

Exam Questions SCS-C01

AWS Certified Security- Specialty

<https://www.2passeasy.com/dumps/SCS-C01/>



NEW QUESTION 1

- (Exam Topic 1)

A company has an AWS account and allows a third-party contractor who uses another AWS account, to assume certain IAM roles. The company wants to ensure that IAM roles can be assumed by the contractor only if the contractor has multi-factor authentication enabled on their IAM user accounts

What should the company do to accomplish this?

A)

Add the following condition to the IAM policy attached to all IAM roles:

```
"Effect" : "Deny",  
"Condition" : { "BoolIfExists" : { "aws:MultiFactorAuthPresent" : false } }
```

B)

Add the following condition to the IAM policy attached to all IAM roles:

```
"Effect" : "Deny",  
"Condition" : { "Bool" : { "aws:MultiFactorAuthPresent" : false } }
```

C)

Add the following condition to the IAM policy attached to all IAM roles:

```
"Effect" : "Allow",  
"Condition" : { "Null" : { "aws:MultiFactorAuthPresent" : false } }
```

D)

Add the following condition to the IAM policy attached to all IAM roles:

```
"Effect" : "Allow",  
"Condition" : { "BoolIfExists" : { "aws:MultiFactorAuthPresent" : false } }
```

A. Option A

B. Option B

C. Option C

D. Option D

Answer: A

NEW QUESTION 2

- (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 AWS 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 3

- (Exam Topic 1)

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

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

A. Place the application behind an Application Load Balancer (ALB). Use Amazon Cognito as authentication (or the ALB). Define a SAML-based Amazon Cognito user pool and connect it to ADFS. Implement AWS SSO in the master account and link it to ADFS as an identity provider. Define the EC2 instance as a managed resource, then apply an IAM policy on the resource.

B. Define an Amazon Cognito identity pool, then install the connector on the Active Directory server. Use the Amazon Cognito SDK on the application instance to authenticate the employees using their

C. Active Directory user names and passwords.

D. Create an AWS Lambda custom authorizer as the authenticator for a reverse proxy on Amazon EC2. Ensure the security group on Amazon EC2 only allows access from the Lambda function.

Answer: B

NEW QUESTION 4

- (Exam Topic 1)

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

- A trusted forensic environment must be provisioned

- Automated response processes must be orchestrated

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

A. AWS CloudFormation

B. Amazon GuardDuty

C. Amazon Inspector

D. Amazon Macie

E. AWS Step Functions

Answer: AE

NEW QUESTION 5

- (Exam Topic 1)

A company wants to encrypt the private network between its on-premises environment and AWS. The company also wants a consistent network experience for its employees.

What should the company do to meet these requirements?

- A. Establish an AWS Direct Connect connection with AWS and set up a Direct Connect gateway
- B. In the Direct Connect gateway configuration, enable IPsec and BGP, and then leverage native AWS network encryption between Availability Zones and Regions,
- C. Establish an AWS Direct Connect connection with AWS and set up a Direct Connect gateway
- D. Using the Direct Connect gateway, create a private virtual interface and advertise the customer gateway private IP address
- E. Create a VPN connection using the customer gateway and the virtual private gateway
- F. Establish a VPN connection with the AWS virtual private cloud over the internet
- G. Establish an AWS Direct Connect connection with AWS and establish a public virtual interface
- H. For prefixes that need to be advertised, enter the customer gateway public IP address
- I. Create a VPN connection over Direct Connect using the customer gateway and the virtual private gateway.

Answer: C

NEW QUESTION 6

- (Exam Topic 1)

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

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

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

Answer: D

NEW QUESTION 7

- (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 AWS 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 AWS SDK
- 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 AWS Systems Manager Agent on the instances. Configure an automation document to copy the application log files to AWS 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 8

- (Exam Topic 1)

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

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

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

Answer: BC

NEW QUESTION 9

- (Exam Topic 1)

A company uses Microsoft Active Directory for access management for on-premises resources and wants to use the same mechanism for accessing its AWS accounts. Additionally, the development team plans to launch a public-facing application for which they need a separate authentication solution.

Which combination of the following would satisfy these requirements? (Select TWO)

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

Answer: CD

NEW QUESTION 10

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 10

- (Exam Topic 1)

A company's Director of Information Security wants a daily email report from AWS that contains recommendations for each company account to meet AWS Security best practices. Which solution would meet these requirements?

- A. In every AWS account, configure AWS Lambda to query the AWS Support API for AWS 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 AWS CloudTrail. Create a daily Amazon CloudWatch trigger to run the report daily and email it using Amazon SNS.
- D. Use AWS 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 15

- (Exam Topic 1)

A company requires that SSH commands used to access its AWS 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 AWS 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 AWS 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 18

- (Exam Topic 1)

A Security Engineer is looking for a way to control access to data that is being encrypted under a CMK. The Engineer is also looking to use additional authenticated data (AAD) to prevent tampering with ciphertext. Which action would provide the required functionality?

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

Answer: B

NEW QUESTION 19

- (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.aws.amazon.com/AWSEC2/latest/UserGuide/security-group-rules-reference.html#sg-rules-other-ins>

NEW QUESTION 21

- (Exam Topic 1)

A Solutions Architect is designing a web application that uses Amazon CloudFront, an Elastic Load Balancing Application Load Balancer, and an Auto Scaling group of Amazon EC2 instances. The load balancer and EC2 instances are in the US West (Oregon) region. It has been decided that encryption in transit is necessary by using a customer-branded domain name from the client to CloudFront and from CloudFront to the load balancer. Assuming that AWS Certificate Manager is used, how many certificates will need to be generated?

- A. One in the US West (Oregon) region and one in the US East (Virginia) region.
- B. Two in the US West (Oregon) region and none in the US East (Virginia) region.
- C. One in the US West (Oregon) region and none in the US East (Virginia) region.
- D. Two in the US East (Virginia) region and none in the US West (Oregon) region.

Answer: B

NEW QUESTION 25

- (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 (FIPS) 140-2 Level 3. Which solution meets these requirements?

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

Answer: B

NEW QUESTION 29

- (Exam Topic 1)

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

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

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

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

Answer: ABF

NEW QUESTION 31

- (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?

- A. Enable AWS Shield Advanced and AWS WA
- B. Configure an AWS WAF custom filter for egress traffic on port 5353
- C. Enable Amazon Inspector on Amazon ECS and configure a custom assessment to evaluate containers that have port 5353 ope
- D. Update the NACLs to block port 5353 outbound.
- E. 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.
- F. Use Amazon Athena to query AWS 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 35

- (Exam Topic 1)

An company is using AWS Secrets Manager to store secrets that are encrypted using a CMK and are stored in the security account 111122223333. One of the company's production accounts. 444455556666, must to retrieve the secret values from the security account 111122223333. A security engineer needs to apply a policy to the secret in the security account based on least privilege access so the production account can retrieve the secret value only.

Which policy should the security engineer apply?

- A.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "secretsmanager:*",
      "Principal": {"AWS": "444455556666"},
      "Resource": "*"
    }
  ]
}
```
- B.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "secretsmanager:*",
      "Principal": {"AWS": "111122223333"},
      "Resource": "*"
    }
  ]
}
```
- C.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "secretsmanager:GetSecretValue",
      "Principal": {"AWS": "111122223333"},
      "Resource": "*"
    }
  ]
}
```
- D.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "secretsmanager:GetSecretValue",
      "Principal": {"AWS": "444455556666"},
      "Resource": "*"
    }
  ]
}
```

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

Answer: A

NEW QUESTION 40

- (Exam Topic 1)

A company has a VPC with an IPv6 address range and a public subnet with an IPv6 address block. The VPC currently hosts some public Amazon EC2 instances but a Security Engineer needs to migrate a second application into the VPC that also requires IPv6 connectivity.

This new application will occasionally make API requests to an external, internet-accessible endpoint to receive updates. However, the Security team does not want the application's EC2 instance exposed directly to the internet. The Security Engineer intends to create a private subnet with a custom route table and to associate the route table with the private subnet.

What else does the Security Engineer need to do to ensure the application will not be exposed directly to the internet, but can still communicate as required?

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

Answer: D

NEW QUESTION 41

- (Exam Topic 1)

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

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

A security engineer needs to address the immediate issue and ensure that it will not occur again. Which combination of steps should the security engineer take to accomplish this? (Select TWO.)

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

Answer: AD

NEW QUESTION 42

- (Exam Topic 1)

A company is outsourcing its operational support 1o an external company. The company's security officer must implement an access solution fen delegating operational support that minimizes overhead.

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

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

Answer: B

NEW QUESTION 43

- (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 AWS 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 45

- (Exam Topic 1)

A company's Security Engineer has been asked to monitor and report all AWS account root user activities. Which of the following would enable the Security Engineer to monitor and report all root user activities?

(Select TWO)

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

Answer: BE

NEW QUESTION 46

- (Exam Topic 1)

Unapproved changes were previously made to a company's Amazon S3 bucket. A security engineer configured AWS 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 AWS Config to record changes to the buckets.
- B. Configure policies attached to S3 buckets to allow AWS Config to record changes to the buckets.
- C. Attach the AmazonS3ReadOnryAccess managed policy to the IAM user.
- D. Verify the security engineer's IAM user has an attached policy that allows all AWS Config actions.

E. Assign the AWSConfigRole managed policy to the AWS Config role

Answer: BE

NEW QUESTION 48

- (Exam Topic 1)

A company's architecture requires that its three Amazon EC2 instances run behind an Application Load Balancer (ALB). The EC2 instances transmit sensitive data between each other. Developers use SSL certificates to encrypt the traffic between the public users and the ALB. However, the Developers are unsure of how to encrypt the data in transit between the ALB and the EC2 instances and the traffic between the EC2 instances.

Which combination of activities must the company implement to meet its encryption requirements? (Select TWO)

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

Answer: BC

NEW QUESTION 51

- (Exam Topic 1)

A Developer signed in to a new account within an AWS 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: B

NEW QUESTION 53

- (Exam Topic 1)

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

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

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

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

Answer: C

NEW QUESTION 54

- (Exam Topic 1)

A company's development team is designing an application using AWS Lambda and Amazon Elastic Container Service (Amazon ECS). The development team needs to create IAM roles to support these systems. The company's security team wants to allow the developers to build IAM roles directly, but the security team wants to retain control over the permissions the developers can delegate to those roles. The development team needs access to more permissions than those required for the application's AWS services. The solution must minimize management overhead.

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

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

Answer: A

NEW QUESTION 55

- (Exam Topic 1)

A company has recently recovered from a security incident that required the restoration of Amazon EC2 instances from snapshots. After performing a gap analysis of its disaster recovery procedures and backup strategies, the company is concerned that, next time, it will not be able to recover the EC2 instances if the AWS account was compromised and Amazon EBS snapshots were deleted. All EBS snapshots are encrypted using an AWS KMS CMK. Which solution would solve this problem?

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

Answer: A

NEW QUESTION 58

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 59

- (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:

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

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

Answer: AD

NEW QUESTION 61

- (Exam Topic 1)

A company uses multiple AWS accounts managed with AWS Organizations Security engineers have created a standard set of security groups for all these accounts. The security policy requires that these security groups be used for all applications and delegates modification authority to the security team only. A recent security audit found that the security groups are inconsistently implemented across accounts and that unauthorized changes have been made to the security groups. A security engineer needs to recommend a solution to improve consistency and to prevent unauthorized changes in the individual accounts in the future. Which solution should the security engineer recommend?

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

Answer: B

NEW QUESTION 63

- (Exam Topic 1)

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

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

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

Answer: AD

Explanation:

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

NEW QUESTION 65

- (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 AWS 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 68

- (Exam Topic 1)

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

- The Lambda function has internet access.
- The relational database is publicly accessible.
- The database credentials are not stored in an encrypted state.

Which combination of steps should the company take to resolve these security issues? (Select THREE.)

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

Answer: ABE

NEW QUESTION 72

- (Exam Topic 1)

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

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

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

Answer: BDF

NEW QUESTION 74

- (Exam Topic 1)

A company is using AWS Organizations to manage multiple AWS 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 AWS 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 76

- (Exam Topic 1)

While securing the connection between a company's VPC and its on-premises data center, a Security Engineer sent a ping command from an on-premises host (IP address 203.0.113.12) to an Amazon EC2 instance (IP address 172.31.16.139). The ping command did not return a response. The flow log in the VPC showed the following:

```
2 123456789010 eni-1235b8ca 203.0.113.12 172.31.16.139 0 0 1 4 336 1432917027 1432917142 ACCEPT OK
```

```
2 123456789010 eni-1235b8ca 172.31.16.139 203.0.113.12 0 0 1 4 336 1432917094 1432917142 REJECT OK
```

What action should be performed to allow the ping to work?

- A. In the security group of the EC2 instance, allow inbound ICMP traffic.
- B. In the security group of the EC2 instance, allow outbound ICMP traffic.
- C. In the VPC's NACL, allow inbound ICMP traffic.
- D. In the VPC's NACL, allow outbound ICMP traffic.

Answer: D

NEW QUESTION 79

- (Exam Topic 1)

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

Which actions will meet the program requirements that address security?

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

Answer: B

NEW QUESTION 82

- (Exam Topic 1)

A security engineer has been tasked with implementing a solution that allows the company's development team to have interactive command line access to Amazon EC2 Linux instances using the AWS Management Console.

Which steps should the security engineer take to satisfy this requirement while maintaining least privilege?

- A. Enable AWS Systems Manager in the AWS Management Console and configure for access to EC2 instances using the default AmazonEC2RoleforSSM rol
- B. Install the Systems Manager Agent on all EC2 Linux instances that need interactive acces
- C. Configure IAM user policies to allow development team access to the Systems Manager Session Manager and attach to the team's IAM users.
- D. Enable console SSH access in the EC2 consol
- E. Configure IAM user policies to allow development team access to the AWS Systems Manager Session Manager and attach to the development team's IAM users.
- F. Enable AWS Systems Manager in the AWS Management Console and configure to access EC2 instances using the default AmazonEC2RoleforSSM rol
- G. Install the Systems Manager Agent on all EC2 Linux instances that need interactive acces
- H. Configure a security group that allows SSH port 22 from all published IP addresse
- I. Configure IAM user policies to allow development team access to the AWS Systems Manager Session Manager and attach to the team's IAM users.
- J. Enable AWS Systems Manager in the AWS Management Console and configure to access EC2 instances using the default AmazonEC2RoleforSSM role Install the Systems Manager Agent on all EC2 Linux instances that need interactive acces
- K. Configure IAM policies to allow development team access to the EC2 console and attach to the teams IAM users.

Answer: A

NEW QUESTION 83

- (Exam Topic 1)

A Developer reported that AWS CloudTrail was disabled on their account. A Security Engineer investigated the account and discovered the event was undetected by the current security solution. The Security Engineer must recommend a solution that will detect future changes to the CloudTrail configuration and send alerts when changes occur.

What should the Security Engineer do to meet these requirements?

- A. Use AWS Resource Access Manager (AWS RAM) to monitor the AWS CloudTrail configuratio
- B. Send notifications using Amazon SNS.
- C. Create an Amazon CloudWatch Events rule to monitor Amazon GuardDuty finding
- D. Send email notifications using Amazon SNS.
- E. Update security contact details in AWS account settings for AWS Support to send alerts when suspicious activity is detected.
- F. Use Amazon Inspector to automatically detect security issue
- G. Send alerts using Amazon SNS.

Answer: B

NEW QUESTION 88

- (Exam Topic 1)

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

Which solution meets these requirements?

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

Answer: C

NEW QUESTION 92

- (Exam Topic 1)

A company is setting up products to deploy in AWS 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 AWS CloudFormation template backing the product to include a service role configuration.

Answer: C

NEW QUESTION 96

- (Exam Topic 1)

A Security Engineer creates an Amazon S3 bucket policy that denies access to all users. A few days later, the Security Engineer adds an additional statement to the bucket policy to allow read-only access to one other employee. Even after updating the policy the employee still receives an access denied message.

What is the likely cause of this access denial?

- A. The ACL in the bucket needs to be updated.
- B. The IAM policy does not allow the user to access the bucket
- C. It takes a few minutes for a bucket policy to take effect
- D. The allow permission is being overridden by the deny.

Answer: D

NEW QUESTION 100

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

Answer: A

NEW QUESTION 103

- (Exam Topic 1)

A company recently performed an annual security assessment of its AWS 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 AWS 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 AWS Artifact to archive AWS CloudTrail logs. Configure AWS 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 AWS CloudTrail to provide a notification when a policy change is made to resources.
- E. Create an AWS CloudTrail trail that stores audit logs in Amazon S3. Configure an AWS Config rule to provide a notification when a policy change is made to resources.

Answer: A

NEW QUESTION 104

- (Exam Topic 1)

A Security Engineer is troubleshooting a connectivity issue between a web server that is writing log files to the logging server in another VPC. The Engineer has confirmed that a peering relationship exists between the two VPCs. VPC flow logs show that requests sent from the web server are accepted by the logging server but the web server never receives a reply

Which of the following actions could fix this issue?

- A. Add an inbound rule to the security group associated with the logging server that allows requests from the web server
- B. Add an outbound rule to the security group associated with the web server that allows requests to the logging server.
- C. Add a route to the route table associated with the subnet that hosts the logging server that targets the peering connection
- D. Add a route to the route table associated with the subnet that hosts the web server that targets the peering connection

Answer: C

NEW QUESTION 107

- (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 AWS X-Ray to trace the end-to-end application flow

Answer: C

NEW QUESTION 108

- (Exam Topic 2)

A Security Engineer who was reviewing AWS Key Management Service (AWS KMS) key policies found this statement in each key policy in the company AWS 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 AWS 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 113

- (Exam Topic 2)

You have a web site that is sitting behind AWS Cloudfront. You need to protect the web site against threats such as SQL injection and Cross site scripting attacks.

Which of the following service can help in such a scenario

Please select:

- A. AWS Trusted Advisor
- B. AWS WAF
- C. AWS Inspector
- D. AWS Config

Answer: B

Explanation:

The AWS Documentation mentions the following

AWS WAF is a web application firewall that helps detect and block malicious web requests targeted at your web applications. AWS WAF allows you to create rules that can help protect against common web exploits like SQL injection and cross-site scripting. With AWS WAF you first identify the resource (either an Amazon CloudFront distribution or an Application Load Balancer) that you need to protect.

Option A is invalid because this will only give advise on how you can better the security in your AWS account but not protect against threats mentioned in the question.

Option C is invalid because this can be used to scan EC2 Instances for vulnerabilities but not protect against threats mentioned in the question.

Option D is invalid because this can be used to check config changes but not protect against threats mentioned in the quest

For more information on AWS WAF, please visit the following URL: <https://aws.amazon.com/waf/details>;

The correct answer is: AWS WAF

Submit your Feedback/Queries to our Experts

NEW QUESTION 118

- (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": "Stmnt1502987487640",  
      "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:aws: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.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies.html>

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

NEW QUESTION 119

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

NEW QUESTION 122

- (Exam Topic 2)

A Systems Administrator has written the following Amazon S3 bucket policy designed to allow access to an S3 bucket for only an authorized AWS IAM user from the IP address range 10.10.10.0/24:

```
{
  "Version": "2012-10-17",
  "Id": "S3Policy1",
  "Statement": [
    {
      "Sid": ["OfficeAllowIP"],
      "Effect": ["Allow"],
      "Principal": ["*"],
      "Action": ["s3:*"],
      "Resource": ["arn:aws:s3:::Bucket"],
      "Condition": {
        "IpAddress": [
          {
            "aws:SourceIp": "10.10.10.0/24"
          }
        ]
      }
    }
  ]
}
```

When trying to download an object from the S3 bucket from 10.10.10.40, the IAM user receives an access denied message. What does the Administrator need to change to grant access to the user?

- A. Change the "Resource" from "arn: aws:s3:::Bucket" to "arn:aws:s3:::Bucket/*".
- B. Change the "Principal" from "*" to {AWS:"arn:aws:iam: : account-number: user/username"}
- C. Change the "Version" from "2012-10-17" to the last revised date of the policy
- D. Change the "Action" from ["s3:*"] to ["s3:GetObject", "s3:ListBucket"]

Answer: A

NEW QUESTION 125

- (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, AWS 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 AWS Key Management Service (AWS KMS). Create an IAM role with access to AWS 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 AWS 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 AWS 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 AWS 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 126

- (Exam Topic 2)

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

logs.

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

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

Answer: ACE

Explanation:

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

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

NEW QUESTION 129

- (Exam Topic 2)

A company wants to have an Intrusion detection system available for their VPC in AWS. They want to have complete control over the system. Which of the following would be ideal to implement?

Please select:

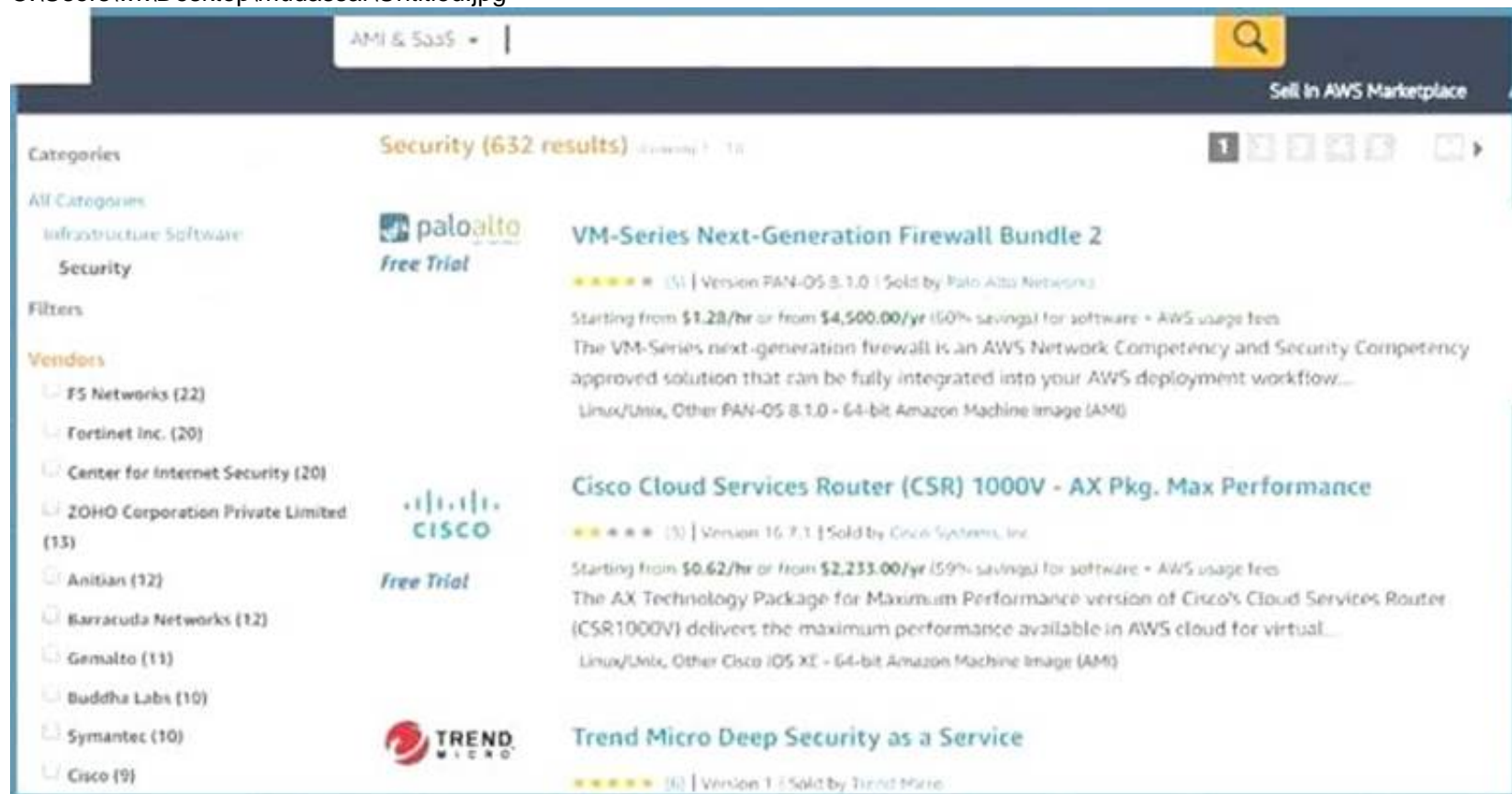
- A. Use AWS WAF to catch all intrusions occurring on the systems in the VPC
- B. Use a custom solution available in the AWS Marketplace
- C. Use VPC Flow logs to detect the issues and flag them accordingly.
- D. Use AWS Cloudwatch to monitor all traffic

Answer: B

Explanation:

Sometimes companies want to have custom solutions in place for monitoring intrusions to their systems. In such a case, you can use the AWS Marketplace for looking at custom solutions.

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



Option A.C and D are all invalid because they cannot be used to conduct intrusion detection or prevention. For more information on using custom security solutions please visit the below URL https://d1.awsstatic.com/Marketplace/security/AWSMP_Security_Solution%20verview.pdf

For more information on using custom security solutions please visit the below URL: https://d1.awsstatic.com/Marketplace/security/AWSMP_Security_Solution%20Overview.pdf

The correct answer is: Use a custom solution available in the AWS Marketplace Submit your Feedback/Queries to our Experts

NEW QUESTION 132

- (Exam Topic 2)

An organization is using Amazon CloudWatch Logs with agents deployed on its Linux Amazon EC2 instances. The agent configuration files have been checked and the application log files to be pushed are configured correctly. A review has identified that logging from specific instances is missing.

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

- A. Use an EC2 run command to confirm that the "awslogs" service is running on all instances.
- B. Verify that the permissions used by the agent allow creation of log groups/streams and to put log events.
- C. Check whether any application log entries were rejected because of invalid time stamps by reviewing/var/cwlogs/rejects.log.

- D. Check that the trust relationship grants the service “cwlogs.amazonaws.com” permission to write objects to the Amazon S3 staging bucket.
- E. Verify that the time zone on the application servers is in UTC.

Answer: AB

Explanation:

EC2 run command - can run scripts, install software, collect metrics and log files, manage patches and more. Bringing these two services together - can create CloudWatch Events rules that use EC2 Run Command to perform actions on EC2 instances or on-premises servers.

NEW QUESTION 136

- (Exam Topic 2)

A pharmaceutical company has digitized versions of historical prescriptions stored on premises. The company would like to move these prescriptions to AWS and perform analytics on the data in them. Any operation with this data requires that the data be encrypted in transit and at rest.

Which application flow would meet the data protection requirements on AWS?

- A. Digitized files -> Amazon Kinesis Data Analytics
- B. Digitized files -> Amazon Kinesis Data Firehose -> Amazon S3 -> Amazon Athena
- C. Digitized files -> Amazon Kinesis Data Streams -> Kinesis Client Library consumer -> Amazon S3 -> Athena
- D. Digitized files -> Amazon Kinesis Data Firehose -> Amazon Elasticsearch

Answer: B

NEW QUESTION 138

- (Exam Topic 2)

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

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

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

Answer: BEF

NEW QUESTION 141

- (Exam Topic 2)

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

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

Why did GuardDuty fail to alert to this behavior?

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

Answer: B

Explanation:

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

NEW QUESTION 145

- (Exam Topic 2)

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

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

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

Answer: A

Explanation:

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

NEW QUESTION 147

- (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 AWS.

- C. Release the volumes back to AW
- D. AWS immediately wipes the disk after it is deprovisioned.
- E. Delete the encryption key used to encrypt the EBS volum
- F. Then, release the EBS volumes back to AWS.
- 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 AWS.

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.awsstatic.com/whitepapers/aws-security-whitepaper.pdf>

NEW QUESTION 152

- (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 AWS account to help optimize costs.

The Security Engineer for Example Corp. has been tasked with providing AnyCompany with access to the required Example Corp. AWS resources. The Engineer has created an IAM role and granted permission to AnyCompany's AWS 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:Externald to the role's trust policy.
- D. Require two-factor authentication by adding a condition to the role's trust policy with aws:MultiFactorAuthPresent.
- E. Request an IP range from AnyCompany and add a condition with aws:SourceIp to the role's trust policy.

Answer: B

NEW QUESTION 153

- (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 AWS Systems Manager Parameter Store and notifies the Engineer that the application needs to be restarted.
- C. Configure automatic rotation of credentials in AWS Secrets Manager.
- D. Store the credential in an encrypted string parameter in AWS Systems Manager Parameter Stor
- E. Grant permission to the instance role associated with the EC2 instance to access the parameter and the AWS KMS key that is used to encrypt it.
- F. Configure the Java application to catch a connection failure and make a call to AWS Secrets Manager to retrieve updated credentials when the password is rotate
- G. Grant permission to the instance role associated with the EC2 instance to access Secrets Manager.

Answer: CE

NEW QUESTION 157

- (Exam Topic 2)

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

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

- A. The Amazon WorkMail and Amazon SES services have delegated KMS encrypt and decrypt permissions to the ExampleUser principal in the 111122223333 account.
- B. The ExampleUser principal can transparently encrypt and decrypt email exchanges specifically between ExampleUser and AWS.
- C. The CMK is to be used for encrypting and decrypting only when the principal is ExampleUser and the request comes from WorkMail or SES in the specified region.
- D. The key policy allows WorkMail or SES to encrypt or decrypt on behalf of the user for any CMK in the account.

Answer: C

NEW QUESTION 160

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 165

- (Exam Topic 2)

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

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

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

Answer: B

NEW QUESTION 169

- (Exam Topic 2)

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

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

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

Answer: A

Explanation:

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

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



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

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

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

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

Submit your Feedback/Queries to our Experts

NEW QUESTION 170

- (Exam Topic 2)

An AWS 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.

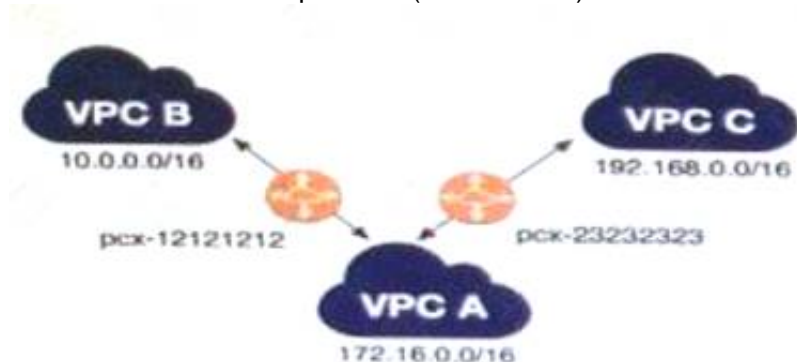
Answer: A

NEW QUESTION 175

- (Exam Topic 2)

A company has multiple VPCs in their account that are peered, as shown in the diagram. A Security Engineer wants to perform penetration tests of the Amazon EC2 instances in all three VPCs.

How can this be accomplished? (Choose two.)



- A. Deploy a pre-authorized scanning engine from the AWS Marketplace into VPC B, and use it to scan instances in all three VPC
- B. Do not complete the penetration test request form.
- C. Deploy a pre-authorized scanning engine from the Marketplace into each VPC, and scan instances in each VPC from the scanning engine in that VP
- D. Do not complete the penetration test request form.
- E. Create a VPN connection from the data center to VPC
- F. Use an on-premises scanning engine to scan the instances in all three VPC
- G. Complete the penetration test request form for all three VPCs.
- H. Create a VPN connection from the data center to each of the three VPC
- I. Use an on-premises scanning engine to scan the instances in each VP
- J. Do not complete the penetration test request form.
- K. Create a VPN connection from the data center to each of the three VPC
- L. Use an on-premises scanning engine to scan the instances in each VP
- M. Complete the penetration test request form for all three VPCs.

Answer: BD

Explanation:

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

NEW QUESTION 180

- (Exam Topic 2)

You are designing a custom IAM policy that would allow uses 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 `aws: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 181

- (Exam Topic 2)

An organization has three applications running on AWS, each accessing the same data on Amazon S3. The data on Amazon S3 is server-side encrypted by using an AWS 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 AWS 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 182

- (Exam Topic 2)

In response to the past DDoS attack experiences, a Security Engineer has set up an Amazon CloudFront distribution for an Amazon S3 bucket. There is concern that some users may bypass the CloudFront distribution and access the S3 bucket directly.

What must be done to prevent users from accessing the S3 objects directly by using URLs?

A. Change the S3 bucket/object permission so that only the bucket owner has access.

B. Set up a CloudFront origin access identity (OAI), and change the S3 bucket/object permission so that only the OAI has access.

C. Create IAM roles for CloudFront, and change the S3 bucket/object permission so that only the IAM role has access.

D. Redirect S3 bucket access to the corresponding CloudFront distribution.

Answer: B

Explanation:

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

NEW QUESTION 185

- (Exam Topic 2)

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

What should the Security Engineer use to accomplish this?

A. Server-side encryption with Amazon S3-managed keys (SSE-S3)

B. Server-side encryption with AWS KMS-managed keys (SSE-KMS)

C. Server-side encryption with customer-provided keys (SSE-C)

D. Client-side encryption with an AWS KMS-managed CMK

Answer: B

Explanation:

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

NEW QUESTION 186

- (Exam Topic 2)

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

-Storage is accessible by using only VPCs.

-Service has tamper-evident controls.

-Access logging is enabled.

-Storage has high availability.

Which of the following services meets these requirements?

A. Amazon S3 with default encryption

B. AWS CloudHSM

C. Amazon DynamoDB with server-side encryption

D. AWS Systems Manager Parameter Store

Answer: B

NEW QUESTION 190

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

Answer: D

Explanation:

AWS Shield is mainly for DDos Attacks. AWS 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.aws.amazon.com/vpc/latest/userguide/flow-logs.html>

NEW QUESTION 192

- (Exam Topic 2)

A distributed web application is installed across several EC2 instances in public subnets residing in two Availability Zones. Apache logs show several intermittent brute-force attacks from hundreds of IP addresses at the layer 7 level over the past six months.
What would be the BEST way to reduce the potential impact of these attacks in the future?

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

Answer: D

Explanation:

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

NEW QUESTION 196

- (Exam Topic 2)

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

- Content Security-Policy
- X-Frame-Options
- X-XSS-Protection

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

- A. Configure an Amazon Route 53 routing policy to send all web traffic that does not include the required headers to a black hole.
- B. Implement an AWS Lambda@Edge origin response function that inserts the required headers.
- C. Migrate the legacy application to an Amazon S3 static website and front it with an Amazon CloudFront distribution.
- D. Construct an AWS WAF rule to replace existing HTTP headers with the required security headers by using regular expressions.

Answer: B

NEW QUESTION 200

- (Exam Topic 2)





Your company has a set of resources defined in the AWS Cloud. Their IT audit department has requested to get a list of resources that have been defined across the account. How can this be achieved in the easiest manner?
Please select:

- A. Create a powershell script using the AWS CL
- B. Query for all resources with the tag of production.
- C. Create a bash shell script with the AWS CL
- D. Query for all resources in all region
- E. Store the results in an S3 bucket.
- F. Use Cloud Trail to get the list of all resources
- G. Use AWS Config to get the list of all resources

Answer: D

Explanation:

The most feasible option is to use AWS Config. When you turn on AWS Config, you will get a list of resources defined in your AWS Account.
A sample snapshot of the resources dashboard in AWS Config is shown below [C:\Users\wk\Desktop\mudassar\Untitled.jpg](#)

Resources	
Total resource count	131
Top 10 resource types	Total
 IAM Policy	45
 IAM Role	40
 EC2 Subnet	7
 EC2 SecurityGroup	6
 EC2 RouteTable	6
 EC2 VPC	4
 EC2 NetworkAcl	4

Option A is incorrect because this would give the list of production based resources and now all resources Option B is partially correct But this will just add more maintenance overhead.

Option C is incorrect because this can be used to log API activities but not give an account of all resou For more information on AWS Config, please visit the below URL: <https://docs.aws.amazon.com/config/latest/developereuide/how-does-confie-work.html>

The correct answer is: Use AWS Config to get the list of all resources Submit your Feedback/Queries to our Experts

NEW QUESTION 203

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

Answer: A

Explanation:

The AWS Documentation mentions the following on AWS KMS

AWS Key Management Service (AWS KMS) is a managed service that makes it easy for you to create and control the encryption keys used to encrypt your data. AWS KMS is integrated with other AWS 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 AWS 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 AWS KMS, please visit the following URL: <https://docs.aws.amazon.com/kms/latest/developereuide/overview.html> The correct answer is: AWS KMS API

Submit your Feedback/Queries to our Experts

NEW QUESTION 208

- (Exam Topic 2)

A security team is responsible for reviewing AWS API call activity in the cloud environment for security violations. These events must be recorded and retained in a centralized location for both current and future AWS regions.

What is the SIMPLEST way to meet these requirements?

- A. Enable AWS Trusted Advisor security checks in the AWS Console, and report all security incidents for all regions.
- B. Enable AWS CloudTrail by creating individual trails for each region, and specify a single Amazon S3 bucket to receive log files for later analysis.
- C. Enable AWS CloudTrail by creating a new trail and applying the trail to all region
- D. Specify a single Amazon S3 bucket as the storage location.
- E. Enable Amazon CloudWatch logging for all AWS services across all regions, and aggregate them to a single Amazon S3 bucket for later analysis.

Answer: C

NEW QUESTION 212

- (Exam Topic 2)

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

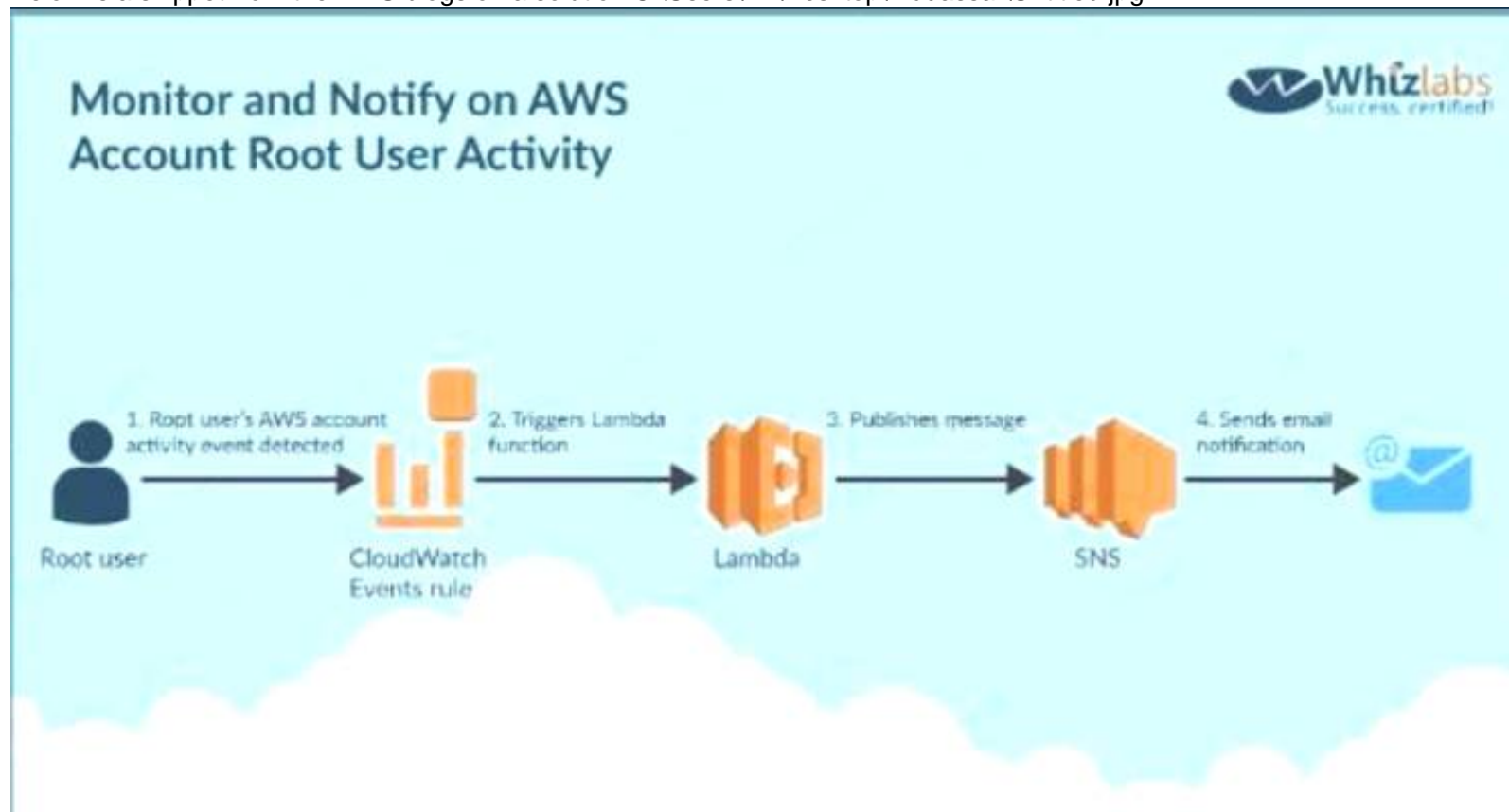
Please select:

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

Answer: AC

Explanation:

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



Option B is invalid because you need to create a Cloudwatch Events Rule and there is such thing as a Cloudwatch Logs Rule Option D is invalid because Cloud Trail API calls can be recorded but cannot be used to send across notifications For more information on this blog article, please visit the following URL: <https://aws.amazon.com/blogs/mt/monitor-and-notify-on-aws-account-root-user-activity> The correct answers are: Create a Cloudwatch Events Rule, Use a Lambda function Submit your Feedback/Queries to our Experts

NEW QUESTION 217

- (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 AWS 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 AWS 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 AWS account per region.

References:

NEW QUESTION 220

- (Exam Topic 2)

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

Which configuration will ensure continued connectivity between sites MOST securely?

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

Answer: C

Explanation:

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

NEW QUESTION 223

- (Exam Topic 2)

Your company has an EC2 Instance that is hosted in an AWS 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.aws.amazon.com/AmazonCloudWatch/latest/logs/Working>

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

* <https://docs.aws.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 228

- (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 AWS 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 232

- (Exam Topic 2)

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

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

Answer: C

Explanation:

Prerequisites to establish Federation Services in AWS - You have a working AD directory and AD FS server. - You have created an identity provider (IdP) in your AWS account using your XML file from your AD FS server. Remember the name of your IdP because you will use it later in this solution. -You have created the appropriate IAM roles in your AWS account, which will be used for federated access. <https://aws.amazon.com/blogs/security/how-to-establish-federated-access-to-your-aws-resources-by-using-activ>

NEW QUESTION 237

- (Exam Topic 2)

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

DNS.

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

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

Answer: D

Explanation:

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

NEW QUESTION 239

- (Exam Topic 2)

An Amazon EC2 instance is denied access to a newly created AWS 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 AWS 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: A

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

References:

NEW QUESTION 243

- (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 AWS resource.
- C. Use AWS 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://aws.amazon.com/answers/networking/vpc-security-capabilities/> Security Group is stateful and hypervisor level.

NEW QUESTION 247

- (Exam Topic 2)

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

Please select:

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

Answer: C

Explanation:

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

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

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

The AWS Documentation mentions the following

AWS Shield Advanced provides enhanced protections for your applications running on Amazon EC2, Elastic Load Balancing (ELB), Amazon CloudFront and Route 53 against larger and more sophisticated attacks. AWS Shield Advanced is available to AWS Business Support and AWS Enterprise Support customers.

AWS Shield Advanced protection provides always-on, flow-based monitoring of network traffic and active application monitoring to provide near real-time notifications of DDos attacks. AWS Shield Advanced also gives customers highly flexible controls over attack mitigations to take actions instantly. Customers can also engage the DDos Response Team (DRT) 24x7 to manage and mitigate their application layer DDos attacks.

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

The correct answer is: Consider using the AWS Shield Advanced Service

Submit your Feedback/Queries to our Experts

NEW QUESTION 249

- (Exam Topic 2)

A company runs an application on AWS that needs to be accessed only by employees. Most employees work from the office, but others work remotely or travel.

How can the Security Engineer protect this workload so that only employees can access it?

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

Answer: C

Explanation:

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

NEW QUESTION 254

- (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 258

- (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 AWS resources that are encrypted by AWS KMS?

- A. Copy the application's AWS 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 AWS KMS to automatically synchronize the CMK between regions so that it can be used to decrypt the resource in the target region.
- C. Use AWS 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 AWS service to communicate with the source region's AWS KMS so that it can decrypt the resource in the target region.

Answer: C

NEW QUESTION 260

- (Exam Topic 2)

An organization wants to be alerted when an unauthorized Amazon EC2 instance in its VPC performs a network port scan against other instances in the VPC. When the Security team performs its own internal tests in a separate account by using pre-approved third-party scanners from the AWS Marketplace, the Security team also then receives multiple Amazon GuardDuty events from Amazon CloudWatch alerting on its test activities.

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

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

Answer: B

Explanation:

Trusted IP lists consist of IP addresses that you have whitelisted for secure communication with your AWS 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 AWS account per region. Threat lists consist of known malicious IP addresses. GuardDuty generates findings based on threat lists. At any given time, you can have up to six uploaded threat lists per AWS account per region. https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_upload_lists.html

NEW QUESTION 265

- (Exam Topic 3)

A company has a web-based application using Amazon CloudFront and running on Amazon Elastic Container Service (Amazon ECS) behind an Application Load Balancer (ALB). The ALB is terminating TLS and balancing load across ECS service tasks. A security engineer needs to design a solution to ensure that application content is accessible only through CloudFront and that it is never accessible directly.

How should the security engineer build the MOST secure solution?

- A. Add an origin custom header Set the viewer protocol policy to HTTP and HTTPS Set the origin protocol policy to HTTPS only Update the application to validate the CloudFront custom header
- B. Add an origin custom header Set the viewer protocol policy to HTTPS only Set the origin protocol policy to match viewer Update the application to validate the CloudFront custom header.
- C. Add an origin custom header Set the viewer protocol policy to redirect HTTP to HTTPS Set the origin protocol policy to HTTP only Update the application to validate the CloudFront custom header.
- D. Add an origin custom header Set the viewer protocol policy to redirect HTTP to HTTP
- E. Set the origin protocol policy to HTTPS only Update the application to validate the CloudFront custom header

Answer: D

NEW QUESTION 267

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 269

- (Exam Topic 3)

A company created an AWS account for its developers to use for testing and learning purposes. Because the account will be shared among multiple teams of developers, the company wants to restrict the ability to stop and terminate Amazon EC2 instances so that a team can perform these actions only on the instances it owns.

Developers were instructed to tag all their instances with a Team tag key and use the team name in the tag value. One of the first teams to use this account is Business Intelligence. A security engineer needs to develop a

highly scalable solution for providing developers with access to the appropriate resources within the account. The security engineer has already created individual IAM roles for each team.

Which additional configuration steps should the security engineer take to complete the task?

- A. For each team, create an IAM policy similar to the one that follows. Populate the `ec2:ResourceTag/Team` condition key with a proper team name. Attach resulting policies to the corresponding IAM roles.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "NotAction": [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "ec2:ResourceTag/Team": "BusinessIntelligence"
        }
      }
    }
  ]
}
```

- B. For each team, create an IAM policy similar to the one that follows. Populate the `aws:TagKeys/Team` condition key with a proper team name.

- C. Attach the resulting policies to the corresponding IAM roles.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "NotAction": [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws:TagKeys/Team": "BusinessIntelligence"
        }
      }
    }
  ]
}
```

- D. Tag each IAM role with a Team tag key.

- E. and use the team name in the tag value.

- F. Create an IAM policy similar to the one that follows, and attach it to all the IAM roles used by developers.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "NotAction": [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "ec2:ResourceTag/Team": "${aws:PrincipalTag/Team}"
        }
      }
    }
  ]
}
```

G. Tag each IAM role with the Team key, and use the team name in the tag value

H. Create an IAM policy similar to the one that follows, and attach it to all the IAM roles used by developers.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "NotAction": [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws:TagKeys/Team": "${aws:PrincipalTag/Team}"
        }
      }
    }
  ]
}
```

Answer: A

NEW QUESTION 270

- (Exam Topic 3)

You are trying to use the Systems Manager to patch a set of EC2 systems. Some of the systems are not getting covered in the patching process. Which of the following can be used to troubleshoot the issue? Choose 3 answers from the options given below.

Please select:

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

Answer: ACD

Explanation:

For ensuring that the instances are configured properly you need to ensure the following .

- 1) You installed the latest version of the SSM Agent on your instance
- 2) Your instance is configured with an AWS Identity and Access Management (IAM) role that enables the instance to communicate with the Systems Manager API
- 3) You can use the Amazon EC2 Health API to quickly determine the following information about Amazon EC2 instances
 - The status of one or more instances
 - The last time the instance sent a heartbeat value
 - The version of the SSM Agent
 - The operating system
 - The version of the EC2Config service (Windows)
 - The status of the EC2Config service (Windows)

Option B is invalid because IAM users are not supposed to be directly granted permissions to EC2 Instances For more information on troubleshooting AWS SSM, please visit the following URL:

<https://docs.aws.amazon.com/systems-manager/latest/userguide/troubleshooting-remote-commands.html> The correct answers are: Check to see if the right role has been assigned to the EC2 Instances, Ensure that agent is running on the Instances., Check the Instance status by using the Health API.

Submit your Feedback/Queries to our Experts

NEW QUESTION 271

- (Exam Topic 3)

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

Please select:

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

Answer: C

Explanation:

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

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

Option D is incorrect as we need to enable the Inbound SSH traffic on the EC2 instance Security Group since the traffic originate' , from the IT admin's workstation. The correct answer is: Ensure that the security group allows Inbound SSH traffic from the IT Administrator's Workstation Submit your Feedback/Queries to our Experts

NEW QUESTION 274

- (Exam Topic 3)

You have an Amazon VPC that has a private subnet and a public subnet in which you have a NAT instance server. You have created a group of EC2 instances that configure themselves at startup by downloading a bootstrapping script from S3 that deploys an application via GIT.

Which one of the following setups would give us the highest level of security? Choose the correct answer from the options given below.

Please select:

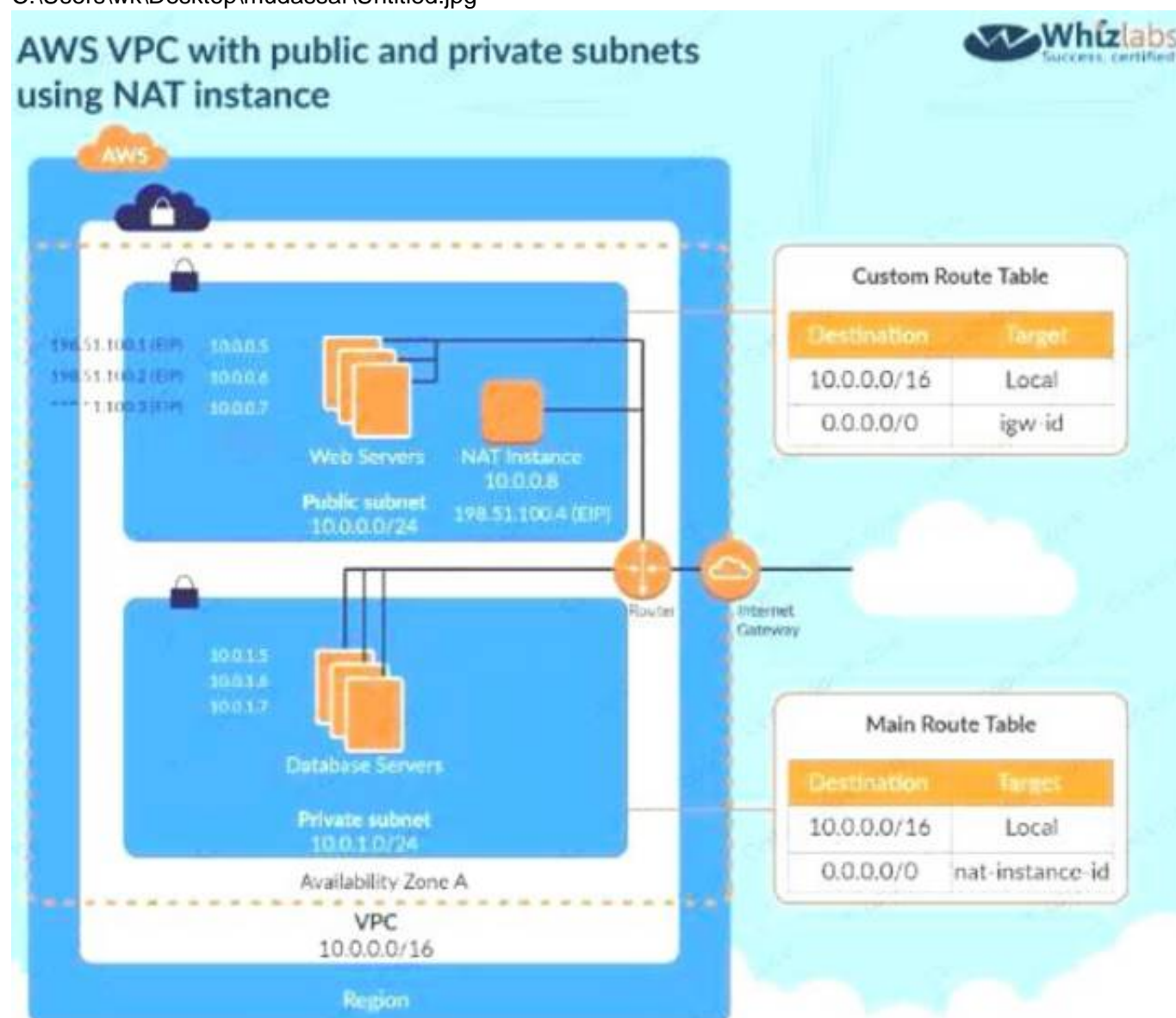
- A. EC2 instances in our public subnet, no EIPs, route outgoing traffic via the IGW
- B. EC2 instances in our public subnet, assigned EIPs, and route outgoing traffic via the NAT
- C. EC2 instance in our private subnet, assigned EIPs, and route our outgoing traffic via our IGW
- D. EC2 instances in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

Answer: D

Explanation:

The below diagram shows how the NAT instance works. To make EC2 instances very secure, they need to be in a private sub such as the database server shown below with no EIP and all traffic routed via the NAT.

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



Options A and B are invalid because the instances need to be in the private subnet

Option C is invalid because since the instance needs to be in the private subnet, you should not attach an EIP to the instance

For more information on NAT instance, please refer to the below Link: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/PC_Instance.html

The correct answer is: EC2 instances in our private subnet no EIPs, route outgoing traffic via the NAT Submit your Feedback/Queries to our Experts

NEW QUESTION 278

- (Exam Topic 3)

A company has set up EC2 instances on the AWS Cloud. There is a need to see all the IP addresses which are accessing the EC2 Instances. Which service can help achieve this?

Please select:

- A. Use the AWS Inspector service
- B. Use AWS VPC Flow Logs
- C. Use Network ACL's
- D. Use Security Groups

Answer: B

Explanation:

The AWS Documentation mentions the following:

A flow log record represents a network flow in your flow log. Each record captures the network flow for a specific 5-tuple, for a specific capture window. A 5-tuple is a set of five different values that specify the source, destination, and protocol for an internet protocol (IP) flow.

Options A, C and D are all invalid because these services/tools cannot be used to get the IP addresses which are accessing the EC2 Instances

For more information on VPC Flow Logs please visit the URL <https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/flow-logs.html>

The correct answer is: Use AWS VPC Flow Logs Submit your Feedback/Queries to our Experts

NEW QUESTION 279

- (Exam Topic 3)

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

Please select:

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

Answer: C

Explanation:

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

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

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

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

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

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

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

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

NEW QUESTION 282

- (Exam Topic 3)

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

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

Which change should the security engineer make to the AWS KMS configuration to meet these requirements?

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

Answer: B

NEW QUESTION 284

- (Exam Topic 3)

Your company manages thousands of EC2 Instances. There is a mandate to ensure that all servers don't have any critical security flaws. Which of the following can be done to ensure this? Choose 2 answers from the options given below.

Please select:

- A. Use AWS Config to ensure that the servers have no critical flaws.
- B. Use AWS inspector to ensure that the servers have no critical flaws.
- C. Use AWS inspector to patch the servers
- D. Use AWS SSM to patch the servers

Answer: BD

Explanation:

The AWS Documentation mentions the following on AWS Inspector

Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for vulnerabilities or deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity. These findings can be reviewed directly or as part of detailed assessment reports which are available via the Amazon Inspector console or API.

Option A is invalid because the AWS Config service is not used to check the vulnerabilities on servers Option C is invalid because the AWS Inspector service is not used to patch servers

For more information on AWS Inspector, please visit the following URL: <https://aws.amazon.com/inspector>

Once you understand the list of servers which require critical updates, you can rectify them by installing the required patches via the SSM tool.

For more information on the Systems Manager, please visit the following URL: <https://docs.aws.amazon.com/systems-manager/latest/APIReference/Welcome.html>

The correct answers are: Use AWS Inspector to ensure that the servers have no critical flaws.. Use AWS SSM to patch the servers

(

NEW QUESTION 289

- (Exam Topic 3)

Your organization is preparing for a security assessment of your use of AWS. In preparation for this assessment, which three IAM best practices should you consider implementing?

Please select:

- A. Create individual IAM users
- B. Configure MFA on the root account and for privileged IAM users

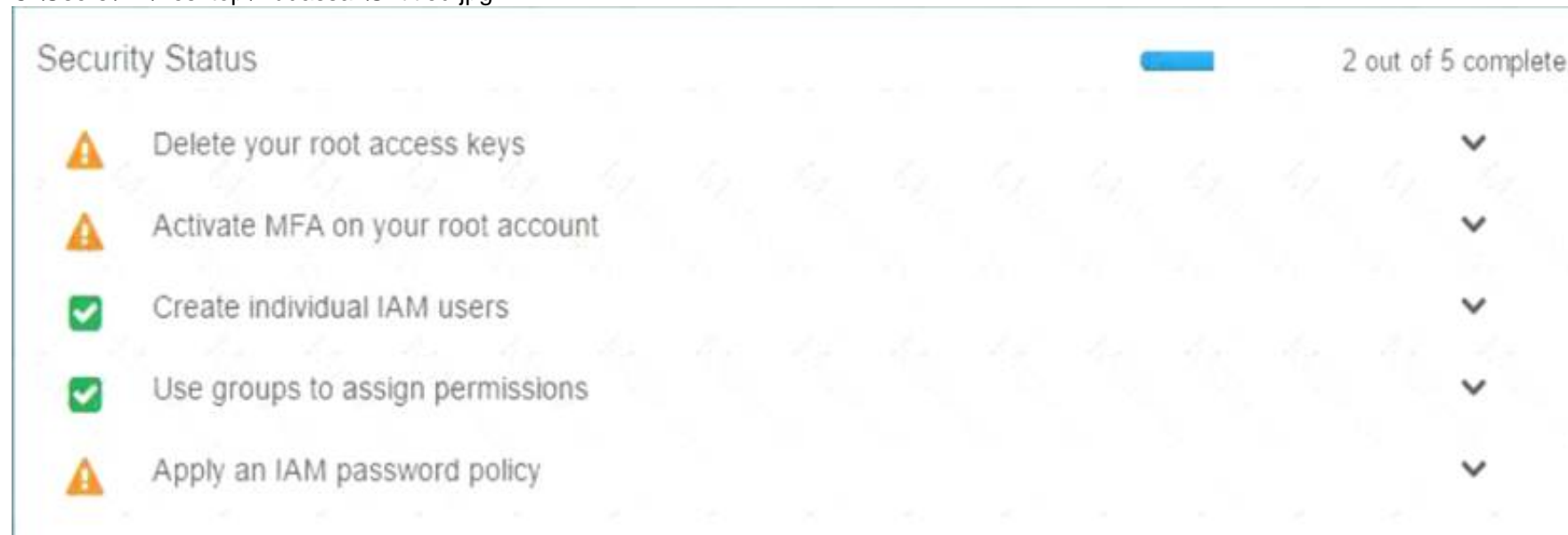
- C. Assign IAM users and groups configured with policies granting least privilege access
- D. Ensure all users have been assigned and are frequently rotating a password, access ID/secret key, and X.509 certificate

Answer: ABC

Explanation:

When you go to the security dashboard, the security status will show the best practices for initiating the first level of security.

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



Option D is invalid because as per the dashboard, this is not part of the security recommendation. For more information on best security practices, please visit the URL:

<https://aws.amazon.com/whitepapers/aws-security-best-practices>;

The correct answers are: Create individual IAM users, Configure MFA on the root account and for privileged IAM users. Assign IAM users and groups configured with policies granting least privilege access.

Submit your Feedback/Queries to our Experts

NEW QUESTION 291

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SCS-C01 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SCS-C01 Product From:

<https://www.2passeasy.com/dumps/SCS-C01/>

Money Back Guarantee

SCS-C01 Practice Exam Features:

- * SCS-C01 Questions and Answers Updated Frequently
- * SCS-C01 Practice Questions Verified by Expert Senior Certified Staff
- * SCS-C01 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * SCS-C01 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year