

Exam Questions SCS-C02

AWS Certified Security - Specialty

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



NEW QUESTION 1

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 2

- (Exam Topic 1)

An application running on Amazon EC2 instances generates log files in a folder on a Linux file system. The instances block access to the console and file transfer utilities, such as Secure Copy Protocol (SCP) and Secure File Transfer Protocol (SFTP). The Application Support team wants to automatically monitor the application log files so the team can set up notifications in the future.

A Security Engineer must design a solution that meets the following requirements:

- Make the log files available through an IAM managed service.
- Allow for automatic monitoring of the logs.
- Provide an interface for analyzing logs.
- Minimize effort.

Which approach meets these requirements?

- A. Modify the application to use the IAM SD
- B. Write the application logs to an Amazon S3 bucket
- C. Install the unified Amazon CloudWatch agent on the instances. Configure the agent to collect the application log files on the EC2 file system and send them to Amazon CloudWatch Logs
- D. Install IAM Systems Manager Agent on the instances. Configure an automation document to copy the application log files to IAM DeepLens
- E. Install Amazon Kinesis Agent on the instances. Stream the application log files to Amazon Kinesis Data Firehose and set the destination to Amazon Elasticsearch Service

Answer: D

NEW QUESTION 3

- (Exam Topic 1)

Which of the following are valid configurations for using SSL certificates with Amazon CloudFront? (Select THREE)

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

Answer: ACD

NEW QUESTION 4

- (Exam Topic 1)

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

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

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

Answer: A

Explanation:

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

NEW QUESTION 5

- (Exam Topic 1)

An external Auditor finds that a company's user passwords have no minimum length. The company is currently using two identity providers:

- IAM IAM federated with on-premises Active Directory
- Amazon Cognito user pools to accessing an IAM Cloud application developed by the company Which combination o1 actions should the Security Engineer take to solve this issue? (Select TWO.)

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

Answer: AD

NEW QUESTION 6

- (Exam Topic 1)

A Security Engineer discovered a vulnerability in an application running on Amazon ECS. The vulnerability allowed attackers to install malicious code. Analysis of the code shows it exfiltrates data on port 5353 in batches at random time intervals.

While the code of the containers is being patched, how can Engineers quickly identify all compromised hosts and stop the egress of data on port 5353?

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

Answer: C

NEW QUESTION 7

- (Exam Topic 1)

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

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

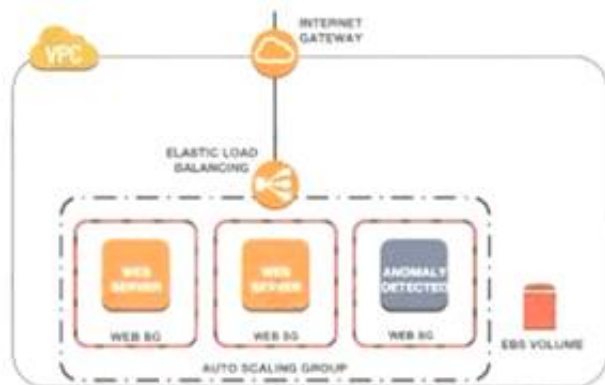
- Use IAM Certificate Manager to encrypt all traffic between the client and application servers.
- Review the application security groups to ensure that only the necessary ports are open.
- Use Elastic Load Balancing to offload Secure Sockets Layer encryption.
- Use Amazon Inspector to periodically scan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

Answer: BD

NEW QUESTION 8

- (Exam Topic 1)

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



- Remove the instance from the Auto Scaling group Place the instance within an isolation security group, detach the EBS volume launch an EC2 instance with a forensic toolkit and attach the E8S volume to investigate
- 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.
- Remove the instance from the Auto Scaling group Place the Instance within an isolation security group, launch an EC2 Instance with a forensic toolkit and use the forensic toolkit imago to deploy an ENI as a network span port to inspect all traffic coming from the suspicious instance.
- 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 9

- (Exam Topic 1)

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

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

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

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

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

Answer: B

NEW QUESTION 10

- (Exam Topic 1)

A security engineer needs to configure monitoring and auditing for IAM Lambda.

Which combination of actions using IAM services should the security engineer take to accomplish this goal? (Select TWO.)

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

Answer: AB

NEW QUESTION 10

- (Exam Topic 1)

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

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

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

Answer: B

NEW QUESTION 13

- (Exam Topic 1)

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

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

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

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

Answer: C

NEW QUESTION 16

- (Exam Topic 1)

A security engineer is designing a solution that will provide end-to-end encryption between clients and Docker containers running in Amazon Elastic Container Service (Amazon ECS). This solution will also handle volatile traffic patterns

Which solution would have the MOST scalability and LOWEST latency?

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

Answer: A

NEW QUESTION 18

- (Exam Topic 1)

A website currently runs on Amazon EC2 with mostly static content on the site. Recently, the site was subjected to a DDoS attack, and a Security Engineer was tasked with redesigning the edge security to help mitigate this risk in the future

What are some ways the Engineer could achieve this? (Select THREE)

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

Answer: BDF

NEW QUESTION 19

- (Exam Topic 1)

Unapproved changes were previously made to a company's Amazon S3 bucket. A security engineer configured IAM Config to record configuration changes made to the company's S3 buckets. The engineer discovers there are S3 configuration changes being made, but no Amazon SNS notifications are being sent. The engineer has already checked the configuration of the SNS topic and has confirmed the configuration is valid.

Which combination of steps should the security engineer take to resolve the issue? (Select TWO.)

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

Answer: BE

NEW QUESTION 24

- (Exam Topic 1)

A company requires that SSH commands used to access its IAM instance be traceable to the user who executed each command.

How should a Security Engineer accomplish this?

- A. Allow inbound access on port 22 at the security group attached to the instance Use IAM Systems Manager Session Manager for shell access to Amazon EC2 instances with the user tag defined Enable Amazon CloudWatch logging for Systems Manager sessions
- B. Use Amazon S3 to securely store one Privacy Enhanced Mail Certificate (PEM file) for each user Allow Amazon EC2 to read from Amazon S3 and import every user that wants to use SSH to access EC2 instances Allow inbound access on port 22 at the security group attached to the instance Install the Amazon CloudWatch agent on the EC2 instance and configure it to ingest audit logs for the instance
- C. Deny inbound access on port 22 at the security group attached to the instance Use IAM Systems Manager Session Manager for shell access to Amazon EC2 instances with the user tag defined Enable Amazon CloudWatch logging for Systems Manager sessions
- D. Use Amazon S3 to securely store one Privacy Enhanced Mail Certificate (PEM file) for each team or group Allow Amazon EC2 to read from Amazon S3 and import every user that wants to use SSH to access EC2 instances Allow inbound access on port 22 at the security group attached to the instance Install the Amazon CloudWatch agent on the EC2 instance and configure it to ingest audit logs for the instance

Answer: C

NEW QUESTION 27

- (Exam Topic 1)

A company recently performed an annual security assessment of its IAM environment. The assessment showed that audit logs are not available beyond 90 days and that unauthorized changes to IAM policies are made without detection.

How should a security engineer resolve these issues?

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

Answer: D

Explanation:

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

"For an ongoing record of events in your IAM account, you must create a trail. Although CloudTrail provides 90 days of event history information for management events in the CloudTrail console without creating a trail, it is not a permanent record, and it does not provide information about all possible types of events. For an ongoing record, and for a record that contains all the event types you specify, you must create a trail, which delivers log files to an Amazon S3 bucket that you specify."

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

NEW QUESTION 32

- (Exam Topic 1)

A company's security engineer is configuring Amazon S3 permissions to ban all current and future public buckets. However, the company hosts several websites directly off S3 buckets with public access enabled.

The engineer needs to block the public S3 buckets without causing any outages on the existing websites. The engineer has set up an Amazon CloudFront distribution (or each website).

Which set of steps should the security engineer implement next?

- A. Configure an S3 bucket as the origin and origin access identity (OAI) for the CloudFront distribution. Switch the DNS records from websites to point to the CloudFront distribution. Enable Block public access settings at the account level.
- B. Configure an S3 bucket as the origin with an origin access identity (OAI) for the CloudFront distribution. Switch the DNS records for the websites to point to the CloudFront distribution. Then, for each S3 bucket, enable block public access settings.
- C. Configure an S3 bucket as the origin with an origin access identity (OAI) for the CloudFront distribution. Enable block public access settings at the account level.

D. Configure an S3 bucket as the origin for me CloudFront distribution
Configure the S3 bucket policy to accept connections from the CloudFront points of presence only
Switch the DNS records for the websites to point to the CloudFront distribution
Enable block public access settings at me account level

Answer: A

NEW QUESTION 34

- (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 35

- (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 38

- (Exam Topic 1)

A large government organization is moving to the cloud and has specific encryption requirements. The first workload to move requires that a customer's data be immediately destroyed when the customer makes that request.

Management has asked the security team to provide a solution that will securely store the data, allow only authorized applications to perform encryption and decryption and allow for immediate destruction of the data.

Which solution will meet these requirements?

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

Answer: A

NEW QUESTION 40

- (Exam Topic 1)

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

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

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

Answer: BCE

NEW QUESTION 42

- (Exam Topic 1)

A company's on-premises data center forwards DNS logs to a third-party security incident events management (SIEM) solution that alerts on suspicious behavior. The company wants to introduce a similar capability to its IAM accounts that includes automatic remediation. The company expects to double in size within the next few months.

Which solution meets the company's current and future logging requirements?

- A. Enable Amazon GuardDuty and IAM Security Hub in all Regions and all account

- B. Designate a master security account to receive all alerts from the child account
- C. Set up specific rules within Amazon EventBridge to trigger an IAM Lambda function for remediation steps.
- D. Ingest all IAM CloudTrail logs, VPC Flow Logs, and DNS logs into a single Amazon S3 bucket in a designated security account
- E. Use the current on-premises SIEM to monitor the logs and send a notification to an Amazon SNS topic to alert the security team of remediation steps.
- F. Ingest all IAM CloudTrail logs, VPC Flow Logs, and DNS logs into a single Amazon S3 bucket in a designated security account
- G. Launch an Amazon EC2 instance and install the current SIEM to monitor the logs and send a notification to an Amazon SNS topic to alert the security team of remediation steps.
- H. Enable Amazon GuardDuty and IAM Security Hub in all Regions and all account
- I. Designate a master security account to receive all alerts from the child account
- J. Create an IAM Organizations SCP that denies access to certain API calls that are on an ignore list.

Answer: A

NEW QUESTION 43

- (Exam Topic 1)

A security engineer needs 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 48

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 52

- (Exam Topic 1)

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

- A. Create a new trail with the updated log file prefix, and then delete the original trail. Update the existing bucket policy in the Amazon S3 console with the new log file prefix, and then update the log file prefix in the CloudTrail console
- B. Update the existing bucket policy in the Amazon S3 console to allow the security engineers principal to perform PutBucketPolicy
- 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 53

- (Exam Topic 1)

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

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

Answer: BDF

NEW QUESTION 55

- (Exam Topic 1)

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

What policy should the Engineer implement?

A

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

B

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

C

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


D

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

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

Answer: B

NEW QUESTION 58

- (Exam Topic 1)

A company is designing the securely architecture (or a global latency-sensitive web application it plans to deploy to IAM. A Security Engineer needs to configure a highly available and secure two-tier architecture. The security design must include controls to prevent common attacks such as DDoS, cross-site scripting, and SQL injection.

Which solution meets these requirements?

- A. Create an Application Load Balancer (ALB) that uses public subnets across multiple Availability Zones within a single Region
- B. Point the ALB to an Auto Scaling group with Amazon EC2 instances in private subnets across multiple Availability Zones within the same Region
- C. Create an AmazonCloudFront distribution that uses the ALB as its origin
- D. Create appropriate IAM WAF ACLs and enable them on the CloudFront distribution.
- E. Create an Application Load Balancer (ALB) that uses private subnets across multiple Availability Zones within a single Region
- F. Point the ALB to an Auto Scaling group with Amazon EC2 instances in private subnets across multiple Availability Zones within the same Region
- G. Create an Amazon CloudFront distribution that uses the ALB as its origin
- H. Create appropriate IAM WAF ACLs and enable them on the CloudFront distribution.
- I. Create an Application Load Balancer (ALB) that uses public subnets across multiple Availability Zones within a single Region
- J. Point the ALB to an Auto Scaling group with Amazon EC2 instances in private subnets across multiple Availability Zones within the same Region
- K. Create appropriate IAM WAF ACLs and enable them on the ALB.
- L. Create an Application Load Balancer (ALB) that uses private subnets across multiple Availability Zones within a single Region
- M. Point the ALB to an Auto Scaling group with Amazon EC2 instances in private subnets across multiple Availability Zones within the same Region
- N. Create appropriate IAM WAF ACLs and enable them on the ALB.

Answer: A

NEW QUESTION 60

- (Exam Topic 1)

A Security Engineer for a large company is managing a data processing application used by 1,500 subsidiary companies. The parent and subsidiary companies all use IAM. The application uses TCP port 443 and runs on Amazon EC2 behind a Network Load Balancer (NLB). For compliance reasons, the application should only be accessible to the subsidiaries and should not be available on the public internet. To meet the compliance requirements for restricted access, the Engineer has received the public and private CIDR block ranges for each subsidiary

What solution should the Engineer use to implement the appropriate access restrictions for the application?

- A. Create a NACL to allow access on TCP port 443 from the 1,500 subsidiary CIDR block ranges. Associate the NACL to both the NLB and EC2 instances
- B. Create an IAM security group to allow access on TCP port 443 from the 1,500 subsidiary CIDR block range
- C. Associate the security group to the NL
- D. Create a second security group for EC2 instances with access on TCP port 443 from the NLB security group.
- E. Create an IAM PrivateLink endpoint service in the parent company account attached to the NL
- F. Create an IAM security group for the instances to allow access on TCP port 443 from the IAM PrivateLink endpoint
- G. Use IAM PrivateLink interface endpoints in the 1,500 subsidiary IAM accounts to connect to the data processing application.
- H. Create an IAM security group to allow access on TCP port 443 from the 1,500 subsidiary CIDR block range
- I. Associate the security group with EC2 instances.

Answer: D

NEW QUESTION 63

- (Exam Topic 1)

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

What could be causing these terminations?

- A. The IAM user launching those instances is missing ec2:RunInstances permission.

- B. The AMI used as encrypted and the IAM does not have the required IAM KMS permissions.
- C. The instance profile used with the EC2 instances is unable to query instance metadata.
- D. IAM currently does not have sufficient capacity in the Region.

Answer: B

Explanation:

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

NEW QUESTION 67

- (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 70

- (Exam Topic 1)

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

Network error: Connection timed out.

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

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

Answer: BDF

NEW QUESTION 73

- (Exam Topic 1)

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

Which solution would meet these requirements?

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

Answer: A

NEW QUESTION 74

- (Exam Topic 1)

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

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

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

Answer: A

Explanation:

"To turn off access to instance metadata on an existing instance....." <https://docs.IAM.amazon.com/IAMEC2/latest/UserGuide/configuring-instance-metadata-service.html> You can disable the service for existing (running or stopped) EC2 instances. <https://docs.IAM.amazon.com/cli/latest/reference/ec2/modify-instance-metadata-options.html>

NEW QUESTION 79

- (Exam Topic 1)

A company's information security team want to do near-real-time anomaly detection on Amazon EC2 performance and usage statistics. Log aggregation is the responsibility of a security engineer. To do the study, the Engineer needs gather logs from all of the company's IAM accounts in a single place. How should the Security Engineer go about doing this?

- A. Log in to each account four times a day and filter the IAM CloudTrail log data, then copy and paste the logs in to the Amazon S3 bucket in the destination account.
- B. Set up Amazon CloudWatch to stream data to an Amazon S3 bucket in each source account
- C. Set up bucket replication for each source account into a centralized bucket owned by the Security Engineer.
- D. Set up an IAM Config aggregator to collect IAM configuration data from multiple sources.
- E. Set up Amazon CloudWatch cross-account log data sharing with subscriptions in each account
- F. Send the logs to Amazon Kinesis Data Firehose in the Security Engineer's account.

Answer: D

Explanation:

Read the prerequisites in the question carefully. The solution must support "near real time" analysis of the log data. Cloudwatch doesn't stream logs to S3; it supports exporting them to S3 with an up to 12 hour expected delay:

<https://docs.IAM.amazon.com/AmazonCloudWatch/latest/logs/S3Export.html>

"Log data can take up to 12 hours to become available for export. For near real-time analysis of log data, see Analyzing log data with CloudWatch Logs Insights or Real-time processing of log data with subscriptions instead."

<https://docs.IAM.amazon.com/AmazonCloudWatch/latest/logs/Subscriptions.html>

"You can use subscriptions to get access to a real-time feed of log events from CloudWatch Logs and have it delivered to other services such as an Amazon Kinesis stream, an Amazon Kinesis Data Firehose stream, or IAM Lambda for custom processing, analysis, or loading to other systems. When log events are sent to the receiving service, they are Base64 encoded and compressed with the gzip format."

<https://docs.IAM.amazon.com/AmazonCloudWatch/latest/logs/CrossAccountSubscriptions.html>

NEW QUESTION 84

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 89

- (Exam Topic 1)

A security engineer has noticed an unusually high amount of traffic coming from a single IP address. This was discovered by analyzing the Application Load Balancer's access logs. How can the security engineer limit the number of requests from a specific IP address without blocking the IP address?

- A. Add a rule to the Application Load Balancer to route the traffic originating from the IP address in question and show a static webpage.
- B. Implement a rate-based rule with IAM WAF
- C. Use IAM Shield to limit the originating traffic hit rate.
- D. Implement the GeoLocation feature in Amazon Route 53.

Answer: C

NEW QUESTION 94

- (Exam Topic 1)

A convoys 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 id Federal information Processing Standards (FPS) 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 97

- (Exam Topic 1)

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

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

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

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

Answer: C

NEW QUESTION 102

- (Exam Topic 1)

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

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

Answer: AD

Explanation:

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

NEW QUESTION 107

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 110

- (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 113

- (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 117

- (Exam Topic 1)

A company is using IAM Organizations to manage multiple IAM accounts. The company has an application that allows users to assume the AppUser IAM role to download files from an Amazon S3 bucket that is encrypted with an IAM KMS CMK. However, when users try to access the files in the S3 bucket, they get an access denied error.

What should a Security Engineer do to troubleshoot this error? (Select THREE)

- A. Ensure the KMS policy allows the AppUser role to have permission to decrypt for the CMK
- B. Ensure the S3 bucket policy allows the AppUser role to have permission to get objects for the S3 bucket
- C. Ensure the CMK was created before the S3 bucket.
- D. Ensure the S3 block public access feature is enabled for the S3 bucket.
- E. Ensure that automatic key rotation is disabled for the CMK
- F. Ensure the SCPs within Organizations allow access to the S3 bucket.

Answer: ABF

NEW QUESTION 122

- (Exam Topic 1)

A company is operating an open-source software platform that is internet facing. The legacy software platform no longer receives security updates. The software platform operates using Amazon Route 53 weighted load balancing to send traffic to two Amazon EC2 instances that connect to an Amazon RDS cluster. A recent report suggests this software platform is vulnerable to SQL injection attacks, with samples of attacks provided. The company's security engineer must secure this system against SQL injection attacks within 24 hours. The secure, engineer's solution involve the least amount of effort and maintain normal operations during implementation.

What should the security engineer do to meet these requirements?

- A. Create an Application Load Balancer with the existing EC2 instances as a target group. Create an IAM WAF web ACL containing rules that protect the application from this attack.
- B. then apply it to the ALB. Test to ensure the vulnerability has been mitigated, then redirect the Route 53 records to point to the ALB. Update security groups on the EC2 instances to prevent direct access from the internet.
- C. Create an Amazon CloudFront distribution specifying one EC2 instance as an origin. Create an IAM WAF web ACL containing rules that protect the application from this attack, then apply it to the distribution. Test to ensure the vulnerability has been mitigated, then redirect the Route 53 records to point to CloudFront.
- D. Obtain the latest source code for the platform and make the necessary updates. Test the updated code to ensure that the vulnerability has been mitigated, then deploy the patched version of the platform to the EC2 instances.
- E. Update the security group that is attached to the EC2 instances, removing access from the internet to the TCP port used by the SQL database. Create an IAM WAF web ACL containing rules that protect the application from this attack, then apply it to the EC2 instances. Test to ensure the vulnerability has been mitigated.
- F. then restore the security group to the original setting.

Answer: A

NEW QUESTION 123

- (Exam Topic 1)

Two Amazon EC2 instances in different subnets should be able to connect to each other but cannot. It has been confirmed that other hosts in the same subnets are able to communicate successfully, and that security groups have valid ALLOW rules in place to permit this traffic.

Which of the following troubleshooting steps should be performed?

- A. Check inbound and outbound security groups, looking for DENY rules.
- B. Check inbound and outbound Network ACL rules, looking for DENY rules.
- C. Review the rejected packet reason codes in the VPC Flow Logs.
- D. Use IAM X-Ray to trace the end-to-end application flow.

Answer: C

NEW QUESTION 127

- (Exam Topic 1)

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

- A.

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

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

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

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

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

Answer: C

NEW QUESTION 131

- (Exam Topic 1)

A Security Engineer is setting up a new IAM account. The Engineer has been asked to continuously monitor the company's IAM account using automated compliance checks based on IAM best practices and Center for Internet Security (CIS) IAM Foundations Benchmarks. How can the Security Engineer accomplish this using IAM services?

- A. Enable IAM Config and set it to record all resources in all Regions and global resource
 B. Then enable IAM Security Hub and confirm that the CIS IAM Foundations compliance standard is enabled
 C. Enable Amazon Inspector and configure it to scan all Regions for the CIS IAM Foundations Benchmark
 D. Then enable IAM Security Hub and configure it to ingest the Amazon Inspector findings
 E. Enable Amazon Inspector and configure it to scan all Regions for the CIS IAM Foundations Benchmark
 F. Then enable IAM Shield in all Regions to protect the account from DDoS attacks.
 G. Enable IAM Config and set it to record all resources in all Regions and global resources. Then enable Amazon Inspector and configure it to enforce CIS IAM Foundations Benchmarks using IAM Config rules.

Answer: A

Explanation:

<https://docs.IAM.amazon.com/securityhub/latest/userguide/securityhub-standards-cis-config-resources.html>

NEW QUESTION 136

- (Exam Topic 1)

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

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

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

Answer: D

Explanation:

<https://docs.IAM.amazon.com/IAM/EC2/latest/UserGuide/security-group-rules-reference.html#sg-rules-other-in>

NEW QUESTION 137

- (Exam Topic 2)

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

Please select:

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

Answer: A

Explanation:

The IAM Documentation mentions the following on IAM KMS

IAM Key Management Service (IAM KMS) is a managed service that makes it easy for you to create and control the encryption keys used to encrypt your data.

IAM KMS is integrated with other IAM services including Amazon Elastic Block Store (Amazon EBS), Amazon Simple Storage Service (Amazon S3), Amazon Redshift Amazon Elastic Transcoder, Amazon WorkMail, Amazon Relational Database Service (Amazon RDS), and others to make it simple to encrypt your data with encryption keys that you manage

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

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

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

IAM KMS API

Submit your Feedback/Queries to our Experts

NEW QUESTION 142

- (Exam Topic 2)

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

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

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

- A. The policy allows access for the IAM account 111122223333 to manage key access though IAM policies.
- B. The policy allows all IAM users in account 111122223333 to have full access to the KMS key.
- C. The policy allows the root user in account 111122223333 to have full access to the KMS key.
- D. The policy allows the KMS service-linked role in account 111122223333 to have full access to the KMS key.
- E. The policy allows all IAM roles in account 111122223333 to have full access to the KMS key.

Answer: AC

Explanation:

Giving the IAM account full access to the CMK does this; it enables you to use IAM policies to give IAM users and roles in the account access to the CMK. It does not by itself give any IAM users or roles access to the CMK, but it enables you to use IAM policies to do so.

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

NEW QUESTION 147

- (Exam Topic 2)

Your company has an EC2 Instance that is hosted in an IAM VPC. There is a requirement to ensure that logs files from the EC2 Instance are stored accordingly.

The access should also be limited for the destination of the log files. How can this be accomplished? Choose 2 answers from the options given below. Each answer forms part of the solution

Please select:

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

Answer: BD

Explanation:

You can create a Log group and send all logs from the EC2 Instance to that group. You can then limit the access to the Log groups via an IAM policy.

Option A is invalid because Cloudtrail is used to record API activity and not for storing log files Option C is invalid because Cloudtrail is the wrong service to be used for this requirement

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

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

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

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

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

Submit your Feedback/Queries to our Experts

NEW QUESTION 152

- (Exam Topic 2)

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

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

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

Answer: B

Explanation:

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

NEW QUESTION 153

- (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 154

- (Exam Topic 2)

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

Please select:

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

Answer: B

Explanation:

The IAM Documentation mentions the following:

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

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

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

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

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

NEW QUESTION 159

- (Exam Topic 2)

You have an instance setup in a test environment in IAM. You installed the required application and promoted the server to a production environment. Your IT Security team has advised that there may be traffic flowing in from an unknown IP address to port 22. How can this be mitigated immediately?

Please select:

- A. Shutdown the instance.
- B. Remove the rule for incoming traffic on port 22 for the Security Group.
- C. Change the AMI for the instance.
- D. Change the Instance type for the instance.

Answer: B

Explanation:

In the test environment, the security groups might have been opened to all IP addresses for testing purposes. Always ensure to remove this rule once all testing is completed.

Option A, C, and D are all invalid because this would affect the application running on the server. The easiest way is just to remove the rule for access on port 22.

For more information on authorizing access to an instance, please visit the below URL: <https://docs.IAM.amazon.com/IAMEC2/latest/UserGuide/authorizing-access-to-an-instance.html>

The correct answer is: Remove the rule for incoming traffic on port 22 for the Security Group Submit your Feedback/Queries to our Experts

NEW QUESTION 162

- (Exam Topic 2)

You want to get a list of vulnerabilities for an EC2 Instance as per the guidelines set by the Center of Internet Security. How can you go about doing this?

Please select:

- A. Enable IAM Guard Duty for the Instance
- B. Use IAM Trusted Advisor
- C. Use IAM inspector
- D. Use IAM Macie

Answer: C

Explanation:

The IAM Inspector service can inspect EC2 Instances based on specific Rules. One of the rules packages is based on the guidelines set by the Center of Internet Security

Center for Internet security (CIS) Benchmarks

The CIS Security Benchmarks program provides well-defined, un-biased and consensus-based industry best practices to help organizations assess and improve their security. Amazon Web Services is a CIS Security Benchmarks Member company and the list of Amazon Inspector certifications can be viewed here.

Option A is invalid because this can be used to protect an instance but not give the list of vulnerabilities Options B and D are invalid because these services cannot give a list of vulnerabilities For more information

on the guidelines, please visit the below URL:

* https://docs.IAM.amazon.com/inspector/latest/userguide/inspector_cis.html The correct answer is: Use IAM Inspector

Submit your Feedback/Queries to our Experts

NEW QUESTION 164

- (Exam Topic 2)

A company has enabled Amazon GuardDuty in all Regions as part of its security monitoring strategy. In one of the VPCs, the company hosts an Amazon EC2 instance working as an FTP server that is contacted by a high number of clients from multiple locations. This is identified by GuardDuty as a brute force attack due to the high number of connections that happen every hour.

The finding has been flagged as a false positive. However, GuardDuty keeps raising the issue. A Security Engineer has been asked to improve the signal-to-noise ratio. The Engineer needs to ensure that changes do not compromise the visibility of potential anomalous behavior.

How can the Security Engineer address the issue?

- A. Disable the FTP rule in GuardDuty in the Region where the FTP server is deployed
- B. Add the FTP server to a trusted IP list and deploy it to GuardDuty to stop receiving the notifications
- C. Use GuardDuty filters with auto archiving enabled to close the findings
- D. Create an IAM Lambda function that closes the finding whenever a new occurrence is reported

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.

NEW QUESTION 167

- (Exam Topic 2)

Example.com hosts its internal document repository on Amazon EC2 instances. The application runs on EC2 instances and previously stored the documents on encrypted Amazon EBS volumes. To optimize the application for scale, example.com has moved the files to Amazon S3. The security team has mandated that all the files are securely deleted from the EBS volume, and it must certify that the data is unreadable before releasing the underlying disks.

Which of the following methods will ensure that the data is unreadable by anyone else?

- A. Change the volume encryption on the EBS volume to use a different encryption mechanism
- B. Then, release the EBS volumes back to IAM.
- C. Release the volumes back to IA
- D. IAM immediately wipes the disk after it is deprovisioned.
- E. Delete the encryption key used to encrypt the EBS volume
- F. Then, release the EBS volumes back to IAM.
- G. Delete the data by using the operating system delete command
- H. Run Quick Format on the drive and then release the EBS volumes back to IAM.

Answer: D

Explanation:

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

<https://d0.IAMstatic.com/whitepapers/IAM-security-whitepaper.pdf>

NEW QUESTION 169

- (Exam Topic 2)

An organization has three applications running on IAM, each accessing the same data on Amazon S3. The data on Amazon S3 is server-side encrypted by using an IAM KMS Customer Master Key (CMK).

What is the recommended method to ensure that each application has its own programmatic access control permissions on the KMS CMK?

- A. Change the key policy permissions associated with the KMS CMK for each application when it must access the data in Amazon S3.
- B. Have each application assume an IAM role that provides permissions to use the IAM Certificate Manager CMK.
- C. Have each application use a grant on the KMS CMK to add or remove specific access controls on the KMS CMK.
- D. Have each application use an IAM policy in a user context to have specific access permissions on the KMS CMK.

Answer: C

NEW QUESTION 171

- (Exam Topic 2)

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

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

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

Answer: A

NEW QUESTION 174

- (Exam Topic 2)

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

How can the security team fulfill these requirements?

Please select:

- A. Use Amazon QuickSight and Cloud Trail to generate the report of out of compliance instances/servers.Redeploy all out of compliance instances/servers using an AMI with the latest patches.
- B. Use Systems 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 of1 compliance instances/servers using an AMI with the latest patches.
- E. Use Trusted Advisor to generate the report of out of compliance instances/server
- F. Use Systems 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 176

- (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 180

- (Exam Topic 2)

An organization wants to deploy a three-tier web application whereby the application servers run on Amazon EC2 instances. These EC2 instances need access to credentials that they will use to authenticate their SQL connections to an Amazon RDS DB instance. Also, IAM Lambda functions must issue queries to the RDS

database by using the same database credentials.

The credentials must be stored so that the EC2 instances and the Lambda functions can access them. No other access is allowed. The access logs must record when the credentials were accessed and by whom.

What should the Security Engineer do to meet these requirements?

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

Answer: D

NEW QUESTION 184

- (Exam Topic 2)

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

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

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

Answer: BDE

NEW QUESTION 185

- (Exam Topic 2)

A Software Engineer is trying to figure out why network connectivity to an Amazon EC2 instance does not appear to be working correctly. Its security group allows inbound HTTP traffic from 0.0.0.0/0, and the outbound rules have not been modified from the default. A custom network ACL associated with its subnet allows inbound HTTP traffic from 0.0.0.0/0 and has no outbound rules.

What would resolve the connectivity issue?

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

Answer: C

Explanation:

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

NEW QUESTION 187

- (Exam Topic 2)

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

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

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

Answer: AD

Explanation:

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

NEW QUESTION 192

- (Exam Topic 2)

A company is using CloudTrail to log all IAM API activity for all regions in all of its accounts. The CISO has asked that additional steps be taken to protect the integrity of the log files.

What combination of steps will protect the log files from intentional or unintentional alteration? Choose 2 answers from the options given below
Please select:

- A. Create an S3 bucket in a dedicated log account and grant the other accounts write only access
- B. Deliver all log files from every account to this S3 bucket.
- C. Write a Lambda function that queries the Trusted Advisor Cloud Trail check
- D. Run the function every 10 minutes.
- E. Enable CloudTrail log file integrity validation
- F. Use Systems Manager Configuration Compliance to continually monitor the access policies of S3 buckets containing Cloud Trail logs.
- G. Create a Security Group that blocks all traffic except calls from the CloudTrail service
- H. Associate the security group with) all the Cloud Trail destination S3 buckets.

Answer: AC

Explanation:

The IAM Documentation mentions the following

To determine whether a log file was modified, deleted, or unchanged after CloudTrail delivered it you can use CloudTrail log file integrity validation. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.

Option B is invalid because there is no such thing as Trusted Advisor Cloud Trail checks Option D is invalid because Systems Manager cannot be used for this purpose.

Option E is invalid because Security Groups cannot be used to block calls from other services For more information on Cloudtrail log file validation, please visit the below URL:

<https://docs.IAM.amazon.com/IAMcloudtrail/latest/userguide/cloudtrail-loc-file-validation-intro.html> For more information on delivering Cloudtrail logs from multiple accounts, please visit the below URL:

<https://docs.IAM.amazon.com/IAMcloudtrail/latest/userguide/cloudtrail-receive-logs-from-multiple-accounts.html>

The correct answers are: Create an S3 bucket in a dedicated log account and grant the other accounts write only access. Deliver all log files from every account to this S3 bucket, Enable Cloud Trail log file integrity validation

Submit your Feedback/Queries to our Experts

NEW QUESTION 194

- (Exam Topic 2)

A company's security policy requires that VPC Flow Logs are enabled on all VPCs. A Security Engineer is looking to automate the process of auditing the VPC resources for compliance.

What combination of actions should the Engineer take? (Choose two.)

- A. Create an IAM Lambda function that determines whether Flow Logs are enabled for a given VPC.
- B. Create an IAM Config configuration item for each VPC in the company IAM account.
- C. Create an IAM Config managed rule with a resource type of IAM:: Lambda:: Function.
- D. Create an Amazon CloudWatch Event rule that triggers on events emitted by IAM Config.
- E. Create an IAM Config custom rule, and associate it with an IAM Lambda function that contains the evaluating logic.

Answer: AE

Explanation:

<https://medium.com/mudita-misra/how-to-audit-your-aws-resources-for-security-compliance-by-using-custom-l>

NEW QUESTION 196

- (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 200

- (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 202

- (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 206

- (Exam Topic 2)

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

How can the Application team's requirements be met?

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

Answer: A

NEW QUESTION 209

- (Exam Topic 2)

The Accounting department at Example Corp. has made a decision to hire a third-party firm, AnyCompany, to monitor Example Corp.'s IAM account to help optimize costs.

The Security Engineer for Example Corp. has been tasked with providing AnyCompany with access to the required Example Corp. IAM resources. The Engineer has created an IAM role and granted permission to AnyCompany's IAM account to assume this role.

When customers contact AnyCompany, they provide their role ARN for validation. The Engineer is concerned that one of AnyCompany's other customers might deduce Example Corp.'s role ARN and potentially compromise the company's account.

What steps should the Engineer perform to prevent this outcome?

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

Answer: B

NEW QUESTION 212

- (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 216

- (Exam Topic 2)

The Information Technology department has stopped using Classic Load Balancers and switched to Application Load Balancers to save costs. After the switch, some users on older devices are no longer able to connect to the website.

What is causing this situation?

- A. Application Load Balancers do not support older web browsers.
- B. The Perfect Forward Secrecy settings are not configured correctly.
- C. The intermediate certificate is installed within the Application Load Balancer.
- D. The cipher suites on the Application Load Balancers are blocking connections.

Answer: D

Explanation:

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

NEW QUESTION 221

- (Exam Topic 2)

A Security Engineer is building a Java application that is running on Amazon EC2. The application communicates with an Amazon RDS instance and authenticates with a user name and password.

Which combination of steps can the Engineer take to protect the credentials and minimize downtime when the credentials are rotated? (Choose two.)

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

Answer: CE

NEW QUESTION 222

- (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 227

- (Exam Topic 2)

Which of the following minimizes the potential attack surface for applications?

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

Answer: A

Explanation:

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

NEW QUESTION 229

- (Exam Topic 2)

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

Please select:

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

Answer: B

Explanation:

The IAM Documentation mentions the following.

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

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

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

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

Submit your Feedback/Queries to our Experts

NEW QUESTION 231

- (Exam Topic 2)

A company has a forensic logging use case whereby several hundred applications running on Docker on EC2 need to send logs to a central location. The Security Engineer must create a logging solution that is able to perform real-time analytics on the log files, grants the ability to replay events, and persists data.

Which IAM Services, together, can satisfy this use case? (Select two.)

- A. Amazon Elasticsearch
- B. Amazon Kinesis
- C. Amazon SQS
- D. Amazon CloudWatch
- E. Amazon Athena

Answer: AB

Explanation:

<https://docs.aws.amazon.com/whitepapers/latest/IAM-overview/analytics.html#amazon-athena>

NEW QUESTION 236

- (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/logging-using-cloudtrail.html> The correct answer is: Enable a trail in Cloudtrail

Submit your Feedback/Queries to our Experts

NEW QUESTION 241

- (Exam Topic 2)

Due to new compliance requirements, a Security Engineer must enable encryption with customer-provided keys on corporate data that is stored in DynamoDB.

The company wants to retain full control of the encryption keys.

Which DynamoDB feature should the Engineer use to achieve compliance?

- A. Use IAM Certificate Manager to request a certificate
- B. Use that certificate to encrypt data prior to uploading it to DynamoDB.
- C. Enable S3 server-side encryption with the customer-provided key
- D. Upload the data to Amazon S3, and then use S3Copy to move all data to DynamoDB
- E. Create a KMS master key
- F. Generate per-record data keys and use them to encrypt data prior to uploading it to DynamoDB
- G. Dispose of the cleartext and encrypted data keys after encryption without storing.
- H. Use the DynamoDB Java encryption client to encrypt data prior to uploading it to DynamoDB.

Answer: D

Explanation:

Follow the link:

<https://docs.IAM.amazon.com/dynamodb-encryption-client/latest/devguide/what-is-ddb-encrypt.html>

NEW QUESTION 242

- (Exam Topic 2)

A Security Administrator has a website hosted in Amazon S3. The Administrator has been given the following requirements:

- Users may access the website by using an Amazon CloudFront distribution.
- Users may not access the website directly by using an Amazon S3 URL.

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

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

Answer: AC

NEW QUESTION 247

- (Exam Topic 2)

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

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

Please select:

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

Answer: A

Explanation:

Your answer is incorrect Answer-A

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

- Scenario 1: Suppose that you are hosting a website in an Amazon S3 bucket named website as described in Hosting a Static Website on Amazon S3. Your users load the website endpoint <http://website.s3-website-us-east-1.amazonaws.com>. Now you want to use JavaScript on the webpages that are stored in this bucket to be able to make authenticated GET and PUT requests against the same bucket by using the Amazon S3 API endpoint for the bucket website.s3.amazonaws.com. A browser would normally block JavaScript from allowing those requests, but with CORS you can configure your bucket to explicitly enable cross-origin requests from website.s3-website-us-east-1.amazonaws.com.
- Scenario 2: Suppose that you want to host a web font from your S3 bucket. Again, browsers require a CORS check (also called a preflight check) for loading web fonts. You would configure the bucket that is hosting the web font to allow any origin to make these requests.

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

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

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

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

Submit your Feedback/Queries to our Experts

NEW QUESTION 252

- (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 name
- 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 254

- (Exam Topic 2)

An IAM Lambda function was misused to alter data, and a Security Engineer must identify who invoked the function and what output was produced. The Engineer cannot find any logs created by the Lambda function in Amazon CloudWatch Logs.

Which of the following explains why the logs are not available?

- A. The execution role for the Lambda function did not grant permissions to write log data to CloudWatch Logs.
- B. The Lambda function was executed by using Amazon API Gateway, so the logs are not stored in CloudWatch Logs.
- C. The execution role for the Lambda function did not grant permissions to write to the Amazon S3 bucket where CloudWatch Logs stores the logs.
- D. The version of the Lambda function that was executed was not current.

Answer: A

NEW QUESTION 259

- (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 264

- (Exam Topic 2)

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

Please select:

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

Answer: B

Explanation:

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

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



Option A is invalid because IAM Inspector is used to detect security vulnerabilities in instances and not for security groups.

Option C is invalid because this can be used to detect changes in security groups but not show you security groups that have compromised access.

Option D is partially valid but would just be a maintenance overhead

For more information on the IAM Trusted Advisor, please visit the below URL: <https://IAM.amazon.com/premiumsupport/trustedadvisor/best-practices>;

The correct answer is: Use the IAM Trusted Advisor to see which security groups have compromised access. Submit your Feedback/Queries to our Experts

NEW QUESTION 265

- (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 269

- (Exam Topic 2)

You are designing a custom IAM policy that would allow users to list buckets in S3 only if they are MFA authenticated. Which of the following would best match this requirement?

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

```
"Version": "2012-10-17",
"Statement": {
  "Effect": "Allow",
  "Action": [
    "s3:ListAllMyBuckets",
    "s3:GetBucketLocation"
  ],
  "Resource": "Resource": "arn:aws:s3:*:*:*",
  "Condition": {
    "Bool": {"aws:MultiFactorAuthPresent": true}
  }
}
```

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

```
"Version": "2012-10-17",
"Statement": {
  "Effect": "Allow",
  "Action": [
    "s3:ListAllMyBuckets",
    "s3:GetBucketLocation"
  ],
  "Resource": "Resource": "arn:aws:s3:*:*:*",
  "Condition": {
    "Bool": {"aws:MultiFactorAuthPresent": false}
  }
}
```

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

```
"Version": "2012-10-17",
"Statement": {
  "Effect": "Allow",
  "Action": [
    "s3:ListAllMyBuckets",
    "s3:GetBucketLocation"
  ],
  "Resource": "Resource": "arn:aws:s3:*:*:*",
  "Condition": {
    "aws:MultiFactorAuthPresent": false
  }
}
```

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

```
"Version": "2012-10-17",
"Statement": {
  "Effect": "Allow",
  "Action": [
    "s3:ListAllMyBuckets",
    "s3:GetBucketLocation"
  ],
  "Resource": "Resource": "arn:aws:s3:::*",
  "Condition": {
    "aws:MultiFactorAuthPresent": true
  }
}
```

Answer: A

Explanation:

The Condition clause can be used to ensure users can only work with resources if they are MFA authenticated. Option B and C are wrong since the IAM:MultiFactorAuthPresent clause should be marked as true. Here you are saying that onl if the user has been MFA activated, that means it is true, then allow access.

Option D is invalid because the "boor clause is missing in the evaluation for the condition clause. Boolean conditions let you construct Condition elements that restrict access based on comparing a key to "true" or "false."

Here in this scenario the `boot` attribute in the condition element will return a value `True` for option A which will ensure that access is allowed on S3 resources. For more information on an example on such a policy, please visit the following URL:

NEW QUESTION 271

- (Exam Topic 2)

A Security Engineer received an IAM Abuse Notice listing EC2 instance IDs that are reportedly abusing other hosts. Which action should the Engineer take based on this situation? (Choose three.)

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

Answer: BEF

NEW QUESTION 275

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 276

- (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 279

- (Exam Topic 2)

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

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

Answer: D

Explanation:

The IAM Documentation states the following

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

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

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

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

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

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

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

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

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

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

Rotation period for CMKs is as follows:

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

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

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

Submit your Feedback/Queries to our Experts

NEW QUESTION 280

- (Exam Topic 2)

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

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

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

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

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

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


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

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

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

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

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

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

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

Answer: A

NEW QUESTION 283

- (Exam Topic 2)

The Security Engineer is managing a web application that processes highly sensitive personal information. The application runs on Amazon EC2. The application has strict compliance requirements, which instruct that all incoming traffic to the application is protected from common web exploits and that all outgoing traffic from the EC2 instances is restricted to specific whitelisted URLs.

Which architecture should the Security Engineer use to meet these requirements?

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

Answer: D

Explanation:

IAM Shield is mainly for DDos Attacks. IAM WAF is mainly for some other types of attacks like Injection and XSS etc. In this scenario, It seems it is WAF functionality that is needed. VPC logs do show the source and destination IP and Port, they never show any URL .. because URL are level 7 while VPC are concerned about lower network levels.

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

NEW QUESTION 286

- (Exam Topic 2)

A Security Engineer has created an Amazon CloudWatch event that invokes an IAM Lambda function daily. The Lambda function runs an Amazon Athena query that checks IAM CloudTrail logs in Amazon S3 to detect whether any IAM user accounts or credentials have been created in the past 30 days. The results of the

Athena query are created in the same S3 bucket. The Engineer runs a test execution of the Lambda function via the IAM Console, and the function runs successfully.

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

Security Engineer

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

Lambda function execution role

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

What is causing the error?

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

Answer: D

NEW QUESTION 288

- (Exam Topic 2)

A company's database developer has just migrated an Amazon RDS database credential to be stored and managed by IAM Secrets Manager. The developer has also enabled rotation of the credential within the Secrets Manager console and set the rotation to change every 30 days.

After a short period of time, a number of existing applications have failed with authentication errors. What is the MOST likely cause of the authentication errors?

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

Answer: B

Explanation:

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

NEW QUESTION 291

- (Exam Topic 2)

You have just recently set up a web and database tier in a VPC and hosted the application. When testing the app, you are not able to reach the home page for the app. You have verified the security groups. What can help you diagnose the issue.

Please select:

- A. Use the IAM Trusted Advisor to see what can be done.
- B. Use VPC Flow logs to diagnose the traffic
- C. Use IAM WAF to analyze the traffic
- D. Use IAM Guard Duty to analyze the traffic

Answer: B

Explanation:

Option A is invalid because this can be used to check for security issues in your account, but not verify as to why you cannot reach the home page for your application

Option C is invalid because this used to protect your app against application layer attacks, but not verify as to why you cannot reach the home page for your application

Option D is invalid because this used to protect your instance against attacks, but not verify as to why you cannot reach the home page for your application

The IAM Documentation mentions the following

VPC Flow Logs capture network flow information for a VPC, subnet or network interface and stores it in Amazon CloudWatch Logs. Flow log data can help customers troubleshoot network issues; for example, to diagnose why specific traffic is not reaching an instance, which might be a result of overly restrictive security group rules. Customers can also use flow logs as a security tool to monitor the traffic that reaches their instances, to profile network traffic, and to look for abnormal traffic behaviors.

For more information on IAM Security, please visit the following URL: <https://IAM.amazon.com/answers/networking/vpc-security-capabilities>>

The correct answer is: Use VPC Flow logs to diagnose the traffic Submit your Feedback/Queries to our Experts

NEW QUESTION 296

- (Exam Topic 2)

An organization receives an alert that indicates that an EC2 instance behind an ELB Classic Load Balancer has been compromised.

What techniques will limit lateral movement and allow evidence gathering?

- A. Remove the instance from the load balancer and terminate it.
- B. Remove the instance from the load balancer, and shut down access to the instance by tightening the security group.
- C. Reboot the instance and check for any Amazon CloudWatch alarms.
- D. Stop the instance and make a snapshot of the root EBS volume.

Answer: B

Explanation:

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

NEW QUESTION 301

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

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

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

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

Money Back Guarantee

SCS-C02 Practice Exam Features:

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