

Exam Questions SCS-C02

AWS Certified Security - Specialty

<https://www.2passeasy.com/dumps/SCS-C02/>



NEW QUESTION 1

- (Exam Topic 1)

An application is currently secured using network access control lists and security groups. Web servers are located in public subnets behind an Application Load Balancer (ALB); application servers are located in private subnets.

How can edge security be enhanced to safeguard the Amazon EC2 instances against attack? (Choose two.)

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

Answer: BC

NEW QUESTION 2

- (Exam Topic 1)

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

How should this be accomplished?

- A. 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 3

- (Exam Topic 1)

The Security Engineer is managing a traditional three-tier web application that is running on Amazon EC2 instances. The application has become the target of increasing numbers of malicious attacks from the Internet.

What steps should the Security Engineer take to check for known vulnerabilities and limit the attack surface? (Choose two.)

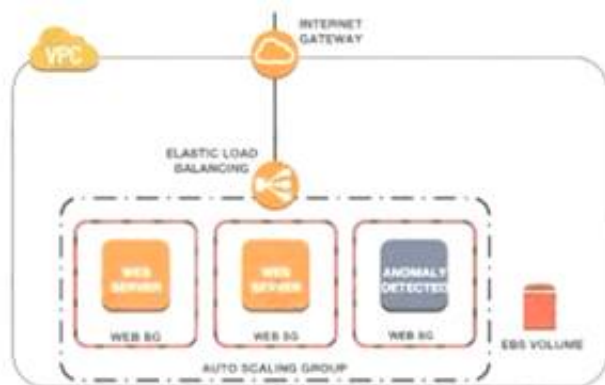
- A. Use IAM Certificate Manager to encrypt all traffic between the client and application servers.
- B. Review the application security groups to ensure that only the necessary ports are open.
- C. Use Elastic Load Balancing to offload Secure Sockets Layer encryption.
- D. Use Amazon Inspector to periodically scan the backend instances.
- E. Use IAM Key Management Services to encrypt all the traffic between the client and application servers.

Answer: BD

NEW QUESTION 4

- (Exam Topic 1)

A Security Engineer noticed an anomaly within a company EC2 instance as shown in the image. The Engineer must now investigate what is causing the anomaly. What are the MOST effective steps to take to ensure that the instance is not further manipulated while allowing the Engineer to understand what happened?



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

Answer: B

NEW QUESTION 5

- (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 tile 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 6

- (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 7

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 8

- (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-destaddr fields in the log format.
- G. Include the subnet-id and instance-id fields in the log format.

Answer: AE

NEW QUESTION 9

- (Exam Topic 1)

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

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

Answer: AB

Explanation:

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

NEW QUESTION 10

- (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 10

- (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 12

- (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 snare 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 17

- (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 19

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

Answer: C

Explanation:

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

NEW QUESTION 20

- (Exam Topic 1)

A company is trying to replace its on-premises bastion hosts used to access on-premises Linux servers with IAM Systems Manager Session Manager. A security

engineer has installed the Systems Manager Agent on all servers. The security engineer verifies that the agent is running on all the servers, but Session Manager cannot connect to them. The security engineer needs to perform verification steps before Session Manager will work on the servers. Which combination of steps should the security engineer perform? (Select THREE.)

- A. Open inbound port 22 to 0.0.0.0/0 on all Linux servers.
- B. Enable the advanced-instances tier in Systems Manager.
- C. Create a managed-instance activation for the on-premises servers.
- D. Reconfigure the Systems Manager Agent with the activation code and ID.
- E. Assign an IAM role to all of the on-premises servers.
- F. Initiate an inventory collection with Systems Manager on the on-premises servers

Answer: CEF

NEW QUESTION 21

- (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 26

- (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 29

- (Exam Topic 1)

A company is setting up products to deploy in IAM Service Catalog. Management is concerned that when users launch products, elevated IAM privileges will be required to create resources. How should the company mitigate this concern?

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

Answer: B

Explanation:

<https://docs.IAM.amazon.com/servicecatalog/latest/adminguide/constraints-launch.html>

Launch constraints apply to products in the portfolio (product-portfolio association). Launch constraints do not apply at the portfolio level or to a product across all portfolios. To associate a launch constraint with all products in a portfolio, you must apply the launch constraint to each product individually.

NEW QUESTION 31

- (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 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 points at the S3 bucket the CloudTrail trails are being written to. Use Athena to run queries against the trails.

Answer: D

NEW QUESTION 35

- (Exam Topic 1)

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

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

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

Answer: A

Explanation:

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

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

NEW QUESTION 39

- (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 40

- (Exam Topic 1)

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

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

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

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

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

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

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

Answer: BEF

NEW QUESTION 41

- (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 46

- (Exam Topic 1)

The Development team receives an error message each time the team members attempt to encrypt or decrypt a Secure String parameter from the SSM Parameter Store by using an IAM KMS customer managed key (CMK). Which CMK-related issues could be responsible? (Choose two.)

- A. The CMK specified in the application does not exist.
- B. The CMK specified in the application is currently in use.
- C. The CMK specified in the application is using the CMK KeyID instead of CMK Amazon Resource Name.
- D. The CMK specified in the application is not enabled.
- E. The CMK specified in the application is using an alias.

Answer: AD

Explanation:

https://docs.amazonaws.cn/en_us/kms/latest/developerguide/services-parameter-store.html

NEW QUESTION 51

- (Exam Topic 1)

A company has an encrypted Amazon S3 bucket. An Application Developer has an IAM policy that allows access to the S3 bucket, but the Application Developer is unable to access objects within the bucket. What is a possible cause of the issue?

- A. The S3 ACL for the S3 bucket fails to explicitly grant access to the Application Developer.
- B. The IAM KMS key for the S3 bucket fails to list the Application Developer as an administrator.
- C. The S3 bucket policy fails to explicitly grant access to the Application Developer.
- D. The S3 bucket policy explicitly denies access to the Application Developer.

Answer: C

NEW QUESTION 54

- (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 56

- (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 CloudHSM.
- 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 57

- (Exam Topic 1)

An application developer is using an IAM Lambda function that must use IAM KMS to perform encrypt and decrypt operations for API keys that are less than 2 KB. Which key policy would allow the application to do this while granting least privilege?

- A.

```
{
  "Sid": "AllowUseOfTheKey",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::444455556666:role/EncryptionApp"},
  "Action": [
    "kms:*"
  ],
  "Resource": "*"
}
```
- B.

```
{
  "Sid": "AllowUseOfTheKey",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::444455556666:role/EncryptionApp"},
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt"
  ],
  "Resource": "*"
}
```
- C.

```
{
  "Sid": "AllowUseOfTheKey",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::444455556666:role/EncryptionApp"},
  "Action": [
    "kms:DescribeKey",
    "kms:GenerateDataKey*",
    "kms:Encrypt",
    "kms:ReEncrypt*",
    "kms:Decrypt"
  ]
}
```
- D.

```
{
  "Sid": "AllowUseOfTheKey",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::444455556666:role/EncryptionApp"},
  "Action": [
    "kms:DescribeKey",
    "kms:GenerateDataKey*",
    "kms:Encrypt",
    "kms:ReEncrypt*",
    "kms:Disable*",
    "kms:Decrypt"
  ],
}
```

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

Answer: C

NEW QUESTION 61

- (Exam Topic 1)

A company has a compliance requirement to rotate its encryption keys on an annual basis. A Security Engineer needs a process to rotate the KMS Customer Master Keys (CMKs) that were created using imported key material.

How can the Engineer perform the key rotation process MOST efficiently?

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

Answer: A

NEW QUESTION 65

- (Exam Topic 2)

A company wants to control access to its IAM resources by using identities and groups that are defined in its existing Microsoft Active Directory. What must the company create in its IAM account to map permissions for IAM services to Active Directory user attributes?

- A. IAM IAM groups
B. IAM IAM users
C. IAM IAM roles
D. IAM IAM access keys

Answer: C

Explanation:

Prerequisites to establish Federation Services in IAM - You have a working AD directory and AD FS server. - You have created an identity provider (IdP) in your IAM account using your XML file from your AD FS server. Remember the name of your IdP because you will use it later in this solution. -You have created the appropriate IAM roles in your IAM account, which will be used for federated access.

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

NEW QUESTION 66

- (Exam Topic 2)

During a recent security audit, it was discovered that multiple teams in a large organization have placed restricted data in multiple Amazon S3 buckets, and the data may have been exposed. The auditor has requested that the organization identify all possible objects that contain personally identifiable information (PII) and then determine whether this information has been accessed.

What solution will allow the Security team to complete this request?

- A. Using Amazon Athena, query the impacted S3 buckets by using the PII query identifier functio
- B. Then, create a new Amazon CloudWatch metric for Amazon S3 object access to alert when the objects are accessed.
- C. Enable Amazon Macie on the S3 buckets that were impacted, then perform data classificatio
- D. For identified objects that contain PII, use the research function for auditing IAM CloudTrail logs and S3 bucket logs for GET operations.
- E. Enable Amazon GuardDuty and enable the PII rule set on the S3 buckets that were impacted, then perform data classificatio
- F. Using the PII findings report from GuardDuty, query the S3 bucket logs by using Athena for GET operations.
- G. Enable Amazon Inspector on the S3 buckets that were impacted, then perform data classificatio
- H. For identified objects that contain PII, query the S3 bucket logs by using Athena for GET operations.

Answer: B

NEW QUESTION 67

- (Exam Topic 2)

You have an S3 bucket hosted in IAM. This is used to host promotional videos uploaded by yourself. You need to provide access to users for a limited duration of time. How can this be achieved?

Please select:

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

Answer: B

Explanation:

The IAM Documentation mentions the following

All objects by default are private. Only the object owner has permission to access these objects. However, the object owner can optionally share objects with others by creating a pre-signed URL using their own security credentials, to grant time-limited permission to download the objects.

Option A is invalid because this can be used to prevent accidental deletion of objects Option C is invalid because timestamps are not possible for Roles

Option D is invalid because policies is not the right way to limit access based on time For more information on pre-signed URL's, please visit the URL:

<https://docs.IAM.ama2on.com/AmazonS3/latest/dev/ShareObjectPreSignedURL.html>

The correct answer is: Use Pre-signed URL's Submit your Feedback/Queries to our Experts

NEW QUESTION 68

- (Exam Topic 2)

The Security Engineer for a mobile game has to implement a method to authenticate users so that they can save their progress. Because most of the users are part of the same OpenID-Connect compatible social media website, the Security Engineer would like to use that as the identity provider.

Which solution is the SIMPLEST way to allow the authentication of users using their social media identities?

- A. Amazon Cognito
- B. AssumeRoleWithWebIdentity API
- C. Amazon Cloud Directory
- D. Active Directory (AD) Connector

Answer: A

NEW QUESTION 70

- (Exam Topic 2)

An organization operates a web application that serves users globally. The application runs on Amazon EC2 instances behind an Application Load Balancer. There is an Amazon CloudFront distribution in front of the load balancer, and the organization uses IAM WAF. The application is currently experiencing a volumetric attack whereby the attacker is exploiting a bug in a popular mobile game.

The application is being flooded with HTTP requests from all over the world with the User-Agent set to the following string: Mozilla/5.0 (compatible; ExampleCorp; ExampleGame/1.22; Mobile/1.0)

What mitigation can be applied to block attacks resulting from this bug while continuing to service legitimate requests?

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

Answer: A

Explanation:

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

NEW QUESTION 75

- (Exam Topic 2)

Which of the following is the most efficient way to automate the encryption of IAM CloudTrail logs using a Customer Master Key (CMK) in IAM KMS?

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

Answer: C

Explanation:

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

NEW QUESTION 77

- (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 82

- (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 83

- (Exam Topic 2)

What is the function of the following IAM Key Management Service (KMS) key policy attached to a customer master key (CMK)?

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:user/ExampleUser"
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:GenerateDataKey*",
    "kms:CreateGrant",
    "kms:ListGrants"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:ViaService": [
        "workmail.us-west-2.amazonaws.com",
        "ses.us-west-2.amazonaws.com"
      ]
    }
  }
}
```

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

region.

D. The key policy allows WorkMail or SES to encrypt or decrypt on behalf of the user for any CMK in the account.

Answer: C

NEW QUESTION 86

- (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 91

- (Exam Topic 2)

A company has contracted with a third party to audit several IAM accounts. To enable the audit, cross-account IAM roles have been created in each account targeted for audit. The Auditor is having trouble accessing some of the accounts.

Which of the following may be causing this problem? (Choose three.)

A. The external ID used by the Auditor is missing or incorrect.

B. The Auditor is using the incorrect password.

C. The Auditor has not been granted sts:AssumeRole for the role in the destination account.

D. The Amazon EC2 role used by the Auditor must be set to the destination account role.

E. The secret key used by the Auditor is missing or incorrect.

F. The role ARN used by the Auditor is missing or incorrect.

Answer: ACF

Explanation:

Using IAM to grant access to a Third-Party Account 1) Create a role to provide access to the require resources 1.1) Create a role policy that specifies the IAM

Account ID to be accessed, "sts:AssumeRole" as action, and "sts:ExternalID" as condition 1.2) Create a role using the role policy just created 1.3) Assign a

resouce policy to the role. This will provide permission to access resource ARNs to the auditor 2) Repeat steps 1 and 2 on all IAM accounts 3) The auditor

connects to the IAM account IAM Security Token Service (STS). The auditor must provide its ExternalID from step 1.2, the ARN of the role he is trying to assume

from step 1.3, sts:ExternalID 4) STS provide the auditor with temporary credentials that provides the role access from step 1

https://docs.IAM.amazon.com/IAM/latest/UserGuide/id_roles_create_for-user_externalid.html

<https://IAM.amazon.com/blogs/security/how-to-audit-cross-account-roles-using-IAM-cloudtrail-and-amazon-clo>

NEW QUESTION 94

- (Exam Topic 2)

A Security Engineer must add additional protection to a legacy web application by adding the following HTTP security headers:

-Content Security-Policy

-X-Frame-Options

-X-XSS-Protection

The Engineer does not have access to the source code of the legacy web application. Which of the following approaches would meet this requirement?

A. Configure an Amazon Route 53 routing policy to send all web traffic that does not include the required headers to a black hole.

B. Implement an IAM Lambda@Edge origin response function that inserts the required headers.

C. Migrate the legacy application to an Amazon S3 static website and front it with an Amazon CloudFront distribution.

D. Construct an IAM WAF rule to replace existing HTTP headers with the required security headers by using regular expressions.

Answer: B

NEW QUESTION 95

- (Exam Topic 2)

A company uses IAM Organization to manage 50 IAM accounts. The finance staff members log in as IAM 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 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 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 98

- (Exam Topic 2)

An Amazon EC2 instance is denied access to a newly created IAM KMS CMK used for decrypt actions. The environment has the following configuration:

- The instance is allowed the kms:Decrypt action in its IAM role for all resources
 - The IAM KMS CMK status is set to enabled
 - The instance can communicate with the KMS API using a configured VPC endpoint
- What is causing the issue?

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

Answer: D

Explanation:

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

NEW QUESTION 103

- (Exam Topic 2)

An IAM account includes two S3 buckets: bucket1 and bucket2. The bucket2 does not have a policy defined, but bucket1 has the following bucket policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": { "AWS": "arn:aws:iam: : 123456789012: user/alice" },
      "Action": "s3:*",
      "Resource": [ "arn:aws:s3: : bucket1", "arn:aws:s3: : bucket1/*" ]
    }
  ]
}
```

In addition, the same account has an IAM User named "alice", with the following IAM policy.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "s3:*",
    "Resource": [ "arn:aws:s3: : bucket2", "arn:aws:s3: : bucket2/*" ]
  }]
}
```

Which buckets can user "alice" access?

- A. Bucket1 only
- B. Bucket2 only
- C. Both bucket1 and bucket2
- D. Neither bucket1 nor bucket2

Answer: C

Explanation:

Both S3 policies and IAM policies can be used to grant access to buckets. IAM policies specify what actions are allowed or denied on what IAM resources (e.g. allow ec2:TerminateInstance on the EC2 instance with instance_id=i-8b3620ec). You attach IAM policies to IAM users, groups, or roles, which are then subject to the permissions you've defined. In other words, IAM policies define what a principal can do in your IAM environment. S3 bucket policies, on the other hand, are attached only to S3 buckets. S3 bucket policies specify what actions are allowed or denied for which principals on the bucket that the bucket policy is attached to (e.g. allow user Alice to PUT but not DELETE objects in the bucket).

<https://IAM.amazon.com/blogs/security/iam-policies-and-bucket-policies-and-acls-oh-my-controlling-access-to>

NEW QUESTION 106

- (Exam Topic 2)

A corporate cloud security policy states that communications between the company's VPC and KMS must travel entirely within the IAM network and not use public service endpoints.

Which combination of the following actions MOST satisfies this requirement? (Choose two.)

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

Answer: AC

Explanation:

An IAM policy can deny access to KMS except through your VPC endpoint with the following condition statement:

```
"Condition": { "StringNotEquals": {  
  "IAM:sourceVpce": "vpce-0295a3caf8414c94a"  
}  
}
```

If you select the Enable Private DNS Name option, the standard IAM KMS DNS hostname (<https://kms.<region>.amazonIAM.com>) resolves to your VPC endpoint.

NEW QUESTION 107

- (Exam Topic 2)

A company maintains sensitive data in an Amazon S3 bucket that must be protected using an IAM KMS CMK. The company requires that keys be rotated automatically every year. How should the bucket be configured?

- A. Select server-side encryption with Amazon S3-managed keys (SSE-S3) and select an IAM-managed CMK.
- B. Select Amazon S3-IAM KMS managed encryption keys (S3-KMS) and select a customer-managed CMK with key rotation enabled.
- C. Select server-side encryption with Amazon S3-managed keys (SSE-S3) and select a customer-managed CMK that has imported key material.
- D. Select server-side encryption with IAM KMS-managed keys (SSE-KMS) and select an alias to an IAM-managed CMK.

Answer: B

NEW QUESTION 108

- (Exam Topic 2)

You are hosting a web site via website hosting on an S3 bucket - [http://demo.s3-website-us-east-1](http://demo.s3-website-us-east-1.amazonaws.com)

.amazonIAM.com. You have some web pages that use Javascript that access resources in another bucket which has web site hosting also enabled. But when users access the web pages, they are getting a blocked Javascript error. How can you rectify this?

Please select:

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

Answer: A

Explanation:

Your answer is incorrect Answer-A

Such a scenario is also given in the IAM Documentation Cross-Origin Resource Sharing: Use-case Scenarios The following are example scenarios for using CORS:

- Scenario 1: Suppose that you are hosting a website in an Amazon S3 bucket named website as described in Hosting a Static Website on Amazon S3. Your users load the website endpoint <http://website.s3-website-us-east-1.amazonaws.com>. Now you want to use JavaScript on the webpages that are stored in this bucket to be able to make authenticated GET and PUT requests against the same bucket by using the Amazon S3 API endpoint for the bucket website.s3.amazonaws.com. A browser would normally block JavaScript from allowing those requests, but with CORS you can configure your bucket to explicitly enable cross-origin requests from website.s3-website-us-east-1.amazonaws.com.

- Scenario 2: Suppose that you want to host a web font from your S3 bucket. Again, browsers require a CORS check (also called a preflight check) for loading web fonts. You would configure the bucket that is hosting the web font to allow any origin to make these requests.

Option B is invalid because versioning is only to create multiple versions of an object and can help in accidental deletion of objects

Option C is invalid because this is used as an extra measure of caution for deletion of objects Option D is invalid because this is used for Cross region replication of objects

For more information on Cross Origin Resource sharing, please visit the following URL

- <https://docs.IAM.amazonaws.com/AmazonS3/latest/dev/cors.html> The correct answer is: Enable CORS for the bucket

Submit your Feedback/Queries to our Experts

NEW QUESTION 109

- (Exam Topic 2)

A company has five IAM accounts and wants to use IAM CloudTrail to log API calls. The log files must be stored in an Amazon S3 bucket that resides in a new account specifically built for centralized services with a unique top-level prefix for each trail. The configuration must also enable detection of any modification to the logs.

Which of the following steps will implement these requirements? (Choose three.)

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

Answer: ACE

Explanation:

<https://docs.IAM.amazon.com/IAMcloudtrail/latest/userguide/best-practices-security.html>

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

NEW QUESTION 112

- (Exam Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 113

- (Exam Topic 2)

A security alert has been raised for an Amazon EC2 instance in a customer account that is exhibiting strange behavior. The Security Engineer must first isolate the EC2 instance and then use tools for further investigation.

What should the Security Engineer use to isolate and research this event? (Choose three.)

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

Answer: ADF

Explanation:

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

NEW QUESTION 117

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 119

- (Exam Topic 2)

A Security Engineer must design a solution that enables the Incident Response team to audit for changes to a user's IAM permissions in the case of a security incident.

How can this be accomplished?

- A. Use IAM Config to review the IAM policy assigned to users before and after the incident.
- B. Run the GenerateCredentialReport via the IAM CLI, and copy the output to Amazon S3 daily for auditing purposes.
- C. Copy IAM CloudFormation templates to S3, and audit for changes from the template.
- D. Use Amazon EC2 Systems Manager to deploy images, and review IAM CloudTrail logs for changes.

Answer: A

Explanation:

<https://IAM.amazon.com/blogs/security/how-to-record-and-govern-your-iam-resource-configurations-using-IAM>

NEW QUESTION 120

- (Exam Topic 2)

A Developer who is following IAM best practices for secure code development requires an application to encrypt sensitive data to be stored at rest, locally in the application, using IAM KMS. What is the simplest and MOST secure way to decrypt this data when required?

- A. Request KMS to provide the stored unencrypted data key and then use the retrieved data key to decrypt the data.
- B. Keep the plaintext data key stored in Amazon DynamoDB protected with IAM policies
- C. Query DynamoDB to retrieve the data key to decrypt the data
- D. Use the Encrypt API to store an encrypted version of the data key with another customer managed key. Decrypt the data key and use it to decrypt the data when required.
- E. Store the encrypted data key alongside the encrypted data
- F. Use the Decrypt API to retrieve the data key to decrypt the data when required.

Answer: D

Explanation:

We recommend that you use the following pattern to locally encrypt data: call the GenerateDataKey API, use the key returned in the Plaintext response field to locally encrypt data, and then erase the plaintext data key from memory. Store the encrypted data key (contained in the CiphertextBlob field) alongside of the locally encrypted data. The Decrypt API returns the plaintext key from the encrypted key.

<https://docs.IAM.amazon.com/sdkfornet/latest/apidocs/items/MKeyManagementServiceKeyManagementService>

NEW QUESTION 123

- (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 125

- (Exam Topic 2)

A company uses identity federation to authenticate users into an identity account (987654321987) where the users assume an IAM role named IdentityRole. The users then assume an IAM role named JobFunctionRole in the target IAM account (123456789123) to perform their job functions.

A user is unable to assume the IAM role in the target account. The policy attached to the role in the identity account is:

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

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

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

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

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

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

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

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

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

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

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

Answer: A

NEW QUESTION 130

- (Exam Topic 2)

Your company has a requirement to monitor all root user activity by notification. How can this best be achieved? Choose 2 answers from the options given below. Each answer forms part of the solution

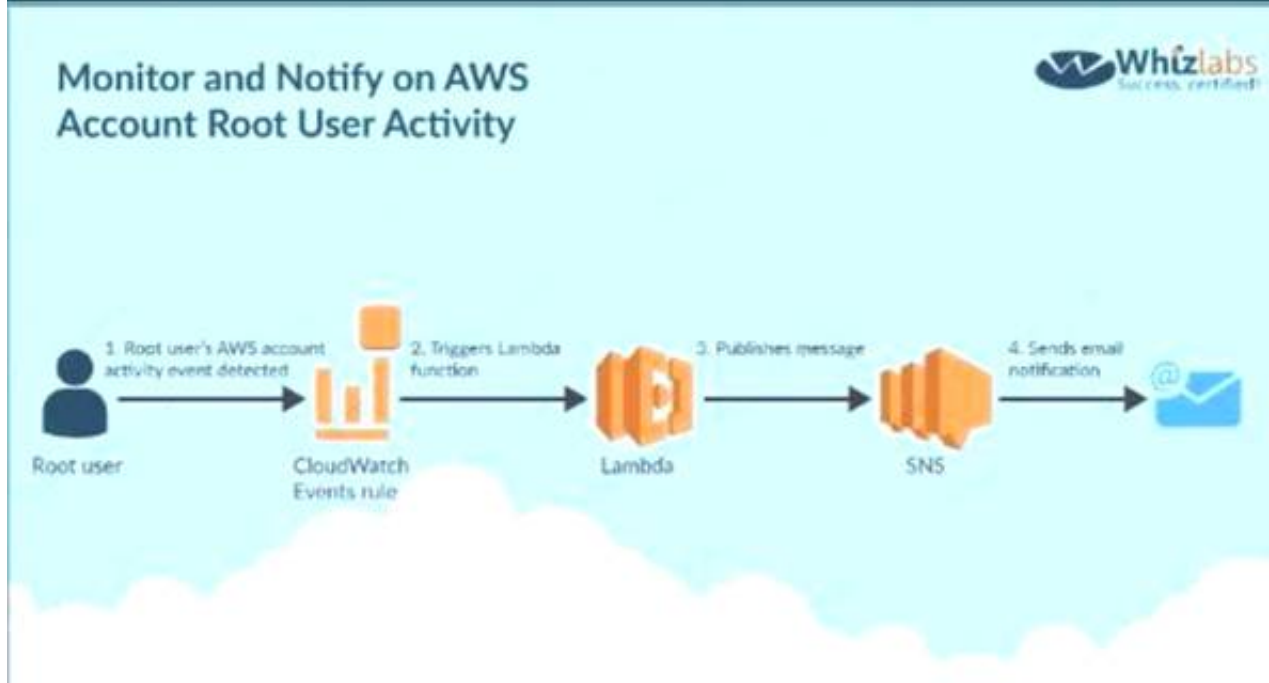
Please select:

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

Answer: AC

Explanation:

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



Option B is invalid because you need to create a Cloudwatch Events Rule and there is such thing as a Cloudwatch Logs Rule Option D is invalid because Cloud Trail API calls can be recorded but cannot be used to send across notifications For more information on this blog article, please visit the following URL:

<https://IAM.amazon.com/blogs/mt/monitor-and-notify-on-IAM-account-root-user-activity> The correct answers are: Create a Cloudwatch Events Rule, Use a Lambda function

Submit your Feedback/Queries to our Experts

NEW QUESTION 132

- (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 135

- (Exam Topic 2)

Your IT Security team has advised to carry out a penetration test on the resources in their company's IAM Account. This is as part of their capability to analyze the security of the Infrastructure. What should be done first in this regard?

Please select:

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

Answer: C

Explanation:

This concept is given in the IAM Documentation

How do I submit a penetration testing request for my IAM resources? Issue

I want to run a penetration test or other simulated event on my IAM architecture. How do I get permission from IAM to do that?

Resolution

Before performing security testing on IAM resources, you must obtain approval from IAM. After you submit your request IAM will reply in about two business days. IAM might have additional questions about your test which can extend the approval process, so plan accordingly and be sure that your initial request is as detailed as possible.

If your request is approved, you'll receive an authorization number.

Option A.B and D are all invalid because the first step is to get prior authorization from IAM for penetration tests

For more information on penetration testing, please visit the below URL

* <https://IAM.amazon.com/security/penetration-testing/>

* <https://IAM.amazon.com/premiumsupport/knowledge-center/penetration-testing/> (

The correct answer is: Submit a request to IAM Support Submit your Feedback/Queries to our Experts

NEW QUESTION 138

- (Exam Topic 2)

A distributed web application is installed across several EC2 instances in public subnets residing in two Availability Zones. Apache logs show several intermittent brute-force attacks from hundreds of IP addresses at the layer 7 level over the past six months.

What would be the BEST way to reduce the potential impact of these attacks in the future?

- A. Use custom route tables to prevent malicious traffic from routing to the instances.
- B. Update security groups to deny traffic from the originating source IP addresses.
- C. Use network ACLs.
- D. Install intrusion prevention software (IPS) on each instance.

Answer: D

Explanation:

<https://docs.IAM.amazon.com/vpc/latest/userguide/amazon-vpc-limits.html> NACL has limit 20 (can increase to maximum 40 rule), and more rule will make more low-latency

NEW QUESTION 143

- (Exam Topic 2)

A company hosts a critical web application on the IAM Cloud. This is a key revenue generating application for the company. The IT Security team is worried about potential DDos attacks against the web site. The senior management has also specified that immediate action needs to be taken in case of a potential DDos attack. What should be done in this regard?

Please select:

- A. Consider using the IAM Shield Service
- B. Consider using VPC Flow logs to monitor traffic for DDos attack and quickly take actions on a trigger of a potential attack.
- C. Consider using the IAM Shield Advanced Service
- D. Consider using Cloudwatch logs to monitor traffic for DDos attack and quickly take actions on a trigger of a potential attack.

Answer: C

Explanation:

Option A is invalid because the normal IAM Shield Service will not help in immediate action against a DDos attack. This can be done via the IAM Shield Advanced Service

Option B is invalid because this is a logging service for VPCs traffic flow but cannot specifically protect against DDos attacks.

Option D is invalid because this is a logging service for IAM Services but cannot specifically protect against DDos attacks.

The IAM Documentation mentions the following

IAM Shield Advanced provides enhanced protections for your applications running on Amazon EC2, Elastic Load Balancing (ELB), Amazon CloudFront and Route 53 against larger and more sophisticated attacks. IAM Shield Advanced is available to IAM Business Support and IAM Enterprise Support customers. IAM Shield Advanced protection provides always-on, flow-based monitoring of network traffic and active application monitoring to provide near real-time notifications of DDos attacks. IAM Shield Advanced also gives customers highly flexible controls over attack mitigations to take actions instantly. Customers can also engage the DDos Response Team (DRT) 24X7 to manage and mitigate their application layer DDos attacks.

For more information on IAM Shield, please visit the below URL: <https://IAM.amazon.com/shield/faqs>;

The correct answer is: Consider using the IAM Shield Advanced Service Submit your Feedback/Queries to our Experts

NEW QUESTION 146

- (Exam Topic 2)

Which approach will generate automated security alerts should too many unauthorized IAM API requests be identified?

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

Answer: A

Explanation:

<https://docs.IAM.amazon.com/IAMcloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail.html#cloudwatc> Open the CloudWatch console at

<https://console.IAM.amazon.com/cloudwatch/>. In the navigation pane,

choose Logs. In the list of log groups, select the check box next to the log group that you created for CloudTrail log events. Choose Create Metric Filter. On the Define Logs Metric Filter screen, choose Filter Pattern and then type the following: { (\$errorCode = "**UnauthorizedOperation") || (\$errorCode = "AccessDenied")} Choose Assign Metric. For Filter Name, type AuthorizationFailures. For Metric Namespace, type CloudTrailMetrics. For Metric Name, type AuthorizationFailureCount.

NEW QUESTION 149

- (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 154

- (Exam Topic 2)

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

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

Answer: AB

Explanation:

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

NEW QUESTION 159

- (Exam Topic 2)

An application has been built with Amazon EC2 instances that retrieve messages from Amazon SQS. Recently, IAM changes were made and the instances can no longer retrieve messages.

What actions should be taken to troubleshoot the issue while maintaining least privilege. (Select two.)

- A. Configure and assign an MFA device to the role used by the instances.
- B. Verify that the SQS resource policy does not explicitly deny access to the role used by the instances.
- C. Verify that the access key attached to the role used by the instances is active.
- D. Attach the AmazonSQSFullAccess managed policy to the role used by the instances.
- E. Verify that the role attached to the instances contains policies that allow access to the queue.

Answer: BE

NEW QUESTION 160

- (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 161

- (Exam Topic 2)

A Security Analyst attempted to troubleshoot the monitoring of suspicious security group changes. The Analyst was told that there is an Amazon CloudWatch alarm in place for these IAM CloudTrail log events.

The Analyst tested the monitoring setup by making a configuration change to the security group but did not receive any alerts.

Which of the following troubleshooting steps should the Analyst perform?

- A. Ensure that CloudTrail and S3 bucket access logging is enabled for the Analyst's IAM account.
- B. Verify that a metric filter was created and then mapped to an alar
- C. Check the alarm notification action.
- D. Check the CloudWatch dashboards to ensure that there is a metric configured with an appropriate dimension for security group changes.
- E. Verify that the Analyst's account is mapped to an IAM policy that includes permissions for cloudwatch: GetMetricStatistics and Cloudwatch: ListMetrics.

Answer: B

Explanation:

MetricFilter:

Type: 'IAM::Logs::MetricFilter' Properties:

LogGroupName: " FilterPattern: >{ (\$eventName = AuthorizeSecurityGroupIngress) || (\$eventName = AuthorizeSecurityGroupEgress) || (\$eventName = RevokeSecurityGroupIngress) || (\$eventName = RevokeSecurityGroupEgress) || (\$eventName = CreateSecurityGroup) || (\$eventName = DeleteSecurityGroup) }

MetricTransformations:

- MetricValue: '1'

MetricNamespace: CloudTrailMetrics MetricName: SecurityGroupEventCount

NEW QUESTION 163

- (Exam Topic 2)

A company is hosting a website that must be accessible to users for HTTPS traffic. Also port 22 should be open for administrative purposes. The administrator's workstation has a static IP address of 203.0.113.1/32. Which of the following security group configurations are the MOST secure but still functional to support these requirements? Choose 2 answers from the options given below

Please select:

- A. Port 443 coming from 0.0.0.0/0
- B. Port 443 coming from 10.0.0.0/16
- C. Port 22 coming from 0.0.0.0/0
- D. Port 22 coming from 203.0.113.1/32

Answer: AD

Explanation:

Since HTTPS traffic is required for all users on the Internet, Port 443 should be open on all IP addresses. For port 22, the traffic should be restricted to an internal subnet.

Option B is invalid, because this only allow traffic from a particular CIDR block and not from the internet Option C is invalid because allowing port 22 from the internet is a security risk

For more information on IAM Security Groups, please visit the following UR

<https://docs.IAM.amazon.com/IAMEC2/latest/UserGuide/usins-network-security.html>

The correct answers are: Port 443 coming from 0.0.0.0/0, Port 22 coming from 203.0.113.1 /32 Submit your Feedback/Queries to our Experts

NEW QUESTION 164

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 167

- (Exam Topic 2)

Amazon CloudWatch Logs agent is successfully delivering logs to the CloudWatch Logs service. However, logs stop being delivered after the associated log stream has been active for a specific number of hours.

What steps are necessary to identify the cause of this phenomenon? (Choose two.)

- A. Ensure that file permissions for monitored files that allow the CloudWatch Logs agent to read the file have not been modified.
- B. Verify that the OS Log rotation rules are compatible with the configuration requirements for agent streaming.
- C. Configure an Amazon Kinesis producer to first put the logs into Amazon Kinesis Streams.
- D. Create a CloudWatch Logs metric to isolate a value that changes at least once during the period before logging stops.
- E. Use IAM CloudFormation to dynamically create and maintain the configuration file for the CloudWatch Logs agent.

Answer: AB

Explanation:

https://acloud.guru/forums/IAM-certified-security-specialty/discussion/-Lm5A3w6_NybQPhh6tRP/Cloudwatch

NEW QUESTION 172

- (Exam Topic 3)

When managing permissions for the API gateway, what can be used to ensure that the right level of permissions are given to developers, IT admins and users? These permissions should be easily managed.

Please select:

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

Answer: B

Explanation:

The IAM Documentation mentions the following

You control access to Amazon API Gateway with IAM permissions by controlling access to the following two API Gateway component processes:

* To create, deploy, and manage an API in API Gateway, you must grant the API developer permissions to perform the required actions supported by the API management component of API Gateway.

* To call a deployed API or to refresh the API caching, you must grant the API caller permissions to perform required IAM actions supported by the API execution

component of API Gateway.

Option A, C and D are invalid because these cannot be used to control access to IAM services. This needs to be done via policies. For more information on permissions with the API gateway, please visit the following URL:

<https://docs.IAM.amazon.com/apisateway/latest/developerguide/permissions.html>

The correct answer is: Use IAM Policies to create different policies for the different types of users. Submit your Feedback/Queries to our Experts

NEW QUESTION 173

- (Exam Topic 3)

What is the result of the following bucket policy?

```
{
  "Statement": [
    {
      "Sid": "Sid1",
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::mybucket/*.",
      "Principal": {
        "AWS": ["arn:aws:iam::111111111:user/mark"]}
    },
    {
      "Sid": "Sid2",
      "Action": "s3:*",
      "Effect": "Deny",
      "Resource": "arn:aws:s3:::mybucket/*",
      "Principal": {
        "AWS": [
          "*"
        ]
      }
    }
  ]
}
```

Choose the correct Answer Please select:

- A. It will allow all access to the bucket mybucket
- B. It will allow the user mark from IAM account number 111111111 all access to the bucket but deny everyone else all access to the bucket
- C. It will deny all access to the bucket mybucket
- D. None of these

Answer: C

Explanation:

The policy consists of 2 statements, one is the allow for the user mark to the bucket and the next is the deny policy for all other users. The deny permission will override the allow and hence all users will not have access to the bucket.

Options A,B and D are all invalid because this policy is used to deny all access to the bucket mybucket For examples on S3 bucket policies, please refer to the below Link: <http://docs.IAM.amazon.com/AmazonS3/latest/dev/example-bucket-policies.html>

The correct answer is: It will deny all access to the bucket mybucket Submit your Feedback/Quenes to our Experts

NEW QUESTION 174

- (Exam Topic 3)

An employee keeps terminating EC2 instances on the production environment. You've determined the best way to ensure this doesn't happen is to add an extra layer of defense against terminating the instances. What is the best method to ensure the employee does not terminate the production instances? Choose the 2 correct answers from the options below

Please select:

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

Answer: AB

Explanation:

Tags enable you to categorize your IAM resources in different ways, for example, by purpose, owner, or environment. This is useful when you have many resources of the same type — you can quickly identify a specific resource based on the tags you've assigned to it. Each tag consists of a key and an optional value, both of which you define

Options C&D are incorrect because it will not ensure that the employee cannot terminate the instance. For more information on tagging answer resources please refer to the below URL:

http://docs.IAM.amazon.com/IAMEC2/latest/UserGuide/Usins_Tags.html

The correct answers are: Tag the instance with a production-identifying tag and add resource-level permissions to the employe user with an explicit deny on the terminate API call to instances with the production tag.. Tag the instance with a production-identifying tag and modify the employees group to allow only start stop, and reboot API calls and not the terminate instance
Submit your Feedback/Queries to our Experts

NEW QUESTION 177

- (Exam Topic 3)

Your company is planning on developing an application in IAM. This is a web based application. The application user will use their facebook or google identities for authentication. You want to have the ability to manage user profiles without having to add extra coding to manage this. Which of the below would assist in this. Please select:

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

Answer: C

Explanation:

The IAM Documentation mentions the following

A user pool is a user directory in Amazon Cognito. With a user pool, your users can sign in to your web or mobile app through Amazon Cognito. Your users can also sign in through social identity providers like Facebook or Amazon, and through SAML identity providers. Whether your users sign in directly or through a third party, all members of the user pool have a directory profile that you can access through an SDK.

User pools provide:

Sign-up and sign-in services.

A built-in, customizable web UI to sign in users.

Social sign-in with Facebook, Google, and Login with Amazon, as well as sign-in with SAML identity providers from your user pool.

User directory management and user profiles.

Security features such as multi-factor authentication (MFA), checks for compromised credentials, account takeover protection, and phone and email verification.

Customized workflows and user migration through IAM Lambda triggers. Options A and B are invalid because these are not used to manage users Option D is invalid because this would be a maintenance overhead

For more information on Cognito User Identity pools, please refer to the below Link: <https://docs.IAM.amazon.com/coenito/latest/developerguide/cognito-user-identity-pools.html>

The correct answer is: Use IAM Cognito to manage the user profiles Submit your Feedback/Queries to our Experts

NEW QUESTION 178

- (Exam Topic 3)

Which of the following is the correct sequence of how KMS manages the keys when used along with the Redshift cluster service Please select:

- A. The master keys encrypts the cluster ke
- B. The cluster key encrypts the database ke
- C. The database key encrypts the data encryption keys.
- D. The master keys encrypts the database ke
- E. The database key encrypts the data encryption keys.
- F. The master keys encrypts the data encryption key
- G. The data encryption keys encrypts the database key
- H. The master keys encrypts the cluster key, database key and data encryption keys

Answer: A

Explanation:

This is mentioned in the IAM Documentation

Amazon Redshift uses a four-tier, key-based architecture for encryption. The architecture consists of data encryption keys, a database key, a cluster key, and a master key.

Data encryption keys encrypt data blocks in the cluster. Each data block is assigned a randomly-generated AES-256 key. These keys are encrypted by using the database key for the cluster.

The database key encrypts data encryption keys in the cluster. The database key is a randomly-generated AES-256 key. It is stored on disk in a separate network from the Amazon Redshift cluster and passed to the cluster across a secure channel.

The cluster key encrypts the database key for the Amazon Redshift cluster.

Option B is incorrect because the master key encrypts the cluster key and not the database key

Option C is incorrect because the master key encrypts the cluster key and not the data encryption keys Option D is incorrect because the master key encrypts the cluster key only

For more information on how keys are used in Redshift, please visit the following URL: <https://docs.IAM.amazon.com/kms/latest/developereuide/services-redshift.html>

The correct answer is: The master keys encrypts the cluster key. The cluster key encrypts the database key. The database key encrypts the data encryption keys. Submit your Feedback/Queries to our Experts

NEW QUESTION 179

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 183

- (Exam Topic 3)

Your application currently uses customer keys which are generated via IAM KMS in the US east region. You now want to use the same set of keys from the EU-Central region. How can this be accomplished?

Please select:

- A. Export the key from the US east region and import them into the EU-Central region
- B. Use key rotation and rotate the existing keys to the EU-Central region
- C. Use the backing key from the US east region and use it in the EU-Central region
- D. This is not possible since keys from KMS are region specific

Answer: D

Explanation:

Option A is invalid because keys cannot be exported and imported across regions. Option B is invalid because key rotation cannot be used to export keys

Option C is invalid because the backing key cannot be used to export keys This is mentioned in the IAM documentation

What geographic region are my keys stored in?

Keys are only stored and used in the region in which they are created. They cannot be transferred to another region. For example; keys created in the EU-Central (Frankfurt) region are only stored and used within the EU-Central (Frankfurt) region

For more information on KMS please visit the following URL: <https://IAM.amazon.com/kms/faqs/>

The correct answer is: This is not possible since keys from KMS are region specific Submit your Feedback/Queries to our Experts

NEW QUESTION 186

- (Exam Topic 3)

You are planning on using the IAM KMS service for managing keys for your application. For which of the following can the KMS CMK keys be used for encrypting?

Choose 2 answers from the options given below

Please select:

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

Answer: CD

Explanation:

The CMK keys themselves can only be used for encrypting data that is maximum 4KB in size. Hence it can be used for encrypting information such as passwords and RSA keys.

Option A and B are invalid because the actual CMK key can only be used to encrypt small amounts of data and not large amounts of data. You have to generate the data key from the CMK key in order to encrypt high amounts of data

For more information on the concepts for KMS, please visit the following URL: <https://docs.IAM.amazon.com/kms/latest/developerguide/concepts.html>

The correct answers are: Password, RSA Keys Submit your Feedback/Queries to our Experts

NEW QUESTION 189

- (Exam Topic 3)

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

Please select:

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

Answer: A

Explanation:

Amazon Glacier is a secure, durable, and extremely low-cost cloud storage service for data archiving and long-term backup. Customers can reliably store large or small amounts of data for as little as \$0,004 per gigabyte per month, a significant savings compared to on-premises solutions.

With Amazon lifecycle policies you can create transition actions in which you define when objects transition to another Amazon S3 storage class. For example, you may choose to transition objects to the STANDARD_IA (IA, for infrequent access) storage class 30 days after creation, or archive objects to the GLACIER storage class one year after creation.

Option B is invalid because lifecycle policies are not available for EBS volumes Option C is invalid because IAM policies cannot be used to move data to Glacier

Option D is invalid because lifecycle policies are not used to move data to Redshift For more information on S3 lifecycle policies, please visit the URL:

<http://docs.IAM.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html>

The correct answer is: Upload data to S3 and use lifecycle policies to move the data into Glacier for long-term archiving.

Submit your Feedback/Queries to our Experts

NEW QUESTION 192

- (Exam Topic 3)

You need to ensure that the CloudTrail logs which are being delivered in your IAM account is encrypted. How can this be achieved in the easiest way possible?

Please select:

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

Answer: A

Explanation:

The IAM Documentation mentions the following

By default the log files delivered by CloudTrail to your bucket are encrypted by Amazon server-side encryption with Amazon S3-managed encryption keys (SSE-S3)

Option B,C and D are all invalid because by default all logs are encrypted when they sent by Cloudtrail to S3 buckets

For more information on IAM Cloudtrail log encryption, please visit the following URL: <https://docs.IAM.amazon.com/IAMcloudtrail/latest/userguide/encrypting-cloudtrail-log-files-with-IAM-kms.htm> The correct answer is: Don't do anything since CloudTrail logs are automatically encrypted. Submit your

Feedback/Queries to our Experts

NEW QUESTION 195

- (Exam Topic 3)

One of the EC2 Instances in your company has been compromised. What steps would you take to ensure that you could apply digital forensics on the Instance.

Select 2 answers from the options given below

Please select:

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

Answer: BC

Explanation:

Option A is invalid because removing the role will not help completely in such a situation

Option D is invalid because terminating the instance means that you cannot conduct forensic analysis on the instance

One way to isolate an affected EC2 instance for investigation is to place it in a Security Group that only the forensic investigators can access. Close all ports except to receive inbound SSH or RDP traffic from one single IP address from which the investigators can safely examine the instance.

For more information on security scenarios for your EC2 Instance, please refer to below URL: <https://d1.IAMstatic.com/Marketplace/scenarios/security/SEC 11 TSB Final.pdf>

The correct answers are: Create a separate forensic instance. Ensure that the security groups only allow communication to this forensic instance

Submit your Feedback/Queries to our Experts

NEW QUESTION 200

- (Exam Topic 3)

Your company has been using IAM for the past 2 years. They have separate S3 buckets for logging the various IAM services that have been used. They have hired an external vendor for analyzing their log files. They have their own IAM account. What is the best way to ensure that the partner account can access the log files in the company account for analysis. Choose 2 answers from the options given below

Please select:

- A. Create an IAM user in the company account
- B. Create an IAM Role in the company account
- C. Ensure the IAM user has access for read-only to the S3 buckets
- D. Ensure the IAM Role has access for read-only to the S3 buckets

Answer: BD

Explanation:

The IAM Documentation mentions the following

To share log files between multiple IAM accounts, you must perform the following general steps. These steps are explained in detail later in this section.

Create an IAM role for each account that you want to share log files with.

For each of these IAM roles, create an access policy that grants read-only access to the account you want to share the log files with.

Have an IAM user in each account programmatically assume the appropriate role and retrieve the log files. Options A and C are invalid because creating an IAM user and then sharing the IAM user credentials with the vendor is a direct 'NO' practise from a security perspective.

For more information on sharing cloudtrail logs files, please visit the following URL <https://docs.IAM.amazon.com/IAMcloudtrail/latest/userguide/cloudtrail-sharing-log-files.html>

The correct answers are: Create an IAM Role in the company account Ensure the IAM Role has access for read-only to the S3 buckets

Submit your Feedback/Queries to our Experts

NEW QUESTION 203

- (Exam Topic 3)

Your company hosts critical data in an S3 bucket. There is a requirement to ensure that all data is encrypted. There is also metadata about the information stored in the bucket that needs to be encrypted as well. Which of the below measures would you take to ensure that the metadata is encrypted?

Please select:

- A. Put the metadata as metadata for each object in the S3 bucket and then enable S3 Server side encryption.
- B. Put the metadata as metadata for each object in the S3 bucket and then enable S3 Server KMS encryption.
- C. Put the metadata in a DynamoDB table and ensure the table is encrypted during creation time.
- D. Put thp metadata in thp S3 hurkpf itself.

Answer: C

Explanation:

Option A ,B and D are all invalid because the metadata will not be encrypted in any case and this is a key requirement from the question.

One key thing to note is that when the S3 bucket objects are encrypted, the meta data is not encrypted. So the best option is to use an encrypted DynamoDB table Important

All GET and PUT requests for an object protected by IAM KMS will fail if they are not made via SSL or by using SigV4. SSE-KMS encrypts only the object data.

Any object metadata is not encrypted. For more information on using KMS encryption for S3, please refer to below URL: 1

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

The correct answer is: Put the metadata in a DynamoDB table and ensure the table is encrypted during creation time. Submit your Feedback/Queries to our Experts

NEW QUESTION 208

- (Exam Topic 3)

Your application currently use IAM Cognito for authenticating users. Your application consists of different types of users. Some users are only allowed read access to the application and others are given contributor access. How wou you manage the access effectively?

Please select:

- A. Create different cognito endpoints, one for the readers and the other for the contributors.
- B. Create different cognito groups, one for the readers and the other for the contributors.
- C. You need to manage this within the application itself
- D. This needs to be managed via Web security tokens

Answer: B

Explanation:

The IAM Documentation mentions the following

You can use groups to create a collection of users in a user pool, which is often done to set the permissions for those users. For example, you can create separate groups for users who are readers, contributors, and editors of your website and app.

Option A is incorrect since you need to create cognito groups and not endpoints

Options C and D are incorrect since these would be overheads when you can use IAM Cognito For more information on IAM Cognito user groups please refer to the below Link:

<https://docs.IAM.amazon.com/coenito/latest/developersuide/cognito-user-pools-user-groups.html>

The correct answer is: Create different cognito groups, one for the readers and the other for the contributors. Submit your Feedback/Queries to our Experts

NEW QUESTION 209

- (Exam Topic 3)

A company has been using the IAM KMS service for managing its keys. They are planning on carrying out housekeeping activities and deleting keys which are no longer in use. What are the ways that can be incorporated to see which keys are in use? Choose 2 answers from the options given below

Please select:

- A. Determine the age of the master key
- B. See who is assigned permissions to the master key
- C. See Cloudtrail for usage of the key
- D. Use IAM cloudwatch events for events generated for the key

Answer: BC

Explanation:

The direct ways that can be used to see how the key is being used is to see the current access permissions and cloudtrail logs

Option A is invalid because seeing how long ago the key was created would not determine the usage of the key

Option D is invalid because Cloudtrail Event is better for seeing for events generated by the key This is also mentioned in the IAM Documentation

Examining CMK Permissions to Determine the Scope of Potential Usage

Determining who or what currently has access to a customer master key (CMK) might help you determine how widely the CM was used and whether it is still needed. To learn how to determine who or what currently has access to a CMK, go to Determining Access to an IAM KMS Customer Master Key.

Examining IAM CloudTrail Logs to Determine Actual Usage

IAM KMS is integrated with IAM CloudTrail, so all IAM KMS API activity is recorded in CloudTrail log files. If you have CloudTrail turned on in the region where your customer master key (CMK) is located, you can examine your CloudTrail log files to view a history of all IAM KMS API activity for a particular CMK, and thus its usage history. You might be able to use a CMK's usage history to help you determine whether or not you still need it

For more information on determining the usage of CMK keys, please visit the following URL:

➤ <https://docs.IAM.amazon.com/kms/latest/developerguide/deleting-keys-determining-usage.html>

The correct answers are: See who is assigned permissions to the master key. See Cloudtrail for usage of the key Submit your Feedback/Queries to our Experts

NEW QUESTION 213

- (Exam Topic 3)

You have just developed a new mobile application that handles analytics workloads on large scale datasets that are stored on Amazon Redshift. Consequently, the application needs to access Amazon Redshift tables. Which of the below methods would be the best both practically and security-wise, to access the tables?

Choose the correct answer from the options below

Please select:

- A. Create an IAM user and generate encryption keys for that use
- B. Create a policy for Redshift read-only acces
- C. Embed th keys in the application.
- D. Create an HSM client certificate in Redshift and authenticate using this certificate.
- E. Create a Redshift read-only access policy in IAM and embed those credentials in the application.
- F. Use roles that allow a web identity federated user to assume a role that allows access to the Redshift table by providing temporary credentials.

Answer: D

Explanation:

The IAM Documentation mentions the following

"When you write such an app, you'll make requests to IAM services that must be signed with an IAM access key. However, we strongly recommend that you do not embed or distribute long-term IAM credentials with apps that a user downloads t device, even in an encrypted store. Instead, build your app so that it requests temporary IAM security credentials dynamica when needed using web identify federation. The supplied temporary credentials map to an IAM role that has only the permissioi needed to perform the tasks required by the mobile app".

Option A.B and C are all automatically incorrect because you need to use IAM Roles for Secure access to services For more information on web identity federation please refer to the below Link:

➤ http://docs.IAM.amazon.com/IAM/latest/UserGuide/id_roles_providers_oidc.html

The correct answer is: Use roles that allow a web identity federated user to assume a role that allows access to the RedShift table by providing temporary credentials.

Submit your Feedback/Queries to our Experts

NEW QUESTION 217

- (Exam Topic 3)

A company has a requirement to create a DynamoDB table. The company's software architect has provided the following CLI command for the DynamoDB table

```
--table-name Customers \
--attribute-definitions \
    AttributeName=ID,AttributeType=S \
    AttributeName=Name,AttributeType=S \
--key-schema \
    AttributeName=ID,KeyType=HASH \
    AttributeName=Name,KeyType=RANGE \
--provisioned-throughput \
    ReadCapacityUnits=10,WriteCapacityUnits=5 \
--sse-specification Enabled=true
```

Which of the following has been taken of from a security perspective from the above command? Please select:

- A. Since the ID is hashed, it ensures security of the underlying table.
- B. The above command ensures data encryption at rest for the Customer table
- C. The above command ensures data encryption in transit for the Customer table
- D. The right throughput has been specified from a security perspective

Answer: B

Explanation:

The above command with the "-sse-specification Enabled=true" parameter ensures that the data for the DynamoDB table is encrypted at rest.

Options A,C and D are all invalid because this command is specifically used to ensure data encryption at rest For more information on DynamoDB encryption, please visit the URL: <https://docs.IAM.amazon.com/amazondynamodb/latest/developerguide/encryption.tutorial.html>

The correct answer is: The above command ensures data encryption at rest for the Customer table

NEW QUESTION 218

- (Exam Topic 3)

Your company has just started using IAM and created an IAM account. They are aware of the potential issues when root access is enabled. How can they best safeguard the account when it comes to root access? Choose 2 answers fro the options given below

Please select:

- A. Delete the root access account
- B. Create an Admin IAM user with the necessary permissions
- C. Change the password for the root account.
- D. Delete the root access keys

Answer: BD

Explanation:

The IAM Documentation mentions the following

All IAM accounts have root user credentials (that is, the credentials of the account owner). These credentials allow full access to all resources in the account.

Because you cant restrict permissions for root user credentials, we recommend that you delete your root user access keys. Then create IAM Identity and Access Management (IAM) user credentials for everyday interaction with IAM.

Option A is incorrect since you cannot delete the root access account

Option C is partially correct but cannot be used as the ideal solution for safeguarding the account For more information on root access vs admin IAM users, please refer to below URL: <https://docs.IAM.amazon.com/eeneral/latest/er/root-vs-iam.html>

The correct answers are: Create an Admin IAM user with the necessary permissions. Delete the root access keys Submit your Feedback/Queries to our Experts

NEW QUESTION 221

- (Exam Topic 3)

Your company looks at the gaming domain and hosts several Ec2 Instances as game servers. The servers each experience user loads in the thousands. There is a concern of DDos attacks on the EC2 Instances which could cause a huge revenue loss to the company. Which of the following can help mitigate this security concern and

also ensure minimum downtime for the servers. Please select:

- A. Use VPC Flow logs to monitor the VPC and then implement NACL's to mitigate attacks
- B. Use IAM Shield Advanced to protect the EC2 Instances
- C. Use IAM Inspector to protect the EC2 Instances
- D. Use IAM Trusted Advisor to protect the EC2 Instances

Answer: B

Explanation:

Below is an excerpt from the IAM Documentation on some of the use cases for IAM Shield C:\Users\wk\Desktop\mudassar\Untitled.jpg

Example AWS Shield Advanced Use Cases		
You can use Shield Advanced to protect your resources in many types of scenarios. However, in some cases you should use other services or combine other services with Shield Advanced to offer the best protection. Following are examples of how to use Shield Advanced or other AWS services to help protect your resources.		
Goal	Suggested services	Related service documentation
Protect a web application and RESTful APIs against a DDoS attack	Shield Advanced protecting an Amazon CloudFront distribution and an Application Load Balancer	Amazon Elastic Load Balancing Documentation , Amazon CloudFront Documentation
Protect a TCP-based application against a DDoS attack	Shield Advanced protecting a Network Load Balancer attached to an Elastic IP address	Amazon Elastic Load Balancing Documentation
Protect a UDP-based game server against a DDoS attack	Shield Advanced protecting an Amazon EC2 instance attached to an Elastic IP address	Amazon Elastic Compute Cloud Documentation

NEW QUESTION 226

- (Exam Topic 3)

A user has enabled versioning on an S3 bucket. The user is using server side encryption for data at Rest. If the user is supplying his own keys for encryption SSE-C, which of the below mentioned statements is true?

Please select:

- A. The user should use the same encryption key for all versions of the same object
- B. It is possible to have different encryption keys for different versions of the same object
- C. IAM S3 does not allow the user to upload his own keys for server side encryption
- D. The SSE-C does not work when versioning is enabled

Answer: B

Explanation:

Managing your own encryption keys, you

You can encrypt the object and send it across to S3

Option A is invalid because ideally you should use different encryption keys Option C is invalid because you can use your own encryption keys Option D is invalid because encryption works even if versioning is enabled For more information on client side encryption please visit the below Link:

""Keys.html <https://docs.IAM.amazonaws.com/AmazonS3/latest/dev/UsingClientSideEncryption.html>

The correct answer is: It is possible to have different encryption keys for different versions of the same object Submit your Feedback/Queries to our Experts

NEW QUESTION 230

- (Exam Topic 3)

A web application runs in a VPC on EC2 instances behind an ELB Application Load Balancer. The application stores data in an RDS MySQL DB instance. A Linux bastion host is used to apply schema updates to the database - administrators connect to the host via SSH from a corporate workstation. The following security groups are applied to the infrastructure

* sgLB - associated with the ELB

* sgWeb - associated with the EC2 instances.

* sgDB - associated with the database

* sgBastion - associated with the bastion host Which security group configuration will allow the application to be secure and functional?

Please select:

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

Answer: D

Explanation:

The Load Balancer should accept traffic on port 80 and 443 traffic from 0.0.0.0/0 The backend EC2 Instances should accept traffic from the Load Balancer

The database should allow traffic from the Web server

And the Bastion host should only allow traffic from a specific corporate IP address range Option A is incorrect because the Web group should only allow traffic from the Load balancer For more information on IAM Security Groups, please refer to below URL: <https://docs.IAM.amazonaws.com/IAM/latest/UserGuide/using-network-security.html>

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

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

NEW QUESTION 234

- (Exam Topic 3)

A company is planning on using IAM for hosting their applications. They want complete separation and isolation of their production , testing and development environments. Which of the following is an ideal way to design such a setup?

Please select:

- A. Use separate VPCs for each of the environments
- B. Use separate IAM Roles for each of the environments
- C. Use separate IAM Policies for each of the environments
- D. Use separate IAM accounts for each of the environments

Answer: D

Explanation:

A recommendation from the IAM Security Best practices highlights this as well option A is partially valid, you can segregate resources, but a best practise is to have multiple accounts for this setup.
Options B and C are invalid because from a maintenance perspective this could become very difficult For more information on the Security Best practices, please visit the following URL:
https://dl.IAMstatic.com/whitepapers/Security/IAM_Security_Best_Practices.pdf
The correct answer is: Use separate IAM accounts for each of the environments Submit your Feedback/Queries to our Experts

NEW QUESTION 237

- (Exam Topic 3)

A large organization is planning on IAM to host their resources. They have a number of autonomous departments that wish to use IAM. What could be the strategy to adopt for managing the accounts.
Please select:

- A. Use multiple VPCs in the account each VPC for each department
- B. Use multiple IAM groups, each group for each department
- C. Use multiple IAM roles, each group for each department
- D. Use multiple IAM accounts, each account for each department

Answer: D

Explanation:

A recommendation for this is given in the IAM Security best practices Option A is incorrect since this would be applicable for resources in a VPC Options B and C are incorrect since operationally it would be difficult to manage For more information on IAM Security best practices please refer to the below URL
https://d1.IAMstatic.com/whitepapers/Security/IAM_Security_Best_Practices.pdf
The correct answer is: Use multiple IAM accounts, each account for each department Submit your Feedback/Queries to our Experts

NEW QUESTION 242

- (Exam Topic 3)

The CFO of a company wants to allow one of his employees to view only the IAM usage report page. Which of the below mentioned IAM policy statements allows the user to have access to the IAM usage report page?
Please select:

- A. "Effect": "Allow", "Action": ["Describe"], "Resource": "Billing"
- B. "Effect": "Allow", "Action": ["AccountUsage"], "Resource": "*"
- C. "Effect": "Allow", "Action": ["IAM-portal:ViewUsage", "IAM-portal:ViewBilling"], "Resource": "*"
- D. "Effect": "Allow", "Action": ["IAM-portal: ViewBilling"], "Resource": "*"

Answer: C

Explanation:

the IAM documentation, below is the access required for a user to access the Usage reports page and as per this, Option C is the right answer.
C:\Users\wk\Desktop\mudassar\Untitled.jpg



NEW QUESTION 244

- (Exam Topic 3)

An enterprise wants to use a third-party SaaS application. The SaaS application needs to have access to issue several API commands to discover Amazon EC2 resources running within the enterprise's account. The enterprise has internal security policies that require any outside access to their environment must conform to the principles of least privilege and there must be controls in place to ensure that the credentials used by the SaaS vendor cannot be used by any other third party. Which of the following would meet all of these conditions?
Please select:

- A. From the IAM Management Console, navigate to the Security Credentials page and retrieve the access and secret key for your account.
- B. Create an IAM user within the enterprise account assign a user policy to the IAM user that allows only the actions required by the SaaS applicatio
- C. Create a new access and secret key for the user and provide these credentials to the SaaS provider.
- D. Create an IAM role for cross-account access allows the SaaS provider's account to assume the role and assign it a policy that allows only the actions required by the SaaS application.
- E. Create an IAM role for EC2 instances, assign it a policy that allows only the actions required tor the Saas application to work, provide the role ARN to the SaaS provider to use when launching their application instances.

Answer: C

Explanation:

The below diagram from an IAM blog shows how access is given to other accounts for the services in your own account
C:\Users\wk\Desktop\mudassar\Untitled.jpg



Options A and B are invalid because you should not use IAM users or IAM Access keys Options D is invalid because you need to create a role for cross account access

For more information on Allowing access to external accounts, please visit the below URL:

<https://IAM.amazon.com/blogs/apn/how-to-best-architect-your-IAM-marketplace-saas-subscription-across-mult> The correct answer is: Create an IAM role for cross-account access allows the SaaS provider's account to assume the role and assign it a policy that allows only the actions required by the SaaS application.

Submit your Feedback/Queries to our Experts

NEW QUESTION 249

- (Exam Topic 3)

You have a requirement to serve up private content using the keys available with Cloudfront. How can this be achieved?

Please select:

- A. Add the keys to the backend distribution.
- B. Add the keys to the S3 bucket
- C. Create pre-signed URL's
- D. Use IAM Access keys

Answer: C

Explanation:

Option A and B are invalid because you will not add keys to either the backend distribution or the S3 bucket. Option D is invalid because this is used for programmatic access to IAM resources

You can use Cloudfront key pairs to create a trusted pre-signed URL which can be distributed to users Specifying the IAM Accounts That Can Create Signed URLs and Signed Cookies (Trusted Signers) Topics

- Creating CloudFront Key Pairs for Your Trusted Signers
- Reformatting the CloudFront Private Key (.NET and Java Only)
- Adding Trusted Signers to Your Distribution
- Verifying that Trusted Signers Are Active (Optional) 1 Rotating CloudFront Key Pairs

To create signed URLs or signed cookies, you need at least one IAM account that has an active CloudFront key pair. This account is known as a trusted signer. The trusted signer has two purposes:

- As soon as you add the IAM account ID for your trusted signer to your distribution, CloudFront starts to require that users use signed URLs or signed cookies to access your objects.

' When you create signed URLs or signed cookies, you use the private key from the trusted signer's key pair to sign a portion of the URL or the cookie. When someone requests a restricted object CloudFront compares the signed portion of the URL or cookie with the unsigned portion to verify that the URL or cookie hasn't been tampered with. CloudFront also verifies that the URL or cookie is valid, meaning, for example, that the expiration date and time hasn't passed.

For more information on Cloudfront private trusted content please visit the following URL:

- <https://docs.IAM.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-trusted-s> The correct answer is: Create pre-signed URL's Submit your Feedback/Queries to our Experts

NEW QUESTION 251

- (Exam Topic 3)

A security engineer must ensure that all infrastructure launched in the company IAM account be monitored for deviation from compliance rules, specifically that all EC2 instances are launched from one of a specified list of AMIs and that all attached EBS volumes are encrypted. Infrastructure not in compliance should be terminated. What combination of steps should the Engineer implement? Select 2 answers from the options given below.

Please select:

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

Answer: BD

Explanation:

You can use IAM Config to monitor for such Event

Option A is invalid because you cannot set Cloudwatch events based on Trusted Advisor checks.

Option C is invalid Amazon inspector cannot be used to check whether instances are launched from a specific AMI

Option E is invalid because triggering a CLI command is not the preferred option, instead you should use Lambda functions for all automation purposes.

For more information on Config Rules please see the below Link: <https://docs.IAM.amazon.com/config/latest/developerguide/evaluate-config-rules.html>

These events can then trigger a lambda function to terminate instances For more information on Cloudwatch events please see the below Link:

<https://docs.IAM.amazon.com/AmazonCloudWatch/latest/events/WhatIsCloudWatchEvents.> (

The correct answers are: Trigger a Lambda function from a scheduled Cloudwatch event that terminates non-compliant infrastructure., Monitor compliance with IAM Config Rules triggered by configuration changes
Submit your Feedback/Queries to our Experts

NEW QUESTION 253

- (Exam Topic 3)

A company is deploying a new web application on IAM. Based on their other web applications, they anticipate being the target of frequent DDoS attacks. Which steps can the company use to protect their application?

Select 2 answers from the options given below. Please select:

- A. Associate the EC2 instances with a security group that blocks traffic from blacklisted IP addresses.
- B. Use an ELB Application Load Balancer and Auto Scaling group to scale to absorb application layer traffic.
- C. Use Amazon Inspector on the EC2 instances to examine incoming traffic and discard malicious traffic.
- D. Use CloudFront and IAM WAF to prevent malicious traffic from reaching the application
- E. Enable GuardDuty to block malicious traffic from reaching the application

Answer: BD

Explanation:

The below diagram from IAM shows the best case scenario for avoiding DDos attacks using services such as IAM Cloudfro WAF, ELB and Autoscaling

Option A is invalid because by default security groups don't allow access Option C is invalid because IAM Inspector cannot be used to examine traffic

Option E is invalid because this can be used for attacks on EC2 Instances but not against DDos attacks on the entire application For more information on DDos mitigation from IAM, please visit the below URL:

<https://IAM.amazon.com/answers/networking/IAM-ddos-attack-mitieationi>

The correct answers are: Use an ELB Application Load Balancer and Auto Scaling group to scale to absorb application layer traffic., Use CloudFront and IAM WAF to prevent malicious traffic from reaching the application

Submit your Feedback/Queries to our Experts

NEW QUESTION 255

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SCS-C02 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SCS-C02 Product From:

<https://www.2passeasy.com/dumps/SCS-C02/>

Money Back Guarantee

SCS-C02 Practice Exam Features:

- * SCS-C02 Questions and Answers Updated Frequently
- * SCS-C02 Practice Questions Verified by Expert Senior Certified Staff
- * SCS-C02 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * SCS-C02 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year