

Amazon

Exam Questions AWS-Certified-Security-Specialty

Amazon AWS Certified Security - Specialty



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

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

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

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

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

Answer: B

NEW QUESTION 3

- (Exam Topic 1)

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

What could be causing these terminations?

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

Answer: C

NEW QUESTION 4

- (Exam Topic 1)

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

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

Answer: BD

NEW QUESTION 5

- (Exam Topic 1)

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

- A.

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

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

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

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

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

Answer: B

NEW QUESTION 6

- (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 7

- (Exam Topic 1)

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

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

D. Implement the GeoLocation feature in Amazon Route 53.

Answer: B

NEW QUESTION 8

- (Exam Topic 1)

A company plans to use custom AMIs to launch Amazon EC2 instances across multiple AWS accounts in a single Region to perform security monitoring and analytics tasks. The EC2 instances are launched in EC2 Auto Scaling groups. To increase the security of the solution, a Security Engineer will manage the lifecycle of the custom AMIs in a centralized account and will encrypt them with a centrally managed AWS KMS CMK. The Security Engineer configured the KMS key policy to allow cross-account access. However, the EC2 instances are still not being properly launched by the EC2 Auto Scaling groups. Which combination of configuration steps should the Security Engineer take to ensure the EC2 Auto Scaling groups have been granted the proper permissions to execute tasks?

- A. Create a customer-managed CMK in the centralized account
- B. Allow other applicable accounts to use that key for cryptographic operations by applying proper cross-account permissions in the key policy. Create an IAM role in all applicable accounts and configure its access policy to allow the use of the centrally managed CMK for cryptographic operation
- C. Configure EC2 Auto Scaling groups within each applicable account to use the created IAM role to launch EC2 instances.
- D. Create a customer-managed CMK in the centralized account
- E. Allow other applicable accounts to use that key for cryptographic operations by applying proper cross-account permissions in the key policy
- F. Create an IAM role in all applicable accounts and configure its access policy with permissions to create grants for the centrally managed CMK
- G. Use this IAM role to create a grant for the centrally managed CMK with permissions to perform cryptographic operations and with the EC2 Auto Scaling service-linked role defined as the grantee principal.
- H. Create a customer-managed CMK or an AWS managed CMK in the centralized account
- I. Allow other applicable accounts to use that key for cryptographic operations by applying proper cross-account permissions in the key policy
- J. Use the CMK administrator to create a CMK grant that includes permissions to perform cryptographic operations that define EC2 Auto Scaling service-linked roles from all other accounts as the grantee principal.
- K. Create a customer-managed CMK or an AWS managed CMK in the centralized account
- L. Allow other applicable accounts to use that key for cryptographic operations by applying proper cross-account permissions in the key policy
- M. Modify the access policy for the EC2 Auto Scaling roles to perform cryptographic operations against the centrally managed CMK.

Answer: B

NEW QUESTION 9

- (Exam Topic 1)

A company is outsourcing its operational support to an external company. The company's security officer must implement an access solution for delegating operational support that minimizes overhead. Which approach should the security officer take to meet these requirements?

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

Answer: B

NEW QUESTION 10

- (Exam Topic 1)

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 10

- (Exam Topic 1)

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

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

Answer: CE

NEW QUESTION 11

- (Exam Topic 1)

A global company must mitigate and respond to DDoS attacks at Layers 3, 4 and 7 All of the company's AWS applications are serverless with static content hosted on Amazon S3 using Amazon CloudFront and Amazon Route 53
 Which solution will meet these requirements?

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

Answer: C

NEW QUESTION 14

- (Exam Topic 1)

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

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

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

Answer: BD

NEW QUESTION 16

- (Exam Topic 1)

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

What will enable the security engineer to save the change?

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

Answer: B

NEW QUESTION 17

- (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 AmazonS3ReadOnlyAccess 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 21

- (Exam Topic 1)

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

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

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

```

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

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

```

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

```

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

Answer: BEF

NEW QUESTION 25

- (Exam Topic 1)

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

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

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

Answer: BC

NEW QUESTION 26

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

Answer: C

NEW QUESTION 29

- (Exam Topic 1)

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

Which solution meets these requirements?

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

Answer: A

NEW QUESTION 31

- (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 volume of requests 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 security engineer is concerned 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 the 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 roles for each IAM user. Ensure that users who use the same IAM credentials cannot assume the same IAM role at the same time.

Answer: B

NEW QUESTION 35

- (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 36

- (Exam Topic 1)

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

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

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

Answer: A

NEW QUESTION 41

- (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 43

- (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 46

- (Exam Topic 1)

A Security Engineer has discovered that, although encryption was enabled on the Amazon S3 bucket example bucket, anyone who has access to the bucket has the ability to retrieve the files. The Engineer wants to limit access to each IAM user to only an assigned folder.

What should the Security Engineer do to achieve this?

- A. Use envelope encryption with the AWS-managed CMK aws/s3.
- B. Create a customer-managed CMK with a key policy granting "kms:Decrypt" based on the "\${aws:username}" variable.
- C. Create a customer-managed CMK for each user
- D. Add each user as a key user in their corresponding key policy.
- E. Change the applicable IAM policy to grant S3 access to "Resource": "arn:aws:s3:::examplebucket/\${aws:username}/*"

Answer: B

Explanation:

Reference: <https://aws.amazon.com/premiumsupport/knowledge-center/iam-s3-user-specific-folder/>

NEW QUESTION 48

- (Exam Topic 1)

A company's security information events management (SIEM) tool receives new AWS CloudTrail logs from an Amazon S3 bucket that is configured to send all object created event notification to an Amazon SNS topic. An Amazon SQS queue is subscribed to this SNS topic. The company's SEM tool then ports this SQS queue for new messages using an IAM role and fetches new log events from the S3 bucket based on the SQS messages. After a recent security review that resulted in restricted permissions, the SEM tool has stopped receiving new CloudTrail logs. Which of the following are possible causes of this issue? (Select THREE)

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

Answer: ADF

NEW QUESTION 49

- (Exam Topic 2)

A Software Engineer wrote a customized reporting service that will run on a fleet of Amazon EC2 instances. The company security policy states that application logs for the reporting service must be centrally collected. What is the MOST efficient way to meet these requirements?

- A. Write an AWS Lambda function that logs into the EC2 instance to pull the application logs from the EC2 instance and persists them into an Amazon S3 bucket.
- B. Enable AWS CloudTrail logging for the AWS account, create a new Amazon S3 bucket, and then configure Amazon CloudWatch Logs to receive the application logs from CloudTrail.
- C. Create a simple cron job on the EC2 instances that synchronizes the application logs to an Amazon S3 bucket by using rsync.
- D. Install the Amazon CloudWatch Logs Agent on the EC2 instances, and configure it to send the application logs to CloudWatch Logs.

Answer: D

Explanation:

<https://aws.amazon.com/blogs/aws/cloudwatch-log-service/>

NEW QUESTION 52

- (Exam Topic 2)

Your development team has started using AWS resources for development purposes. The AWS account has just been created. Your IT Security team is worried about possible leakage of AWS keys. What is the first level of measure that should be taken to protect the AWS account. Please select:

- A. Delete the AWS keys for the root account
- B. Create IAM Groups
- C. Create IAM Roles
- D. Restrict access using IAM policies

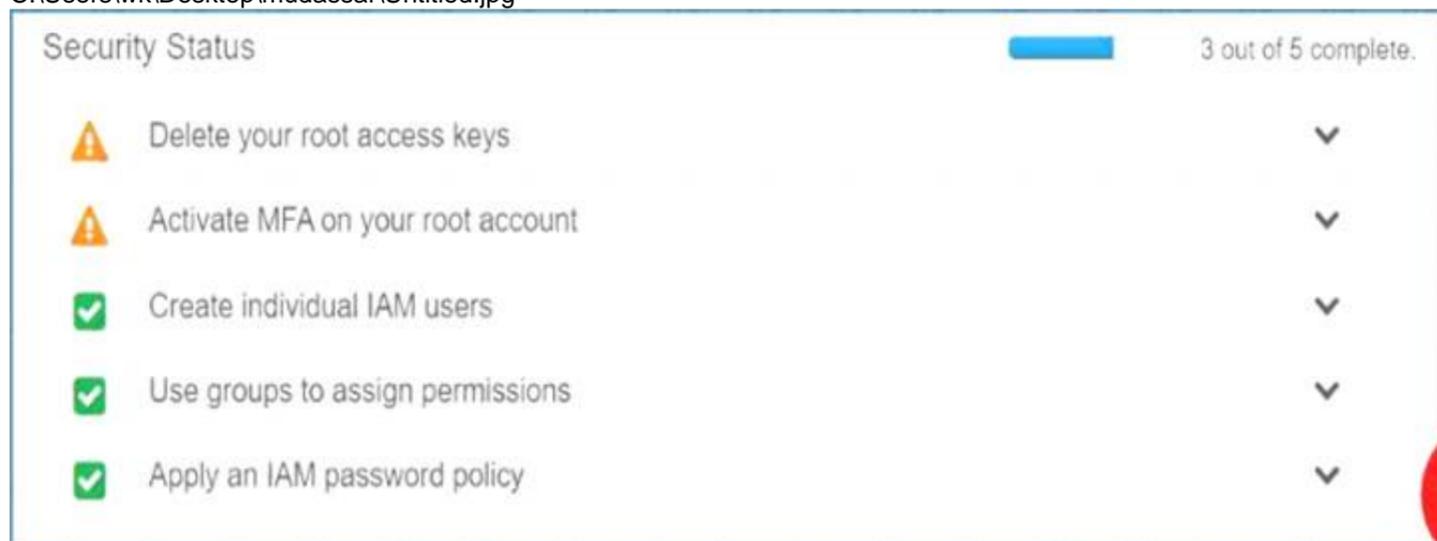
Answer: A

Explanation:

The first level of measure that should be taken is to delete the keys for the IAM root user.

When you log into your account and go to your Security Access dashboard, this is the first step that can be seen:

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



Option B and C are wrong because creation of IAM groups and roles will not change the impact of leakage of AWS root access keys.

Option D is wrong because the first key aspect is to protect the access keys for the root account. For more information on best practices for Security Access keys, please visit the below URL:

<https://docs.aws.amazon.com/eeneral/latest/gr/aws-access-keys-best-practices.html>

The correct answer is: Delete the AWS keys for the root account. Submit your Feedback/Queries to our Experts

NEW QUESTION 53

- (Exam Topic 2)

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

Which of the following actions would resolve this issue?

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

Answer: C

NEW QUESTION 58

- (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 60

- (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 63

- (Exam Topic 2)

Your company is planning on hosting an internal network in AWS. They want machines in the VPC to authenticate using private certificates. They want to minimize the work and maintenance in working with certificates. What is the ideal way to fulfil this requirement. Please select:

- A. Consider using Windows Server 2016 Certificate Manager
- B. Consider using AWS Certificate Manager
- C. Consider using AWS Access keys to generate the certificates
- D. Consider using AWS Trusted Advisor for managing the certificates

Answer: B

Explanation:

The AWS Documentation mentions the following

ACM is tightly linked with AWS Certificate Manager Private Certificate Authority. You can use ACM PCA to create a private certificate authority (CA) and then use ACM to issue private certificates. These are SSL/TLS X.509 certificates that identify users, computers, applications, services, servers, and other devices internally. Private certificates cannot be publicly trusted

Option A is partially invalid. Windows Server 2016 Certificate Manager can be used but since there is a requirement to "minimize the work and maintenance", AWS Certificate Manager should be used

Option C and D are invalid because these cannot be used for managing certificates. For more information on ACM, please visit the below URL:

<https://docs.aws.amazon.com/acm/latest/userguide/acm-overview.html>

The correct answer is: Consider using AWS Certificate Manager Submit your Feedback/Queries to our Experts

NEW QUESTION 65

- (Exam Topic 2)

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

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

Answer: A

Explanation:

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

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

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

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

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

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

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

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

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

NEW QUESTION 70

- (Exam Topic 2)

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

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

Please select:

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

Answer: AC

Explanation:

The AWS Documentation mentions the following

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

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

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

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

<https://docs.aws.amazon.com/awsccloudtrail/latest/userguide/cloudtrail-receive-logs-from-multiple-accounts.htm>

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

Submit your Feedback/Queries to our Experts

NEW QUESTION 71

- (Exam Topic 2)

A company stores data on an Amazon EBS volume attached to an Amazon EC2 instance. The data is asynchronously replicated to an Amazon S3 bucket. Both the EBS volume and the S3 bucket are encrypted with the same AWS KMS Customer Master Key (CMK). A former employee scheduled a deletion of that CMK before leaving the company.

The company's Developer Operations department learns about this only after the CMK has been deleted. Which steps must be taken to address this situation?

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

Answer: C

NEW QUESTION 75

- (Exam Topic 2)

An IAM user with full EC2 permissions could bot start an Amazon EC2 instance after it was stopped for a maintenance task. Upon starting the instance, the instance state would change to "Pending", but after a few seconds, it would switch back to "Stopped".

An inspection revealed that the instance has attached Amazon EBS volumes that were encrypted by using a Customer Master Key (CMK). When these encrypted volumes were detached, the IAM user was able to start the EC2 instances.

The IAM user policy is as follows:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        <Action>
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:012345678910:key/ebs-encryption-key"
      ]
      <CONDITION>
    }
  ]
}
```

What additional items need to be added to the IAM user policy? (Choose two.)

- A. kms:GenerateDataKey
- B. kms:Decrypt
- C. kms:CreateGrant
- D. "Condition": {"Bool": {"kms:ViaService": "ec2.us-west-2.amazonaws.com"}}
- E. "Condition": {"Bool": {"kms:GrantIsForAWSResource": true}}

Answer: CE

Explanation:

The EBS which is AWS resource service is encrypted with CMK and to allow EC2 to decrypt, the IAM user should create a grant (action) and a boolean condition for the AWS resource. This link explains how AWS keys work. <https://docs.aws.amazon.com/kms/latest/developerguide/key-policies.html>

NEW QUESTION 76

- (Exam Topic 2)

An organization receives an alert that indicates that an EC2 instance behind an ELB Classic Load Balancer has been compromised. What techniques will limit lateral movement and allow evidence gathering?

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

Answer: B

Explanation:

https://d1.awsstatic.com/whitepapers/aws_security_incident_response.pdf

NEW QUESTION 80

- (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 Store.
- 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 rotated.
- G. Grant permission to the instance role associated with the EC2 instance to access Secrets Manager.

Answer: CE

NEW QUESTION 81

- (Exam Topic 2)

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

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

Answer: B

Explanation:

The AWS Documentation states the following

AWS KMS is integrated with CloudTrail, a service that captures API calls made by or on behalf of AWS KMS in your AWS account and delivers the log files to an

Amazon S3 bucket that you specify. CloudTrail captures API calls from the AWS KMS console or from the AWS KMS API. Using the information collected by CloudTrail, you can determine what request was made, the source IP address from which the request was made, who made the request when it was made, and so on.

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

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

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

Submit your Feedback/Queries to our Experts

NEW QUESTION 84

- (Exam Topic 2)

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

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

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

Answer: D

Explanation:

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

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

NEW QUESTION 87

- (Exam Topic 2)

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

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

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

Answer: ACE

Explanation:

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

NEW QUESTION 88

- (Exam Topic 2)

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

Please select:

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

Answer: C

Explanation:

This concept is given in the AWS Documentation

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

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

Resolution

Before performing security testing on AWS resources, you must obtain approval from AWS. After you submit your request AWS will reply in about two business days.

AWS might have additional questions about your test which can extend the approval process, so plan accordingly and be sure that your initial request is as detailed as possible.

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

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

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

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

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

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

NEW QUESTION 90

- (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 95

- (Exam Topic 2)

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

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

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

Answer: B

NEW QUESTION 100

- (Exam Topic 2)

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

Pattern: "randomID_datestamp_PII.csv" Example:

"1234567_12302017_000-00-0000 csv"

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

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

Answer: C

Explanation:

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

NEW QUESTION 103

- (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 108

- (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 113

- (Exam Topic 2)

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

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

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

Answer: AC

Explanation:

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

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

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

NEW QUESTION 114

- (Exam Topic 2)

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

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

Answer: AB

Explanation:

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

NEW QUESTION 115

- (Exam Topic 2)

Due to new compliance requirements, a Security Engineer must enable encryption with customer-provided keys on corporate data that is stored in DynamoDB. The company wants to retain full control of the encryption keys.

Which DynamoDB feature should the Engineer use to achieve compliance'?

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

Answer: D

Explanation:

Follow the link:

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

NEW QUESTION 119

- (Exam Topic 2)

A Security Analyst attempted to troubleshoot the monitoring of suspicious security group changes. The Analyst was told that there is an Amazon CloudWatch alarm in place for these AWS CloudTrail log events. The Analyst tested the monitoring setup by making a configuration change to the security group but did not receive any alerts.

Which of the following troubleshooting steps should the Analyst perform?

- A. Ensure that CloudTrail and S3 bucket access logging is enabled for the Analyst's AWS accoun
- B. Verify that a metric filter was created and then mapped to an alar

- C. Check the alarm notification action.
- D. Check the CloudWatch dashboards to ensure that there is a metric configured with an appropriate dimension for security group changes.
- E. Verify that the Analyst's account is mapped to an IAM policy that includes permissions for cloudwatch: GetMetricStatistics and Cloudwatch: ListMetrics.

Answer: B

Explanation:

MetricFilter:

Type: 'AWS::Logs::MetricFilter' Properties:

LogGroupName: " FilterPattern: >

```
{ ($.eventName = AuthorizeSecurityGroupIngress) || ($.eventName = AuthorizeSecurityGroupEgress) || ($.eventName = RevokeSecurityGroupIngress) || ($.eventName = RevokeSecurityGroupEgress) || ($.eventName = CreateSecurityGroup) || ($.eventName = DeleteSecurityGroup) }
```

MetricTransformations:

- MetricValue: '1'

MetricNamespace: CloudTrailMetrics MetricName: SecurityGroupEventCount

NEW QUESTION 124

- (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 126

- (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 131

- (Exam Topic 2)

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

Please select:

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

Answer: A

Explanation:

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

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

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

Submit your Feedback/Queries to our Experts

NEW QUESTION 136

- (Exam Topic 2)

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

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

Answer: B

Explanation:

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

Option A, C and D are all invalid because this would affect the application running on the server. The easiest way is just to remove the rule for access on port 22. For more information on authorizing access to an instance, please visit the below URL: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/authorizing-access-to-an-instance.html>

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

NEW QUESTION 137

- (Exam Topic 2)

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

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

Answer: B

Explanation:

The AWS Documentation mentions the following.

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

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

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

The correct answer is: There is no need to do anything since the logs will already be encrypted Submit your Feedback/Queries to our Experts

NEW QUESTION 139

- (Exam Topic 2)

A Systems Engineer has been tasked with configuring outbound mail through Simple Email Service (SES) and requires compliance with current TLS standards. The mail application should be configured to connect to which of the following endpoints and corresponding ports?

- A. email.us-east-1.amazonaws.com over port 8080
- B. email-pop3.us-east-1.amazonaws.com over port 995
- C. email-smtp.us-east-1.amazonaws.com over port 587
- D. email-imap.us-east-1.amazonaws.com over port 993

Answer: C

Explanation:

<https://docs.aws.amazon.com/ses/latest/DeveloperGuide/smtp-connect.html>

NEW QUESTION 142

- (Exam Topic 2)

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

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

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

Answer: BDE

NEW QUESTION 147

- (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 150

- (Exam Topic 2)

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

Please select:

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

Answer: CD

Explanation:

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

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

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

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

Option E is invalid because this configuration is valid For more information on the parameter store, please visit the below URL:

<https://docs.aws.amazon.com/kms/latest/developerguide/services-parameter-store.html>

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

Submit your Feedback/Queries to our Experts

NEW QUESTION 154

- (Exam Topic 2)

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

- A. Use the KMS direct encrypt function on the log data every time a CloudTrail log is generated.
- B. Use the default Amazon S3 server-side encryption with S3-managed keys to encrypt and decrypt the CloudTrail logs.

- C. Configure CloudTrail to use server-side encryption using KMS-managed keys to encrypt and decrypt CloudTrail logs.
- D. Use encrypted API endpoints so that all AWS API calls generate encrypted CloudTrail log entries using the TLS certificate from the encrypted API call.

Answer: C

Explanation:

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

NEW QUESTION 156

- (Exam Topic 2)

Compliance requirements state that all communications between company on-premises hosts and EC2 instances be encrypted in transit. Hosts use custom proprietary protocols for their communication, and EC2 instances need to be fronted by a load balancer for increased availability.

Which of the following solutions will meet these requirements?

- A. Offload SSL termination onto an SSL listener on a Classic Load Balancer, and use a TCP connection between the load balancer and the EC2 instances.
- B. Route all traffic through a TCP listener on a Classic Load Balancer, and terminate the TLS connection on the EC2 instances.
- C. Create an HTTPS listener using an Application Load Balancer, and route all of the communication through that load balancer.
- D. Offload SSL termination onto an SSL listener using an Application Load Balancer, and re-spawn and SSL connection between the load balancer and the EC2 instances.

Answer: B

Explanation:

<https://aws.amazon.com/blogs/compute/maintaining-transport-layer-security-all-the-way-to-your-container-usin>

NEW QUESTION 157

- (Exam Topic 2)

A Security Engineer discovers that developers have been adding rules to security groups that allow SSH and RDP traffic from 0.0.0.0/0 instead of the organization firewall IP.

What is the most efficient way to remediate the risk of this activity?

- A. Delete the internet gateway associated with the VPC.
- B. Use network access control lists to block source IP addresses matching 0.0.0.0/0.
- C. Use a host-based firewall to prevent access from all but the organization's firewall IP.
- D. Use AWS Config rules to detect 0.0.0.0/0 and invoke an AWS Lambda function to update the security group with the organization's firewall IP.

Answer: D

NEW QUESTION 161

- (Exam Topic 2)

A Security Engineer is working with the development team to design a supply chain application that stores sensitive inventory data in an Amazon S3 bucket. The application will use an AWS KMS customer master key (CMK) to encrypt the data on Amazon S3. The inventory data on Amazon S3 will be shared of vendors. All vendors will use AWS principals from their own AWS accounts to access the data on Amazon S3. The vendor list may change weekly, and the solution must support cross-account access.

What is the MOST efficient way to manage access control for the KMS CMK?

- A. Use KMS grants to manage key acces
- B. Programmatically create and revoke grants to manage vendor access.
- C. Use an IAM role to manage key acces
- D. Programmatically update the IAM role policies to manage vendor access.
- E. Use KMS key policies to manage key acces
- F. Programmatically update the KMS key policies to manage vendor access.
- G. Use delegated access across AWS accounts by using IAM roles to manage key access. Programmatically update the IAM trust policy to manage cross-account vendor access.

Answer: A

NEW QUESTION 165

- (Exam Topic 2)

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

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

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

Answer: D

Explanation:

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

The AWS Documentation additionally mentions the following

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

If your Lambda function code accesses other AWS resources, such as to read an object from an S3 bucket or write logs to CloudWatch Logs, you need to grant

permissions for relevant Amazon S3 and CloudWatch actions to the role.

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

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

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

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

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

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

Submit your Feedback/Queries to our Exp

NEW QUESTION 168

- (Exam Topic 2)

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

What can be done to implement the above policy?

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

Answer: D

Explanation:

https://docs.aws.amazon.com/en_pv/kms/latest/developerguide/rotate-keys.html#rotate-keys-manually

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

NEW QUESTION 169

- (Exam Topic 2)

During a security event, it is discovered that some Amazon EC2 instances have not been sending Amazon CloudWatch logs.

Which steps can the Security Engineer take to troubleshoot this issue? (Select two.)

- A. Connect to the EC2 instances that are not sending the appropriate logs and verify that the CloudWatch Logs agent is running.
- B. Log in to the AWS account and select CloudWatch Log
- C. Check for any monitored EC2 instances that are in the "Alerting" state and restart them using the EC2 console.
- D. Verify that the EC2 instances have a route to the public AWS API endpoints.
- E. Connect to the EC2 instances that are not sending log
- F. Use the command prompt to verify that the right permissions have been set for the Amazon SNS topic.
- G. Verify that the network access control lists and security groups of the EC2 instances have the access to send logs over SNMP.

Answer: AB

Explanation:

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/cloudwatch-and-interface-VPC.html>

NEW QUESTION 173

- (Exam Topic 2)

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

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

Answer: B

Explanation:

The AWS Documentation mentions the following

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

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

The correct answer is: Key pairs

Submit your Feedback/Queries to our Experts

NEW QUESTION 177

- (Exam Topic 2)

A Security Engineer must design a system that can detect whether a file on an Amazon EC2 host has been modified. The system must then alert the Security Engineer of the modification.

What is the MOST efficient way to meet these requirements?

- A. Install antivirus software and ensure that signatures are up-to-dat
- B. Configure Amazon CloudWatch alarms to send alerts for security events.
- C. Install host-based IDS software to check for file integrit
- D. Export the logs to Amazon CloudWatch Logs for monitoring and alerting.
- E. Export system log files to Amazon S3. Parse the log files using an AWS Lambda function that will send alerts of any unauthorized system login attempts through

Amazon SNS.

F. Use Amazon CloudWatch Logs to detect file system change

G. If a change is detected, automatically terminate and recreate the instance from the most recent AM

H. Use Amazon SNS to send notification of the event.

Answer: B

NEW QUESTION 178

- (Exam Topic 2)

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

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

Security Engineer

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

Lambda function execution role

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

What is causing the error?

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

Answer: D

NEW QUESTION 181

- (Exam Topic 2)

A company maintains sensitive data in an Amazon S3 bucket that must be protected using an AWS KMS CMK. The company requires that keys be rotated automatically every year.

How should the bucket be configured?

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

Answer: B

NEW QUESTION 183

- (Exam Topic 2)

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

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

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

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

Answer: A

Explanation:

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

NEW QUESTION 188

- (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:

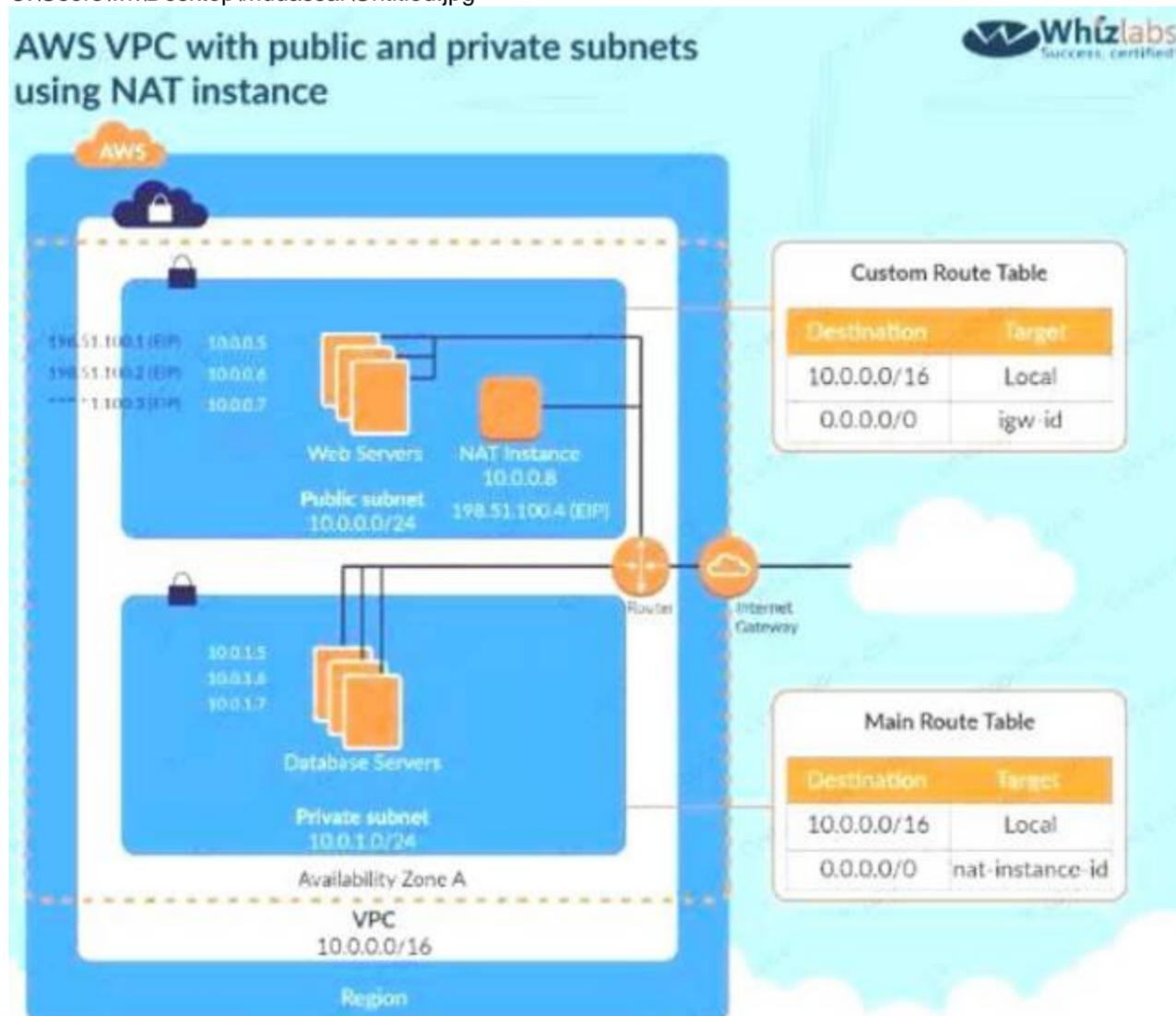
- A. EC2 instances in our public subnet, no EIPs, route outgoing traffic via the IGW
- B. EC2 instances in our public subnet, assigned EIPs, and route outgoing traffic via the NAT
- C. EC2 instance in our private subnet, assigned EIPs, and route our outgoing traffic via our IGW
- D. EC2 instances in 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/UserGuideA/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 189

- (Exam Topic 3)

An employee keeps terminating EC2 instances on the production environment. You've determined the best way to ensure this doesn't happen is to add an extra

layer of defense against terminating the instances. What is the best method to ensure the employee does not terminate the production instances? Choose the 2 correct answers from the options below
Please select:

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

Answer: AB

Explanation:

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

Options C&D are incorrect because it will not ensure that the employee cannot terminate the instance. For more information on tagging answer resources please refer to the below URL: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Usins_Tags.html

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

Submit your Feedback/Queries to our Experts

NEW QUESTION 190

- (Exam Topic 3)

Your company has a set of EC2 Instances that are placed behind an ELB. Some of the applications hosted on these instances communicate via a legacy protocol. There is a security mandate that all traffic between the client and the EC2 Instances need to be secure. How would you accomplish this?
Please select:

- A. Use an Application Load balancer and terminate the SSL connection at the ELB
- B. Use a Classic Load balancer and terminate the SSL connection at the ELB
- C. Use an Application Load balancer and terminate the SSL connection at the EC2 Instances
- D. Use a Classic Load balancer and terminate the SSL connection at the EC2 Instances

Answer: D

Explanation:

Since there are applications which work on legacy protocols, you need to ensure that the ELB can be used at the network layer as well and hence you should choose the Classic ELB. Since the traffic needs to be secure till the EC2 Instances, the SSL termination should occur on the EC2 Instances.

Option A and C are invalid because you need to use a Classic Load balancer since this is a legacy application. Option B is incorrect since encryption is required until the EC2 Instance

For more information on HTTPS listeners for classic load balancers, please refer to below URL

<https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-https-load-balancers.html>

The correct answer is: Use a Classic Load balancer and terminate the SSL connection at the EC2 Instances Submit your Feedback/Queries to our Experts

NEW QUESTION 192

- (Exam Topic 3)

A company uses Amazon RDS for MySQL as a database engine for its applications. A recent security audit revealed an RDS instance that is not compliant with company policy for encrypting data at rest. A security engineer at the company needs to ensure that all existing RDS databases are encrypted using server-side encryption and that any future deviations from the policy are detected.

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

- A. Create an AWS Config rule to detect the creation of unencrypted RDS database
- B. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to trigger on the AWS Config rules compliance state change and use Amazon Simple Notification Service (Amazon SNS) to notify the security operations team.
- C. Use AWS System Manager State Manager to detect RDS database encryption configuration drift
- D. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to track state changes and use Amazon Simple Notification Service (Amazon SNS) to notify the security operations team.
- E. Create a read replica for the existing unencrypted RDS database and enable replica encryption in the process
- F. Once the replica becomes active, promote it into a standalone database instance and terminate the unencrypted database instance.
- G. Take a snapshot of the unencrypted RDS database
- H. Copy the snapshot and enable snapshot encryption in the process
- I. Restore the database instance from the newly created encrypted snapshot
- J. Terminate the unencrypted database instance.
- K. Enable encryption for the identified unencrypted RDS instance by changing the configurations of the existing database

Answer: AD

NEW QUESTION 197

- (Exam Topic 3)

A development team is using an AWS Key Management Service (AWS KMS) CMK to try to encrypt and decrypt a secure string parameter from AWS Systems Manager Parameter Store. However, the development team receives an error message on each attempt.

Which issues that are related to the CMK could be reasons for the error? (Select TWO.)

- A. The CMK that is used in the attempt does not exist.
- B. The CMK that is used in the attempt needs to be rotated.
- C. The CMK that is used in the attempt is using the CMK's key ID instead of the CMK ARN.
- D. The CMK that is used in the attempt is not enabled.

E. The CMK that is used in the attempt is using an alias.

Answer: AD

NEW QUESTION 200

- (Exam Topic 3)

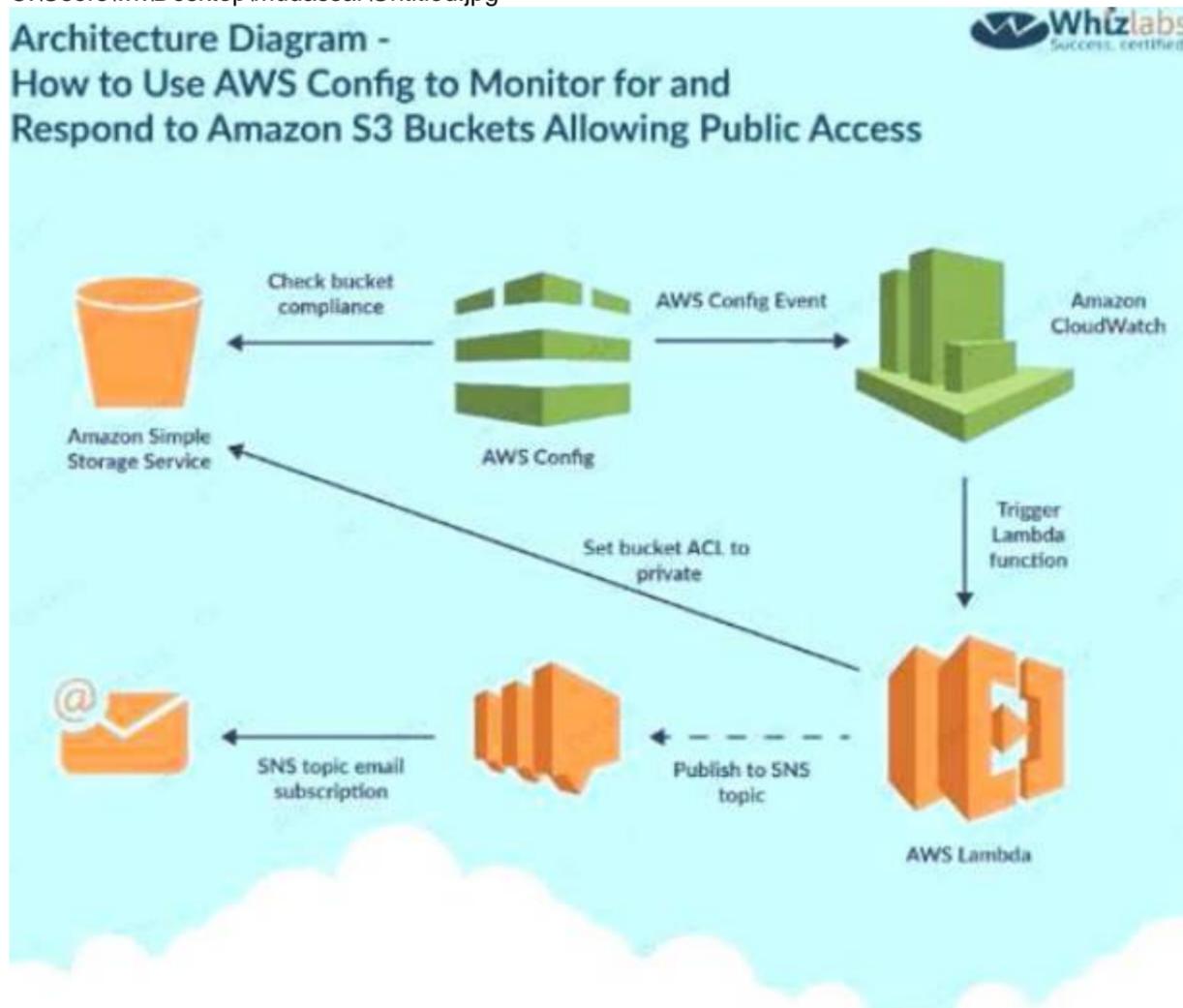
A company is hosting sensitive data in an AWS S3 bucket. It needs to be ensured that the bucket always remains private. How can this be ensured continually? Choose 2 answers from the options given below Please select:

- A. Use AWS Config to monitor changes to the AWS Bucket
- B. Use AWS Lambda function to change the bucket policy
- C. Use AWS Trusted Advisor API to monitor the changes to the AWS Bucket
- D. Use AWS Lambda function to change the bucket ACL

Answer: AD

Explanation:

One of the AWS Blogs mentions the usage of AWS Config and Lambda to achieve this. Below is the diagram representation of this C:\Users\wk\Desktop\mudassar\Untitled.jpg



ption C is invalid because the Trusted Advisor API cannot be used to monitor changes to the AWS Bucket Option B doesn't seem to be the most appropriate. * 1. If the object is in a bucket in which all the objects need to be private and the object is not private anymore, the Lambda function makes a PutObjectAcl call to S3 to make the object private.

[<https://aws.amazon.com/blogs/security/how-to-detect-and-automatically-remediate-unintended-permissions-in-a> The following link also specifies that Create a new Lambda function to examine an Amazon S3 buckets ACL and bucket policy. If the bucket ACL is found to allow public access, the Lambda function overwrites it to be private. If a bucket policy is found, the Lambda function creates an SNS message, puts the policy in the message body, and publishes it to the Amazon SNS topic we created. Bucket policies can be complex, and overwriting your policy may cause unexpected loss of access, so this Lambda function doesn't attempt to alter your policy in any way.

<https://aws.amazon.com/blogs/security/how-to-use-aws-config-to-monitor-for-and-respond-to-amazon-s3-buckets-allowing-public-access> Based on these facts Option D seems to be more appropriate than Option B.

For more information on implementation of this use case, please refer to the Link: <https://aws.amazon.com/blogs/security/how-to-use-aws-config-to-monitor-for-and-respond-to-amazon-s3-buckets-allowing-public-access>

The correct answers are: Use AWS Config to monitor changes to the AWS Bucket Use AWS Lambda function to change the bucket ACL

NEW QUESTION 205

- (Exam Topic 3)

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

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

Answer: BD

Explanation:

The AWS Documentation mentions the following

All AWS accounts have root user credentials (that is, the credentials of the account owner). These credentials allow full access to all resources in the account. Because you can't restrict permissions for root user credentials, we recommend that you delete your root user access keys. Then create AWS Identity and Access Management (IAM) user credentials for everyday interaction with AWS.

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

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

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

NEW QUESTION 209

- (Exam Topic 3)

Your company has a set of EBS volumes defined in AWS. The security mandate is that all EBS volumes are encrypted. What can be done to notify the IT admin staff if there are any unencrypted volumes in the account.

Please select:

- A. Use AWS Inspector to inspect all the EBS volumes
- B. Use AWS Config to check for unencrypted EBS volumes
- C. Use AWS Guard duty to check for the unencrypted EBS volumes
- D. Use AWS Lambda to check for the unencrypted EBS volumes

Answer: B

Explanation:

The enc

config rule for AWS Config can be used to check for unencrypted volumes. encrypted-volumr

5 volumes that are in an attached state are encrypted. If you specify the ID of a KMS key for encryption using the kmsId parameter, the rule checks if the EBS volumes in an attached state are encrypted with that KMS key*1.

Options A and C are incorrect since these services cannot be used to check for unencrypted EBS volumes. Option D is incorrect because even though this is possible, trying to implement the solution alone with just the Lambda servk would be too difficult.

For more information on AWS Config and encrypted volumes, please refer to below URL:

<https://docs.aws.amazon.com/config/latest/developerguide/encrypted-volumes.html>

Submit your Feedback/Queries to our Experts

NEW QUESTION 211

- (Exam Topic 3)

A company wants to monitor the deletion of customer managed CMKs. A security engineer must create an alarm that will notify the company before a CMK is deleted. The security engineer has configured the integration of AWS CloudTrail with Amazon CloudWatch.

What should the security engineer do next to meet this requirement?

Within AWS Key Management Service (AWS KMS) specify the deletion time of the key material during CMK creation. AWS KMS will automatically create a CloudWatch.

Create an Amazon Eventbridge (Amazon CloudWatch Events) rule to look for API calls of DeleteAlias. Create an AWS Lambda function to send an Amazon Simple Notification Service (Amazon SNS) messages to the company. Add the Lambda functions as the target of the Eventbridge (CloudWatch Events) rule.

Create an Amazon EventBridge (Amazon CloudWath Events) rule to look for API calls of DisableKey and ScheduleKeyDelection. Create an AWS Lambda function to generate the alarm and send the notification to the company. Add the lambda function as the target of the SNS policy.

- A. Use inbound rule 100 to allow traffic on TCP port 443. Use inbound rule 200 to deny traffic on TCP port 3306. Use outbound rule 100 to allow traffic on TCP port 443.
- B. Use inbound rule 100 to deny traffic on TCP port 3306. Use inbound rule 200 to allow traffic on TCP port range 1024-65535. Use outbound rule 100 to allow traffic on TCP port 443.
- C. Use inbound rule 100 to allow traffic on TCP port range 1024-65535. Use inbound rule 200 to deny traffic on TCP port 3306. Use outbound rule 100 to allow traffic on TCP port 443.
- D. Use inbound rule 100 to deny traffic on TCP port 3306. Use inbound rule 200 to allow traffic on TCP port 443. Use outbound rule 100 to allow traffic on TCP port 443.

Answer: A

NEW QUESTION 212

- (Exam Topic 3)

A company has multiple Amazon S3 buckets encrypted with customer-managed CMKs. Due to regulatory requirements the keys must be rotated every year. The company's Security Engineer has enabled automatic key rotation for the CMKs; however the company wants to verify that the rotation has occurred.

What should the Security Engineer do to accomplish this?

- A. Filter AWS CloudTrail logs for KeyRotaton events
- B. Monitor Amazon CloudWatch Events for any AWS KMS CMK rotation events
- C. Using the AWS CL
- D. run the aws kms get-key-rotation-status operation with the --key-id parameter to check the CMK rotation date
- E. Use Amazon Athena to query AWS CloudTrail logs saved in an S3 bucket to filter Generate New Key events

Answer: C

NEW QUESTION 216

- (Exam Topic 3)

A company's security engineer has been tasked with restricting a contractor's IAM account access to the company's Amazon EC2 console without providing access to any other AWS services. The contractor's IAM account must not be able to gain access to any other AWS service, even if the IAM account is assigned additional permissions based on IAM group membership.

What should the security engineer do to meet these requirements?"

- A. Create an IAM user policy that allows for Amazon EC2 access for the contractor's IAM user

- B. Create an 1AM permissions boundary policy that allows Amazon EC2 access Associate the contractor's 1AM account with the 1AM permissions boundary policy
- C. Create an 1AM group with an attached policy that allows for Amazon EC2 access Associate the contractor's 1AM account with the 1AM group
- D. Create a 1AM role that allows for EC2 and explicitly denies all other services Instruct the contractor to always assume this role

Answer: B

NEW QUESTION 217

- (Exam Topic 3)

During a manual review of system logs from an Amazon Linux EC2 instance, a Security Engineer noticed that there are sudo commands that were never properly alerted or reported on the Amazon CloudWatch Logs agent
 Why were there no alerts on the sudo commands?

- A. There is a security group blocking outbound port 80 traffic that is preventing the agent from sending the logs
- B. The IAM instance profile on the EC2 instance was not properly configured to allow the CloudWatch Logs agent to push the logs to CloudWatch
- C. CloudWatch Logs status is set to ON versus SECURE, which prevents it from pulling in OS security event logs
- D. The VPC requires that all traffic go through a proxy, and the CloudWatch Logs agent does not support a proxy configuration.

Answer: B

NEW QUESTION 219

- (Exam Topic 3)

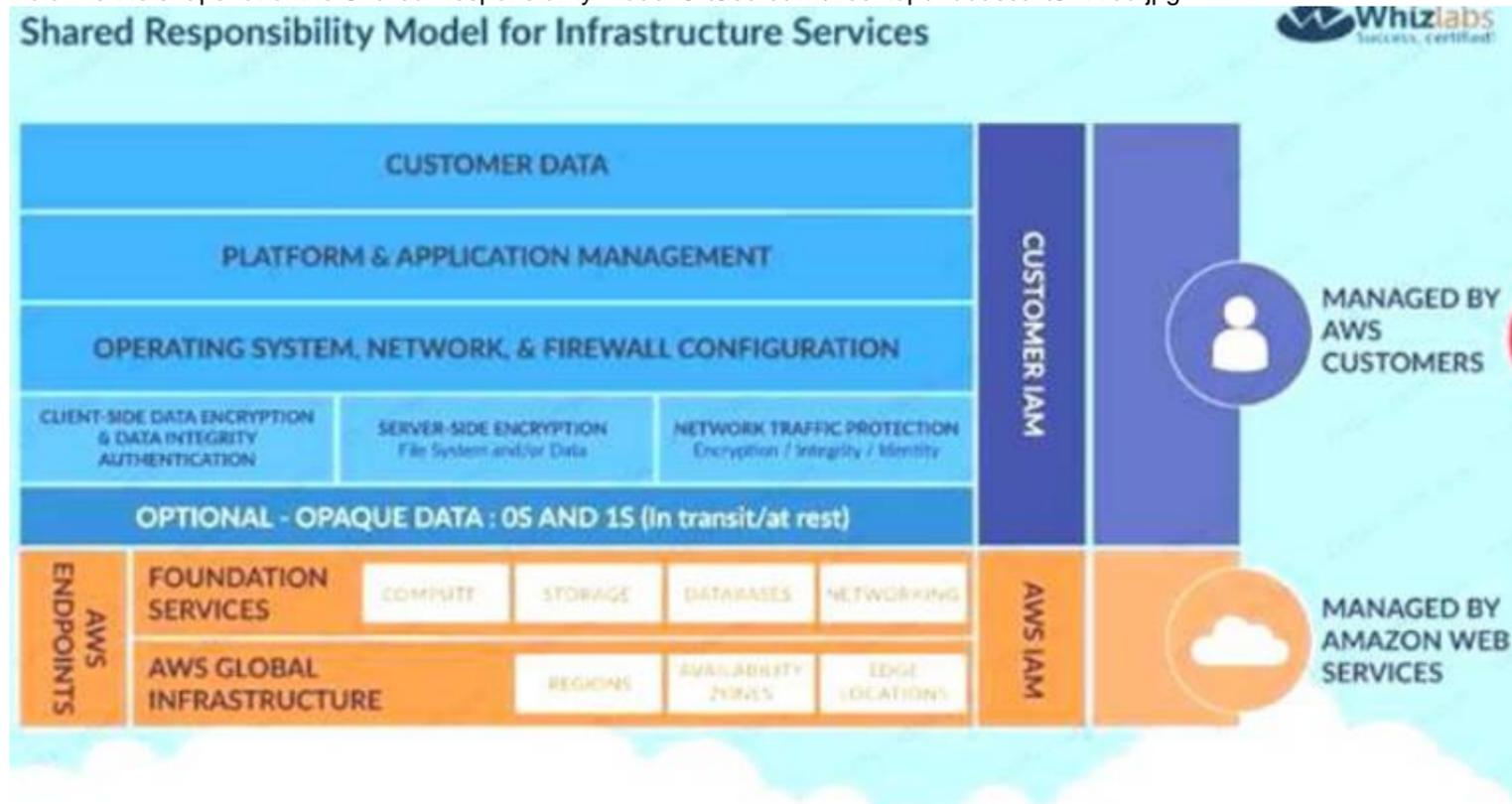
Which of the following is the responsibility of the customer? Choose 2 answers from the options given below. Please select:

- A. Management of the Edge locations
- B. Encryption of data at rest
- C. Protection of data in transit
- D. Decommissioning of old storage devices

Answer: BC

Explanation:

Below is the snapshot of the Shared Responsibility Model C:\Users\wk\Desktop\mudassar\Untitled.jpg



For more information on AWS Security best practises, please refer to below URL [awsstatic.com/whitepapers/Security/AWS Practices](https://awsstatic.com/whitepapers/Security/AWS_Practices).
 The correct answers are: Encryption of data at rest Protection of data in transit Submit your Feedback/Queries to our Experts

NEW QUESTION 222

- (Exam Topic 3)

A company's application team needs to host a MySQL database on AWS. According to the company's security policy, all data that is stored on AWS must be encrypted at rest. In addition, all cryptographic material must be compliant with FIPS 140-2 Level 3 validation.
 The application team needs a solution that satisfies the company's security requirements and minimizes operational overhead.
 Which solution will meet these requirements?

- A. Host the database on Amazon RD
- B. Use Amazon Elastic Block Store (Amazon EBS) for encryption.Use an AWS Key Management Service (AWS KMS) custom key store that is backed by AWS CloudHSM for key management.
- C. Host the database on Amazon RD
- D. Use Amazon Elastic Block Store (Amazon EBS) for encryption.Use an AWS managed CMK in AWS Key Management Service (AWS KMS) for key management.
- E. Host the database on an Amazon EC2 instanc
- F. Use Amazon Elastic Block Store (Amazon EBS) for encryptio
- G. Use a customer managed CMK in AWS Key Management Service (AWS KMS) for key management.
- H. Host the database on an Amazon EC2 instanc
- I. Use Transparent Data Encryption (TDE) for encryption and key management.

Answer: B

NEW QUESTION 223

- (Exam Topic 3)

Your company has confidential documents stored in the simple storage service. Due to compliance requirements, you have to ensure that the data in the S3 bucket is available in a different geographical location. As an architect what is the change you would make to comply with this requirement. Please select:

- A. Apply Multi-AZ for the underlying S3 bucket
- B. Copy the data to an EBS Volume in another Region
- C. Create a snapshot of the S3 bucket and copy it to another region
- D. Enable Cross region replication for the S3 bucket

Answer: D

Explanation:

This is mentioned clearly as a use case for S3 cross-region replication

You might configure cross-region replication on a bucket for various reasons, including the following:

- Compliance requirements - Although, by default Amazon S3 stores your data across multiple geographically distant Availability Zones, compliance requirements might dictate that you store data at even further distances. Cross-region replication allows you to replicate data between distant AWS Regions to satisfy these compliance requirements.

Option A is invalid because Multi-AZ cannot be used to S3 buckets

Option B is invalid because copying it to an EBS volume is not a recommended practice Option C is invalid because creating snapshots is not possible in S3

For more information on S3 cross-region replication, please visit the following URL: <https://docs.aws.amazon.com/AmazonS3/latest/dev/crr.html>

The correct answer is: Enable Cross region replication for the S3 bucket Submit your Feedback/Queries to our Experts

NEW QUESTION 227

- (Exam Topic 3)

A developer is building a serverless application hosted on AWS that uses Amazon Redshift in a data store. The application has separate modules for read/write and read-only functionality. The modules need their own database users for compliance reasons.

Which combination of steps should a security engineer implement to grant appropriate access? (Select TWO)

- A. Configure cluster security groups for each application module to control access to database users that are required for read-only and read/write.
- B. Configure a VPC endpoint for Amazon Redshift Configure an endpoint policy that maps database users to each application module, and allow access to the tables that are required for read-only and read/write
- C. Configure an IAM policy for each module Specify the ARN of an Amazon Redshift database user that allows the GetClusterCredentials API call
- D. Create focal database users for each module
- E. Configure an IAM policy for each module Specify the ARN of an IAM user that allows the GetClusterCredentials API call

Answer: AE

NEW QUESTION 228

- (Exam Topic 3)

A website currently runs on Amazon EC2, with mostly static content on the site. Recently the site was subjected to a DDoS attack a security engineer was asked to redesign the edge security to help mitigate this risk in the future.

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

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

Answer: BDF

NEW QUESTION 233

- (Exam Topic 3)

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

* sgLB - associated with the ELB

* sgWeb - associated with the EC2 instances.

* sgDB - associated with the database

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

Please select:

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

Answer: D

Explanation:

The Load Balancer should accept traffic on port 80 and 443 traffic from 0.0.0.0/0 The backend EC2 Instances should accept traffic from the Load Balancer
The database should allow traffic from the Web server
And the Bastion host should only allow traffic from a specific corporate IP address range Option A is incorrect because the Web group should only allow traffic from the Load balancer For more information on AWS Security Groups, please refer to below URL: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/usins-network-security.html>
The correct answer is: sgLB :allow port 80 and 443 traffic from 0.0.0.0/0 sgWeb :allow port 80 and 443 traffic from sgLB
sgDB :allow port 3306 traffic from sgWeb and sgBastion
sgBastion: allow port 22 traffic from the corporate IP address range Submit your Feedback/Queries to our Experts

NEW QUESTION 235

- (Exam Topic 3)

Your company has defined a set of S3 buckets in AWS. They need to monitor the S3 buckets and know the source IP address and the person who make requests to the S3 bucket. How can this be achieved?
Please select:

- A. Enable VPC flow logs to know the source IP addresses
- B. Monitor the S3 API calls by using Cloudtrail logging
- C. Monitor the S3 API calls by using Cloudwatch logging
- D. Enable AWS Inspector for the S3 bucket

Answer: B

Explanation:

The AWS Documentation mentions the following
Amazon S3 is integrated with AWS CloudTrail. CloudTrail is a service that captures specific API calls made to Amazon S3 from your AWS account and delivers the log files to an Amazon S3 bucket that you specify. It captures API calls made from the Amazon S3 console or from the Amazon S3 API.
Using the information collected by CloudTrail, you can determine what request was made to Amazon S3, the source IP address from which the request was made, who made the request when it was made, and so on Options A,C and D are invalid because these services cannot be used to get the source IP address of the calls to S3 buckets
For more information on Cloudtrail logging, please refer to the below Link: <https://docs.aws.amazon.com/AmazonS3/latest/dev/cloudtrail-loggings.html>
The correct answer is: Monitor the S3 API calls by using Cloudtrail logging Submit your Feedback/Queries to our Experts

NEW QUESTION 239

- (Exam Topic 3)

You need to have a requirement to store objects in an S3 bucket with a key that is automatically managed and rotated. Which of the following can be used for this purpose?
Please select:

- A. AWS KMS
- B. AWS S3 Server side encryption
- C. AWS Customer Keys
- D. AWS Cloud HSM

Answer: B

Explanation:

The AWS Documentation mentions the following
Server-side encryption protects data at rest. Server-side encryption with Amazon S3-managed encryption keys (SSE-S3) uses strong multi-factor encryption. Amazon S3 encrypts each object with a unique key. As an additional safeguard, it encrypts the key itself with a master key that it rotates regularly. Amazon S3 server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt your data.
All other options are invalid since here you need to ensure the keys are manually rotated since you manage the entire key set Using AWS S3 Server side encryption, AWS will manage the rotation of keys automatically.
For more information on Server side encryption, please visit the following URL:
<https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingServerSideEncryption.html>
The correct answer is: AWS S3 Server side encryption Submit your Feedback/Queries to our Experts

NEW QUESTION 242

- (Exam Topic 3)

Your company is hosting a set of EC2 Instances in AWS. They want to have the ability to detect if any port scans occur on their AWS EC2 Instances. Which of the following can help in this regard?
Please select:

- A. Use AWS inspector to consciously inspect the instances for port scans
- B. Use AWS Trusted Advisor to notify of any malicious port scans
- C. Use AWS Config to notify of any malicious port scans
- D. Use AWS Guard Duty to monitor any malicious port scans

Answer: D

Explanation:

The AWS blogs mention the following to support the use of AWS GuardDuty
GuardDuty voraciously consumes multiple data streams, including several threat intelligence feeds, staying aware of malicious addresses, devious domains, and more importantly, learning to accurately identify malicious or unauthorized behavior in your AWS accounts. In combination with information gleaned from your VPC Flow Logs, AWS CloudTrail Event Logs, and DNS logs, th allows GuardDuty to detect many different types of dangerous and mischievous behavior including probes for known vulnerabilities, port scans and probes, and access from unusual locations. On the AWS side, it looks for suspicious AWS account activity such as unauthorized deployments, unusual CloudTrail activity, patterns of access to AWS API functions, and attempts to exceed multiple service limits. GuardDuty will also look for compromised EC2 instances talking to malicious entities or services, data exfiltration attempts, and instances that are mining cryptocurrency.
Options A, B and C are invalid because these services cannot be used to detect port scans For more information on AWS Guard Duty, please refer to the below Link:

<https://aws.amazon.com/blogs/aws/amazon-guardduty-continuous-security-monitoring-threat-detection/>; (
The correct answer is: Use AWS Guard Duty to monitor any malicious port scans Submit your Feedback/Queries to our Experts

NEW QUESTION 246

- (Exam Topic 3)

An application team wants to use AWS Certificate Manager (ACM) to request public certificates to ensure that data is secured in transit. The domains that are being used are not currently hosted on Amazon Route 53

The application team wants to use an AWS managed distribution and caching solution to optimize requests to its systems and provide better points of presence to customers The distribution solution will use a primary domain name that is customized The distribution solution also will use several alternative domain names The certificates must renew automatically over an indefinite period of time

Which combination of steps should the application team take to deploy this architecture? (Select THREE.)

- A. Request a certificate (from ACM in the us-west-2 Region Add the domain names that the certificate will secure
- B. Send an email message to the domain administrators to request vacation of the domains for ACM
- C. Request validation of the domains for ACM through DNS Insert CNAME records into each domain's DNS zone
- D. Create an Application Load Balancer for the caching solution Select the newly requested certificate from ACM to be used for secure connections
- E. Create an Amazon CloudFront distribution for the caching solution Enter the main CNAME record as the Origin Name Enter the subdomain names or alternate names in the Alternate Domain Names Distribution Settings Select the newly requested certificate from ACM to be used for secure connections
- F. Request a certificate from ACM in the us-east-1 Region Add the domain names that the certificate will secure

Answer: CDF

NEW QUESTION 248

- (Exam Topic 3)

Your CTO thinks your AWS account was hacked. What is the only way to know for certain if there was unauthorized access and what they did, assuming your hackers are very sophisticated AWS engineers and doing everything they can to cover their tracks?

Please select:

- A. Use CloudTrail Log File Integrity Validation.
- B. Use AWS Config SNS Subscriptions and process events in real time.
- C. Use CloudTrail backed up to AWS S3 and Glacier.
- D. Use AWS Config Timeline forensics.

Answer: A

Explanation:

The AWS Documentation mentions the following

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

Validated log files are invaluable in security and forensic investigations. For example, a validated log file enables you to assert positively that the log file itself has not changed, or that particular user credentials performed specific API activity. The CloudTrail log file integrity validation process also lets you know if a log file has been deleted or changed, or assert positively that no log files were delivered to your account during a given period of time.

Options B.C and D is invalid because you need to check for log File Integrity Validation for cloudtrail logs

For more information on Cloudtrail log file validation, please visit the below URL: <http://docs.aws.amazon.com/awsccloudtrail/latest/userguide/cloudtrail-log-file-validation-intro.html> The correct answer is: Use CloudTrail Log File Integrity Validation.

omit your Feedback/Queries to our Expert

NEW QUESTION 250

- (Exam Topic 3)

A company deploys a set of standard IAM roles in AWS accounts. The IAM roles are based on job functions within the company. To balance operational efficiency and security, a security engineer implemented AWS Organizations SCPs to restrict access to critical security services in all company accounts.

All of the company's accounts and OUs within AWS Organizations have a default FullAWSAccess SCP that is attached. The security engineer needs to ensure that no one can disable Amazon GuardDuty and AWS Security Hub. The security engineer also must not override other permissions that are granted by IAM policies that are defined in the accounts.

Which SCP should the security engineer attach to the root of the organization to meet these requirements?

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

Is this bucket policy sufficient to ensure that the data is not publicly accessible?

A)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "guardduty:DeleteDetector",
        "guardduty:UpdateDetector",
        "securityhub:DisableSecurityHub"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

B)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "*",
      "Resource": "*"
    },
    {
      "Effect": "Deny",
      "NotAction": [
        "guardduty:DeleteDetector",
        "guardduty:UpdateDetector",
        "securityhub:DisableSecurityHub"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

C)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "NotAction": [
        "guardduty:DeleteDetector",
        "guardduty:UpdateDetector",
        "securityhub:DisableSecurityHub"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

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

Answer: C

NEW QUESTION 254

- (Exam Topic 3)

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

Please select:

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

Answer: A

Explanation:

The AWS Documentation mentions the following

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

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

[https://aws.amazon.com/blogs/security/control-access-to-aws-resources-by-using-the-aws-organization-of-iam-p \(](https://aws.amazon.com/blogs/security/control-access-to-aws-resources-by-using-the-aws-organization-of-iam-p/)

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

NEW QUESTION 258

- (Exam Topic 3)

A company wants to use Cloudtrail for logging all API activity. They want to segregate the logging of data events and management events. How can this be achieved? Choose 2 answers from the options given below

Please select:

- A. Create one Cloudtrail log group for data events
- B. Create one trail that logs data events to an S3 bucket
- C. Create another trail that logs management events to another S3 bucket
- D. Create another Cloudtrail log group for management events

Answer: BC

Explanation:

The AWS Documentation mentions the following

You can configure multiple trails differently so that the trails process and log only the events that you specify. For example, one trail can log read-only data and management events, so that all read-only events are delivered to one S3 bucket. Another trail can log only write-only data and management events, so that all write-only events are delivered to a separate S3 bucket

Options A and D are invalid because you have to create a trail and not a log group

For more information on managing events with cloudtrail, please visit the following URL: <https://docs.aws.amazon.com/awscloudtrail/latest/userguide/loHEing-manasement-and-data-events-with-cloudtr> The correct answers are: Create one trail that logs data events to an S3 bucket. Create another trail that logs management events to another S3 bucket

Submit your Feedback/Queries to our Experts

NEW QUESTION 262

- (Exam Topic 3)

Amazon GuardDuty has detected communications to a known command and control endpoint from a company's Amazon EC2 instance. The instance was found to be running a vulnerable version of a common web framework. The company's security operations team wants to quickly identify other compute resources with the specific version of that framework installed.

Which approach should the team take to accomplish this task?

- A. Scan all the EC2 instances for noncompliance with AWS Config
- B. Use Amazon Athena to query AWS CloudTrail logs for the framework installation
- C. Scan all the EC2 instances with the Amazon Inspector Network Reachability rules package to identify instances running a web server with RecognizedPortWithListener findings
- D. Scan all the EC2 instances with AWS Systems Manager to identify the vulnerable version of the web framework
- E. Scan all the EC2 instances with AWS Resource Access Manager to identify the vulnerable version of the web framework

Answer: C

NEW QUESTION 267

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 268

- (Exam Topic 3)

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

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

Answer: D

Explanation:

A recommendation from the AWS Security Best practices highlights this as well C:\Users\wk\Desktop\mudassar\Untitled.jpg

Strategies for Using Multiple AWS Accounts

Design your AWS account strategy to maximize security and follow your business and governance requirements. Table 3 discusses possible strategies.

Business Requirement	Proposed Design	Comments
Centralized security management	Single AWS account	Centralize information security management and minimize overhead.
Separation of production, development, and testing environments	Three AWS accounts	Create one AWS account for production services, one for development, and one for testing.

Option A is partially valid, you can segregate resources, but a best practise is to have multiple accounts for this setup.
 Options B and C are invalid because from a maintenance perspective this could become very difficult
 For more information on the Security Best practices, please visit the following URL:

option A is partially valid, you can segregate resources, but a best practise is to have multiple accounts for this setup.
 Options B and C are invalid because from a maintenance perspective this could become very difficult For more information on the Security Best practices, please visit the following URL:

https://dl.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf

The correct answer is: Use separate AWS accounts for each of the environments Submit your Feedback/Queries to our Experts

NEW QUESTION 273

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

AWS-Certified-Security-Specialty Practice Exam Features:

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

100% Actual & Verified — Instant Download, Please Click
[Order The AWS-Certified-Security-Specialty Practice Test Here](#)