



Amazon-Web-Services

Exam Questions SCS-C02

AWS Certified Security - Specialty

About ExamBible

[Your Partner of IT Exam](#)

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

- (Exam Topic 1)

A Security Engineer has several thousand Amazon EC2 instances split across production and development environments. Each instance is tagged with its environment. The Engineer needs to analyze and patch all the development EC2 instances to ensure they are not currently exposed to any common vulnerabilities or exposures (CVEs)

Which combination of steps is the MOST efficient way for the Engineer to meet these requirements? (Select TWO.)

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

Answer: CD

NEW QUESTION 2

- (Exam Topic 1)

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

Which solution meets these requirements?

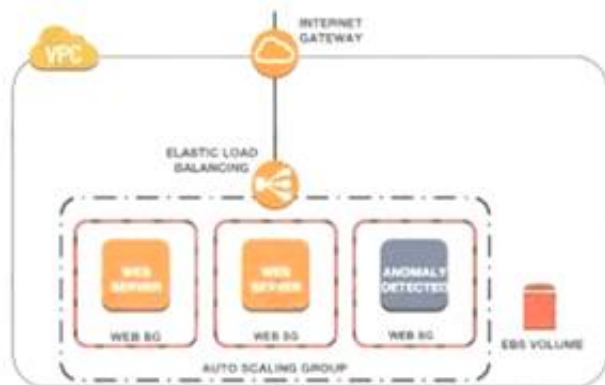
- A. Create an IAM role that allows CloudFront to access the specific S3 bucket
- B. Modify the S3 bucket policy to allow only the new IAM role to access its content
- C. Create an interface VPC endpoint for CloudFront to securely communicate with the ALB.
- D. Create an IAM role that allows CloudFront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

Answer: C

NEW QUESTION 3

- (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 4

- (Exam Topic 1)

A security engineer is designing an incident response plan to address the risk of a compromised Amazon EC2 instance. The plan must recommend a solution to meet the following requirements:

- A trusted forensic environment must be provisioned
- Automated response processes must be orchestrated

Which IAM services should be included in the plan? (Select TWO)

- A. IAM CloudFormation
- B. Amazon GuardDuty

- C. Amazon Inspector
- D. Amazon Macie
- E. IAM Step Functions

Answer: AE

NEW QUESTION 5

- (Exam Topic 1)

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

- Set up the proxy software on the EC2 instances.
- Modified the route tables on the private subnets to use the proxy EC2 instances as the default route.
- Created a security group rule opening inbound port 80 and 443 TCP protocols on the proxy EC2 instance security group.

However, the proxy EC2 instances are not successfully forwarding traffic to the internet.

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

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

Answer: B

NEW QUESTION 6

- (Exam Topic 1)

A company is outsourcing its operational support to an external company. The company's security officer must implement an access solution for delegating operational support that minimizes overhead.

Which approach should the security officer take to meet these requirements?

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

Answer: B

NEW QUESTION 7

- (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 8

- (Exam Topic 1)

After multiple compromises of its Amazon EC2 instances, a company's Security Officer is mandating that memory dumps of compromised instances be captured for further analysis. A Security Engineer just received an EC2 abuse notification report from IAM stating that an EC2 instance running the most recent Windows Server 2019 Base AMI is compromised.

How should the Security Engineer collect a memory dump of the EC2 instance for forensic analysis?

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

Answer: C

Explanation:

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

NEW QUESTION 9

- (Exam Topic 1)

A global company must mitigate and respond to DDoS attacks at Layers 3, 4 and 7. All of the company's IAM applications are serverless with static content hosted on Amazon S3 using Amazon CloudFront and Amazon Route 53.

Which solution will meet these requirements?

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

Answer: C

NEW QUESTION 10

- (Exam Topic 1)

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

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

Answer: CD

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 15

- (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 18

- (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 19

- (Exam Topic 1)

A company's Developers plan to migrate their on-premises applications to Amazon EC2 instances running Amazon Linux AMIs. The applications are accessed by a group of partner companies The Security Engineer needs to implement the following host-based security measures for these instances:

- Block traffic from documented known bad IP addresses
- Detect known software vulnerabilities and CIS Benchmarks compliance. Which solution addresses these requirements?

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

Answer: D

NEW QUESTION 23

- (Exam Topic 1)

A company has decided to migrate sensitive documents from on-premises data centers to Amazon S3. Currently, the hard drives are encrypted to meet a compliance requirement regarding data encryption. The CISO wants to improve security by encrypting each file using a different key instead of a single key. Using a different key would limit the security impact of a single exposed key.

Which of the following requires the LEAST amount of configuration when implementing this approach?

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

Answer: D

Explanation:

References:

<https://docs.IAM.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html>

Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3) When you use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3), each object is encrypted with a unique key. Server-Side Encryption with Customer Master Keys (CMKs) Stored in IAM Key Management Service (SSE-KMS) is similar to SSE-S3, but with some additional benefits and charges for using this service.

When you use SSE-KMS to protect your data without an S3 Bucket Key, Amazon S3 uses an individual IAM KMS data key for every object. It makes a call to IAM KMS every time a request is made against a

KMS-encrypted object. <https://docs.IAM.amazon.com/AmazonS3/latest/dev/bucket-key.html>

<https://docs.IAM.amazon.com/kms/latest/developerguide/symmetric-asymmetric.html>

NEW QUESTION 25

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 29

- (Exam Topic 1)

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

Which set of steps should the software engineering team take?

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

Answer: A

NEW QUESTION 31

- (Exam Topic 1)

A company uses SAML federation with IAM Identity and Access Management (IAM) to provide internal users with SSO for their IAM accounts. The company's identity provider certificate was rotated as part of its normal lifecycle. Shortly after, users started receiving the following error when attempting to log in:

"Error: Response Signature Invalid (Service: IAMSecurityTokenService; Status Code: 400; Error Code: InvalidIdentityToken)"

A security engineer needs to address the immediate issue and ensure that it will not occur again. Which combination of steps should the security engineer take to

accomplish this? (Select TWO.)

- A. Download a new copy of the SAML metadata file from the identity provider Create a new IAM identity provider entity
- B. Upload the new metadata file to the new IAM identity provider entity.
- C. During the next certificate rotation period and before the current certificate expires, add a new certificate as the secondary to the identity provide
- D. Generate a new metadata file and upload it to the IAM identity provider entity
- E. Perform automated or manual rotation of the certificate when required.
- F. Download a new copy of the SAML metadata file from the identity provider Upload the new metadata to the IAM identity provider entity configured for the SAML integration in question.
- G. During the next certificate rotation period and before the current certificate expires, add a new certificate as the secondary to the identity provide
- H. Generate a new copy of the metadata file and create a new IAM identity provider entity
- I. Upload the metadata file to the new IAM identity provider entity
- J. Perform automated or manual rotation of the certificate when required.
- K. Download a new copy of the SAML metadata file from the identity provider Create a new IAM identity provider entity
- L. Upload the new metadata file to the new IAM identity provider entity
- M. Update the identity provider configurations to pass a new IAM identity provider entity name in the SAML assertion.

Answer: AD

NEW QUESTION 35

- (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 38

- (Exam Topic 1)

A company's web application is hosted on Amazon EC2 instances running behind an Application Load Balancer (ALB) in an Auto Scaling group. An IAM WAF web ACL is associated with the ALB. IAM CloudTrail is enabled, and stores logs in Amazon S3 and Amazon CloudWatch Logs.

The operations team has observed some EC2 instances reboot at random. After rebooting, all access logs on the instances have been deleted. During an investigation, the operations team found that each reboot happened just after a PHP error occurred on the new-user-creation.php file. The operations team needs to view log information to determine if the company is being attacked.

Which set of actions will identify the suspect attacker's IP address for future occurrences?

- A. Configure VPC Flow Logs on the subnet where the ALB is located, and stream the data CloudWatch. Search for the new-user-creation.php occurrences in CloudWatch.
- B. Configure the CloudWatch agent on the ALB Configure the agent to send application logs to CloudWatch Update the instance role to allow CloudWatch Logs access
- C. Export the logs to CloudWatch Search for the new-user-creation.php occurrences in CloudWatch.
- D. Configure the ALB to export access logs to an Amazon Elasticsearch Service cluster, and use the service to search for the new-user-creation.php occurrences.
- E. Configure the web ACL to send logs to Amazon Kinesis Data Firehose, which delivers the logs to an S3 bucket Use Amazon Athena to query the logs and find the new-user-creation.php occurrences.

Answer: D

Explanation:

You send logs from your web ACL to an Amazon Kinesis Data Firehose with a configured storage destination. After you enable logging, IAM WAF delivers logs to your storage destination through the HTTPS endpoint of Kinesis Data Firehose. <https://docs.IAM.amazon.com/waf/latest/developerguide/logging.html>

NEW QUESTION 42

- (Exam Topic 1)

A global company that deals with International finance is investing heavily in cryptocurrencies and wants to experiment with mining technologies using IAM. The company's security team has enabled Amazon GuardDuty and is concerned by the number of findings being generated by the accounts. The security team wants to minimize the possibility of GuardDuty finding false negatives for compromised instances that are performing mining

How can the security team continue using GuardDuty while meeting these requirements?

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

Answer: A

NEW QUESTION 44

- (Exam Topic 1)

A company's Security Officer is concerned about the risk of IAM account root user logins and has assigned a Security Engineer to implement a notification solution for near-real-time alerts upon account root user logins.
How should the Security Engineer meet these requirements?

- A. Create a cron job that runs a script to download the IAM IAM security credentials W
- B. parse the file for account root user logins and email the Security team's distribution list
- C. Run IAM CloudTrail logs through Amazon CloudWatch Events to detect account root user logins and trigger an IAM Lambda function to send an Amazon SNS notification to the Security team's distribution list.
- D. Save IAM CloudTrail logs to an Amazon S3 bucket in the Security team's account Process the CloudTrail logs with the Security Engineer's logging solution for account root user logins Send an Amazon SNS notification to the Security team upon encountering the account root user login events
- E. Save VPC Flow Logs to an Amazon S3 bucket in the Security team's account and process the VPC Flow Logs with their logging solutions for account root user logins Send an Amazon SNS notification to the Security team upon encountering the account root user login events

Answer: B

NEW QUESTION 47

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 52

- (Exam Topic 1)

A company has a VPC with an IPv6 address range and a public subnet with an IPv6 address block. The VPC currently hosts some public Amazon EC2 instances but a Security Engineer needs to migrate a second application into the VPC that also requires IPv6 connectivity.
This new application will occasionally make API requests to an external, internet-accessible endpoint to receive updates However, the Security team does not want the application's EC2 instance exposed directly to the internet The Security Engineer intends to create a private subnet with a custom route table and to associate the route table with the private subnet
What else does the Security Engineer need to do to ensure the application will not be exposed directly to the internet, but can still communicate as required?

- A. Launch a NAT instance in the public subnet Update the custom route table with a new route to the NAT instance
- B. Remove the internet gateway, and add Amazon PrivateLink to the VPC Then update the custom route table with a new route to Amazon PrivateLink
- C. Add a managed NAT gateway to the VPC Update the custom route table with a new route to the gateway
- D. Add an egress-only internet gateway to the VPC
- E. Update the custom route table with a new route to the gateway

Answer: D

NEW QUESTION 53

- (Exam Topic 1)

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

- A. Within the Auto Scaling lifecycle, add a hook to create and attach an Amazon Elastic Block Store (Amazon EBS) log volume each time an EC2 instance is created
- B. When the instance is terminated, the EBS volume can be reattached to another instance for log review.
- C. Create an Amazon Elastic File System (Amazon EFS) file system and add a command in the user data section of the Auto Scaling launch template to mount the EFS file system during EC2 instance creation Configure a process on the instance to copy the logs once a day from an instance Amazon Elastic Block Store (Amazon EBS) volume to a directory in the EFS file system.
- D. Build the Amazon CloudWatch agent into the AMI used in the Auto Scaling group
- E. Configure the CloudWatch agent to send the logs to Amazon CloudWatch Logs for review.
- F. Within the Auto Scaling lifecycle, add a lifecycle hook at the terminating state transition and alert the engineering team by using a lifecycle notification to Amazon Simple Notification Service (Amazon SNS). Configure the hook to remain in the Terminating:Wait state for 1 hour to allow manual review of the security logs prior to instance termination.

Answer: B

NEW QUESTION 56

- (Exam Topic 1)

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


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

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

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

Answer: D

Explanation:

https://docs.IAM.amazon.com/organizations/latest/APIReference/API_DetachPolicy.html

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

NEW QUESTION 60

- (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 61

- (Exam Topic 1)

An employee accidentally exposed an IAM access key and secret access key during a public presentation. The company Security Engineer immediately disabled the key.

How can the Engineer assess the impact of the key exposure and ensure that the credentials were not misused? (Choose two.)

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

Answer: AD

Explanation:

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

NEW QUESTION 64

- (Exam Topic 1)

A developer is creating an IAM Lambda function that requires environment variables to store connection information and logging settings. The developer is required to use an IAM KMS Customer Master Key (CMK) supplied by the information security department in order to adhere to company standards for securing Lambda environment variables.

Which of the following are required for this configuration to work? (Select TWO.)

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

Answer: BC

NEW QUESTION 66

- (Exam Topic 1)

A financial institution has the following security requirements:

- > Cloud-based users must be contained in a separate authentication domain.
- > Cloud-based users cannot access on-premises systems.

As part of standing up a cloud environment, the financial institution is creating a number of Amazon managed databases and Amazon EC2 instances. An Active Directory service exists on-premises that has all the administrator accounts, and these must be able to access the databases and instances.

How would the organization manage its resources in the MOST secure manner? (Choose two.)

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

Answer: AD

Explanation:

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

NEW QUESTION 68

- (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 70

- (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 function.
- 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 classification.
- 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 classification.
- 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 classification.
- H. For identified objects that contain PII, query the S3 bucket logs by using Athena for GET operations.

Answer: B

NEW QUESTION 73

- (Exam Topic 2)

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

Pattern: "randomID_datestamp_PII.csv" Example:

"1234567_12302017_000-00-0000.csv"

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

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

Answer: C

Explanation:

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

NEW QUESTION 74

- (Exam Topic 2)

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

Please select:

- A. Use Amazon QuickSight and Cloud Trail to generate the report of out of compliance instances/servers. Redeploy all out of compliance instances/servers using an AMI with the latest patches.
- B. Use Systems Manager Patch Manager to generate the report of out of compliance instances/ server
- C. Use Systems Manager Patch Manager to install the missing patches.
- D. Use Systems Manager Patch Manager to generate the report of out of compliance instances/ servers. Redeploy all out of 1 compliance instances/servers using an AMI with the latest patches.
- E. Use Trusted Advisor to generate the report of out of compliance instances/server
- F. Use Systems Manager Patch Manager to install the missing patches.

Answer: B

Explanation:

Use the Systems Manager Patch Manager to generate the report and also install the missing patches. The IAM Documentation mentions the following IAM Systems Manager Patch Manager automates the process of patching managed instances with security-related updates. For Linux-based instances, you can also install patches for non-security updates. You can patch fleets of Amazon EC2 instances or your on-premises servers and virtual machines (VMs) by operating system type. This includes supported versions of Windows, Ubuntu Server, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), and Amazon Linux. You can scan instances to see only a report of missing patches, or you can scan and automatically install all missing patches.

Option A is invalid because Amazon QuickSight and Cloud Trail cannot be used to generate the list of servers that don't meet compliance needs.

Option C is wrong because deploying instances via new AMI'S would impact the applications hosted on these servers

Option D is invalid because Amazon Trusted Advisor cannot be used to generate the list of servers that don't meet compliance needs.

For more information on the IAM Patch Manager, please visit the below URL: <https://docs.IAM.amazon.com/systems-manager/latest/userguide/systems-manager-patch.html> (

The correct answer is: Use Systems Manager Patch Manager to generate the report of out of compliance instances/ servers. Use Systems Manager Patch Manager to install the missing patches.

Submit your Feedback/Queries to our Experts

NEW QUESTION 79

- (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 80

- (Exam Topic 2)

A Security Administrator is restricting the capabilities of company root user accounts. The company uses IAM Organizations and has enabled it for all feature sets, including consolidated billing. The top-level account is used for billing and administrative purposes, not for operational IAM resource purposes.

How can the Administrator restrict usage of member root user accounts across the organization?

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

Answer: C

Explanation:

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

https://docs.IAM.amazon.com/organizations/latest/userguide/orgs_manage_policies.html

NEW QUESTION 85

- (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 86

- (Exam Topic 2)

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

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

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

Answer: A

Explanation:

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

NEW QUESTION 90

- (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 93

- (Exam Topic 2)

Which of the following are valid event sources that are associated with web access control lists that trigger IAM WAF rules? (Choose two.)

- A. Amazon S3 static web hosting
- B. Amazon CloudFront distribution
- C. Application Load Balancer
- D. Amazon Route 53
- E. VPC Flow Logs

Answer: BC

Explanation:

A web access control list (web ACL) gives you fine-grained control over the web requests that your Amazon API Gateway API, Amazon CloudFront distribution or Application Load Balancer responds to.

NEW QUESTION 94

- (Exam Topic 2)

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

Please select:

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

Answer: D

Explanation:

The IAM Documentation mentions the following

The IAM CloudHSM service helps you meet corporate, contractual and regulatory compliance requirements for data security by using dedicated Hardware Security Module (HSM) instances within the IAM cloud. IAM and IAM Marketplace partners offer a variety of solutions for protecting sensitive data within the IAM platform,

but for some applications and data subject to contractual or regulatory mandates for managing cryptographic keys, additional protection may be necessary. CloudHSM complements existing data protection solutions and allows you to protect your encryption keys within HSMs that are design and validated to government standards for secure key management. CloudHSM allows you to securely generate, store and manage cryptographic keys used for data encryption in a way that keys are accessible only by you.

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

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

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

NEW QUESTION 98

- (Exam Topic 2)

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

Which of the following mitigations should be recommended?

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

Answer: A

Explanation:

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

NEW QUESTION 101

- (Exam Topic 2)

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

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

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

Answer: C

Explanation:

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

NEW QUESTION 104

- (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 106

- (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 107

- (Exam Topic 2)

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

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

Answer: B

Explanation:

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

NEW QUESTION 110

- (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 111

- (Exam Topic 2)

A company has deployed a custom DNS server in IAM. The Security Engineer wants to ensure that Amazon EC2 instances cannot use the Amazon-provided DNS.

How can the Security Engineer block access to the Amazon-provided DNS in the VPC?

- A. Deny access to the Amazon DNS IP within all security groups.
- B. Add a rule to all network access control lists that deny access to the Amazon DNS IP.
- C. Add a route to all route tables that black holes traffic to the Amazon DNS IP.
- D. Disable DNS resolution within the VPC configuration.

Answer: D

Explanation:

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

NEW QUESTION 114

- (Exam Topic 2)

An organization wants to be alerted when an unauthorized Amazon EC2 instance in its VPC performs a network port scan against other instances in the VPC.

When the Security team performs its own internal tests in a separate account by using pre-approved third-party scanners from the IAM Marketplace, the Security team also then receives multiple Amazon GuardDuty events from Amazon CloudWatch alerting on its test activities.

How can the Security team suppress alerts about authorized security tests while still receiving alerts about the unauthorized activity?

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

Answer: B

Explanation:

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

NEW QUESTION 118

- (Exam Topic 2)

Your company has mandated that all calls to the IAM KMS service be recorded. How can this be achieved? Please select:

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

Answer: B

Explanation:

The IAM Documentation states the following

IAM KMS is integrated with CloudTrail, a service that captures API calls made by or on behalf of IAM KMS in your IAM account and delivers the log files to an Amazon S3 bucket that you specify. CloudTrail captures

API calls from the IAM KMS console or from the IAM KMS API. Using the information collected by CloudTrail, you can determine what request was made, the source IP address from which the request was made, who made the request when it was made, and so on.

Option A is invalid because logging is not possible in the KMS service

Option C and D are invalid because Cloudwatch cannot be used to monitor API calls For more information on logging using Cloudtrail please visit the below URL

<https://docs.IAM.amazon.com/kms/latest/developerguide/loeeing-usine-cloudtrail.html> The correct answer is: Enable a trail in Cloudtrail

Submit your Feedback/Queries to our Experts

NEW QUESTION 123

- (Exam Topic 2)

An organization has a system in IAM that allows a large number of remote workers to submit data files. File sizes vary from a few kilobytes to several megabytes.

A recent audit highlighted a concern that data files are not encrypted while in transit over untrusted networks.

Which solution would remediate the audit finding while minimizing the effort required?

- A. Upload an SSL certificate to IAM, and configure Amazon CloudFront with the passphrase for the private key.
- B. Call KMS.Encrypt() in the client, passing in the data file contents, and call KMS.Decrypt() server-side.
- C. Use IAM Certificate Manager to provision a certificate on an Elastic Load Balancing in front of the web service's servers.
- D. Create a new VPC with an Amazon VPC VPN endpoint, and update the web service's DNS record.

Answer: C

NEW QUESTION 124

- (Exam Topic 2)

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

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

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

Answer: B

Explanation:

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

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

NEW QUESTION 129

- (Exam Topic 2)

You are devising a policy to allow users to have the ability to access objects in a bucket called appbucket. You define the below custom bucket policy

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

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

- A. Change the IAM permissions by applying PutBucketPolicy permissions.
- B. Verify that the policy has the same name as the bucket nam
- C. If no
- D. make it the same.

- E. Change the Resource section to "arn:IAM:s3:::appbucket/*".
- F. Create the bucket "appbucket" and then apply the policy.

Answer: C

Explanation:

When you define access to objects in a bucket you need to ensure that you specify to which objects in the bucket access needs to be given to. In this case, the * can be used to assign the permission to all objects in the bucket

Option A is invalid because the right permissions are already provided as per the question requirement Option B is invalid because it is not necessary that the policy has the same name as the bucket

Option D is invalid because this should be the default flow for applying the policy For more information on bucket policies please visit the below URL:

<https://docs.IAM.amazon.com/AmazonS3/latest/dev/example-bucket-policies.html>

The correct answer is: Change the Resource section to "arn:IAM:s3:::appbucket/" Submit your Feedback/Queries to our Experts

NEW QUESTION 133

- (Exam Topic 2)

A Security Architect is evaluating managed solutions for storage of encryption keys. The requirements are:

-Storage is accessible by using only VPCs.

-Service has tamper-evident controls.

-Access logging is enabled.

-Storage has high availability.

Which of the following services meets these requirements?

- A. Amazon S3 with default encryption
- B. IAM CloudHSM
- C. Amazon DynamoDB with server-side encryption
- D. IAM Systems Manager Parameter Store

Answer: B

NEW QUESTION 135

- (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 136

- (Exam Topic 2)

A Security Engineer who was reviewing IAM Key Management Service (IAM KMS) key policies found this statement in each key policy in the company IAM account.

```
{
  "Sid": "Enable IAM User Permissions",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:root"
  },
  "Action": "kms:*",
  "Resource": "*"
}
```

What does the statement allow?

- A. All principals from all IAM accounts to use the key.
- B. Only the root user from account 111122223333 to use the key.
- C. All principals from account 111122223333 to use the key but only on Amazon S3.
- D. Only principals from account 111122223333 that have an IAM policy applied that grants access to this key to use the key.

Answer: D

NEW QUESTION 139

- (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 141

- (Exam Topic 2)

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

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

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

Answer: BDE

Explanation:

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

NEW QUESTION 145

- (Exam Topic 2)

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

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

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

Answer: B

Explanation:

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

NEW QUESTION 146

- (Exam Topic 2)

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

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

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

Answer: C

NEW QUESTION 147

- (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 150

- (Exam Topic 2)

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

Please select:

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

Answer: AB

Explanation:

The Web security groups should allow access for ports 80 and 443 for HTTP and HTTPS traffic to all users from the internet.

The database security group should just allow access from the web security group from port 1433. Option C is invalid because this is not a valid configuration

Option D is invalid because database security should not be allowed on the internet For more information on Security Groups please visit the below URL:

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

The correct answers are: wg-123 - Allow ports 80 and 443 from 0.0.0.0/0, db-345 - Allow port 1433 from wg-123

Submit your Feedback/Queries to our Experts

NEW QUESTION 155

- (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 156

- (Exam Topic 2)

The IAM Systems Manager Parameter Store is being used to store database passwords used by an IAM Lambda function. Because this is sensitive data, the parameters are stored as type SecureString and protected by an IAM KMS key that allows access through IAM. When the function executes, this parameter cannot be retrieved as the result of an access denied error.

Which of the following actions will resolve the access denied error?

- A. Update the ssm.amazonaws.com principal in the KMS key policy to allow kms: Decrypt.
- B. Update the Lambda configuration to launch the function in a VPC.
- C. Add a policy to the role that the Lambda function uses, allowing kms: Decrypt for the KMS key.
- D. Add lambda.amazonaws.com as a trusted entity on the IAM role that the Lambda function uses.

Answer: C

Explanation:

https://docs.amazonaws.cn/en_us/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Integrating.Authorizin

NEW QUESTION 157

- (Exam Topic 2)

A company plans to move most of its IT infrastructure to IAM. The company wants to leverage its existing on-premises Active Directory as an identity provider for IAM.

Which steps should be taken to authenticate to IAM services using the company's on-premises Active Directory? (Choose three).

- A. Create IAM roles with permissions corresponding to each Active Directory group.
- B. Create IAM groups with permissions corresponding to each Active Directory group.
- C. Create a SAML provider with IAM.
- D. Create a SAML provider with Amazon Cloud Directory.
- E. Configure IAM as a trusted relying party for the Active Directory
- F. Configure IAM as a trusted relying party for Amazon Cloud Directory.

Answer: ACE

Explanation:

<https://IAM.amazon.com/blogs/security/IAM-federated-authentication-with-active-directory-federation-services>

NEW QUESTION 162

- (Exam Topic 2)

A company has a customer master key (CMK) with imported key materials. Company policy requires that all encryption keys must be rotated every year.

What can be done to implement the above policy?

- A. Enable automatic key rotation annually for the CMK.
- B. Use IAM Command Line Interface to create an IAM Lambda function to rotate the existing CMK annually.
- C. Import new key material to the existing CMK and manually rotate the CMK.
- D. Create a new CMK, import new key material to it, and point the key alias to the new CMK.

Answer: D

Explanation:

https://docs.IAM.amazon.com/en_pv/kms/latest/developerguide/rotate-keys.html#rotate-keys-manually "You might prefer to rotate keys manually so you can control the rotation frequency. It's also a good solution

for CMKs that are not eligible for automatic key rotation, such as asymmetric CMKs, CMKs in custom key stores and CMKs with imported key material. Because the new CMK is a different resource from the current CMK, it has a different key ID and ARN. When you change CMKs, you need to update references to the CMK ID or ARN in your applications. Aliases, which associate a friendly name with a CMK, make this process easier. Use an alias to refer to a CMK in your applications. Then, when you want to change the CMK that the application uses, change the target CMK of the alias. To update the target CMK of an alias, use UpdateAlias operation in the IAM KMS API. "

NEW QUESTION 166

- (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 171

- (Exam Topic 2)

A company will store sensitive documents in three Amazon S3 buckets based on a data classification scheme of "Sensitive," "Confidential," and "Restricted." The security solution must meet all of the following requirements:

- > Each object must be encrypted using a unique key.
- > Items that are stored in the "Restricted" bucket require two-factor authentication for decryption.
- > IAM KMS must automatically rotate encryption keys annually.

Which of the following meets these requirements?

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

J. Use S3 SSE-KMS to encrypt the objects.

Answer: A

Explanation:

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

NEW QUESTION 175

- (Exam Topic 3)

Your company has a set of EC2 Instances defined in IAM. They need to ensure that all traffic packets are monitored and inspected for any security threats. How can this be achieved? Choose 2 answers from the options given below

Please select:

- A. Use a host based intrusion detection system
- B. Use a third party firewall installed on a central EC2 instance
- C. Use VPC Flow logs
- D. Use Network Access control lists logging

Answer: AB

Explanation:

If you want to inspect the packets themselves, then you need to use custom based software A diagram representation of this is given in the IAM Security best practices

Option C is invalid because VPC Flow logs cannot conduct packet inspection. For more information on IAM Security best practices, please refer to below URL:

The correct answers are: Use a host based intrusion detection system. Use a third party firewall installed on a central EC2

Submit your Feedback/Queries to our Experts

NEW QUESTION 180

- (Exam Topic 3)

A company is using a Redshift cluster to store their data warehouse. There is a requirement from the Internal IT Security team to ensure that data gets encrypted for the Redshift database. How can this be achieved?

Please select:

- A. Encrypt the EBS volumes of the underlying EC2 Instances
- B. Use IAM KMS Customer Default master key
- C. Use SSL/TLS for encrypting the data
- D. Use S3 Encryption

Answer: B

Explanation:

The IAM Documentation mentions the following

Amazon Redshift uses a hierarchy of encryption keys to encrypt the database. You can use either IAM Key Management Service (IAM KMS) or a hardware security module (HSM) to manage the top-level encryption keys in this hierarchy. The process that Amazon Redshift uses for encryption differs depending on how you manage keys.

Option A is invalid because it's the cluster that needs to be encrypted

Option C is invalid because this encrypts objects in transit and not objects at rest Option D is invalid because this is used only for objects in S3 buckets

For more information on Redshift encryption, please visit the following URL: <https://docs.IAM.amazon.com/redshift/latest/mgmt/workine-with-db-encryption.html>

The correct answer is: Use IAM KMS Customer Default master key Submit your Feedback/Queries to our Experts

NEW QUESTION 185

- (Exam Topic 3)

A company hosts data in S3. There is a requirement to control access to the S3 buckets. Which are the 2 ways in which this can be achieved?

Please select:

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

Answer: AC

Explanation:

The IAM Documentation mentions the following

Amazon S3 offers access policy options broadly categorized as resource-based policies and user policies. Access policies you attach to your resources (buckets and objects) are referred to as resource-based policies. For example, bucket policies and access control lists (ACLs) are resource-based policies. You can also attach access policies to users in your account. These are called user policies. You may choose to use resource-based policies, user policies, or some combination of these to manage permissions to your Amazon S3 resources.

Option B and D are invalid because these cannot be used to control access to S3 buckets For more information on S3 access control, please refer to the below Link: <https://docs.IAM.amazon.com/AmazonS3/latest/dev/s3-access-control.html>

The correct answers are: Use Bucket policies. Use IAM user policies Submit your Feedback/Queries to our Experts

NEW QUESTION 187

- (Exam Topic 3)

You are working in the media industry and you have created a web application where users will be able to upload photos they create to your website. This web application must be able to call the S3 API in order to be able to function. Where should you store your API credentials whilst maintaining the maximum level of security?

Please select:

- A. Save the API credentials to your PHP files.
- B. Don't save your API credentials, instead create a role in IAM and assign this role to an EC2 instance when you first create it.
- C. Save your API credentials in a public Github repository.
- D. Pass API credentials to the instance using instance userdata.

Answer: B

Explanation:

Applications must sign their API requests with IAM credentials. Therefore, if you are an application developer, you need a strategy for managing credentials for your applications that run on EC2 instances. For example, you can securely distribute your IAM credentials to the instances, enabling the applications on those instances to use your credentials to sign requests, while protecting your credentials from other users. However, it's challenging to securely distribute credentials to each instance. especially those that IAM creates on your behalf, such as Spot Instances or instances in Auto Scaling groups. You must also be able to update the credentials on each instance when you rotate your IAM credentials. IAM roles are designed so that your applications can securely make API requests from your instances, without requiring you manage the security credentials that the applications use.

Option A.C and D are invalid because using IAM Credentials in an application in production is a direct no recommendation 1 secure access

For more information on IAM Roles, please visit the below URL:

<http://docs.IAM.amazon.com/IAMEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html>

The correct answer is: Don't save your API credentials. Instead create a role in IAM and assign this role to an EC2 instance when you first create it

Submit your Feedback/Queries to our Experts

NEW QUESTION 188

- (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/useruide/encryptine-cloudtrail-loe-files-with-IAM-kms.htm> The correct answer is: Don't do anything since CloudTrail logs are automatically encrypted. Submit your

Feedback/Queries to our Experts

NEW QUESTION 192

- (Exam Topic 3)

Your company has many IAM accounts defined and all are managed via IAM Organizations. One IAM account has a S3 bucket that has critical data. How can we ensure that all the users in the IAM organisation have access to this bucket?

Please select:

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

Answer: A

Explanation:

The IAM Documentation mentions the following

IAM Identity and Access Management (IAM) now makes it easier for you to control access to your IAM resources by using the IAM organization of IAM principals (users and roles). For some services, you grant permissions using resource-based policies to specify the accounts and principals that can access the resource and what actions they can perform on it. Now, you can use a new condition key, IAM:PrincipalOrgID, in these policies to require all principals accessing the resource to be from an account in the organization

Option B.C and D are invalid because the condition in the bucket policy has to mention IAM:PrincipalOrgID For more information on controlling access via Organizations, please refer to the below Link:

<https://IAM.amazon.com/blogs/security/control-access-to-IAM-resources-by-usins-the-IAM-organization-of-iam> (

The correct answer is: Ensure the bucket policy has a condition which involves IAM:PrincipalOrgID Submit your Feedback/Queries to our Experts

NEW QUESTION 194

- (Exam Topic 3)

You have a set of Customer keys created using the IAM KMS service. These keys have been used for around 6 months. You are now trying to use the new KMS features for the existing set of key's but are not able to do so. What could be the reason for this.

Please select:

- A. You have not explicitly given access via the key policy
- B. You have not explicitly given access via the IAM policy
- C. You have not given access via the IAM roles
- D. You have not explicitly given access via IAM users

Answer: A

Explanation:

By default, keys created in KMS are created with the default key policy. When features are added to KMS, you need to explicitly update the default key policy for these keys.

Option B,C and D are invalid because the key policy is the main entity used to provide access to the keys. For more information on upgrading key policies please visit the following URL: <https://docs.IAM.amazonaws.com/kms/latest/developerguide/key-policy-upgrading.html>

(
The correct answer is: You have not explicitly given access via the key policy. Submit your Feedback/Queries to our Experts

NEW QUESTION 196

- (Exam Topic 3)

A customer has an instance hosted in the IAM Public Cloud. The VPC and subnet used to host the Instance have been created with the default settings for the Network Access Control Lists. They need to provide an IT Administrator secure access to the underlying instance. How can this be accomplished. Please select:

- A. Ensure the Network Access Control Lists allow Inbound SSH traffic from the IT Administrator's Workstation
- B. Ensure the Network Access Control Lists allow Outbound SSH traffic from the IT Administrator's Workstation
- C. Ensure that the security group allows Inbound SSH traffic from the IT Administrator's Workstation
- D. Ensure that the security group allows Outbound SSH traffic from the IT Administrator's Workstation

Answer: C

Explanation:

Options A & B are invalid as default NACL rule will allow all inbound and outbound traffic.

The requirement is that the IT administrator should be able to access this EC2 instance from his workstation. For that we need to enable the Security Group of EC2 instance to allow traffic from the IT administrator's workstation. Hence option C is correct.

Option D is incorrect as we need to enable the Inbound SSH traffic on the EC2 instance Security Group since the traffic originates from the IT admin's workstation.

The correct answer is: Ensure that the security group allows Inbound SSH traffic from the IT Administrator's Workstation. Submit your Feedback/Queries to our Experts

NEW QUESTION 200

- (Exam Topic 3)

A company stores critical data in an S3 bucket. There is a requirement to ensure that an extra level of security is added to the S3 bucket. In addition, it should be ensured that objects are available in a secondary region if the primary one goes down. Which of the following can help fulfill these requirements? Choose 2 answers from the options given below. Please select:

- A. Enable bucket versioning and also enable CRR
- B. Enable bucket versioning and enable Master Keys
- C. For the Bucket policy add a condition for {"Null": {"IAM:MultiFactorAuthAge": true}}
- D. Enable the Bucket ACL and add a condition for {"Null": {"IAM:MultiFactorAuthAge": true}}

Answer: AC

Explanation:

The IAM Documentation mentions the following: Adding a Bucket Policy to Require MFA

Amazon S3 supports MFA-protected API access, a feature that can enforce multi-factor authentication (MFA) for access to your Amazon S3 resources. Multi-factor authentication provides an extra level of security you can apply to your IAM environment. It is a security feature that requires users to prove physical possession of an MFA device by providing a valid MFA code. For more information, go to IAM Multi-Factor Authentication. You can require MFA authentication for any requests to access your Amazon S3 resources.

You can enforce the MFA authentication requirement using the IAM:MultiFactorAuthAge key in a bucket policy. IAM users can access Amazon S3 resources by using temporary credentials issued by the IAM Security Token Service (STS). You provide the MFA code at the time of the STS request.

When Amazon S3 receives a request with MFA authentication, the IAM:MultiFactorAuthAge key provides a numeric value indicating how long ago (in seconds) the temporary credential was created. If the temporary credential provided in the request was not created using an MFA device, this key value is null (absent). In a bucket policy, you can add a condition to check this value, as shown in the following example bucket policy. The policy denies any Amazon S3 operation on the /taxdocuments folder in the examplebucket bucket if the request is not MFA authenticated. To learn more about MFA authentication, see Using Multi-Factor Authentication (MFA) in IAM in the IAM User Guide.

```
{
  "Version": "2012-10-17",
  "Id": "123",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::examplebucket/taxdocuments/*",
      "Condition": { "Null": { "aws:MultiFactorAuthAge": true } }
    }
  ]
}
```

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

Option B is invalid because just enabling bucket versioning will not guarantee replication of objects Option D is invalid because the condition for the bucket policy needs to be set accordingly For more information on example bucket policies, please visit the following URL: • <https://docs.IAM.amazon.com/AmazonS3/latest/dev/example-bucket-policies.html>
Also versioning and Cross Region replication can ensure that objects will be available in the destination region in case the primary region fails.
For more information on CRR, please visit the following URL: <https://docs.IAM.amazon.com/AmazonS3/latest/dev/crr.html>
The correct answers are: Enable bucket versioning and also enable CRR, For the Bucket policy add a condition for {"Null": { "IAM:MultiFactorAuthAge": true}}
Submit your Feedback/Queries to our Experts

NEW QUESTION 201

- (Exam Topic 3)

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

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

Answer: AC

Explanation:

One of the IAM Security blogs mentions the following

Versioning keeps multiple versions of an object in the same bucket. When you enable it on a bucket Amazon S3 automatically adds a unique version ID to every object stored in the bucket. At that point, a simple DELETE action does not permanently delete an object version; it merely associates a delete marker with the object. If you want to permanently delete an object version, you must specify its version ID in your DELETE request.

You can add another layer of protection by enabling MFA Delete on a versioned bucket. Once you do so, you must provide your IAM accounts access keys and a valid code from the account's MFA device in order to permanently delete an object version or suspend or reactivate versioning on the bucket.

Option B is invalid because enabling encryption does not guarantee risk of data deletion. Option D is invalid because this option does not guarantee risk of data deletion.

For more information on IAM S3 versioning and MFA please refer to the below URL: <https://IAM.amazon.com/blogs/security/securing-access-to-IAM-using-mfa-part-3/>

The correct answers are: Enable versioning on the S3 bucket Enable MFA Delete in the bucket policy Submit your Feedback/Queries to our Experts

NEW QUESTION 204

- (Exam Topic 3)

Your current setup in IAM consists of the following architecture. 2 public subnets, one subnet which has the web servers accessed by users across the internet and the other subnet for the database server. Which of the following changes to the architecture would add a better security boundary to the resources hosted in your setup
Please select:

- A. Consider moving the web server to a private subnet
- B. Consider moving the database server to a private subnet
- C. Consider moving both the web and database server to a private subnet
- D. Consider creating a private subnet and adding a NAT instance to that subnet

Answer: B

Explanation:

The ideal setup is to ensure that the web server is hosted in the public subnet so that it can be accessed by users on the internet. The database server can be hosted in the private subnet.

The below diagram from the IAM Documentation shows how this can be setup

Option A and C are invalid because if you move the web server to a private subnet, then it cannot be accessed by users Option D is invalid because NAT instances should be present in the public subnet

For more information on public and private subnets in IAM, please visit the following url [com/AmazonVPC/latest/UserGuide/VPC Scenario2](https://com/AmazonVPC/latest/UserGuide/VPC%20Scenario2).

The correct answer is: Consider moving the database server to a private subnet Submit your Feedback/Queries to our Experts

NEW QUESTION 205

- (Exam Topic 3)

A company requires that data stored in IAM be encrypted at rest. Which of the following approaches achieve this requirement? Select 2 answers from the options given below.
Please select:

- A. When storing data in Amazon EBS, use only EBS-optimized Amazon EC2 instances.
- B. When storing data in EBS, encrypt the volume by using IAM KMS.
- C. When storing data in Amazon S3, use object versioning and MFA Delete.
- D. When storing data in Amazon EC2 Instance Store, encrypt the volume by using KMS.
- E. When storing data in S3, enable server-side encryption.

Answer: BE

Explanation:

The IAM Documentation mentions the following

To create an encrypted Amazon EBS volume, select the appropriate box in the Amazon EBS section of the Amazon EC2 console. You can use a custom customer master key (CMK) by choosing one from the list that appears below the encryption box. If you do not specify a custom CMK, Amazon EBS uses the IAM-managed CMK for Amazon EBS in your account. If there is no IAM-managed CMK for Amazon EBS in your account, Amazon EBS creates one.

Data protection refers to protecting data while in-transit (as it travels to and from Amazon S3) and at rest (while it is stored on disks in Amazon S3 data centers).

You can protect data in transit by using SSL or by using client-side encryption. You have the following options of protecting data at rest in Amazon S3.

- Use Server-Side Encryption - You request Amazon S3 to encrypt your object before saving it on disks in its data centers and decrypt it when you download the objects.

• Use Client-Side Encryption - You can encrypt data client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, the encryption keys, and related tools.
Option A is invalid because using EBS-optimized Amazon EC2 instances alone will not guarantee protection of instances at rest. Option C is invalid because this will not encrypt data at rest for S3 objects. Option D is invalid because you don't store data in Instance store. For more information on EBS encryption, please visit the below URL:
<https://docs.IAM.amazon.com/kms/latest/developerguide/services-ebs.html> For more information on S3 encryption, please visit the below URL:
<https://docs.IAM.amazon.com/AmazonS3/latest/dev/UsingEncryption.html>
The correct answers are: When storing data in EBS, encrypt the volume by using IAM KMS. When storing data in S3, enable server-side encryption.
Submit your Feedback/Queries to our Experts

NEW QUESTION 206

- (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 from 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 can't 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 207

- (Exam Topic 3)

An organization has setup multiple IAM users. The organization wants that each IAM user accesses the IAM console only within the organization and not from outside. How can it achieve this?
Please select:

- A. Create an IAM policy with the security group and use that security group for IAM console login
- B. Create an IAM policy with a condition which denies access when the IP address range is not from the organization
- C. Configure the EC2 instance security group which allows traffic only from the organization's IP range
- D. Create an IAM policy with VPC and allow a secure gateway between the organization and IAM Console

Answer: B

Explanation:

You can actually use a Deny condition which will not allow the person to log in from outside. The below example shows the Deny condition to ensure that any address specified in the source address is not allowed to access the resources in IAM.

Option A is invalid because you don't mention the security group in the IAM policy Option C is invalid because security groups by default don't allow traffic

Option D is invalid because the IAM policy does not have such an option For more information on IAM policy conditions, please visit the URL:

<http://docs.IAM.amazon.com/IAM/latest/UserGuide/access-pol-examples.htm> [IAM policy example EC2 two condition!](#)

The correct answer is: Create an IAM policy with a condition which denies access when the IP address range is not from the organization
Submit your Feedback/Queries to our Experts

NEW QUESTION 210

- (Exam Topic 3)

Every application in a company's portfolio has a separate IAM account for development and production. The security team wants to prevent the root user and all IAM users in the production accounts from accessing a specific set of unneeded services. How can they control this functionality?
Please select:

- A. Create a Service Control Policy that denies access to the service
- B. Assemble all production accounts in an organizational unit
- C. Apply the policy to that organizational unit.
- D. Create a Service Control Policy that denies access to the service
- E. Apply the policy to the root account.
- F. Create an IAM policy that denies access to the service
- G. Associate the policy with an IAM group and enlist all users and the root users in this group.
- H. Create an IAM policy that denies access to the service
- I. Create a Config Rule that checks that all users have the policy assigned
- J. Trigger a Lambda function that adds the policy when found missing.

Answer: A

Explanation:

As an administrator of the master account of an organization, you can restrict which IAM services and individual API actions the users and roles in each member account can access. This restriction even overrides the administrators of member accounts in the organization. When IAM Organizations blocks access to a service or API action for a member account a user or role in that account can't access any prohibited service or API action, even if an administrator of a member account explicitly grants such permissions in an IAM policy. Organization permissions overrule account permissions.

Option B is invalid because service policies cannot be assigned to the root account at the account level. Option C and D are invalid because IAM policies alone at the account level would not be able to suffice the requirement

For more information, please visit the below URL id=docs_orgs_console <https://docs.IAM.amazon.com/IAM/latest/UserGuide/manage-attach-policy.html>

The correct answer is: Create a Service Control Policy that denies access to the services. Assemble all production accounts in an organizational unit. Apply the policy to that organizational unit

Submit your Feedback/Queries to our Experts

NEW QUESTION 211

- (Exam Topic 3)

You are building a large-scale confidential documentation web server on IAM and all of the documentation for it will be stored on S3. One of the requirements is that it cannot be publicly accessible from S3 directly, and you will need to use CloudFront to accomplish this. Which of the methods listed below would satisfy the requirements as outlined? Choose an answer from the options below

Please select:

- A. Create an Identity and Access Management (IAM) user for CloudFront and grant access to the objects in your S3 bucket to that IAM User.
- B. Create an Origin Access Identity (OAI) for CloudFront and grant access to the objects in your S3 bucket to that OAI.
- C. Create individual policies for each bucket the documents are stored in and in that policy grant access to only CloudFront.
- D. Create an S3 bucket policy that lists the CloudFront distribution ID as the Principal and the target bucket as the Amazon Resource Name (ARN).

Answer: B

Explanation:

If you want to use CloudFront signed URLs or signed cookies to provide access to objects in your Amazon S3 bucket you probably also want to prevent users from accessing your Amazon S3 objects using Amazon S3 URLs. If users access your objects directly in Amazon S3, they bypass the controls provided by CloudFront signed URLs or signed cookies, for example, control over the date and time that a user can no longer access your content and control over which IP addresses can be used to access content. In addition, if user's access objects both through CloudFront and directly by using Amazon S3 URLs, CloudFront access logs are less useful because they're incomplete.

Option A is invalid because you need to create a Origin Access Identity for Cloudfront and not an IAM user

Option C and D are invalid because using policies will not help fulfil the requirement For more information on Origin Access Identity please see the below Link:

<http://docs.IAM.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3>

The correct answer is: Create an Origin Access Identity (OAI) for CloudFront and grant access to the objects in your S3 bucket to that OAI.

(

Submit your Feedback/Queries to our Experts

NEW QUESTION 216

- (Exam Topic 3)

A DevOps team is currently looking at the security aspect of their CI/CD pipeline. They are making use of IAM resource? for their infrastructure. They want to ensure that the EC2 Instances don't have any high security vulnerabilities. They want to ensure a complete DevSecOps process. How can this be achieved?

Please select:

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

Answer: B

Explanation:

Amazon Inspector offers a programmatic way to find security defects or misconfigurations in your operating systems and applications. Because you can use API calls to access both the processing of assessments and the results of your assessments, integration of the findings into workflow and notification systems is simple.

DevOps teams can integrate Amazon Inspector into their CI/CD pipelines and use it to identify any pre-existing issues or when new issues are introduced.

Option A.C and D are all incorrect since these services cannot check for Security Vulnerabilities. These can only be checked by the IAM Inspector service.

For more information on IAM Security best practices, please refer to below URL: [https://d1.IAMstatic.com/whitepapers/Security/IAM Security Best Practices.pdf](https://d1.IAMstatic.com/whitepapers/Security/IAM%20Security%20Best%20Practices.pdf)

The correct answer is: Use IAM Inspector API's in the pipeline for the EC2 Instances Submit your Feedback/Queries to our Experts

NEW QUESTION 217

- (Exam Topic 3)

You have a bucket and a VPC defined in IAM. You need to ensure that the bucket can only be accessed by the VPC endpoint. How can you accomplish this?

Please select:

- A. Modify the security groups for the VPC to allow access to the S3 bucket
- B. Modify the route tables to allow access for the VPC endpoint
- C. Modify the IAM Policy for the bucket to allow access for the VPC endpoint
- D. Modify the bucket Policy for the bucket to allow access for the VPC endpoint

Answer: D

Explanation:

This is mentioned in the IAM Documentation Restricting Access to a Specific VPC Endpoint

The following is an example of an S3 bucket policy that restricts access to a specific bucket, examplebucket only from the VPC endpoint with the ID vpce-

la2b3c4d. The policy denies all access to the bucket if the specified endpoint is not being used. The IAM:sourceVpce condition is used to specify the endpoint.

The IAM:sourceVpce condition does not require an ARN for the VPC endpoint resource, only the VPC endpoint ID. For more information about using conditions in a policy, see Specifying Conditions in a Policy.

Options A and B are incorrect because using Security Groups nor route tables will help to allow access specifically for that bucket via the VPC endpoint Here you specifically need to ensure the bucket policy is changed.

Option C is incorrect because it is the bucket policy that needs to be changed and not the IAM policy. For more information on example bucket policies for VPC endpoints, please refer to below URL:

>

<https://docs.IAM.amazon.com/AmazonS3/latest/dev/example-bucket-policies-vpc-endpoint.html>

The correct answer is: Modify the bucket Policy for the bucket to allow access for the VPC endpoint Submit your Feedback/Queries to our Experts

NEW QUESTION 219

- (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 221

- (Exam Topic 3)

You want to track access requests for a particular S3 bucket. How can you achieve this in the easiest possible way?

Please select:

- A. Enable server access logging for the bucket
- B. Enable Cloudwatch metrics for the bucket
- C. Enable Cloudwatch logs for the bucket
- D. Enable IAM Config for the S3 bucket

Answer: A

Explanation:

The IAM Documentation mentions the foil

To track requests for access to your bucket you can enable access logging. Each access log record provides details about a single access request, such as the requester, bucket name, request time, request action, response status, and error code, if any.

Options B and C are incorrect Cloudwatch is used for metrics and logging and cannot be used to track access requests.

Option D is incorrect since this can be used for Configuration management but for not for tracking S3 bucket requests.

For more information on S3 server logs, please refer to below UF <https://docs.IAM.amazon.com/AmazonS3/latest/dev/ServerLoes.html>

The correct answer is: Enable server access logging for the bucket Submit your Feedback/Queries to our Experts

NEW QUESTION 226

- (Exam Topic 3)

Your company is planning on using IAM EC2 and ELB for deployment for their web applications. The security policy mandates that all traffic should be encrypted.

Which of the following options will ensure that this requirement is met. Choose 2 answers from the options below.

Please select:

- A. Ensure the load balancer listens on port 80
- B. Ensure the load balancer listens on port 443
- C. Ensure the HTTPS listener sends requests to the instances on port 443
- D. Ensure the HTTPS listener sends requests to the instances on port 80

Answer: BC

Explanation:

The IAM Documentation mentions the following

You can create a load balancer that listens on both the HTTP (80) and HTTPS (443) ports. If you specify that the HTTPS listener sends requests to the instances on port 80, the load balancer terminates the requests and communication from the load balancer to the instances is not encrypted, if the HTTPS listener sends requests to the instances on port 443, communication from the load balancer to the instances is encrypted.

Option A is invalid because there is a need for secure traffic, so port 80 should not be used Option D is invalid because for the HTTPS listener you need to use port 443

For more information on HTTPS with ELB, please refer to the below Link: <https://docs.IAM.amazon.com/elasticloadbalancing/latest/classic/elb-create-https-ssl-load-balancer.html>

The correct answers are: Ensure the load balancer listens on port 443, Ensure the HTTPS listener sends requests to the instances on port 443

Submit your Feedback/Queries to our Experts

NEW QUESTION 230

- (Exam Topic 3)

You are trying to use the IAM Systems Manager run command on a set of Instances. The run command on a set of Instances. What can you do to diagnose the issue? Choose 2 answers from the options given

Please select:

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

Answer: AB

Explanation:

The IAM Documentation mentions the following

If you experience problems executing commands using Run Command, there might be a problem with the SSM Agent. Use the following information to help you troubleshoot the agent

View Agent Logs

The SSM Agent logs information in the following files. The information in these files can help you troubleshoot problems.

On Windows

%PROGRAMDATA%\Amazon\SSM\Logs\amazon-ssm-agent.log

%PROGRAMDATA%\Amazon\SSM\Logs\error.log

The default filename of the seelog is seelog-xml.template. If you modify a seelog, you must rename the file to seelog.xml.

On Linux

/var/log/amazon/ssm/amazon-ssm-agentlog /var/log/amazon/ssm/errors.log

Option C is invalid because the right AMI has nothing to do with the issues. The agent which is used to execute run commands can run on a variety of AMI'S

Option D is invalid because security groups does not come into the picture with the communication between the agent and the SSM service

For more information on troubleshooting IAM SSM, please visit the following URL: [https://docs.IAM.amazon.com/systems-](https://docs.IAM.amazon.com/systems-manageer/latest/userguide/troubleshootine-remote-commands.html)

manaeer/latest/userguide/troubleshootine-remote-commands.html The correct answers are: Ensure that the SSM agent is running on the target machine. Check the

/var/log/amazon/ssm/errors.log file

Submit your Feedback/Queries to our Experts

NEW QUESTION 235

- (Exam Topic 3)

You need to ensure that objects in an S3 bucket are available in another region. This is because of the criticality of the data that is hosted in the S3 bucket. How can you achieve this in the easiest way possible?

Please select:

- A. Enable cross region replication for the bucket
- B. Write a script to copy the objects to another bucket in the destination region
- C. Create an S3 snapshot in the destination region
- D. Enable versioning which will copy the objects to the destination region

Answer: A

Explanation:

Option B is partially correct but a big maintenance over head to create and maintain a script when the functionality is already available in S3

Option C is invalid because snapshots are not available in S3 Option D is invalid because versioning will not replicate objects The IAM Documentation mentions the following

Cross-region replication is a bucket-level configuration that enables automatic, asynchronous copying of objects across buck in different IAM Regions.

For more information on Cross region replication in the Simple Storage Service, please visit the below URL:

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

The correct answer is: Enable cross region replication for the bucket Submit your Feedback/Queries to our Experts

NEW QUESTION 236

- (Exam Topic 3)

Your company has an external web site. This web site needs to access the objects in an S3 bucket. Which of the following would allow the web site to access the objects in the most secure manner?

Please select:

- A. Grant public access for the bucket via the bucket policy
- B. Use the IAM:Referer key in the condition clause for the bucket policy
- C. Use the IAM:sites key in the condition clause for the bucket policy
- D. Grant a role that can be assumed by the web site

Answer: B

Explanation:

An example of this is given in the IAM Documentatio Restricting Access to a Specific HTTP Referrer

Suppose you have a website with domain name (www.example.com or example.com) with links to photos and videos stored in your S3 bucket examplebucket. By default, all the S3 resources are private, so only the IAM account that created the resources can access them. To allow read access to these objects from your website, you can add a bucket policy that allows s3:GetObject permission with a condition, using the IAM:referer key, that the get request must originate from specific webpages. The following policy specifies the StringLike condition with the IAM:Referer condition key.

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

```
{
  "Version": "2012-10-17",
  "Id": "http referer policy example",
  "Statement": [
    {
      "Sid": "Allow get requests originating from www.example.com and example.com.",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::examplebucket/*",
      "Condition": {
        "StringLike": {"aws:Referer": ["http://www.example.com/*", "http://example.com/*"]}
      }
    }
  ]
}
```

Option A is invalid because giving public access is not a secure way to provide access Option C is invalid because IAM:sites is not a valid condition key Option D is invalid because IAM roles will not be assigned to web sites

For more information on example bucket policies please visit the below Link:

1 <https://docs.IAM.amazon.com/AmazonS3/latest/dev/example-bucket-policies.html>

The correct answer is: Use the IAM:Referer key in the condition clause for the bucket policy Submit your Feedback/Queries to our Experts

NEW QUESTION 237

.....

Relate Links

100% Pass Your SCS-C02 Exam with Exam Bible Prep Materials

<https://www.exambible.com/SCS-C02-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>