Active Directory service exists on-premises that has all the administrator accounts, and these must be able to access the databases and instances.
How would the organization manage its resources in the MOST secure manner? (Choose two.)

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

Answer: AD

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

NEW QUESTION 44
- (Exam Topic 1)
A company's Security Engineer has been asked to monitor and report all IAM account root user activities. Which of the following would enable the Security Engineer to monitor and report all root user activities?
(Select TWO)

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

Answer: BE

NEW QUESTION 46
- (Exam Topic 1)
A company has a compliance requirement to rotate its encryption keys on an annual basis. A Security Engineer needs a process to rotate the KMS Customer Master Keys (CMKs) that were created using imported key material.
How can the Engineer perform the key rotation process MOST efficiently?

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

Answer: A

NEW QUESTION 49
- (Exam Topic 2)
In response to the past DDoS attack experiences, a Security Engineer has set up an Amazon CloudFront distribution for an Amazon S3 bucket. There is concern that some users may bypass the CloudFront distribution and access the S3 bucket directly.
What must be done to prevent users from accessing the S3 objects directly by using URLs?

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

Answer: B

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

NEW QUESTION 53
- (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 54
- (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 58
- (Exam Topic 2)
A Security Administrator is restricting the capabilities of company root user accounts. The company uses IAM Organizations and has enabled it for all feature sets, including consolidated billing. The top-level account is used for billing and administrative purposes, not for operational IAM resource purposes.
How can the Administrator restrict usage of member root user accounts across the organization?

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

Answer: C

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

NEW QUESTION 61
- (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 65
- (Exam Topic 2)
A Software Engineer is trying to figure out why network connectivity to an Amazon EC2 instance does not appear to be working correctly. Its security group allows inbound HTTP traffic from 0.0.0.0/0, and the outbound rules have not been modified from the default. A custom network ACL associated with its subnet allows inbound HTTP traffic from 0.0.0.0/0 and has no outbound rules.
What would resolve the connectivity issue?

A. The outbound rules on the security group do not allow the response to be sent to the client on the ephemeral port range.
B. The outbound rules on the security group do not allow the response to be sent to the client on the HTTP port.
C. An outbound rule must be added to the network ACL to allow the response to be sent to the client on the ephemeral port range.
D. An outbound rule must be added to the network ACL to allow the response to be sent to the client on the HTTP port.

Answer: C

Explanation:
https://docs.IAM.amazon.com/vpc/latest/userguide/vpc-network-acls.html

NEW QUESTION 68
- (Exam Topic 2)
A Security Engineer is defining the logging solution for a newly developed product. Systems Administrators and Developers need to have appropriate access to event log files in IAM CloudTrail to support and troubleshoot the product.
Which combination of controls should be used to protect against tampering with and unauthorized access to log files? (Choose two.)

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

Answer: AD

NEW QUESTION 69
- (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 72
- (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 77
- (Exam Topic 2)
A company has contracted with a third party to audit several IAM accounts. To enable the audit, cross-account IAM roles have been created in each account targeted for audit. The Auditor is having trouble accessing some of the accounts.
Which of the following may be causing this problem? (Choose three.)

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

Answer: ACF

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

NEW QUESTION 80
- (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 84
- (Exam Topic 2)
A security alert has been raised for an Amazon EC2 instance in a customer account that is exhibiting strange behavior. The Security Engineer must first isolate the EC2 instance and then use tools for further investigation.
What should the Security Engineer use to isolate and research this event? (Choose three.)

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

Answer: ADF

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

NEW QUESTION 89
- (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 93
- (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 95
- (Exam Topic 2)
The Security Engineer is managing a web application that processes highly sensitive personal information. The application runs on Amazon EC2. The application has strict compliance requirements, which instruct that all incoming traffic to the application is protected from common web exploits and that all outgoing traffic from the EC2 instances is restricted to specific whitelisted URLs.
Which architecture should the Security Engineer use to meet these requirements?

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

H. Use a third-party IAM Marketplace solution to restrict egress traffic to specific whitelisted URLs.

Answer: D

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

NEW QUESTION 99
- (Exam Topic 2)
A company's database developer has just migrated an Amazon RDS database credential to be stored and managed by IAM Secrets Manager. The developer has also enabled rotation of the credential within the Secrets Manager console and set the rotation to change every 30 days.
After a short period of time, a number of existing applications have failed with authentication errors. What is the MOST likely cause of the authentication errors?

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

Answer: B

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

NEW QUESTION 101
- (Exam Topic 2)
You have a 2 tier application hosted in IAM. It consists of a web server and database server (SQL Server) hosted on separate EC2 Instances. You are devising the security groups for these EC2 Instances. The Web tier needs to be accessed by users across the Internet. You have created a web security group(wg-123) and database security group(db-345). Which combination of the following security group rules will allow the application to be secure and functional. Choose 2 answers from the options given below.
Please select:

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

Answer: AB

Explanation:
The Web security groups should allow access for ports 80 and 443 for HTTP and HTTPS traffic to all users from the internet.
The database security group should just allow access from the web security group from port 1433. Option C is invalid because this is not a valid configuration
Option D is invalid because database security should not be allowed on the internet For more information on Security Groups please visit the below URL:
https://docs.IAM.amazon.com/IAMEC2/latest/UserGuide/usins-network-security.htmll
The correct answers are: wg-123 - Allow ports 80 and 443 from 0.0.0.0/0, db-345 - Allow port 1433 from wg-123
Submit your Feedback/Queries to our Experts

NEW QUESTION 102
- (Exam Topic 2)
Which approach will generate automated security alerts should too many unauthorized IAM API requests be identified?

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

Answer: A

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

NEW QUESTION 105
- (Exam Topic 2)
A security team is responsible for reviewing IAM API call activity in the cloud environment for security violations. These events must be recorded and retained in a centralized location for both current and future IAM regions.
What is the SIMPLEST way to meet these requirements?

A. Enable IAM Trusted Advisor security checks in the IAM Console, and report all security incidents for all regions.
B. Enable IAM CloudTrail by creating individual trails for each region, and specify a single Amazon S3 bucket to receive log files for later analysis.
C. Enable IAM CloudTrail by creating a new trail and applying the trail to all region

D. Specify a single Amazon S3 bucket as the storage location.
E. Enable Amazon CloudWatch logging for all IAM services across all regions, and aggregate them to a single Amazon S3 bucket for later analysis.

Answer: C

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

NEW QUESTION 109
- (Exam Topic 2)
A company has a few dozen application servers in private subnets behind an Elastic Load Balancer (ELB) in an IAM Auto Scaling group. The application is accessed from the web over HTTPS. The data must always be encrypted in transit. The Security Engineer is worried about potential key exposure due to vulnerabilities in the application software.
Which approach will meet these requirements while protecting the external certificate during a breach?

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

Answer: C

NEW QUESTION 114
- (Exam Topic 2)
While analyzing a company's security solution, a Security Engineer wants to secure the IAM account root user.
What should the Security Engineer do to provide the highest level of security for the account?

A. Create a new IAM user that has administrator permissions in the IAM accoun
B. Delete the password for the IAM account root user.
C. Create a new IAM user that has administrator permissions in the IAM accoun
D. Modify the permissions for the existing IAM users.
E. Replace the access key for the IAM account root use
F. Delete the password for the IAM account root user.
G. Create a new IAM user that has administrator permissions in the IAM accoun
H. Enable multi-factor authentication for the IAM account root user.

Answer: D

Explanation:
If you continue to use the root user credentials, we recommend that you follow the security best practice to enable multi-factor authentication (MFA) for your account. Because your root user can perform sensitive operations in your account, adding an additional layer of authentication helps you to better secure your account. Multiple types of MFA are available.

NEW QUESTION 118
- (Exam Topic 2)
A company will store sensitive documents in three Amazon S3 buckets based on a data classification scheme of "Sensitive," "Confidential," and "Restricted."
The security solution must meet all of the following
requirements:
➢ Each object must be encrypted using a unique key.
➢ Items that are stored in the "Restricted" bucket require two-factor authentication for decryption.
➢ IAM KMS must automatically rotate encryption keys annually.
Which of the following meets these requirements?

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

Answer: A

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

NEW QUESTION 120
- (Exam Topic 3)
Your company has a set of EBS volumes defined in IAM. The security mandate is that all EBS volumes are encrypted. What can be done to notify the IT admin staff if there are any unencrypted volumes in the account.
Please select:

A. Use IAM Inspector to inspect all the EBS volumes
B. Use IAM Config to check for unencrypted EBS volumes
C. Use IAM Guard duty to check for the unencrypted EBS volumes
D. Use IAM Lambda to check for the unencrypted EBS volumes

Answer: B

Explanation:
The enc
config rule for IAM Config can be used to check for unencrypted volumes. encrypted-volurrn
5 volumes that are in an attached state are encrypted. If you specify the ID of a KMS key for encryptio using the kmsld parameter, the rule checks if the EBS volumes in an attached state are encrypted with that KMS key*1.
Options A and C are incorrect since these services cannot be used to check for unencrypted EBS volumes
Option D is incorrect because even though this is possible, trying to implement the solution alone with just the Lambda servk
would be too difficult
For more information on IAM Config and encrypted volumes, please refer to below URL:
> https://docs.IAM.amazon.com/config/latest/developerguide/encrypted-volumes.html
Submit your Feedback/Queries to our Experts

NEW QUESTION 123
- (Exam Topic 3)
Your company has an EC2 Instance hosted in IAM. This EC2 Instance hosts an application. Currently this application is experiencing a number of issues. You need to inspect the network packets to see what the type of error that is occurring? Which one of the below steps can help address this issue?
Please select:

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

Answer: B

NEW QUESTION 126
- (Exam Topic 3)
A company hosts data in S3. There is a requirement to control access to the S3 buckets. Which are the 2 ways in which this can be achieved?
Please select:

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

Answer: AC

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

NEW QUESTION 130
- (Exam Topic 3)
A company has an existing IAM account and a set of critical resources hosted in that account. The employee who was in-charge of the root account has left the company. What must be now done to secure the account. Choose 3 answers from the options given below.
Please select:

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

Answer: CDE

Explanation:
Now if the root account has a chance to be compromised, then you have to carry out the below steps
* 1. Delete the access keys for the root account
* 2. Confirm MFA to a secure device
* 3. Change the password for the root account
This will ensure the employee who has left has no change to compromise the resources in IAM. Option A is invalid because this would hamper the working of the current IAM users
Option B is invalid because this could hamper the current working of services in your IAM account Option F is invalid because this would hamper the working of the current IAM users

For more information on IAM root user, please visit the following URL: https://docs.IAM.amazon.com/IAM/latest/UserGuide/id root-user.html
The correct answers are: Delete the access keys for the root account Confirm MFA to a secure device. Change the password for the root account
Submit Your Feedback/Queries to our Experts

NEW QUESTION 133
- (Exam Topic 3)
You have a set of application , database and web servers hosted in IAM. The web servers are placed behind an ELB. There are separate security groups for the application, database and web servers. The network security groups have been defined accordingly. There is an issue with the communication between the application and database servers. In order to troubleshoot the issue between just the application and database server, what is the ideal set of MINIMAL steps you would take?
Please select:

A. Check the Inbound security rules for the database security group Check the Outbound security rules forthe application security group
B. Check the Outbound security rules for the database security group I Check the inbound security rules for the application security group
C. Check the both the Inbound and Outbound security rules for the database security group Check the inbound security rules for the application security group
D. Check the Outbound security rules for the database security groupCheck the both the Inbound and Outbound security rules for the application security group

Answer: A

Explanation:
Here since the communication would be established inward to the database server and outward from the application server, you need to ensure that just the Outbound rules for application server security groups are checked. And then just the Inbound rules for database server security groups are checked.
Option B can't be the correct answer. It says that we need to check the outbound security group which is not needed.
We need to check the inbound for DB SG and outbound of Application SG. Because, this two group need to communicate with each other to function properly.
Option C is invalid because you don't need to check for Outbound security rules for the database security group
Option D is invalid because you don't need to check for Inbound security rules for the application security group
For more information on Security Groups, please refer to below URL:
The correct answer is: Check the Inbound security rules for the database security group Check the Outbound security rules for the application security group
Submit your Feedback/Queries to our Experts

NEW QUESTION 138
- (Exam Topic 3)
You need to ensure that the cloudtrail logs which are being delivered in your IAM account is encrypted. How can this be achieved in the easiest way possible?
Please select:

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

Answer: A

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

NEW QUESTION 139
- (Exam Topic 3)
Your company has many IAM accounts defined and all are managed via IAM Organizations. One IAM account has a S3 bucket that has critical data. How can we ensure that all the users in the IAM organisation have access to this bucket?
Please select:

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

Answer: A

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

NEW QUESTION 140
- (Exam Topic 3)
A company has several Customer Master Keys (CMK), some of which have imported key material. Each CMK must be rotated annually.
What two methods can the security team use to rotate each key? Select 2 answers from the options given below Please select:

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

Answer: AD

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

NEW QUESTION 144
- (Exam Topic 3)
You have an Amazon VPC that has a private subnet and a public subnet in which you have a NAT instance server. You have created a group of EC2 instances that configure themselves at startup by downloading a bootstrapping script from S3 that deploys an application via GIT.
Which one of the following setups would give us the highest level of security? Choose the correct answer from the options given below.
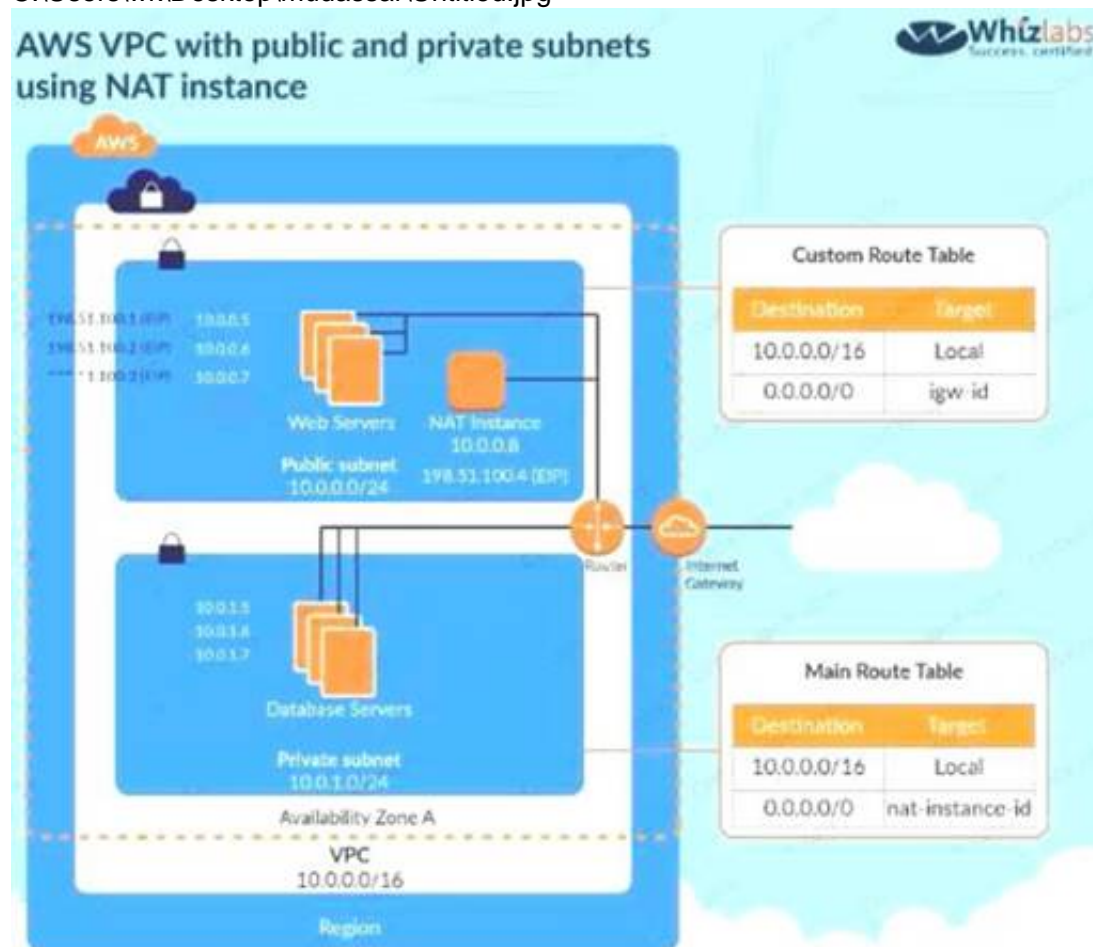Please select:

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

Answer: D

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

AWS VPC with public and private subnets using NAT instance

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

NEW QUESTION 148
- (Exam Topic 3)
A company has set up the following structure to ensure that their S3 buckets always have logging enabled

If there are any changes to the configuration to an S3 bucket, a config rule gets checked. If logging is disabled, then Lambda function is invoked. This Lambda function will again enable logging on the S3 bucket. Now there is an issue being encoutered with the entire flow. You have verified that the Lambda function is being invoked. But when logging is disabled for the bucket, the lambda function does not enable it again. Which of the following could be an issue
Please select:

A. The IAM Config rule is not configured properly
B. The IAM Lambda function does not have appropriate permissions for the bucket
C. The IAM Lambda function should use Node.js instead of python.
D. You need to also use the API gateway to invoke the lambda function

Answer: B

Explanation:
The most probable cause is that you have not allowed the Lambda functions to have the appropriate permissions on the S3 bucket to make the relevant changes. Option A is invalid because this is more of a permission instead of a configuration rule issue. Option C is invalid because changing the language will not be the core solution.
Option D is invalid because you don't necessarily need to use the API gateway service
For more information on accessing resources from a Lambda function, please refer to below URL https://docs.IAM.amazon.com/lambda/latest/ds/accessing-resources.htmll
The correct answer is: The IAM Lambda function does not have appropriate permissions for the bucket Submit your Feedback/Queries to our Experts

NEW QUESTION 150
- (Exam Topic 3)
A company hosts critical data in an S3 bucket. Even though they have assigned the appropriate permissions to the bucket, they are still worried about data deletion. What measures can be taken to restrict the risk of data deletion on the bucket. Choose 2 answers from the options given below
Please select:

A. Enable versioning on the S3 bucket
B. Enable data at rest for the objects in the bucket
C. Enable MFA Delete in the bucket policy
D. Enable data in transit for the objects in the bucket

Answer: AC

Explanation:
One of the IAM Security blogs mentions the followinj
Versioning keeps multiple versions of an object in the same bucket. When you enable it on a bucket Amazon S3 automatically adds a unique version ID to every object stored in the bucket. At that point, a simple DELETE action does not permanently delete an object version; it merely associates a delete marker with the object. If you want to permanently delete an object version, you must specify its version ID in your DELETE request.
You can add another layer of protection by enabling MFA Delete on a versioned bucket. Once you do so, you must provide your IAM accounts access keys and a valid code from the account's MFA device in order to permanently delete an object version or suspend or reactivate versioning on the bucket.
Option B is invalid because enabling encryption does not guarantee risk of data deletion. Option D is invalid because this option does not guarantee risk of data deletion.
For more information on IAM S3 versioning and MFA please refer to the below URL: https://IAM.amazon.com/blogs/security/securing-access-to-IAM-using-mfa-part-3/
The correct answers are: Enable versioning on the S3 bucket Enable MFA Delete in the bucket policy Submit your Feedback/Queries to our Experts

NEW QUESTION 153
- (Exam Topic 3)
A web application runs in a VPC on EC2 instances behind an ELB Application Load Balancer. The application stores data in an RDS MySQL DB instance. A Linux bastion host is used to apply schema updates to the database - administrators connect to the host via SSH from a corporate workstation. The following security groups are applied to the infrastructure
* sgLB - associated with the ELB
* sgWeb - associated with the EC2 instances.
* sgDB - associated with the database
* sgBastion - associated with the bastion host Which security group configuration will allow the application to be secure and functional?
Please select:

A. sgLB :allow port 80 and 443 traffic from 0.0.0.0/0 sgWeb :allow port 80 and 443 traffic from 0.0.0.0/0 sgDB :allow port 3306 traffic from sgWeb and sgBastionsgBastion: allow port 22 traffic from the corporate IP address range
B. sgLB :allow port 80 and 443 traffic from 0.0.0.0/0 sgWeb :allow port 80 and 443 traffic from sgLB sgDB :allow port 3306 traffic from sgWeb and sgLBsgBastion: allow port 22 traffic from the VPC IP address range
C. sgLB :allow port 80 and 443 traffic from 0.0.0.0/0 sgWeb :allow port 80 and 443 traffic from sgLBsgDB :allow port 3306 traffic from sgWeb and sgBastion sgBastion: allow port 22 traffic from the VPC IP address range
D. sgLB :allow port 80 and 443 traffic from 0.0.0.0/0 sgWeb :allow port 80 and 443 traffic from sgLBsgDB :allow port 3306 traffic from sgWeb and sgBastion sgBastion: allow port 22 traffic from the corporate IP address range

Answer: D

Explanation:
The Load Balancer should accept traffic on ow port 80 and 443 traffic from 0.0.0.0/0 The backend EC2 Instances should accept traffic from the Load Balancer
The database should allow traffic from the Web server
And the Bastion host should only allow traffic from a specific corporate IP address range Option A is incorrect because the Web group should only allow traffic from the Load balancer For more information on IAM Security Groups, please refer to below URL: https://docs.IAM.amazon.com/IAMEC2/latest/UserGuide/usins-

network-security.htmll

The correct answer is: sgLB :allow port 80 and 443 traffic from 0.0.0.0/0 sgWeb :allow port 80 and 443 traffic from sgLB

sgDB :allow port 3306 traffic from sgWeb and sgBastion sgBastion: allow port 22 traffic from the corporate IP address range Submit your Feedback/Queries to our Experts

NEW QUESTION 158
- (Exam Topic 3)
Your company has defined a set of S3 buckets in IAM. They need to monitor the S3 buckets and know the source IP address and the person who make requests to the S3 bucket. How can this be achieved?
Please select:

A. Enable VPC flow logs to know the source IP addresses
B. Monitor the S3 API calls by using Cloudtrail logging
C. Monitor the S3 API calls by using Cloudwatch logging
D. Enable IAM Inspector for the S3 bucket

Answer: B

Explanation:
The IAM Documentation mentions the following
Amazon S3 is integrated with IAM CloudTrail. CloudTrail is a service that captures specific API calls made to Amazon S3 from your IAM account and delivers the log files to an Amazon S3 bucket that you specify. It captures API calls made from the Amazon S3 console or from the Amazon S3 API.
Using the information collected by CloudTrail, you can determine what request was made to Amazon S3, the source IP address from which the request was made, who made the request when it was made, and so on Options A,C and D are invalid because these services cannot be used to get the source IP address of the calls to S3 buckets
For more information on Cloudtrail logging, please refer to the below Link: https://docs.IAM.amazon.com/AmazonS3/latest/dev/cloudtrail-logeins.htmll
The correct answer is: Monitor the S3 API calls by using Cloudtrail logging Submit your Feedback/Queries to our Experts

NEW QUESTION 162
- (Exam Topic 3)
Your team is experimenting with the API gateway service for an application. There is a need to implement a custom module which can be used for authentication/authorization for calls made to the API gateway. How can this be achieved?
Please select:

A. Use the request parameters for authorization
B. Use a Lambda authorizer
C. Use the gateway authorizer
D. Use CORS on the API gateway

Answer: B

Explanation:
The IAM Documentation mentions the following
An Amazon API Gateway Lambda authorizer (formerly known as a custom authorize?) is a Lambda function that you provide to control access to your API methods. A Lambda authorizer uses bearer token authentication strategies, such as OAuth or SAML. It can also use information described by headers, paths, query strings, stage variables, or context variables request parameters.
Options A,C and D are invalid because these cannot be used if you need a custom authentication/authorization for calls made to the API gateway
For more information on using the API gateway Lambda authorizer please visit the URL:
https://docs.IAM.amazon.com/apisateway/latest/developerguide/apieateway-use-lambda-authorizer.htmll The correct answer is: Use a Lambda authorizer
Submit your Feedback/Queries to our Experts

NEW QUESTION 167
- (Exam Topic 3)
You need to create a Linux EC2 instance in IAM. Which of the following steps is used to ensure secure authentication the EC2 instance from a windows machine. Choose 2 answers from the options given below.
Please select:

A. Ensure to create a strong password for logging into the EC2 Instance
B. Create a key pair using putty
C. Use the private key to log into the instance
D. Ensure the password is passed securely using SSL

Answer: BC

Explanation:
The IAM Documentation mentions the following
You can use Amazon EC2 to create your key pair. Alternatively, you could use a third-party tool and then import the public key to Amazon EC2. Each key pair requires a name. Be sure to choose a name that is easy to remember. Amazon EC2 associates the public key with the name that you specify as the key name. Amazon EC2 stores the public key only, and you store the private key. Anyone who possesses your private key can decrypt login information, so it's important that you store your private keys in a secure place.
Options A and D are incorrect since you should use key pairs for secure access to Ec2 Instances For more information on EC2 key pairs, please refer to below URL: https://docs.IAM.amazon.com/IAMEC2/latest/UserGuide/ec2-key-pairs.html
The correct answers are: Create a key pair using putty. Use the private key to log into the instance Submit your Feedback/Queries to our Experts

NEW QUESTION 168
- (Exam Topic 3)
A Devops team is currently looking at the security aspect of their CI/CD pipeline. They are making use of IAM resource? for their infrastructure. They want to ensure that the EC2 Instances don't have any high security vulnerabilities. They want to ensure a complete DevSecOps process. How can this be achieved?
Please select:

A. Use IAM Config to check the state of the EC2 instance for any sort of security issues.
B. Use IAM Inspector API's in the pipeline for the EC2 Instances
C. Use IAM Trusted Advisor API's in the pipeline for the EC2 Instances
D. Use IAM Security Groups to ensure no vulnerabilities are present

Answer: B

Explanation:
Amazon Inspector offers a programmatic way to find security defects or misconfigurations in your operating systems and applications. Because you can use API calls to access both the processing of assessments and the results of your assessments, integration of the findings into workflow and notification systems is simple.
DevOps teams can integrate Amazon Inspector into their CI/CD pipelines and use it to identify any pre-existing issues or when new issues are introduced.
Option A.C and D are all incorrect since these services cannot check for Security Vulnerabilities. These can only be checked by the IAM Inspector service.
For more information on IAM Security best practices, please refer to below URL: https://d1.IAMstatic.com/whitepapers/Security/IAM Security Best Practices.pdl
The correct answer is: Use IAM Inspector API's in the pipeline for the EC2 Instances Submit your Feedback/Queries to our Experts

NEW QUESTION 169
- (Exam Topic 3)
You have a bucket and a VPC defined in IAM. You need to ensure that the bucket can only be accessed by the VPC endpoint. How can you accomplish this?
Please select:

A. Modify the security groups for the VPC to allow access to the 53 bucket
B. Modify the route tables to allow access for the VPC endpoint
C. Modify the IAM Policy for the bucket to allow access for the VPC endpoint
D. Modify the bucket Policy for the bucket to allow access for the VPC endpoint

Answer: D

Explanation:
This is mentioned in the IAM Documentation Restricting Access to a Specific VPC Endpoint
The following is an example of an S3 bucket policy that restricts access to a specific bucket, examplebucket only from the VPC endpoint with the ID vpce-la2b3c4d. The policy denies all access to the bucket if the specified endpoint is not being used. The IAM:sourceVpce condition is used to the specify the endpoint. The IAM:sourceVpce condition does not require an ARN for the VPC endpoint resource, only the VPC endpoint ID. For more information about using conditions in a policy, see Specifying Conditions in a Policy.
Options A and B are incorrect because using Security Groups nor route tables will help to allow access specifically for that bucke via the VPC endpoint Here you specifically need to ensure the bucket policy is changed.
Option C is incorrect because it is the bucket policy that needs to be changed and not the IAM policy. For more information on example bucket policies for VPC endpoints, please refer to below URL:
> https://docs.IAM.amazon.com/AmazonS3/latest/dev/example-bucket-policies-vpc-endpoint.html
The correct answer is: Modify the bucket Policy for the bucket to allow access for the VPC endpoint Submit your Feedback/Queries to our Experts

NEW QUESTION 172
- (Exam Topic 3)
Company policy requires that all insecure server protocols, such as FTP, Telnet, HTTP, etc be disabled on all servers. The security team would like to regularly check all servers to ensure compliance with this requirement by using a scheduled CloudWatch event to trigger a review of the current infrastructure. What process will check compliance of the company's EC2 instances?
Please select:

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

Answer: D

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

NEW QUESTION 175
- (Exam Topic 3)
A company has external vendors that must deliver files to the company. These vendors have cross-account that gives them permission to upload objects to one of the company's S3 buckets.
What combination of steps must the vendor follow to successfully deliver a file to the company? Select 2 answers from the options given below
Please select:

A. Attach an IAM role to the bucket that grants the bucket owner full permissions to the object
B. Add a grant to the objects ACL giving full permissions to bucket owner.
C. Encrypt the object with a KMS key controlled by the company.
D. Add a bucket policy to the bucket that grants the bucket owner full permissions to the object

E. Upload the file to the company's S3 bucket

Answer: BE

Explanation:
This scenario is given in the IAM Documentation
A bucket owner can enable other IAM accounts to upload objects. These objects are owned by the accounts that created them. The bucket owner does not own objects that were not created by the bucket owner. Therefore, for the bucket owner to grant access to these objects, the object owner must first grant permission to the bucket owner using an object ACL. The bucket owner can then delegate those permissions via a bucket policy. In this example, the bucket owner delegates permission to users in its own account.
C:\Users\wk\Desktop\mudassar\Untitled.jpg
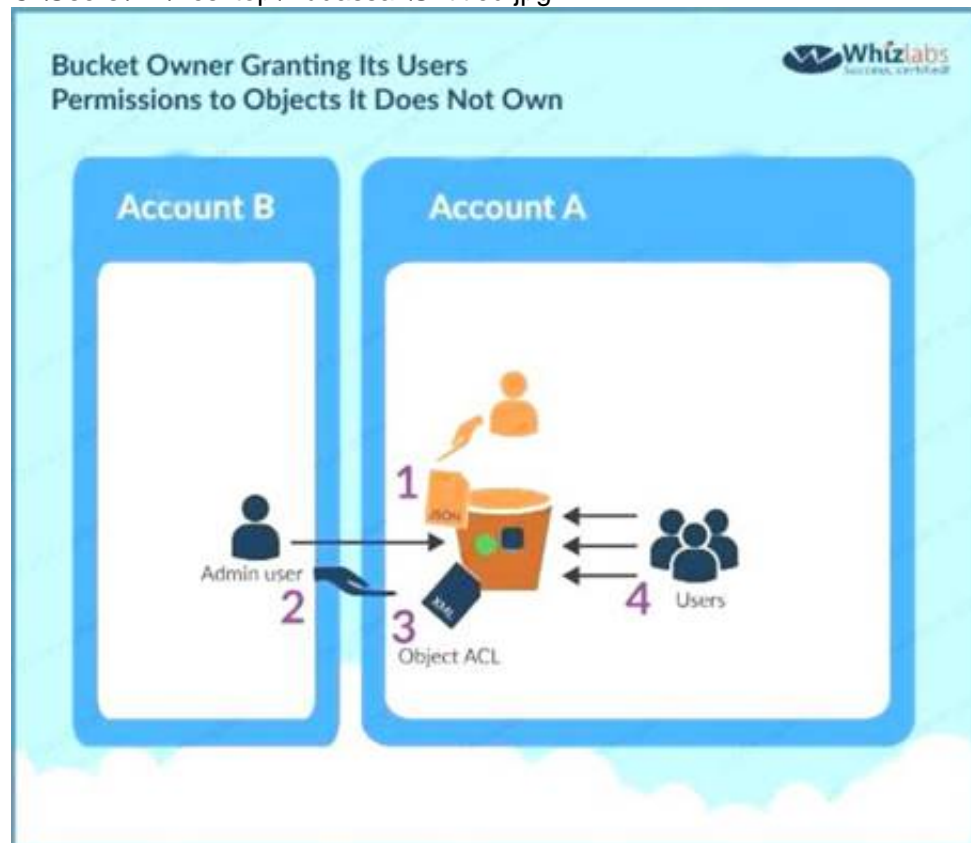
Option A and D are invalid because bucket ACL's are used to give grants to bucket Option C is not required since encryption is not part of the requirement For more information on this scenario please see the below Link:
https://docs.IAM.amazon.com/AmazonS3/latest/dev/example-walkthroushs-manaeing-access-example3.htmll The correct answers are: Add a grant to the objects ACL giving full permissions to bucket owner., Upload the file to the company's S3 bucket
Submit your Feedback/Queries to our Experts

NEW QUESTION 177
- (Exam Topic 3)
A security engineer must ensure that all infrastructure launched in the company IAM account be monitored for deviation from compliance rules, specifically that all EC2 instances are launched from one of a specified list of AM Is and that all attached EBS volumes are encrypted. Infrastructure not in compliance should be terminated. What combination of steps should the Engineer implement? Select 2 answers from the options given below.
Please select:

A. Set up a CloudWatch event based on Trusted Advisor metrics
B. Trigger a Lambda function from a scheduled CloudWatch event that terminates non-compliant infrastructure.
C. Set up a CloudWatch event based on Amazon inspector findings
D. Monitor compliance with IAM Config Rules triggered by configuration changes
E. Trigger a CLI command from a CloudWatch event that terminates the infrastructure

Answer: BD

Explanation:
You can use IAM Config to monitor for such Event
Option A is invalid because you cannot set Cloudwatch events based on Trusted Advisor checks.
Option C is invalid Amazon inspector cannot be used to check whether instances are launched from a specific A
Option E is invalid because triggering a CLI command is not the preferred option, instead you should use Lambda functions for all automation purposes.
For more information on Config Rules please see the below Link: https://docs.IAM.amazon.com/config/latest/developerguide/evaluate-config-rules.html
These events can then trigger a lambda function to terminate instances For more information on Cloudwatch events please see the below Link:
https://docs.IAM.amazon.com/AmazonCloudWatch/latest/events/WhatlsCloudWatchEvents. (
The correct answers are: Trigger a Lambda function from a scheduled Cloudwatch event that terminates
non-compliant infrastructure., Monitor compliance with IAM Config Rules triggered by configuration changes
Submit your Feedback/Queries to our Experts

NEW QUESTION 178
- (Exam Topic 3)
You are trying to use the IAM Systems Manager run command on a set of Instances. The run command on a set of Instances. What can you do to diagnose the issue? Choose 2 answers from the options given
Please select:

A. Ensure that the SSM agent is running on the target machine
B. Check the /var/log/amazon/ssm/errors.log file
C. Ensure the right AMI is used for the Instance
D. Ensure the security groups allow outbound communication for the instance

Answer: AB

Explanation:
The IAM Documentation mentions the following
If you experience problems executing commands using Run Command, there might be a problem with the SSM Agent. Use the following information to help you troubleshoot the agent
View Agent Logs
The SSM Agent logs information in the following files. The information in these files can help you troubleshoot problems.
On Windows
%PROGRAMDATA%\Amazon\SSM\Logs\amazon-ssm-agent.log
%PROGRAMDATA%\Amazon\SSM\Logs\error.log
The default filename of the seelog is seelog-xml.template. If you modify a seelog, you must rename the file to seelog.xml.
On Linux
/var/log/amazon/ssm/amazon-ssm-agentlog /var/log/amazon/ssm/errors.log
Option C is invalid because the right AMI has nothing to do with the issues. The agent which is used to execute run commands can run on a variety of AMI'S
Option D is invalid because security groups does not come into the picture with the communication between the agent and the SSM service
For more information on troubleshooting IAM SSM, please visit the following URL: https://docs.IAM.amazon.com/systems-manaeer/latest/userguide/troubleshootine-remote-commands.htmll The correct answers are: Ensure that the SSM agent is running on the target machine. Check the
/var/log/amazon/ssm/errors.log file
Submit your Feedback/Queries to our Experts

NEW QUESTION 183
- (Exam Topic 3)
You are trying to use the Systems Manager to patch a set of EC2 systems. Some of the systems are not getting covered in the patching process. Which of the following can be used to troubleshoot the issue? Choose 3 answers from the options given below.
Please select:

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

Answer: ACD

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

NEW QUESTION 188
- (Exam Topic 3)
Your team is designing a web application. The users for this web application would need to sign in via an external ID provider such asfacebook or Google. Which of the following IAM service would you use for authentication?
Please select:

A. IAM Cognito
B. IAM SAML
C. IAM IAM
D. IAM Config

Answer: A

Explanation:
The IAM Documentation mentions the following
Amazon Cognito provides authentication, authorization, and user management for your web and mobile apps. Your users ca sign in directly with a user name and password, or through a third party such as Facebook, Amazon, or Google.
Option B is incorrect since this is used for identity federation
Option C is incorrect since this is pure Identity and Access management Option D is incorrect since IAM is a configuration service
For more information on IAM Cognito please refer to the below Link: https://docs.IAM.amazon.com/coenito/latest/developerguide/what-is-amazon-cognito.html The correct answer is: IAM Cognito
Submit your Feedback/Queries to our Experts

NEW QUESTION 190
- (Exam Topic 3)
You work as an administrator for a company. The company hosts a number of resources using IAM. There is an incident of a suspicious API activity which occurred 11 days ago. The Security Admin has asked to get the API activity from that point in time. How can this be achieved?
Please select:

A. Search the Cloud Watch logs to find for the suspicious activity which occurred 11 days ago
B. Search the Cloudtrail event history on the API events which occurred 11 days ago.
C. Search the Cloud Watch metrics to find for the suspicious activity which occurred 11 days ago

D. Use IAM Config to get the API calls which were made 11 days ago.

Answer: B

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

NEW QUESTION 194
- (Exam Topic 3)
A company has a legacy application that outputs all logs to a local text file. Logs from all applications running on IAM must be continually monitored for security related messages.
What can be done to allow the company to deploy the legacy application on Amazon EC2 and still meet the monitoring requirement? Please select:

A. Create a Lambda function that mounts the EBS volume with the logs and scans the logs for security incident
B. Trigger the function every 5 minutes with a scheduled Cloudwatch event.
C. Send the local text log files to CloudWatch Logs and configure a CloudWatch metric filte
D. Trigger cloudwatch alarms based on the metrics.
E. Install the Amazon inspector agent on any EC2 instance running the legacy applicatio
F. Generate CloudWatch alerts a based on any Amazon inspector findings.
G. Export the local text log files to CloudTrai
H. Create a Lambda function that queries the CloudTrail logs for security ' incidents using Athena.

Answer: B

Explanation:
One can send the log files to Cloudwatch Logs. Log files can also be sent from On-premise servers. You can then specify metrii to search the logs for any specific values. And then create alarms based on these metrics.
Option A is invalid because this will be just a long over drawn process to achieve this requirement Option C is invalid because IAM Inspector cannot be used to monitor for security related messages. Option D is invalid because files cannot be exported to IAM Cloudtrail
For more information on Cloudwatch logs agent please visit the below URL:
https://docs.IAM.amazon.com/AmazonCloudWatch/latest/logs/QuickStartEC2Instance.hti
The correct answer is: Send the local text log files to Cloudwatch Logs and configure a Cloudwatch metric filter. Trigger cloudwatch alarms based on the metrics.
Submit your Feedback/Queries to our Experts

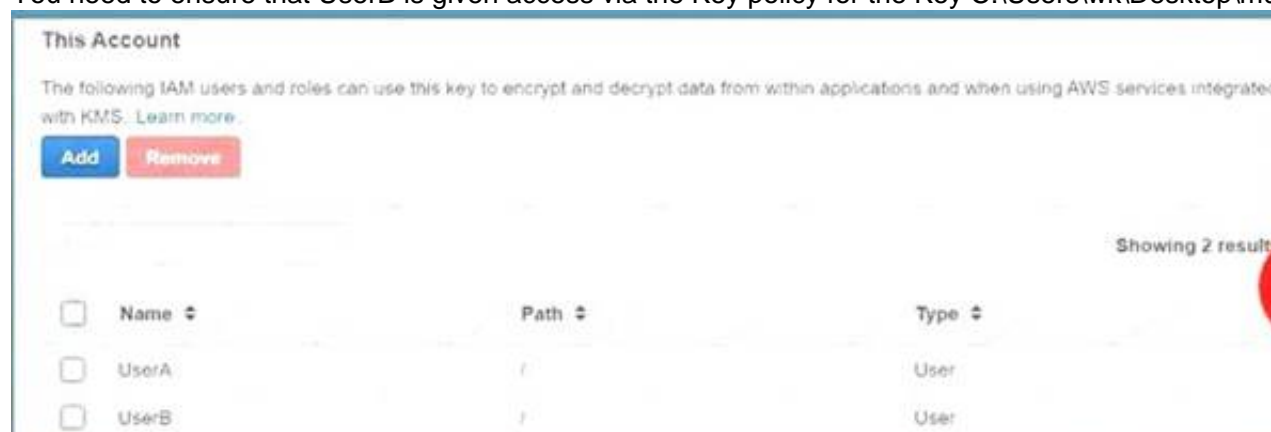**NEW QUESTION 199**
- (Exam Topic 3)
Your developer is using the KMS service and an assigned key in their Java program. They get the below error when running the code
arn:IAM:iam::113745388712:user/UserB is not authorized to perform: kms:DescribeKey Which of the following could help resolve the issue?
Please select:

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

Answer: C

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

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

NEW QUESTION 202
- (Exam Topic 3)
Your company use IAM KMS for management of its customer keys. From time to time, there is a requirement to delete existing keys as part of housekeeping activities. What can be done during the deletion process to verify that the key is no longer being used.

Please select:

A. Use CloudTrail to see if any KMS API request has been issued against existing keys
B. Use Key policies to see the access level for the keys
C. Rotate the keys once before deletion to see if other services are using the keys
D. Change the IAM policy for the keys to see if other services are using the keys

Answer: A

Explanation:
The IAM lentation mentions the following
You can use a combination of IAM CloudTrail, Amazon CloudWatch Logs, and Amazon Simple Notification Service (Amazon SNS) to create an alarm that notifies you of IAM KMS API requests that attempt to use a customer master key (CMK) that is pending deletion. If you receive a notification from such an alarm, you might want to cancel deletion of the CMK to give yourself more time to determine whether you want to delete it
Options B and D are incorrect because Key policies nor IAM policies can be used to check if the keys are being used.
Option C is incorrect since rotation will not help you check if the keys are being used. For more information on deleting keys, please refer to below URL:
https://docs.IAM.amazon.com/kms/latest/developereuide/deletine-keys-creatine-cloudwatch-alarm.html
The correct answer is: Use CloudTrail to see if any KMS API request has been issued against existing keys Submit your Feedback/Queries to our Experts

NEW QUESTION 205
- (Exam Topic 3)
You have a requirement to conduct penetration testing on the IAM Cloud for a couple of EC2 Instances. How could you go about doing this? Choose 2 right answers from the options given below.
Please select:

A. Get prior approval from IAM for conducting the test
B. Use a pre-approved penetration testing tool.
C. Work with an IAM partner and no need for prior approval request from IAM
D. Choose any of the IAM instance type

Answer: AB

Explanation:
You can use a pre-approved solution from the IAM Marketplace. But till date the IAM Documentation still mentions that you have to get prior approval before conducting a test on the IAM Cloud for EC2 Instances.
Option C and D are invalid because you have to get prior approval first. IAM Docs Provides following details:
"For performing a penetration test on IAM resources first of all we need to take permission from IAM and complete a requisition form and submit it for approval. The form should contain information about the
instances you wish to test identify the expected start and end dates/times of your test and requires you to read and agree to Terms and Conditions specific to penetration testing and to the use of appropriate tools for testing. Note that the end date may not be more than 90 days from the start date."
At this time, our policy does not permit testing small or micro RDS instance types. Testing of ml .small, t1
.m icro or t2.nano EC2 instance types is not permitted.
For more information on penetration testing please visit the following URL: https://IAM.amazon.eom/security/penetration-testine/l
The correct answers are: Get prior approval from IAM for conducting the test Use a pre-approved penetration testing tool. Submit your Feedback/Queries to our Experts

NEW QUESTION 209
- (Exam Topic 3)
In order to encrypt data in transit for a connection to an IAM RDS instance, which of the following would you implement
Please select:

A. Transparent data encryption
B. SSL from your application
C. Data keys from IAM KMS
D. Data Keys from CloudHSM

Answer: B

Explanation:
This is mentioned in the IAM Documentation
You can use SSL from your application to encrypt a connection to a DB instance running MySQL MariaDB, Amazon Aurora, SQL Server, Oracle, or PostgreSQL.
Option A is incorrect since Transparent data encryption is used for data at rest and not in transit Options C and D are incorrect since keys can be used for encryption of data at rest
For more information on working with RDS and SSL, please refer to below URL:
https://docs.IAM.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.SSL.html
The correct answer is: SSL from your application Submit your Feedback/Queries to our Experts

NEW QUESTION 213
- (Exam Topic 4)
Within a VPC, a corporation runs an Amazon RDS Multi-AZ DB instance. The database instance is connected to the internet through a NAT gateway via two subnets.
Additionally, the organization has application servers that are hosted on Amazon EC2 instances and use the RDS database. These EC2 instances have been deployed onto two more private subnets inside the same VPC. These EC2 instances connect to the internet through a default route via the same NAT gateway. Each VPC subnet has its own route table.
The organization implemented a new security requirement after a recent security examination. Never allow the database instance to connect to the internet. A security engineer must perform this update promptly without interfering with the network traffic of the application servers.
How will the security engineer be able to comply with these requirements?

A. Remove the existing NAT gatewa
B. Create a new NAT gateway that only the application server subnets can use.

C. Configure the DB instance€™s inbound network ACL to deny traffic from the security group ID of the NAT gateway.
D. Modify the route tables of the DB instance subnets to remove the default route to the NAT gateway.
E. Configure the route table of the NAT gateway to deny connections to the DB instance subnets.

Answer: C

Explanation:
Each subnet has a route table, so modify the routing associated with DB instance subnets to prevent internet access.

NEW QUESTION 218
- (Exam Topic 4)
A Security Engineer has been tasked with enabling IAM Security Hub to monitor Amazon EC2 instances fix CVE in a single IAM account The Engineer has already enabled IAM Security Hub and Amazon Inspector m the IAM Management Console and has installed me Amazon Inspector agent on an EC2 instances that need to be monitored.
Which additional steps should the Security Engineer lake 10 meet this requirement?

A. Configure the Amazon inspector agent to use the CVE rule package
B. Configure the Amazon Inspector agent to use the CVE rule package Configure Security Hub to ingest from IAM inspector by writing a custom resource policy
C. Configure the Security Hub agent to use the CVE rule package Configure IAM Inspector lo ingest from Security Hub by writing a custom resource policy
D. Configure the Amazon Inspector agent to use the CVE rule package Install an additional Integration library Allow the Amazon Inspector agent to communicate with Security Hub

Answer: D

NEW QUESTION 219
- (Exam Topic 4)
A company uses a third-party application to store encrypted data in Amazon S3. The company uses another third-party application trial decrypts the data from Amazon S3 to ensure separation of duties Between the applications A Security Engineer warns to separate the permissions using IAM roles attached to Amazon EC2 instances. The company prefers to use native IAM services.
Which encryption method will meet these requirements?

A. Use encrypted Amazon EBS volumes with Amazon default keys (IAM EBS)
B. Use server-side encryption with customer-provided keys (SSE-C)
C. Use server-side encryption with IAM KMS managed keys (SSE-KMS)
D. Use server-side encryption with Amazon S3 managed keys (SSE-S3)

Answer: C

NEW QUESTION 221
- (Exam Topic 4)
A company's cloud operations team is responsible for building effective security for IAM cross-account access. The team asks a security engineer to help troubleshoot why some developers in the developer account (123456789012) in the developers group are not able to assume a cross-account role (ReadS3) into a production account (999999999999) to read the contents of an Amazon S3 bucket (productionapp). The two account policies are as follows:

```
Developer account 123456789012:
Developer group permissions:
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "sts:AssumeRole",
        "Resource": "arn:aws:iam::999999999999:role/ReadS3"
    }
}


Production account 999999999999:
Production account ReadS3 role policy:
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:ListAllMyBuckets",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
Production account ReadS3 role policy - trust relationship:
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::888888888888:root"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "BoolIfExists": {
                    "aws:MultiFactorAuthPresent": "true"
                }
            }
        }
    ]
}
```

Which recommendations should the security engineer make to resolve this issue? (Select TWO.)

A. Ask the developers to change their password and use a different web browser.
B. Ensure that developers are using multi-factor authentication (MFA) when they log in to their developer account as the developer role.
C. Modify the production account ReadS3 role policy to allow the PutBucketPolicy action on the productionapp S3 bucket.
D. Update the trust relationship policy on the production account S3 role to allow the account number of the developer account.
E. Update the developer group permissions in the developer account to allow access to the productionapp S3 bucket.

Answer: AD

NEW QUESTION 226
- (Exam Topic 4)
A company's IAM account consists of approximately 300 IAM users. Now there is a mandate that an access change is required for 100 IAM users to have unlimited privileges to S3.As a system administrator, how can you implement this effectively so that there is no need to apply the policy at the individual user level?
Please select:

A. Create a new role and add each user to the IAM role
B. Use the IAM groups and add users, based upon their role, to different groups and apply the policy to group
C. Create a policy and apply it to multiple users using a JSON script
D. Create an S3 bucket policy with unlimited access which includes each user's IAM account ID

Answer: B

Explanation:
Option A is incorrect since you don't add a user to the IAM Role Option C is incorrect since you don't assign multiple users to a policy Option D is incorrect since this is not an ideal approach
An IAM group is used to collectively manage users who need the same set of permissions. By having groups, it becomes easier to manage permissions. So if you change the permissions on the group scale, it will affect all the users in that group
For more information on IAM Groups, just browse to the below URL: https://docs.IAM.amazon.com/IAM/latest/UserGuide/id_eroups.html
The correct answer is: Use the IAM groups and add users, based upon their role, to different groups and apply the policy to group

Submit your Feedback/Queries to our Experts

NEW QUESTION 231
- (Exam Topic 4)
An IT department currently has a Java web application deployed on Apache Tomcat running on Amazon EC2 instances. All traffic to the EC2 instances is sent through an internet-facing Application Load Balancer (ALB)
The Security team has noticed during the past two days thousands of unusual read requests coming from hundreds of IP addresses. This is causing the Tomcat server to run out of threads and reject new connections
Which the SIMPLEST change that would address this server issue?

A. Create an Amazon CloudFront distribution and configure the ALB as the origin
B. Block the malicious IPs with a network access list (NACL).
C. Create an IAM Web Application Firewall (WAF). and attach it to the ALB
D. Map the application domain name to use Route 53

Answer: A

NEW QUESTION 232
- (Exam Topic 4)
A company has implemented IAM WAF and Amazon CloudFront for an application. The application runs on Amazon EC2 instances that are part of an Auto Scaling group. The Auto Scaling group is behind an Application Load Balancer (ALB).
The IAM WAF web ACL uses an IAM Managed Rules rule group and is associated with the CloudFront distribution. CloudFront receives the request from IAM WAF and then uses the ALB as the distribution's origin.
During a security review, a security engineer discovers that the infrastructure is susceptible to a large, layer 7 DDoS attack.
How can the security engineer improve the security at the edge of the solution to defend against this type of attack?

A. Configure the CloudFront distribution to use the Lambda@Edge featur
B. Create an IAM Lambda function that imposes a rate limit on CloudFront viewer request
C. Block the request if the rate limit is exceeded.
D. Configure the IAM WAF web ACL so that the web ACL has more capacity units to process all IAM WAF rules faster.
E. Configure IAM WAF with a rate-based rule that imposes a rate limit that automatically blocks requests when the rate limit is exceeded.
F. Configure the CloudFront distribution to use IAM WAF as its origin instead of the ALB.

Answer: C

NEW QUESTION 235
- (Exam Topic 4)
A company wants to protect its website from man in-the-middle attacks by using Amazon CloudFront. Which solution will meet these requirements with the LEAST operational overhead?

A. Use the SimpleCORS managed response headers policy.
B. Use a Lambda@Edge function to add the Strict-Transport-Security response header.
C. Use the SecurityHeadersPolicy managed response headers policy.
D. Include the X-XSS-Protection header in a custom response headers policy.

Answer: C

Explanation:
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/using-managed-response-headers-poli The SecurityHeadersPolicy is a managed policy provided by Amazon CloudFront that includes a set of recommended security headers to enhance the security of your website. These headers help protect against various types of attacks, including man-in-the-middle attacks. By applying the SecurityHeadersPolicy to your CloudFront distribution, the necessary security headers will be automatically added to the responses sent by CloudFront. This reduces operational overhead because you don't have to manually configure or manage the headers yourself.

NEW QUESTION 238
- (Exam Topic 4)
A security engineer needs to create an IAM Key Management Service <IAM KMS) key that will De used to encrypt all data stored in a company's Amazon S3 Buckets in the us-west-1 Region. The key will use
server-side encryption. Usage of the key must be limited to requests coming from Amazon S3 within the company's account.
Which statement in the KMS key policy will meet these requirements?
A)

```
{
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
    },
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:ViaService": "s3.us-west-1.amazonaws.com",
            "kms:CallerAccount": "<CustomerAccountID>"
        }
    }
}
```

B)

```
{
    "Effect": "Allow",
    "Principal": {
        "AWS": "s3.us-west-1.amazonaws.com"
    },
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:CallerAccount": "<CustomerAccountID>"
        }
    }
}
```

C)

```
{
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
    },
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:EncryptionContext:aws:s3:arn": [
                "arn:aws:s3:::*"
            ],
```

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

Answer: A

NEW QUESTION 240
- (Exam Topic 4)
A developer is building a serverless application hosted on AWS that uses Amazon Redshift as a data store The application has separate modules for readwrite and read-only functionality The modules need their own database users for compliance reasons
Which combination of steps should a security engineer implement to grant appropriate access? (Select TWO.)

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

Answer: A

Explanation:
To grant appropriate access to separate modules for read-write and read-only functionality in a serverless application hosted on AWS that uses Amazon Redshift as a data store, a security engineer should configure cluster security groups for each application module to control access to database users that are required for read-only and readwrite, and configure an IAM policy for each module specifying the ARN of an IAM user that allows the GetClusterCredentials API call.
References: : Amazon Redshift - Amazon Web Services : Amazon Redshift - Amazon Web Services : Identity and Access Management - AWS Management Console : AWS Identity and Access Management - AWS Management Console

NEW QUESTION 245
- (Exam Topic 4)
For compliance reasons a Security Engineer must produce a weekly report that lists any instance that does not have the latest approved patches applied. The Engineer must also ensure that no system goes more than 30 days without the latest approved updates being applied
What would the MOST efficient way to achieve these goals?

A. Use Amazon inspector to determine which systems do not have the latest patches applied, and after 30 days, redeploy those instances with the latest AMI version
B. Configure Amazon EC2 Systems Manager to report on instance patch compliance and enforce updates during the defined maintenance windows
C. Examine IAM CloudTrail togs to determine whether any instances have not restarted in the last 30 days, and redeploy those instances
D. Update the AMIs with the latest approved patches and redeploy each instance during the defined maintenance window

Answer: B

NEW QUESTION 246
- (Exam Topic 4)
A company deployed IAM Organizations to help manage its increasing number of IAM accounts. A security engineer wants to ensure only principals in the Organization structure can access a specic Amazon S3 bucket. The solution must also minimize operational overhead
Which solution will meet these requirements?

A. 1 Put all users into an IAM group with an access policy granting access to the J bucket.
B. Have the account creation trigger an IAM Lambda function that manages the bucket policy, allowing access to accounts listed in the policy only.
C. Add an SCP to the Organizations master account, allowing all principals access to the bucket.
D. Specify the organization ID in the global key condition element of a bucket policy, allowing all principals access.

Answer: D

NEW QUESTION 247
- (Exam Topic 4)
A Security Engineer receives alerts that an Amazon EC2 instance on a public subnet is under an SFTP brute force attack from a specific IP address, which is a known malicious bot. What should the Security Engineer do to block the malicious bot?

A. Add a deny rule to the public VPC security group to block the malicious IP
B. Add the malicious IP to IAM WAF backhsted IPs
C. Configure Linux iptables or Windows Firewall to block any traffic from the malicious IP
D. Modify the hosted zone in Amazon Route 53 and create a DNS sinkhole for the malicious IP

Answer: D

NEW QUESTION 250
- (Exam Topic 4)
A company is building a data processing application mat uses AWS Lambda functions. The application's Lambda functions need to communicate with an Amazon RDS OB instance that is deployed within a VPC in the same AWS account
Which solution meets these requirements in the MOST secure way?

A. Configure the DB instance to allow public access Update the DB instance security group to allow access from the Lambda public address space for the AWS Region
B. Deploy the Lambda functions inside the VPC Attach a network ACL to the Lambda subnet Provide outbound rule access to the VPC CIDR range only Update the DB instance security group to allow traffic from 0.0.0.0/0
C. Deploy the Lambda functions inside the VPC Attach a security group to the Lambda functions Provide outbound rule access to the VPC CIDR range only Update the DB instance security group to allow traffic from the Lambda security group
D. Peer the Lambda default VPC with the VPC that hosts the DB instance to allow direct network access without the need for security groups

Answer: C

Explanation:
This solution ensures that the Lambda functions are deployed inside the VPC and can communicate with the Amazon RDS DB instance securely. The security group attached to the Lambda functions only allows outbound traffic to the VPC CIDR range, and the DB instance security group only allows traffic from the Lambda security group. This solution ensures that the Lambda functions can communicate with the DB instance securely and that the DB instance is not exposed to the public internet.

NEW QUESTION 253

- (Exam Topic 4)

A company usesAWS Organizations to run workloads in multiple AWS accounts Currently the individual team members at the company access all Amazon EC2 instances remotely by using SSH or Remote Desktop Protocol (RDP) The company does not have any audit trails and security groups are occasionally open The company must secure access management and implement a centralized togging solution

Which solution will meet these requirements MOST securely?

A. Configure trusted access for AWS System Manager in Organizations Configure a bastion host from the management account Replace SSH and RDP by using Systems Manager Session Manager from the management account Configure Session Manager logging to Amazon CloudWatch Logs

B. Replace SSH and RDP with AWS Systems Manager Session Manager Install Systems Manager Agent (SSM Agent) on the instances Attach the

C. AmazonSSMManagedInstanceCore role to the instances Configure session data streaming to Amazon CloudWatch Logs Create a separate logging account that has appropriate cross-account permissions to audit the log data

D. Install a bastion host in the management account Reconfigure all SSH and RDP to allow access only from the bastion host Install AWS Systems Manager Agent (SSM Agent) on the bastion host Attach the AmazonSSMManagedInstanceCore role to the bastion host Configure session data streaming to Amazon CloudWatch Logs in a separate logging account to audit log data

E. Replace SSH and RDP with AWS Systems Manager State Manager Install Systems Manager Agent (SSM Agent) on the instances Attach theAmazonSSMManagedInstanceCore role to the instances Configure session data streaming to Amazon CloudTrail Use CloudTrail Insights to analyze the trail data

Answer: C

Explanation:

To meet the requirements of securing access management and implementing a centralized logging solution, the most secure solution would be to:

≫ Install a bastion host in the management account.

≫ Reconfigure all SSH and RDP to allow access only from the bastion host.

≫ Install AWS Systems Manager Agent (SSM Agent) on the bastion host.

≫ Attach the AmazonSSMManagedInstanceCore role to the bastion host.

≫ Configure session data streaming to Amazon CloudWatch Logs in a separate logging account to audit log data

This solution provides the following security benefits:

≫ It uses AWS Systems Manager Session Manager instead of traditional SSH and RDP protocols, which provides a secure method for accessing EC2 instances without requiring inbound firewall rules or open

ports.

≫ It provides audit trails by configuring Session Manager logging to Amazon CloudWatch Logs and creating a separate logging account to audit the log data.

≫ It uses the AWS Systems Manager Agent to automate common administrative tasks and improve the security posture of the instances.

≫ The separate logging account with cross-account permissions provides better data separation and improves security posture.

https://aws.amazon.com/solutions/implementations/centralized-logging/

NEW QUESTION 256

- (Exam Topic 4)

A company is using Amazon Elastic Container Service (Amazon ECS) to deploy an application that deals with sensitive data During a recent security audit, the company identified a security issue in which Amazon RDS credentials were stored with the application code In the company's source code repository

A security engineer needs to develop a solution to ensure that database credentials are stored securely and rotated periodically. The credentials should be accessible to the application only The engineer also needs to prevent database administrators from sharing database credentials as plaintext with other teammates. The solution must also minimize administrate overhead

Which solution meets these requirements?

A. Use the IAM Systems Manager Parameter Store to generate database credential

B. Use an IAM profile for ECS tasks to restrict access to database credentials to specific containers only.

C. Use IAM Secrets Manager to store database credential

D. Use an IAM inline policy for ECS tasks to restrict access to database credentials to specific containers only.

E. Use the IAM Systems Manager Parameter Store to store database credential

F. Use IAM roles for ECS tasks to restrict access to database credentials lo specific containers only

G. Use IAM Secrets Manager to store database credential

H. Use IAM roles for ECS tasks to restrict access to database credentials to specific containers only.

Answer: D

NEW QUESTION 261

- (Exam Topic 4)

A company uses an external identity provider to allow federation into different IAM accounts. A security engineer for the company needs to identify the federated user that terminated a production Amazon EC2 instance a week ago.

What is the FASTEST way for the security engineer to identify the federated user?

A. Review the IAM CloudTrail event history logs in an Amazon S3 bucket and look for the TerminateInstances event to identify the federated user from the role session name.

B. Filter the IAM CloudTrail event history for the TerminateInstances event and identify the assumed IAM rol

C. Review the AssumeRoleWithSAML event call in CloudTrail to identify the corresponding username.

D. Search the IAM CloudTrail logs for the TerminateInstances event and note the event tim

E. Review the IAM Access Advisor tab for all federated role

F. The last accessed time should match the time when the instance was terminated.

G. Use Amazon Athena to run a SQL query on the IAM CloudTrail logs stored in an Amazon S3 bucket and filter on the TerminateInstances even

H. Identify the corresponding role and run another query to filter the AssumeRoleWithWebIdentity event for the user name.

Answer: B

NEW QUESTION 265

- (Exam Topic 4)

A company is running an application in The eu-west-1 Region. The application uses an IAM Key Management Service (IAM KMS) CMK to encrypt sensitive data. The company plans to deploy the application in the eu-north-1 Region.

A security engineer needs to implement a key management solution for the application deployment in the new Region. The security engineer must minimize

changes to the application code.
Which change should the security engineer make to the IAM KMS configuration to meet these requirements?

A. Update the key policies in eu-west-1. Point the application in eu-north-1 to use the same CMK as theapplication in eu-west-1.
B. Allocate a new CMK to eu-north-1 to be used by the application that is deployed in that Region.
C. Allocate a new CMK to eu-north-1. Create the same alias name for both key
D. Configure the application deployment to use the key alias.
E. Allocate a new CMK to eu-north-1. Create an alias for eu-'-1. Change the application code to point to the alias for eu-'-1.

Answer: B

NEW QUESTION 267
......

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

SCS-C02 Practice Exam Features:

* SCS-C02 Questions and Answers Updated Frequently

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

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

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

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