



Amazon-Web-Services

Exam Questions SCS-C02

AWS Certified Security - Specialty

NEW QUESTION 1

- (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. Use SCPs
- 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 2

- (Exam Topic 1)

A Developer is building a serverless application that uses Amazon API Gateway as the front end. The application will not be publicly accessible. Other legacy applications running on Amazon EC2 will make calls to the application. A Security Engineer has been asked to review the security controls for authentication and authorization of the application.

Which combination of actions would provide the MOST secure solution? (Select TWO)

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

Answer: AE

NEW QUESTION 3

- (Exam Topic 1)

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 4

- (Exam Topic 1)

A company has a website with an Amazon CloudFront HTTPS distribution, an Application Load Balancer (ALB) with multiple web instances for dynamic website content, and an Amazon S3 bucket for static website content. The company's security engineer recently updated the website security requirements:

- HTTPS needs to be enforced for all data in transit with specific ciphers.
- The CloudFront distribution needs to be accessible from the internet only. Which solution will meet these requirements?

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

Answer: A

Explanation:

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

NEW QUESTION 5

- (Exam Topic 1)

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

Which solution meets these requirements?

- A. Create an IAM role that allows CloudFront to access the specific S3 bucket.

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

Answer: C

NEW QUESTION 6

- (Exam Topic 1)

A company is building a data lake on Amazon S3. The data consists of millions of small files containing sensitive information. The security team has the following requirements for the architecture:

- Data must be encrypted in transit.
- Data must be encrypted at rest.
- The bucket must be private, but if the bucket is accidentally made public, the data must remain confidential. Which combination of steps would meet the requirements? (Select THREE.)

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

Answer: BDF

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 SSL/TLS 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 ALB
- 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 Web Administrator for the website example.com has created an Amazon CloudFront distribution for dev.example.com, with a requirement to configure HTTPS using a custom TLS certificate imported to IAM Certificate Manager.

Which combination of steps is required to ensure availability of the certificate in the CloudFront console? (Choose two.)

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

Answer: DE

NEW QUESTION 9

- (Exam Topic 1)

A company is configuring three Amazon EC2 instances with each instance in a separate Availability Zone. The EC2 instances will be used as transparent proxies for outbound internet traffic for ports 80 and 443 so the proxies can block traffic to certain internet destinations as required by the company's security policies. A Security Engineer completed the following:

- Set up the proxy software on the EC2 instances.
 - Modified the route tables on the private subnets to use the proxy EC2 instances as the default route.
 - Created a security group rule opening inbound port 80 and 443 TCP protocols on the proxy EC2 instance security group.
- However, the proxy EC2 instances are not successfully forwarding traffic to the internet.

What should the Security Engineer do to make the proxy EC2 instances route traffic to the internet?

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

Answer: B

NEW QUESTION 10

- (Exam Topic 1)

A company is outsourcing its operational support to an external company. The company's security officer must implement an access solution for 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 the external company Add a policy to the group that denies IAM modifications Securely provide the credentials to the external company.
- D. Use IAM SSO with the external company's identity provider
- 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's development team is designing an application using IAM Lambda and Amazon Elastic Container Service (Amazon ECS). The development team needs to create IAM roles to support these systems. The company's security team wants to allow the developers to build IAM roles directly, but the security team wants to retain control over the permissions the developers can delegate to those roles. The development team needs access to more permissions than those required for the application's IAM services. The solution must minimize management overhead.

How should the security team prevent privilege escalation for both teams?

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

Answer: A

NEW QUESTION 14

- (Exam Topic 1)

A company has recently recovered from a security incident that required the restoration of Amazon EC2 instances from snapshots.

After performing a gap analysis of its disaster recovery procedures and backup strategies, the company is concerned that, next time, it will not be able to recover the EC2 instances if the IAM account was compromised and Amazon EBS snapshots were deleted.

All EBS snapshots are encrypted using an IAM KMS CMK. Which solution would solve this problem?

- A. Create a new Amazon S3 bucket Use EBS lifecycle policies to move EBS snapshots to the new S3 bucket
- B. Move snapshots to Amazon S3 Glacier using lifecycle policies, and apply Glacier Vault Lock policies to prevent deletion
- C. Use IAM Systems Manager to distribute a configuration that performs local backups of all attached disks to Amazon S3.
- D. Create a new IAM account with limited privilege
- E. Allow the new account to access the IAM KMS key used to encrypt the EBS snapshots, and copy the encrypted snapshots to the new account on a recurring basis
- F. Use IAM Backup to copy EBS snapshots to Amazon S3.

Answer: A

NEW QUESTION 18

- (Exam Topic 1)

A company uses a third-party identity provider and SAML-based SSO for its IAM accounts After the third-party identity provider renewed an expired signing certificate users saw the following message when trying to log in:

```
Error: Response Signature Invalid (Service: AWSSecurityTokenService; Status Code: 400; Error Code: InvalidIdentityToken)
```

A security engineer needs to provide a solution that corrects the error and minimizes operational overhead Which solution meets these requirements?

- A. Upload the third-party signing certificate's new private key to the IAM identity provider entity defined in IAM identity and Access Management (IAM) by using the IAM Management Console
- B. Sign the identity provider's metadata file with the new public key Upload the signature to the IAM identity provider entity defined in IAM Identity and Access Management (IAM) by using the IAM CLI.
- C. Download the updated SAML metadata file from the identity service provider Update the file in the IAM identity provider entity defined in IAM Identity and Access Management (IAM) by using the IAM CLI
- D. Configure the IAM identity provider entity defined in IAM Identity and Access Management (IAM) to synchronously fetch the new public key by using the IAM Management Console.

Answer: C

NEW QUESTION 19

- (Exam Topic 1)

A company has implemented centralized logging and monitoring of IAM CloudTrail logs from all Regions in an Amazon S3 bucket. The log files are encrypted using IAM KMS. A Security Engineer is attempting to review the log files using a third-party tool hosted on an Amazon EC2 instance The Security Engineer is

unable to access the logs in the S3 bucket and receives an access denied error message
What should the Security Engineer do to fix this issue?

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

Answer: C

NEW QUESTION 23

- (Exam Topic 1)

A security engineer is designing a solution that will provide end-to-end encryption between clients and Docker containers running in Amazon Elastic Container Service (Amazon ECS). This solution will also handle volatile traffic patterns
Which solution would have the MOST scalability and LOWEST latency?

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

Answer: A

NEW QUESTION 24

- (Exam Topic 1)

A website currently runs on Amazon EC2 with mostly static content on the site. Recently, the site was subjected to a DDoS attack, and a Security Engineer was tasked with redesigning the edge security to help mitigate this risk in the future
What are some ways the Engineer could achieve this? (Select THREE)

- A. Use IAM X-Ray to inspect the traffic going to the EC2 instances
- B. Move the static content to Amazon S3 and host this with an Amazon CloudFront distribution
- C. Change the security group configuration to block the source of the attack traffic
- D. Use IAM WAF security rules to inspect the inbound traffic
- E. Use Amazon Inspector assessment templates to inspect the inbound traffic
- F. Use Amazon Route 53 to distribute traffic

Answer: BDF

NEW QUESTION 29

- (Exam Topic 1)

Unapproved changes were previously made to a company's Amazon S3 bucket. A security engineer configured IAM Config to record configuration changes made to the company's S3 buckets. The engineer discovers there are S3 configuration changes being made, but no Amazon SNS notifications are being sent. The engineer has already checked the configuration of the SNS topic and has confirmed the configuration is valid.
Which combination of steps should the security engineer take to resolve the issue? (Select TWO.)

- A. Configure the S3 bucket ACLs to allow IAM Config to record changes to the buckets.
- B. Configure policies attached to S3 buckets to allow IAM Config to record changes to the buckets.
- C. Attach the AmazonS3ReadOnlyAccess managed policy to the IAM user.
- D. Verify the security engineer's IAM user has an attached policy that allows all IAM Config actions.
- E. Assign the IAMConfigRole managed policy to the IAM Config role

Answer: BE

NEW QUESTION 31

- (Exam Topic 1)

A company has a VPC with several Amazon EC2 instances behind a NAT gateway. The company's security policy states that all network traffic must be logged and must include the original source and destination IP addresses. The existing VPC Flow Logs do not include this information. A security engineer needs to recommend a solution.

Which combination of steps should the security engineer recommend? (Select TWO)

- A. Edit the existing VPC Flow Log
- B. Change the log format of the VPC Flow Logs from the Amazon default format to a custom format.
- C. Delete and recreate the existing VPC Flow Log
- D. Change the log format of the VPC Flow Logs from the Amazon default format to a custom format.
- E. Change the destination to Amazon CloudWatch Logs.
- F. Include the pkt-srcaddr and pkt-dstaddr fields in the log format.
- G. Include the subnet-id and instance-id fields in the log format.

Answer: AE

NEW QUESTION 33

- (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 days
- 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 38

- (Exam Topic 1)

A security engineer is responsible for providing secure access to IAM resources for thousands of developer in a company's corporate identity provider (idp). The developers access a set of IAM services from the corporate premises using IAM credential. Due to the velum of require for provisioning new IAM users, it is taking a long time to grant access permissions. The security engineer receives reports that developer are sharing their IAM credentials with others to avoid provisioning delays. The causes concern about overall security for the security engineer.

Which actions will meet the program requirements that address security?

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

Answer: B

NEW QUESTION 42

- (Exam Topic 1)

A company's application runs on Amazon EC2 and stores data in an Amazon S3 bucket The company wants additional security controls in place to limit the likelihood of accidental exposure of data to external parties

Which combination of actions will meet this requirement? (Select THREE.)

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

Answer: BCE

NEW QUESTION 45

- (Exam Topic 1)

A Security Engineer is looking for a way to control access to data that is being encrypted under a CMK. The Engineer is also looking to use additional authenticated data (AAD) to prevent tampering with ciphertext.

Which action would provide the required functionality?

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

Answer: C

Explanation:

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

NEW QUESTION 48

- (Exam Topic 1)

A security engineer need to ensure their company's uses of IAM meets IAM security best practices. As part of this, the IAM account root user must not be used for daily work. The root user must be monitored for use, and the Security team must be alerted as quickly as possible if the root user is used.

Which solution meets these requirements?

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

Answer: A

NEW QUESTION 51

- (Exam Topic 1)

A security engineer must develop an encryption tool for a company. The company requires a cryptographic solution that supports the ability to perform cryptographic erasure on all resources protected by the key material in 15 minutes or less

Which IAM Key Management Service (IAM KMS) key solution will allow the security engineer to meet these requirements?

- A. Use Imported key material with CMK
- B. Use an IAM KMS CMK
- C. Use an IAM managed CMK.
- D. Use an IAM KMS customer managed CMK

Answer: C

NEW QUESTION 55

- (Exam Topic 1)

A company uses multiple IAM accounts managed with IAM Organizations Security engineers have created a standard set of security groups for all these accounts. The security policy requires that these security groups be used for all applications and delegates modification authority to the security team only.

A recent security audit found that the security groups are inconsistency implemented across accounts and that unauthorized changes have been made to the security groups. A security engineer needs to recommend a solution to improve consistency and to prevent unauthorized changes in the individual accounts in the future.

Which solution should the security engineer recommend?

- A. Use IAM Resource Access Manager to create shared resources for each required security group and apply an IAM policy that permits read-only access to the security groups only.
- B. Create an IAM CloudFormation template that creates the required security groups Execute the template as part of configuring new accounts Enable Amazon Simple Notification Service (Amazon SNS) notifications when changes occur
- C. Use IAM Firewall Manager to create a security group policy, enable the policy feature to identify and revert local changes, and enable automatic remediation
- D. Use IAM Control Tower to edit the account factory template to enable the share security groups option Apply an SCP to the OU or individual accounts that prohibits security group modifications from local account users

Answer: B

NEW QUESTION 56

- (Exam Topic 1)

A company's security team has defined a set of IAM Config rules that must be enforced globally in all IAM accounts the company owns. What should be done to provide a consolidated compliance overview for the security team?

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

Answer: B

NEW QUESTION 61

- (Exam Topic 1)

An organization policy states that all encryption keys must be automatically rotated every 12 months. Which IAM Key Management Service (KMS) key type should be used to meet this requirement?

- A. IAM managed Customer Master Key (CMK)
- B. Customer managed CMK with IAM generated key material
- C. Customer managed CMK with imported key material
- D. IAM managed data key

Answer: B

NEW QUESTION 63

- (Exam Topic 1)

A company has several critical applications running on a large fleet of Amazon EC2 instances. As part of a security operations review, the company needs to apply a critical operating system patch to EC2 instances within 24 hours of the patch becoming available from the operating system vendor. The company does not have a patching solution deployed on IAM, but does have IAM Systems Manager configured. The solution must also minimize administrative overhead.

What should a security engineer recommend to meet these requirements?

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

Answer: B

NEW QUESTION 68

- (Exam Topic 1)

A security engineer is asked to update an AWS CloudTrail log file prefix for an existing trail. When attempting to save the change in the CloudTrail console, the security engineer receives the following error message. "There is a problem with the bucket policy"

What will enable the security engineer to save the change?

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

Answer: C

Explanation:

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

NEW QUESTION 70

- (Exam Topic 1)

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

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

Answer: BD

NEW QUESTION 75

- (Exam Topic 1)

A company has multiple production IAM accounts. Each account has IAM CloudTrail configured to log to a single Amazon S3 bucket in a central account. Two of the production accounts have trails that are not logging anything to the S3 bucket.

Which steps should be taken to troubleshoot the issue? (Choose three.)

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

Answer: BDF

NEW QUESTION 79

- (Exam Topic 1)

To meet regulatory requirements, a Security Engineer needs to implement an IAM policy that restricts the use of IAM services to the us-east-1 Region. What policy should the Engineer implement?

A

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

B

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

C

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

D

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

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

Answer: B

NEW QUESTION 80

- (Exam Topic 1)

A Security Engineer accidentally deleted the imported key material in an IAM KMS CMK. What should the Security Engineer do to restore the deleted key material?

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

E. Use the original wrapping key and import token Import the original key material into the existing CMK

Answer: C

NEW QUESTION 84

- (Exam Topic 1)

A company hosts a web-based application that captures and stores sensitive data in an Amazon DynamoDB table. A security audit reveals that the application does not provide end-to-end data protection or the ability to detect unauthorized data changes. The software engineering team needs to make changes that will address the audit findings.

Which set of steps should the software engineering team take?

- A. Use an IAM Key Management Service (IAM KMS) CM
- B. Encrypt the data at rest.
- C. Use IAM Certificate Manager (ACM) Private Certificate Authority Encrypt the data in transit.
- D. Use a DynamoDB encryption client
- E. Use client-side encryption and sign the table items
- F. Use the IAM Encryption SD
- G. Use client-side encryption and sign the table items.

Answer: A

NEW QUESTION 87

- (Exam Topic 1)

A Security Engineer has launched multiple Amazon EC2 instances from a private AMI using an IAM CloudFormation template. The Engineer notices instances terminating right after they are launched.

What could be causing these terminations?

- A. The IAM user launching those instances is missing ec2:Runinstances permission.
- B. The AMI used as encrypted and the IAM does not have the required IAM KMS permissions.
- C. The instance profile used with the EC2 instances is unable to query instance metadata.
- D. IAM currently does not have sufficient capacity in the Region.

Answer: B

Explanation:

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

NEW QUESTION 91

- (Exam Topic 1)

Authorized Administrators are unable to connect to an Amazon EC2 Linux bastion host using SSH over the internet. The connection either fails to respond or generates the following error message:

Network error: Connection timed out.

What could be responsible for the connection failure? (Select THREE)

- A. The NAT gateway in the subnet where the EC2 instance is deployed has been misconfigured
- B. The internet gateway of the VPC has been reconfigured
- C. The security group denies outbound traffic on ephemeral ports
- D. The route table is missing a route to the internet gateway
- E. The NACL denies outbound traffic on ephemeral ports
- F. The host-based firewall is denying SSH traffic

Answer: BDF

NEW QUESTION 93

- (Exam Topic 1)

A company's Director of information Security wants a daily email report from IAM that contains recommendations for each company account to meet IAM Security best practices.

Which solution would meet these requirements?

- A. in every IAM account, configure IAM Lambda to query the IAM Support API for IAM Trusted Advisor security checks. Send the results from Lambda to an Amazon SNS topic to send reports.
- B. Configure Amazon GuardDuty in a master account and invite all other accounts to be managed by the master account. Use GuardDuty's integration with Amazon SNS to report on findings.
- C. Use Amazon Athena and Amazon QuickSight to build reports off of IAM CloudTrail. Create a daily Amazon CloudWatch trigger to run the report daily and email it using Amazon SNS.
- D. Use IAM Artifact's prebuilt reports and subscriptions. Subscribe the Director of Information Security to the reports by adding the Director as the security alternate contact for each account.

Answer: A

NEW QUESTION 98

- (Exam Topic 1)

A Security Administrator at a university is configuring a fleet of Amazon EC2 instances. The EC2 instances are shared among students, and non-root SSH access is allowed. The Administrator is concerned about students attacking other IAM account resources by using the EC2 instance metadata service.

What can the Administrator do to protect against this potential attack?

- A. Disable the EC2 instance metadata service.
- B. Log all student SSH interactive session activity.

- C. Implement ip tables-based restrictions on the instances.
- D. Install the Amazon Inspector agent on the instances.

Answer: A

Explanation:

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

NEW QUESTION 99

- (Exam Topic 1)

A company has hundreds of IAM accounts, and a centralized Amazon S3 bucket used to collect IAM CloudTrail for all of these accounts. A security engineer wants to create a solution that will enable the company to run ad hoc queries against its CloudTrail logs dating back 3 years from when the trails were first enabled in the company's IAM account.

How should the company accomplish this with the least amount of administrative overhead?

- A. Run an Amazon EMR cluster that uses a MapReduce job to be examine the CloudTrail trails.
- B. Use the events history/feature of the CloudTrail console to query the CloudTrail trails.
- C. Write an IAM Lambda function to query the CloudTrail trails Configure the Lambda function to be executed whenever a new file is created in the CloudTrail S3 bucket.
- D. Create an Amazon Athena table that tools at the S3 bucket the CloudTrail trails are being written to Use Athena to run queries against the trails.

Answer: D

NEW QUESTION 100

- (Exam Topic 1)

A company has several workloads running on IAM. Employees are required to authenticate using on-premises ADFS and SSO to access the IAM Management Console. Developers migrated an existing legacy web application to an Amazon EC2 instance. Employees need to access this application from anywhere on the internet, but currently, there is no authentication system built into the application.

How should the Security Engineer implement employee-only access to this system without changing the application?

- A. Place the application behind an Application Load Balancer (ALB). Use Amazon Cognito as authentication for the ALB.
- B. Define a SAML-based Amazon Cognito user pool and connect it to ADFS.
- C. Implement IAM SSO in the master account and link it to ADFS as an identity provide
- D. Define the EC2 instance as a managed resource, then apply an IAM policy on the resource.
- E. Define an Amazon Cognito identity pool, then install the connector on the Active Directory serve
- F. Use the Amazon Cognito SDK on the application instance to authenticate the employees using their Active Directory user names and passwords.
- G. Create an IAM Lambda custom authorizer as the authenticator for a reverse proxy on Amazon EC2.Ensure the security group on Amazon EC2 only allows access from the Lambda function.

Answer: A

Explanation:

<https://docs.IAM.amazon.com/elasticloadbalancing/latest/application/listener-authenticate-users.html>

- Authenticate users through social IdPs, such as Amazon, Facebook, or Google, through the user pools supported by Amazon Cognito.
- Authenticate users through corporate identities, using SAML, LDAP, or Microsoft AD, through the user pools supported by Amazon Cognito.

NEW QUESTION 105

- (Exam Topic 1)

A company has the software development teams that are creating applications that store sensitive data in Amazon S3 Each team's data must always be separate. The company's security team must design a data encryption strategy for both teams that provides the ability to audit key usage. The solution must also minimize operational overhead

what should me security team recommend?

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

Answer: A

NEW QUESTION 107

- (Exam Topic 1)

A company uses HTTP Live Streaming (HLS) to stream live video content to paying subscribers by using

Amazon CloudFront. HLS splits the video content into chunks so that the user can request the right chunk based on different conditions Because the video events last for several hours, the total video is made up of thousands of chunks

The origin URL is not disclosed and every user is forced to access the CloudFront URL The company has a web application that authenticates the paying users against an internal repository and a CloudFront key pair that is already issued.

What is the simplest and MOST effective way to protect the content?

- A. Develop the application to use the CloudFront key pair to create signed URLs that users will use to access the content.
- B. Develop the application to use the CloudFront key pair to set the signed cookies that users will use to access the content.

- C. Develop the application to issue a security token that Lambda@Edge will receive to authenticate and authorize access to the content
- D. Keep the CloudFront URL encrypted inside the application, and use IAM KMS to resolve the URL on-the-fly after the user is authenticated.

Answer: B

NEW QUESTION 111

- (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 115

- (Exam Topic 1)

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

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

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

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

Answer: C

NEW QUESTION 117

- (Exam Topic 1)

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

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

Amazon Simple Notification Service (Amazon SNS). Configure the hook to remain in the Terminating:Wait state for 1 hour to allow manual review of the security logs prior to instance termination.

Answer: B

NEW QUESTION 122

- (Exam Topic 1)

A company has several production IAM accounts and a central security IAM account. The security account is used for centralized monitoring and has IAM privileges to all resources in every corporate account. All of the company's Amazon S3 buckets are tagged with a value denoting the data classification of their contents.

A Security Engineer is deploying a monitoring solution in the security account that will enforce bucket policy compliance. The system must monitor S3 buckets in all production accounts and confirm that any policy change is in accordance with the bucket's data classification. If any change is out of compliance; the Security team must be notified quickly.

Which combination of actions would build the required solution? (Choose three.)

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

Answer: DEF

NEW QUESTION 123

- (Exam Topic 1)

A company needs its Amazon Elastic Block Store (Amazon EBS) volumes to be encrypted at all times. During a security incident. EBS snapshots of suspicious instances are shared to a forensics account for analysis A security engineer attempting to share a suspicious EBS snapshot to the forensics account receives the following error

"Unable to share snapshot: An error occurred (OperationNotPermitted) when calling the ModifySnapshotAttribute operation: Encrypted snapshots with EBS default key cannot be shared.

Which combination of steps should the security engineer take in the incident account to complete the sharing operation? (Select THREE)

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

Answer: ABF

NEW QUESTION 125

- (Exam Topic 1)

A company's security information events management (SIEM) tool receives new IAM CloudTrail logs from an Amazon S3 bucket that is configured to send all object created event notification to an Amazon SNS topic An Amazon SQS queue is subscribed to this SNS topic. The company's SEM tool then ports this SQS queue for new messages using an IAM role and fetches new log events from the S3 bucket based on the SQS messages.

After a recent security review that resulted in restricted permissions, the SEM tool has stopped receiving new CloudTrail logs

Which of the following are possible causes of this issue? (Select THREE)

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

Answer: ADF

NEW QUESTION 129

- (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 134

- (Exam Topic 1)

A company has decided to use encryption in its IAM account to secure the objects in Amazon S3 using server-side encryption. Object sizes range from 16.000 B to 5 MB. The requirements are as follows:

- The key material must be generated and stored in a certified Federal Information Processing Standard (FIPS) 140-2 Level 3 machine.
- The key material must be available in multiple Regions. Which option meets these requirements?

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

Answer: D

NEW QUESTION 137

- (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 142

- (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 145

- (Exam Topic 1)

A Security Engineer launches two Amazon EC2 instances in the same Amazon VPC but in separate Availability Zones. Each instance has a public IP address and is able to connect to external hosts on the internet. The two instances are able to communicate with each other by using their private IP addresses, but they are not able to communicate with each other when using their public IP addresses.

Which action should the Security Engineer take to allow communication over the public IP addresses?

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

Answer: D

Explanation:

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

NEW QUESTION 149

- (Exam Topic 1)

A security engineer is auditing a production system and discovers several additional IAM roles that are not required and were not previously documented during the last audit 90 days ago. The engineer is trying to find out who created these IAM roles and when they were created. The solution must have the lowest operational overhead.

Which solution will meet this requirement?

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

Answer: A

NEW QUESTION 150

- (Exam Topic 2)

Your IT Security department has mandated that all data on EBS volumes created for underlying EC2 Instances need to be encrypted. Which of the following can help achieve this?

Please select:

- A. IAM KMS API
- B. IAM Certificate Manager
- C. API Gateway with STS
- D. IAM Access Key

Answer: A

Explanation:

The IAM Documentation mentions the following on IAM KMS

IAM Key Management Service (IAM KMS) is a managed service that makes it easy for you to create and control the encryption keys used to encrypt your data. IAM KMS is integrated with other IAM services including Amazon Elastic Block Store (Amazon EBS), Amazon Simple Storage Service (Amazon S3), Amazon Redshift Amazon Elastic Transcoder, Amazon WorkMail, Amazon Relational Database Service (Amazon RDS), and others to make it simple to encrypt your data with encryption keys that you manage

Option B is incorrect - The IAM Certificate manager can be used to generate SSL certificates that can be used to encrypt traffic transit, but not at rest

Option C is incorrect is again used for issuing tokens when using API gateway for traffic in transit. Option D is used for secure access to EC2 Instances

For more information on IAM KMS, please visit the following URL: <https://docs.IAM.amazon.com/kms/latest/developereuide/overview.html> The correct answer is: IAM KMS API

Submit your Feedback/Queries to our Experts

NEW QUESTION 152

- (Exam Topic 2)

The Security Engineer created a new IAM Key Management Service (IAM KMS) key with the following key policy:

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

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

- A. The policy allows access for the IAM account 111122223333 to manage key access though IAM policies.
- B. The policy allows all IAM users in account 111122223333 to have full access to the KMS key.

- C. The policy allows the root user in account 111122223333 to have full access to the KMS key.
- D. The policy allows the KMS service-linked role in account 111122223333 to have full access to the KMS key.
- E. The policy allows all IAM roles in account 111122223333 to have full access to the KMS key.

Answer: AC

Explanation:

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

NEW QUESTION 157

- (Exam Topic 2)

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

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

Answer: B

Explanation:

Reference <https://IAM.amazon.com/s3/faqs/>

NEW QUESTION 160

- (Exam Topic 2)

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

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

Answer: BD

Explanation:

You can create a Log group and send all logs from the EC2 Instance to that group. You can then limit the access to the Log groups via an IAM policy. Option A is invalid because Cloudtrail is used to record API activity and not for storing log files Option C is invalid because Cloudtrail is the wrong service to be used for this requirement

For more information on Log Groups and Log Streams, please visit the following URL:

* <https://docs.IAM.amazon.com/AmazonCloudWatch/latest/logs/Workin>

For more information on Access to Cloudwatch logs, please visit the following URL:

* <https://docs.IAM.amazon.com/AmazonCloudWatch/latest/logs/auth-and-access-control-cwl.html>

The correct answers are: Stream the log files to a separate Cloudwatch Log group. Create an IAM policy that gives the desired level of access to the Cloudwatch Log group

Submit your Feedback/Queries to our Experts

NEW QUESTION 163

- (Exam Topic 2)

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

Please select:

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

Answer: CD

Explanation:

The below example policy from the IAM Documentation is required to be given to the EC2 Instance in order to read a secure string from IAM KMS. Permissions need to be given to the Get Parameter API and the KMS API call to decrypt the secret.

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

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

Option A is invalid because roles can be attached to EC2 and not EC2 roles to SSM Option B is invalid because the KMS key does not need to decrypt the SSM service role.

Option E is invalid because this configuration is valid For more information on the parameter store, please visit the below URL:
<https://docs.IAM.amazon.com/kms/latest/developerguide/services-parameter-store.html>

The correct answers are: Add permission to read the SSM parameter to the EC2 instance role., Add permission to use the KMS key to decrypt to the EC2 instance role

Submit your Feedback/Queries to our Experts

NEW QUESTION 165

- (Exam Topic 2)

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

What could have been done to detect and automatically remediate the incident?

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

Answer: B

Explanation:

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

NEW QUESTION 167

- (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 170

- (Exam Topic 2)

The Security Engineer has discovered that a new application that deals with highly sensitive data is storing Amazon S3 objects with the following key pattern, which itself contains highly sensitive data.

Pattern: "randomID_datestamp_PII.csv" Example:

"1234567_12302017_000-00-0000 csv"

The bucket where these objects are being stored is using server-side encryption (SSE). Which solution is the most secure and cost-effective option to protect the sensitive data?

- A. Remove the sensitive data from the object name, and store the sensitive data using S3 user-defined metadata.
- B. Add an S3 bucket policy that denies the action s3:GetObject
- C. Use a random and unique S3 object key, and create an S3 metadata index in Amazon DynamoDB using client-side encrypted attributes.
- D. Store all sensitive objects in Binary Large Objects (BLOBS) in an encrypted Amazon RDS instance.

Answer: C

Explanation:

<https://docs.IAM.amazon.com/AmazonS3/latest/dev/UsingMetadata.html> <https://IAM.amazon.com/blogs/database/best-practices-for-securing-sensitive-data-in-IAM-data-stores/>

NEW QUESTION 172

- (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 177

- (Exam Topic 2)

A company has Windows Amazon EC2 instances in a VPC that are joined to on-premises Active Directory servers for domain services. The security team has enabled Amazon GuardDuty on the IAM account to alert on issues with the instances.

During a weekly audit of network traffic, the Security Engineer notices that one of the EC2 instances is attempting to communicate with a known command-and-control server but failing. This alert does not show up in GuardDuty.

Why did GuardDuty fail to alert to this behavior?

- A. GuardDuty did not have the appropriate alerts activated.
- B. GuardDuty does not see these DNS requests.
- C. GuardDuty only monitors active network traffic flow for command-and-control activity.
- D. GuardDuty does not report on command-and-control activity.

Answer: B

Explanation:

https://docs.IAM.amazon.com/guardduty/latest/ug/guardduty_data-sources.html https://docs.IAM.amazon.com/guardduty/latest/ug/guardduty_backdoor.html

NEW QUESTION 178

- (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 root
- 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 user
- 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 183

- (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 policy
- B. Add the role to an EC2 instance profile

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

Answer: D

NEW QUESTION 184

- (Exam Topic 2)

A Security Engineer is working with a Product team building a web application on IAM. The application uses Amazon S3 to host the static content, Amazon API Gateway to provide RESTful services; and Amazon DynamoDB as the backend data store. The users already exist in a directory that is exposed through a SAML identity provider.

Which combination of the following actions should the Engineer take to enable users to be authenticated into the web application and call APIs? (Choose three.)

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

Answer: BDE

NEW QUESTION 189

- (Exam Topic 2)

For compliance reasons, an organization limits the use of resources to three specific IAM regions. It wants to be alerted when any resources are launched in unapproved regions.

Which of the following approaches will provide alerts on any resources launched in an unapproved region?

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

Answer: A

Explanation:

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

NEW QUESTION 191

- (Exam Topic 2)

A company hosts a popular web application that connects to an Amazon RDS MySQL DB instance running in a private VPC subnet that was created with default ACL settings. The IT Security department has a suspicion that a DDos attack is coming from a suspecting IP. How can you protect the subnets from this attack? Please select:

- A. Change the Inbound Security Groups to deny access from the suspecting IP
- B. Change the Outbound Security Groups to deny access from the suspecting IP
- C. Change the Inbound NACL to deny access from the suspecting IP
- D. Change the Outbound NACL to deny access from the suspecting IP

Answer: C

Explanation:

Option A and B are invalid because by default the Security Groups already block traffic. You can use NACL's as an additional security layer for the subnet to deny traffic.

Option D is invalid since just changing the Inbound Rules is sufficient The IAM Documentation mentions the following

A network access control list (ACL) is an optional layer of security for your VPC that acts as a firewall for

controlling traffic in and out of one or more subnets. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC.

The correct answer is: Change the Inbound NACL to deny access from the suspecting IP

NEW QUESTION 194

- (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 195

- (Exam Topic 2)

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

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

Answer: AD

Explanation:

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

NEW QUESTION 199

- (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 204

- (Exam Topic 2)

What are the MOST secure ways to protect the IAM account root user of a recently opened IAM account? (Choose two.)

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

Answer: CE

NEW QUESTION 205

- (Exam Topic 2)

A company wants to have a secure way of generating, storing and managing cryptographic exclusive access for the keys. Which of the following can be used for this purpose?

Please select:

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

Answer: D

Explanation:

The IAM Documentation mentions the following

The IAM CloudHSM service helps you meet corporate, contractual and regulatory compliance requirements for data security by using dedicated Hardware Security Module (HSM) instances within the IAM cloud. IAM and IAM Marketplace partners offer a variety of solutions for protecting sensitive data within the IAM platform, but for some applications and data subject to contractual or regulatory mandates for managing cryptographic keys, additional protection may be necessary.

CloudHSM complements existing data protection solutions and allows you to protect your encryption keys within HSMs that are design and validated to government standards for secure key management. CloudHSM allows you to securely generate, store and manage cryptographic keys used for data encryption in a way that keys are accessible only by you.

Option A.B and Care invalid because in all of these cases, the management of the key will be with IAM. Here the question specifically mentions that you want to have exclusive access over the keys. This can be achieved with Cloud HSM

For more information on CloudHSM, please visit the following URL: <https://IAM.amazon.com/cloudhsm/faq>:

The correct answer is: Use Cloud HSM Submit your Feedback/Queries to our Experts

NEW QUESTION 209

- (Exam Topic 2)

Some highly sensitive analytics workloads are to be moved to Amazon EC2 hosts. Threat modeling has found that a risk exists where a subnet could be maliciously or accidentally exposed to the internet.

Which of the following mitigations should be recommended?

- A. Use IAM Config to detect whether an Internet Gateway is added and use an IAM Lambda function to provide auto-remediation.
- B. Within the Amazon VPC configuration, mark the VPC as private and disable Elastic IP addresses.
- C. Use IPv6 addressing exclusively on the EC2 hosts, as this prevents the hosts from being accessed from the internet.
- D. Move the workload to a Dedicated Host, as this provides additional network security controls and monitorin

Answer: A

Explanation:

By default, Private instance has a private IP address, but no public IP address. These instances can communicate with each other, but can't access the Internet. You can enable Internet access for an instance launched into a nondefault subnet by attaching an Internet gateway to its VPC (if its VPC is not a default VPC) and associating an Elastic IP address with the instance. Alternatively, to allow an instance in your VPC to initiate outbound connections to the Internet but prevent unsolicited inbound connections from the Internet, you can use a network address translation (NAT) instance. NAT maps multiple private IP addresses to a single public IP address. A NAT instance has an Elastic IP address and is connected to the Internet through an Internet gateway. You can connect an instance in a private subnet to the Internet through the NAT instance, which routes traffic from the instance to the Internet gateway, and routes any responses to the instance.

NEW QUESTION 211

- (Exam Topic 2)

An organization has tens of applications deployed on thousands of Amazon EC2 instances. During testing, the Application team needs information to let them know whether the network access control lists (network ACLs) and security groups are working as expected.

How can the Application team's requirements be met?

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

Answer: A

NEW QUESTION 213

- (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 216

- (Exam Topic 2)

A Security Engineer has been asked to create an automated process to disable IAM user access keys that are more than three months old.

Which of the following options should the Security Engineer use?

- A. In the IAM Console, choose the IAM service and select "Users". Review the "Access Key Age" column.
- B. Define an IAM policy that denies access if the key age is more than three months and apply to all users.
- C. Write a script that uses the GenerateCredentialReport, GetCredentialReport, and UpdateAccessKey APIs.
- D. Create an Amazon CloudWatch alarm to detect aged access keys and use an IAM Lambda function to disable the keys older than 90 days.

Answer: C

Explanation:

https://docs.IAM.amazon.com/IAM/latest/APIReference/API_UpdateAccessKey.html

https://docs.IAM.amazon.com/IAM/latest/APIReference/API_GenerateCredentialReport.html

https://docs.IAM.amazon.com/IAM/latest/APIReference/API_GetCredentialReport.html

NEW QUESTION 217

- (Exam Topic 2)

A Security Administrator is performing a log analysis as a result of a suspected IAM account compromise. The Administrator wants to analyze suspicious IAM CloudTrail log files but is overwhelmed by the volume of audit logs being generated.

What approach enables the Administrator to search through the logs MOST efficiently?

- A. Implement a "write-only" CloudTrail event filter to detect any modifications to the IAM account resources.

- B. Configure Amazon Macie to classify and discover sensitive data in the Amazon S3 bucket that contains the CloudTrail audit logs.
- C. Configure Amazon Athena to read from the CloudTrail S3 bucket and query the logs to examine account activities.
- D. Enable Amazon S3 event notifications to trigger an IAM Lambda function that sends an email alarm when there are new CloudTrail API entries.

Answer: C

NEW QUESTION 218

- (Exam Topic 2)

An application has been written that publishes custom metrics to Amazon CloudWatch. Recently, IAM changes have been made on the account and the metrics are no longer being reported.

Which of the following is the LEAST permissive solution that will allow the metrics to be delivered?

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

Answer: C

Explanation:

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

NEW QUESTION 221

- (Exam Topic 2)

A Lambda function reads metadata from an S3 object and stores the metadata in a DynamoDB table. The function is triggered whenever an object is stored within the S3 bucket.

How should the Lambda function be given access to the DynamoDB table? Please select:

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

Answer: D

Explanation:

The ideal way is to create an IAM role which has the required permissions and then associate it with the Lambda function

The IAM Documentation additionally mentions the following

Each Lambda function has an IAM role (execution role) associated with it. You specify the IAM role when you create your Lambda function. Permissions you grant to this role determine what IAM Lambda can do when it assumes the role. There are two types of permissions that you grant to the IAM role:

If your Lambda function code accesses other IAM resources, such as to read an object from an S3 bucket or write logs to CloudWatch Logs, you need to grant permissions for relevant Amazon S3 and CloudWatch actions to the role.

If the event source is stream-based (Amazon Kinesis Data Streams and DynamoDB streams), IAM Lambda polls these streams on your behalf. IAM Lambda needs permissions to poll the stream and read new records on the stream so you need to grant the relevant permissions to this role.

Option A is invalid because the VPC endpoint allows access instances in a private subnet to access DynamoDB

Option B is invalid because resource policies are present for resources such as S3 and KMS, but not IAM Lambda

Option C is invalid because IAM Roles should be used and not IAM Users

For more information on the Lambda permission model, please visit the below URL: <https://docs.IAM.amazon.com/lambda/latest/dg/intro-permission-model.html>

The correct answer is: Create an IAM service role with permissions to write to the DynamoDB table. Associate that role with the Lambda function.

Submit your Feedback/Queries to our Exp

NEW QUESTION 225

- (Exam Topic 2)

A company uses IAM Organization to manage 50 IAM accounts. The finance staff members log in as IAM users in the FinanceDept IAM account. The staff members need to read the consolidated billing information in the MasterPayer IAM account. They should not be able to view any other resources in the MasterPayer IAM account. IAM access to billing has been enabled in the MasterPayer account.

Which of the following approaches grants the finance staff the permissions they require without granting any unnecessary permissions?

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

Answer: D

Explanation:

IAM Region that You Request a Certificate In (for IAM Certificate Manager) If you want to require HTTPS between viewers and CloudFront, you must change the IAM region to US East (N. Virginia) in the IAM Certificate Manager console before you request or import a certificate. If you want to require HTTPS between CloudFront and your origin, and you're using an ELB load balancer as your origin, you can request or import a certificate in any region.

<https://docs.IAM.amazon.com/AmazonCloudFront/latest/DeveloperGuide/cnames-and-https-requirements.html>

NEW QUESTION 229

- (Exam Topic 2)

You have enabled CloudTrail logs for your company's IAM account. In addition, the IT Security department has mentioned that the logs need to be encrypted. How

can this be achieved?
 Please select:

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

Answer: B

Explanation:

The IAM Documentation mentions the following.

By default CloudTrail event log files are encrypted using Amazon S3 server-side encryption (SSE). You can also choose to encryption your log files with an IAM Key Management Service (IAM KMS) key. You can store your log files in your bucket for as long as you want. You can also define Amazon S3 lifecycle rules to archive or delete log files automatically. If you want notifications about lo file delivery and validation, you can set up Amazon SNS notifications.

Option A.C and D are not valid since logs will already be encrypted

For more information on how Cloudtrail works, please visit the following URL: <https://docs.IAM.amazon.com/IAMcloudtrail/latest/useruide/how-cloudtrail-works.html>

The correct answer is: There is no need to do anything since the logs will already be encrypted

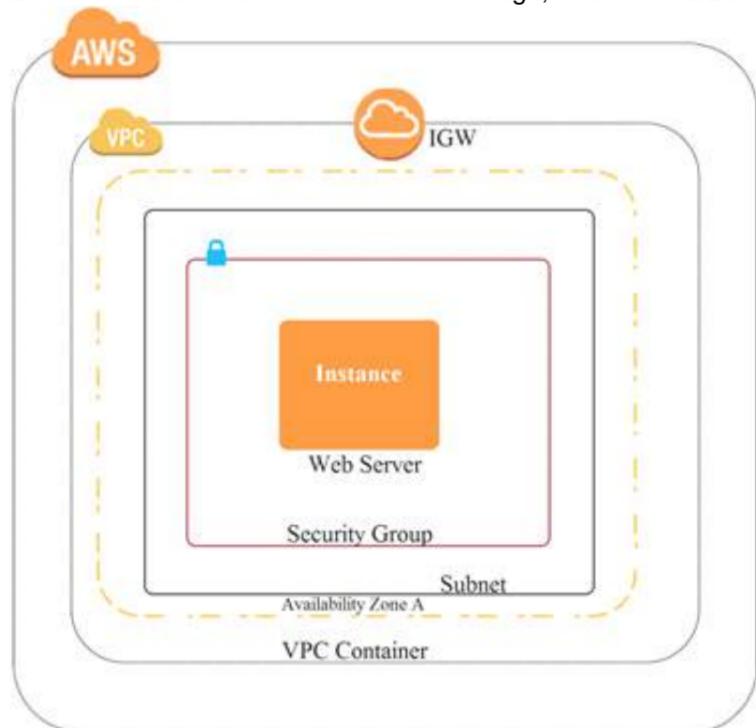
Submit your Feedback/Queries to our Experts

NEW QUESTION 232

- (Exam Topic 2)

A company recently experienced a DDoS attack that prevented its web server from serving content. The website is static and hosts only HTML, CSS, and PDF files that users download.

Based on the architecture shown in the image, what is the BEST way to protect the site against future attacks while minimizing the ongoing operational overhead?



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

Answer: D

Explanation:

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

NEW QUESTION 234

- (Exam Topic 2)

A Security Engineer is trying to determine whether the encryption keys used in an IAM service are in compliance with certain regulatory standards.

Which of the following actions should the Engineer perform to get further guidance?

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

Answer: B

Explanation:

<https://IAM.amazon.com/artifact/>

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

NEW QUESTION 239

- (Exam Topic 2)

A threat assessment has identified a risk whereby an internal employee could exfiltrate sensitive data from production host running inside IAM (Account 1). The threat was documented as follows:

Threat description: A malicious actor could upload sensitive data from Server X by configuring credentials for an IAM account (Account 2) they control and uploading data to an Amazon S3 bucket within their control.

Server X has outbound internet access configured via a proxy server. Legitimate access to S3 is required so that the application can upload encrypted files to an S3 bucket. Server X is currently using an IAM instance role. The proxy server is not able to inspect any of the server communication due to TLS encryption.

Which of the following options will mitigate the threat? (Choose two.)

- A. Bypass the proxy and use an S3 VPC endpoint with a policy that whitelists only certain S3 buckets within Account 1.
- B. Block outbound access to public S3 endpoints on the proxy server.
- C. Configure Network ACLs on Server X to deny access to S3 endpoints.
- D. Modify the S3 bucket policy for the legitimate bucket to allow access only from the public IP addresses associated with the application server.
- E. Remove the IAM instance role from the application server and save API access keys in a trusted and encrypted application config file.

Answer: AB

NEW QUESTION 242

- (Exam Topic 2)

You have an Ec2 Instance in a private subnet which needs to access the KMS service. Which of the following methods can help fulfil this requirement, keeping security in perspective

Please select:

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

Answer: A

Explanation:

The IAM Documentation mentions the following

You can connect directly to IAM KMS through a private endpoint in your VPC instead of connecting over the internet. When you use a VPC endpoint communication between your VPC and IAM KMS is conducted entirely within the IAM network.

Option B is invalid because this could open threats from the internet

Option C is invalid because this is normally used for communication between on-premise environments and IAM.

Option D is invalid because this is normally used for communication between VPCs

For more information on accessing KMS via an endpoint, please visit the following URL <https://docs.IAM.amazon.com/kms/latest/developerguide/kms-vpc-endpoint.html>

The correct answer is: Use a VPC endpoint Submit your Feedback/Queries to our Experts

NEW QUESTION 245

- (Exam Topic 2)

A company uses user data scripts that contain sensitive information to bootstrap Amazon EC2 instances. A Security Engineer discovers that this sensitive information is viewable by people who should not have access to it.

What is the MOST secure way to protect the sensitive information used to bootstrap the instances?

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

Answer: B

NEW QUESTION 246

- (Exam Topic 2)

Your company has defined a number of EC2 Instances over a period of 6 months. They want to know if any of the security groups allow unrestricted access to a resource. What is the best option to accomplish this requirement?

Please select:

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

Answer: B

Explanation:

The IAM Trusted Advisor can check security groups for rules that allow unrestricted access to a resource. Unrestricted access increases opportunities for malicious activity (hacking, denial-of-service attacks, loss of data).

If you go to IAM Trusted Advisor, you can see the details C:\Users\wk\Desktop\mudassar\Untitled.jpg



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

NEW QUESTION 248

- (Exam Topic 2)

An Amazon EC2 instance is part of an EC2 Auto Scaling group that is behind an Application Load Balancer (ALB). It is suspected that the EC2 instance has been compromised.

Which steps should be taken to investigate the suspected compromise? (Choose three.)

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

Answer: BDE

Explanation:

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

NEW QUESTION 252

- (Exam Topic 2)

An organization is moving non-business-critical applications to IAM while maintaining a mission-critical application in an on-premises data center. An on-premises application must share limited confidential information with the applications in IAM. The internet performance is unpredictable.

Which configuration will ensure continued connectivity between sites MOST securely?

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

Answer: C

Explanation:

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

NEW QUESTION 254

- (Exam Topic 2)

Which of the following is used as a secure way to log into an EC2 Linux Instance? Please select:

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

Answer: B

Explanation:

The IAM Documentation mentions the following

Key pairs consist of a public key and a private key. You use the private key to create a digital signature, and then IAM uses the corresponding public key to validate the signature. Key pairs are used only for Amazon EC2 and Amazon CloudFront.

Option A.C and D are all wrong because these are not used to log into EC2 Linux Instances For more information on IAM Security credentials, please visit the below URL: <https://docs.IAM.amazon.com/eeneral/latest/er/IAM-sec-cred-types.html>

The correct answer is: Key pairs

Submit your Feedback/Queries to our Experts

NEW QUESTION 258

- (Exam Topic 2)

A Security Engineer received an IAM Abuse Notice listing EC2 instance IDs that are reportedly abusing other hosts.

Which action should the Engineer take based on this situation? (Choose three.)

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

Answer: BEF

NEW QUESTION 262

- (Exam Topic 2)

A Development team has asked for help configuring the IAM roles and policies in a new IAM account. The team using the account expects to have hundreds of master keys and therefore does not want to manage access control for customer master keys (CMKs).

Which of the following will allow the team to manage IAM KMS permissions in IAM without the complexity of editing individual key policies?

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

Answer: B

Explanation:

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

NEW QUESTION 266

- (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 267

- (Exam Topic 2)

An application has a requirement to be resilient across not only Availability Zones within the application's primary region but also be available within another region altogether.

Which of the following supports this requirement for IAM resources that are encrypted by IAM KMS?

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

Answer: C

NEW QUESTION 269

- (Exam Topic 2)

A security team is creating a response plan in the event an employee executes unauthorized actions on IAM infrastructure. They want to include steps to determine if the employee's IAM permissions changed as part of the incident.

What steps should the team document in the plan? Please select:

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

Answer: A

Explanation:

You can use the IAMConfig history to see the history of a particular item.

The below snapshot shows an example configuration for a user in IAM Config C:\Users\wk\Desktop\mudassar\Untitled.jpg



Option B,C and D are all invalid because these services cannot be used to see the history of a particular configuration item. This can only be accomplished by IAM Config.

For more information on tracking changes in IAM Config, please visit the below URL:

<https://docs.IAM.amazon.com/AmazonCloudFront/latest/DeveloperGuide/TrackineChanees.html>

The correct answer is: Use IAM Config to examine the employee's IAM permissions prior to the incident and compare them the employee's current IAM permissions.

Submit your Feedback/Queries to our Experts

NEW QUESTION 270

- (Exam Topic 2)

When you enable automatic key rotation for an existing CMK key where the backing key is managed by IAM, after how long is the key rotated?

Please select:

- A. After 30 days
- B. After 128 days
- C. After 365 days
- D. After 3 years

Answer: D

Explanation:

The IAM Documentation states the following

- IAM managed CM Ks: You cannot manage key rotation for IAM managed CMKs. IAM KMS automatically rotates IAM managed keys every three years (1095 days).

Note: IAM-managed CMKs are rotated every 3yrs, Customer-Managed CMKs are rotated every 365-days from when rotation is enabled.

Option A, B, C are invalid because the dettings for automatic key rotation is not changeable. For more information on key rotation please visit the below URL

<https://docs.IAM.amazon.com/kms/latest/developereuide/rotate-keys.html>

IAM managed CMKs are CMKs in your account that are created, managed, and used on your behalf by an IAM service that is integrated with IAM KMS. This CMK is unique to your IAM account and region. Only the service that created the IAM managed CMK can use it

You can login to you IAM dashbaord . Click on "Encryption Keys"

You will find the list based on the services you are using as follows:

- IAM/elasticfilesystem 1 IAM/lightsail
- IAM/s3
- IAM/rds and many more Detailed Guide: KMS

You can recognize IAM managed CMKs because their aliases have the format IAM/service-name, such as IAM/redshift. Typically, a service creates its IAM managed CMK in your account when you set up the service or the first time you use the CMfC

The IAM services that integrate with IAM KMS can use it in many different ways. Some services create IAM managed CMKs in your account. Other services require that you specify a customer managed CMK that you have created. And, others support both types of CMKs to allow you the ease of an IAM managed CMK or the control of a customer-managed CMK

Rotation period for CMKs is as follows:

- IAM managed CMKs: 1095 days
- Customer managed CMKs: 365 days

Since question mentions about "CMK where backing keys is managed by IAM", its Amazon(IAM) managed and its rotation period turns out to be 1095 days{every 3 years)

For more details, please check below IAM Docs: <https://docs.IAM.amazon.com/kms/latest/developerguide/concepts.html> The correct answer is: After 3 years

Submit your Feedback/Queries to our Experts

NEW QUESTION 271

- (Exam Topic 2)

Your company has defined privileged users for their IAM Account. These users are administrators for key resources defined in the company. There is now a mandate to enhance the security authentication for these users. How can this be accomplished?

Please select:

- A. Enable MFA for these user accounts
- B. Enable versioning for these user accounts
- C. Enable accidental deletion for these user accounts
- D. Disable root access for the users

Answer: A

Explanation:

The IAM Documentation mentions the following as a best practices for IAM users. For extra security, enable multi-factor authentication (MFA) for privileged IAM users (users who are allowed access to sensitive resources or APIs). With MFA, users have a device that generates unique authentication code (a one-time password, or OTP). Users must provide both their normal credentials (like their user name and password) and the OTP. The MFA device can either be a special piece of hardware, or it can be a virtual device (for example, it can run in an app on a smartphone).

Option B,C and D are invalid because no such security options are available in IAM For more information on IAM best practices, please visit the below URL

<https://docs.IAM.amazon.com/IAM/latest/UserGuide/best-practices.html> The correct answer is: Enable MFA for these user accounts

Submit your Feedback/Queries to our Experts

NEW QUESTION 276

- (Exam Topic 2)

A Security Administrator is configuring an Amazon S3 bucket and must meet the following security requirements:

- > Encryption in transit
- > Encryption at rest
- > Logging of all object retrievals in IAM CloudTrail

Which of the following meet these security requirements? (Choose three.)

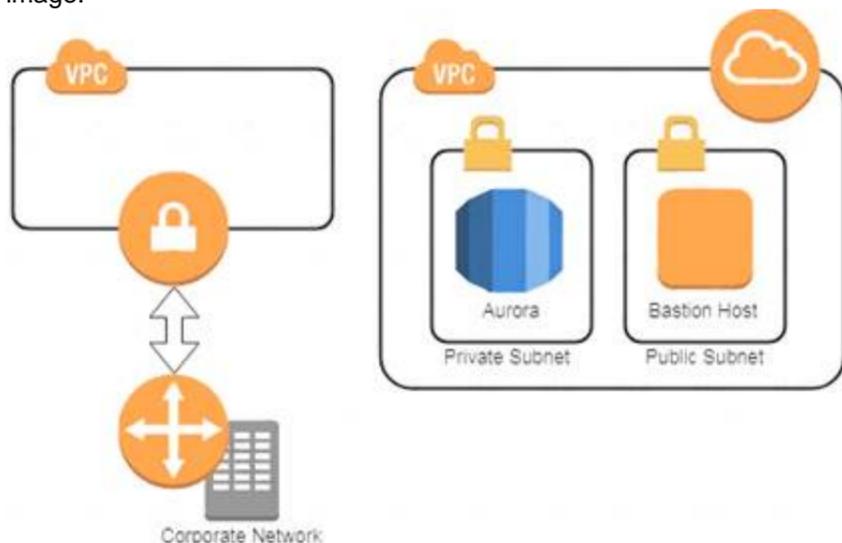
- A. Specify "IAM:SecureTransport": "true" within a condition in the S3 bucket policy.
- B. Enable a security group for the S3 bucket that allows port 443, but not port 80.
- C. Set up default encryption for the S3 bucket.
- D. Enable Amazon CloudWatch Logs for the IAM account.
- E. Enable API logging of data events for all S3 objects.
- F. Enable S3 object versioning for the S3 bucket.

Answer: ACE

NEW QUESTION 277

- (Exam Topic 2)

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



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

How can a Security Engineer securely set up the bastion host?

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

Answer: A

NEW QUESTION 278

- (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 etc. In 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 lower network levels.

<https://docs.IAM.amazon.com/vpc/latest/userguide/flow-logs.html>

NEW QUESTION 279

- (Exam Topic 2)

A Security Engineer has created an Amazon CloudWatch event that invokes an IAM Lambda function daily. The Lambda function runs an Amazon Athena query

that checks IAM CloudTrail logs in Amazon S3 to detect whether any IAM user accounts or credentials have been created in the past 30 days. The results of the Athena query are created in the same S3 bucket. The Engineer runs a test execution of the Lambda function via the IAM Console, and the function runs successfully.

After several minutes, the Engineer finds that his Athena query has failed with the error message: "Insufficient Permissions". The IAM permissions of the Security Engineer and the Lambda function are shown below:

Security Engineer

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

Lambda function execution role

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

What is causing the error?

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

Answer: D

NEW QUESTION 281

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 285

- (Exam Topic 2)

An organization is using IAM CloudTrail, Amazon CloudWatch Logs, and Amazon CloudWatch to send alerts when new access keys are created. However, the alerts are no longer appearing in the Security Operations mail box.

Which of the following actions would resolve this issue?

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

Answer: C

NEW QUESTION 288

- (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 291

- (Exam Topic 2)

Which of the following is not a best practice for carrying out a security audit? Please select:

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

Answer: A

Explanation:

A year's time is generally too long a gap for conducting security audits The IAM Documentation mentions the following

You should audit your security configuration in the following situations: On a periodic basis.

If there are changes in your organization, such as people leaving.

If you have stopped using one or more individual IAM services. This is important for removing permissions that users in your account no longer need.

If you've added or removed software in your accounts, such as applications on Amazon EC2 instances, IAM OpsWor stacks, IAM CloudFormation templates, etc.

If you ever suspect that an unauthorized person might have accessed your account.

Option B, C and D are all the right ways and recommended best practices when it comes to conducting audits For more information on Security Audit guideline, please visit the below URL:

<https://docs.IAM.amazon.com/eeneral/latest/gr/IAM-security-audit-euide.html>

The correct answer is: Conduct an audit on a yearly basis Submit your Feedback/Queries to our Experts

NEW QUESTION 296

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions 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](#)