



Amazon

Exam Questions AWS-Certified-Security-Specialty

Amazon AWS Certified Security - Specialty

NEW QUESTION 1

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 2

- (Exam Topic 1)

A security engineer has created an Amazon Cognito user pool. The engineer needs to manually verify the ID and access token sent by the application for troubleshooting purposes. What is the MOST secure way to accomplish this?

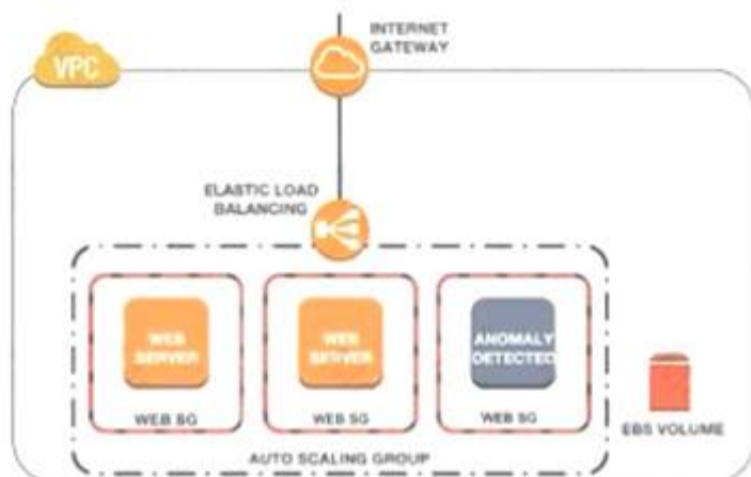
- A. Extract the subject (sub), audience (aud), and cognito:username from the ID token payload. Manually check the subject and audience for the user name in the user pool.
- B. Search for the public key with a key ID that matches the key ID in the header of the token.
- C. Then use a JSON Web Token (JWT) library to validate the signature of the token and extract values, such as the expiry date.
- D. Verify that the token is not expired.
- E. Then use the token_use claim function in Amazon Cognito to validate the key IDs.
- F. Copy the JSON Web Token (JWT) as a JSON document. Obtain the public JSON Web Key (JWK) and convert it to a pem file.
- G. Then use the file to validate the original JWT.

Answer: A

NEW QUESTION 3

- (Exam Topic 1)

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



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

Answer: B

NEW QUESTION 4

- (Exam Topic 1)

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

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

Answer: BDF

NEW QUESTION 5

- (Exam Topic 1)

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

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

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

Answer: BC

NEW QUESTION 6

- (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 7

- (Exam Topic 1)

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

Which solution would meet these requirements?

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

Answer: A

NEW QUESTION 8

- (Exam Topic 1)

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

How should a Security Engineer accomplish this?

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

Answer: C

NEW QUESTION 9

- (Exam Topic 1)

A company is using AWS Organizations to manage multiple AWS member accounts. All of these accounts have Amazon GuardDuty enabled in all Regions. The company's AWS Security Operations Center has a centralized security account for logging and monitoring. One of the member accounts has received an excessively high bill. A security engineer discovers that a compromised Amazon EC2 instance is being used to mine cryptocurrency. The Security Operations Center did not receive a GuardDuty finding in the central security account.

but there was a GuardDuty finding in the account containing the compromised EC2 instance. The security engineer needs to ensure a GuardDuty finding is available in the security account.

What should the security engineer do to resolve this issue?

- A. Set up an Amazon CloudWatch Event rule to forward all GuardDuty findings to the security account. Use an AWS Lambda function as a target to raise findings.
- B. Set up an Amazon CloudWatch Events rule to forward all GuardDuty findings to the security account. Use an AWS Lambda function as a target to raise findings in AWS Security Hub.
- C. Check that GuardDuty in the security account is able to assume a role in the compromised account using the GuardDuty fast findings permission. Schedule an Amazon CloudWatch Events rule and an AWS Lambda function to periodically check for GuardDuty findings.
- D. Use the `aws guardduty get-members` AWS CLI command in the security account to see if the account is listed. Send an invitation from GuardDuty in the security account to GuardDuty in the compromised account. Accept the invitation to forward all future GuardDuty findings.

Answer: D

NEW QUESTION 10

- (Exam Topic 1)

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

A

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

B

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

C

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

D

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

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

Answer: A

NEW QUESTION 10

- (Exam Topic 1)

A company has several production AWS accounts and a central security AWS account. The security account is used for centralized monitoring and has IAM privileges to all resources in every corporate account. All of the company's Amazon S3 buckets are tagged with a value denoting the data classification of their contents.

A Security Engineer is deploying a monitoring solution in the security account that will enforce bucket policy compliance. The system must monitor S3 buckets in all production accounts and confirm that any policy change is in accordance with the bucket's data classification. If any change is out of compliance; the Security team must be notified quickly.

Which combination of actions would build the required solution? (Choose three.)

- A. Configure Amazon CloudWatch Events in the production accounts to send all S3 events to the security account event bus.
- B. Enable Amazon GuardDuty in the security account
- C. and join the production accounts as members.
- D. Configure an Amazon CloudWatch Events rule in the security account to detect S3 bucket creation or modification events.
- E. Enable AWS Trusted Advisor and activate email notifications for an email address assigned to the security contact.
- F. Invoke an AWS Lambda function in the security account to analyze S3 bucket settings in response to S3 events, and send non-compliance notifications to the Security team.
- G. Configure event notifications on S3 buckets for PUT, POST, and DELETE events.

Answer: DEF

NEW QUESTION 15

- (Exam Topic 1)

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

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

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

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

Answer: ABF

NEW QUESTION 20

- (Exam Topic 1)

A company is operating an open-source software platform that is internet facing. The legacy software platform no longer receives security updates. The software

platform operates using Amazon route 53 weighted load balancing to send traffic to two Amazon EC2 instances that connect to an Amazon POS cluster a recent report suggests this software platform is vulnerable to SQL injection attacks. with samples of attacks provided. The company's security engineer must secure this system against SQL injection attacks within 24 hours. The secure, engineer's solution involve the least amount of effort and maintain normal operations during implementation.

What should the security engineer do to meet these requirements?

- A. Create an Application Load Balancer with the existing EC2 instances as a target group Create an AWS WAF web ACL containing rules mat protect the application from this attac
- B. then apply it to the ALB Test to ensure me vulnerability has been mitigated, then redirect thee Route 53 records to point to the ALB Update security groups on the EC 2 instances to prevent direct access from the internet
- C. Create an Amazon CloudFront distribution specifying one EC2 instance as an origin Create an AWS WAF web ACL containing rules that protect the application from this attack, then apply it to me distribution Test to ensure the vulnerability has mitigated, then redirect the Route 53 records to point toCloudFront
- D. Obtain me latest source code for the platform and make ire necessary updates Test me updated code to ensure that the vulnerability has been irrigated, then deploy me patched version of the platform to the EC2 instances
- E. Update the security group mat is attached to the EC2 instances, removing access from the internet to the TCP port used by the SQL database Create an AWS WAF web ACL containing rules mat protect me application from this attack, men apply it to the EC2 instances Test to ensure me vulnerability has been mitigate
- F. then restore the security group to me original setting

Answer: A

NEW QUESTION 25

- (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 26

- (Exam Topic 1)

After a recent security audit involving Amazon S3, a company has asked assistance reviewing its S3 buckets to determine whether data is properly secured. The first S3 bucket on the list has the following bucket policy.

```
{
  "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 publicity accessible?

- A. Yes, the bucket policy makes the whole bucket publicly accessible despite now the S3 bucket ACL orobject ACLs are configured.
- B. Yes, none of the data in the bucket is publicity accessible, regardless of how the S3 bucket ACL and object ACLs are configured.
- C. No, the IAM user policy would need to be examined first to determine whether any data is publicly accessible.
- D. No, the S3 bucket ACL and object ACLs need to be examined first to determine whether any data is publicly accessible.

Answer: A

NEW QUESTION 30

- (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 accoun
- B. Allow other applicable accounts to use that key for cryptographical 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 cryptographical 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 accoun
- E. Allow other applicable accounts to use that key for cryptographical operations by applying proper cross-account permissions in the key polic
- F. Create an IAM role in all applicable accounts and configure its access policy with permissions to create grants for the centrally managed CM
- G. Use this IAM role to create a grant for the centrally managed CMK with permissions to perform cryptographical operations and with the EC2 Auto Scalingservice-linked role defined as the grantee principal.
- H. Create a customer-managed CMK or an AWS managed CMK in the centralized accoun

- 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 31

- (Exam Topic 1)

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

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

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

Answer: C

NEW QUESTION 32

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

Answer: B

NEW QUESTION 34

- (Exam Topic 1)

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

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

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

Answer: BC

NEW QUESTION 39

- (Exam Topic 1)

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

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

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

- A. Move the SCP to the root OU of Organizations to remove the restriction to access Amazon S3.
- B. Add an IAM policy for the Developer, which grants S3 access.

- C. Create a new OU without applying the SCP restricting S3 acces
- D. Move the Developer account to this new OU.
- E. Add an allow list for the Developer account for the S3 service.

Answer: B

NEW QUESTION 40

- (Exam Topic 1)

A company is collecting AWS CloudTrail log data from multiple AWS accounts by managing individual trails in each account and forwarding log data to a centralized Amazon S3 bucket residing in a log archive account. After CloudTrail introduced support for AWS Organizations trails, the company decided to further centralize management and automate deployment of the CloudTrail logging capability across all of its AWS accounts.

The company's security engineer created an AWS Organizations trail in the master account, enabled server-side encryption with AWS KMS managed keys (SSE-KMS) for the log files, and specified the same bucket as the storage location. However, the engineer noticed that logs recorded by the new trail were not delivered to the bucket.

Which factors could cause this issue? (Select TWO.)

- A. The CMK key policy does not allow CloudTrail to make encrypt and decrypt API calls against the key.
- B. The CMK key policy does not allow CloudTrail to make GenerateDataKey API calls against the key.
- C. The IAM role used by the CloudTrail trail does not have permissions to make PutObject API calls against a folder created for the Organizations trail.
- D. The S3 bucket policy does not allow CloudTrail to make PutObject API calls against a folder created for the Organizations trail.
- E. The CMK key policy does not allow the IAM role used by the CloudTrail trail to use the key for crypto graphical operations.

Answer: AD

NEW QUESTION 45

- (Exam Topic 1)

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

The engineer needs to block public S3 buckets without causing any outages on the existing websites. The engineer has set up an Amazon CloudFront distribution for each website. Which set of steps should the security engineer implement next?

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

Answer: A

NEW QUESTION 47

- (Exam Topic 1)

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

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

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

Answer: AD

NEW QUESTION 51

- (Exam Topic 1)

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

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

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

Answer: AD

Explanation:

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

NEW QUESTION 54

- (Exam Topic 1)

A company has implemented centralized logging and monitoring of AWS CloudTrail logs from all Regions in an Amazon S3 bucket. The log files are encrypted using AWS KMS. A Security Engineer is attempting to review the log files using a third-party tool hosted on an Amazon EC2 instance. The Security Engineer is unable to access the logs in the S3 bucket and receives an access denied error message.

What should the Security Engineer do to fix this issue?

- A. Check that the role the Security Engineer uses grants permission to decrypt objects using the KMS CMK.
- B. Check that the role the Security Engineer uses grants permission to decrypt objects using the KMS CMK and gives access to the S3 bucket and objects
- C. Check that the role the EC2 instance profile uses grants permission to decrypt objects using the KMS CMK and gives access to the S3 bucket and objects
- D. Check that the role the EC2 instance profile uses grants permission to decrypt objects using the KMS CMK

Answer: C

NEW QUESTION 55

- (Exam Topic 1)

A security engineer has noticed that VPC Flow Logs are getting a lot REJECT traffic originating from a single Amazon EC2 instance in an Auto Scaling group. The security engineer is concerned that this EC2 instance may be compromised.

What immediate action should the security engineer take? What immediate action should the security engineer take?

- A. Remove the instance from the Auto Scaling group Close the security group mm ingress only from a single forensic IP address to perform an analysis.
- B. Remove the instance from the Auto Scaling group Change the network ACL rules to allow traffic only from a single forensic IP address to perform an analysis. Add a rule to deny all other traffic.
- C. Remove the instance from the Auto Scaling group Enable Amazon GuardDuty in that AWS account Install the Amazon Inspector agent on the suspicious EC2 instance to perform a scan.
- D. Take a snapshot of the suspicious EC2 instance
- E. Create a new EC2 instance from the snapshot in a closed security group with ingress only from a single forensic IP address to perform an analysis

Answer: B

NEW QUESTION 60

- (Exam Topic 1)

A Web Administrator for the website example.com has created an Amazon CloudFront distribution for dev.example.com, with a requirement to configure HTTPS using a custom TLS certificate imported to AWS Certificate Manager.

Which combination of steps is required to ensure availability of the certificate in the CloudFront console? (Choose two.)

- A. Call UploadServerCertificate with /cloudfront/dev/ in the path parameter.
- B. Import the certificate with a 4,096-bit RSA public key.
- C. Ensure that the certificate, private key, and certificate chain are PKCS #12-encoded.
- D. Import the certificate in the us-east-1 (Virginia) Region.
- E. Ensure that the certificate, private key, and certificate chain are PEM-encoded.

Answer: DE

NEW QUESTION 64

- (Exam Topic 1)

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

Which of the following actions could fix this issue?

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

Answer: C

NEW QUESTION 67

- (Exam Topic 1)

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

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

- A. Set up an S3 bucket policy with the awssecuretransport key Configure the CloudFront origin access identity (OAI) with the S3 bucket Configure CloudFront to use specific cipher
- B. Enforce the ALB with an HTTPS listener only and select the appropriate security policy for the ciphers Link the ALB with AWS WAF to allow access from the CloudFront IP ranges.
- C. Set up an S3 bucket policy with the aws:securetransport key
- D. Configure the CloudFront origin access identity (OAI) with the S3 bucket
- E. Enforce the ALB with an HTTPS listener only and select the appropriate security policy for the ciphers.
- F. Modify the CloudFront distribution to use AWS WAF
- G. Force HTTPS on the S3 bucket with specific ciphers in the bucket policy
- H. Configure an HTTPS listener only for the ALB
- I. Set up a security group to limit access to the ALB from the CloudFront IP ranges
- J. Modify the CloudFront distribution to use the ALB as the origin
- K. Enforce an HTTPS listener on the ALB
- L. Create a path-based routing rule on the ALB with proxies that connect to Amazon S3. Create a bucket policy to allow access from these proxies only.
- M. A company is trying to replace its on-premises bastion hosts used to access on-premises Linux servers with AWS Systems Manager Session Manager
- N. A security engineer has installed the Systems Manager Agent on all servers
- O. The security engineer verifies that the agent is running on all the servers, but Session Manager cannot connect to the servers. Which combination of steps should the security engineer take to resolve the issue?

engineer perform? (Select THREE.)

- P. Open inbound port 22 to 0.0.0.0/0 on all Linux servers.
- Q. Enable the advanced-instances tier in Systems Manager.
- R. Create a managed-instance activation for the on-premises servers.
- S. Reconfigure the Systems Manager Agent with the activation code and ID.
- T. Assign an IAM role to all of the on-premises servers.
- . Initiate an inventory collection with Systems Manager on the on-premises servers

Answer: CEF

NEW QUESTION 69

- (Exam Topic 2)

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

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

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

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

Answer: A

NEW QUESTION 72

- (Exam Topic 2)

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

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

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

Answer: B

NEW QUESTION 75

- (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 76

- (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 OpsWorks 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 77

- (Exam Topic 2)

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

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

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

Answer: A

Explanation:

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

NEW QUESTION 82

- (Exam Topic 2)

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

Please select:

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

Answer: D

Explanation:

The AWS Documentation mentions the following

The AWS CloudHSM service helps you meet corporate, contractual and regulatory compliance requirements for data security by using dedicated Hardware Security Module (HSM) instances within the AWS cloud. AWS and AWS Marketplace partners offer a variety of solutions for protecting sensitive data within the AWS platform, but for some applications and data subject to contractual or regulatory mandates for managing cryptographic keys, additional protection may be necessary. CloudHSM complements existing data protection solutions and allows you to protect your encryption keys within HSMs that are design and validated to government standards for secure key management. CloudHSM allows you to securely generate, store and manage cryptographic keys used for data encryption in a way that keys are accessible only by you.

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

For more information on CloudHSM, please visit the following URL: <https://aws.amazon.com/cloudhsm/faq>:
The correct answer is: Use Cloud HSM Submit your Feedback/Queries to our Experts

NEW QUESTION 84

- (Exam Topic 2)

A company has a few dozen application servers in private subnets behind an Elastic Load Balancer (ELB) in an AWS Auto Scaling group. The application is accessed from the web over HTTPS. The data must always be encrypted in transit. The Security Engineer is worried about potential key exposure due to vulnerabilities in the application software.

Which approach will meet these requirements while protecting the external certificate during a breach?

- A. Use a Network Load Balancer (NLB) to pass through traffic on port 443 from the internet to port 443 on the instances.
- B. Purchase an external certificate, and upload it to the AWS Certificate Manager (for use with the ELB) and to the instance
- C. Have the ELB decrypt traffic, and route and re-encrypt with the same certificate.
- D. Generate an internal self-signed certificate and apply it to the instance
- E. Use AWS Certificate Manager to generate a new external certificate for the EL
- F. Have the ELB decrypt traffic, and route and re-encrypt with the internal certificate.
- G. Upload a new external certificate to the load balance
- H. Have the ELB decrypt the traffic and forward it on port 80 to the instances.

Answer: C

NEW QUESTION 88

- (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 91

- (Exam Topic 2)

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

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

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

What steps should the Engineer perform to prevent this outcome?

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

Answer: B

NEW QUESTION 96

- (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 98

- (Exam Topic 2)

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

How can the security team fulfill these requirements?

Please select:

- A. Use Amazon QuickSight and Cloud Trail to generate the report of out of compliance instances/servers. Redeploy all out of compliance instances/servers using an AMI with the latest patches.
- B. Use Systems Manager Patch Manager to generate the report of out of compliance instances/ server

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

Answer: B

Explanation:

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

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

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

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

For more information on the AWS Patch Manager, please visit the below URL:

<https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-patch.html> (

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

Submit your Feedback/Queries to our Experts

NEW QUESTION 102

- (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 103

- (Exam Topic 2)

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

How can the Security Engineer further protect currently running instances?

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

Answer: C

NEW QUESTION 107

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 111

- (Exam Topic 2)

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

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

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

Answer: AB

Explanation:

[https://acloud.guru/forums/aws-certified-security-specialty/discussion/-Lm5A3w6_NybQPhh6tRP/Cloudwatch%](https://acloud.guru/forums/aws-certified-security-specialty/discussion/-Lm5A3w6_NybQPhh6tRP/Cloudwatch%20logs-agent-not-delivering-logs)

NEW QUESTION 115

- (Exam Topic 2)

An application outputs logs to a text file. The logs must be continuously monitored for security incidents.

Which design will meet the requirements with MINIMUM effort?

- A. Create a scheduled process to copy the component's logs into Amazon S3. Use S3 events to trigger a Lambda function that updates Amazon CloudWatch metrics with the log data.
- B. Set up CloudWatch alerts based on the metrics.
- C. Install and configure the Amazon CloudWatch Logs agent on the application's EC2 instance.
- D. Create a CloudWatch metric filter to monitor the application log.
- E. Set up CloudWatch alerts based on the metrics.
- F. Create a scheduled process to copy the application log files to AWS CloudTrail.
- G. Use S3 events to trigger Lambda functions that update CloudWatch metrics with the log data.
- H. Set up CloudWatch alerts based on the metrics.
- I. Create a file watcher that copies data to Amazon Kinesis when the application writes to the log file. Have Kinesis trigger a Lambda function to update Amazon CloudWatch metrics with the log data.
- J. Set up CloudWatch alerts based on the metrics.

Answer: B

Explanation:

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/QuickStartEC2Instance.html>

NEW QUESTION 118

- (Exam Topic 2)

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

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

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

Answer: A

Explanation:

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

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



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

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

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

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

Submit your Feedback/Queries to our Experts

NEW QUESTION 121

- (Exam Topic 2)

The Security Engineer is given the following requirements for an application that is running on Amazon EC2 and managed by using AWS CloudFormation templates with EC2 Auto Scaling groups:

-Have the EC2 instances bootstrapped to connect to a backend database.
-Ensure that the database credentials are handled securely.
-Ensure that retrievals of database credentials are logged.
Which of the following is the MOST efficient way to meet these requirements?

- A. Pass databases credentials to EC2 by using CloudFormation stack parameters with the property set to true
- B. Ensure that the instance is configured to log to Amazon CloudWatch Logs.
- C. Store database passwords in AWS Systems Manager Parameter Store by using SecureString parameters. Set the IAM role for the EC2 instance profile to allow access to the parameters.
- D. Create an AWS Lambda that ingests the database password and persists it to Amazon S3 with server-side encryption
- E. Have the EC2 instances retrieve the S3 object on startup, and log all script invocations to syslog.
- F. Write a script that is passed in as UserData so that it is executed upon launch of the EC2 instance. Ensure that the instance is configured to log to Amazon CloudWatch Logs.

Answer: B

NEW QUESTION 126

- (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 127

- (Exam Topic 2)

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

Please select:

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

Answer: B

Explanation:

The AWS Documentation mentions the following

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

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

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

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

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

NEW QUESTION 128

- (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 130

- (Exam Topic 2)

Which option for the use of the AWS Key Management Service (KMS) supports key management best practices that focus on minimizing the potential scope of data exposed by a possible future key compromise?

- A. Use KMS automatic key rotation to replace the master key, and use this new master key for future encryption operations without re-encrypting previously encrypted data.
- B. Generate a new Customer Master Key (CMK), re-encrypt all existing data with the new CMK, and use it for all future encryption operations.
- C. Change the CMK alias every 90 days, and update key-calling applications with the new key alias.
- D. Change the CMK permissions to ensure that individuals who can provision keys are not the same individuals who can use the keys.

Answer: B

Explanation:

"automatic key rotation has no effect on the data that the CMK protects. It does not rotate the data keys that the CMK generated or re-encrypt any data protected by the CMK, and it will not mitigate the effect of a compromised data key. You might decide to create a new CMK and use it in place of the original CMK. This has the same effect as rotating the key material in an existing CMK, so it's often thought of as manually rotating the key."
<https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html>

NEW QUESTION 134

- (Exam Topic 2)

A security team is responsible for reviewing AWS API call activity in the cloud environment for security violations. These events must be recorded and retained in a centralized location for both current and future AWS regions.
 What is the SIMPLEST way to meet these requirements?

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

Answer: C

NEW QUESTION 138

- (Exam Topic 2)

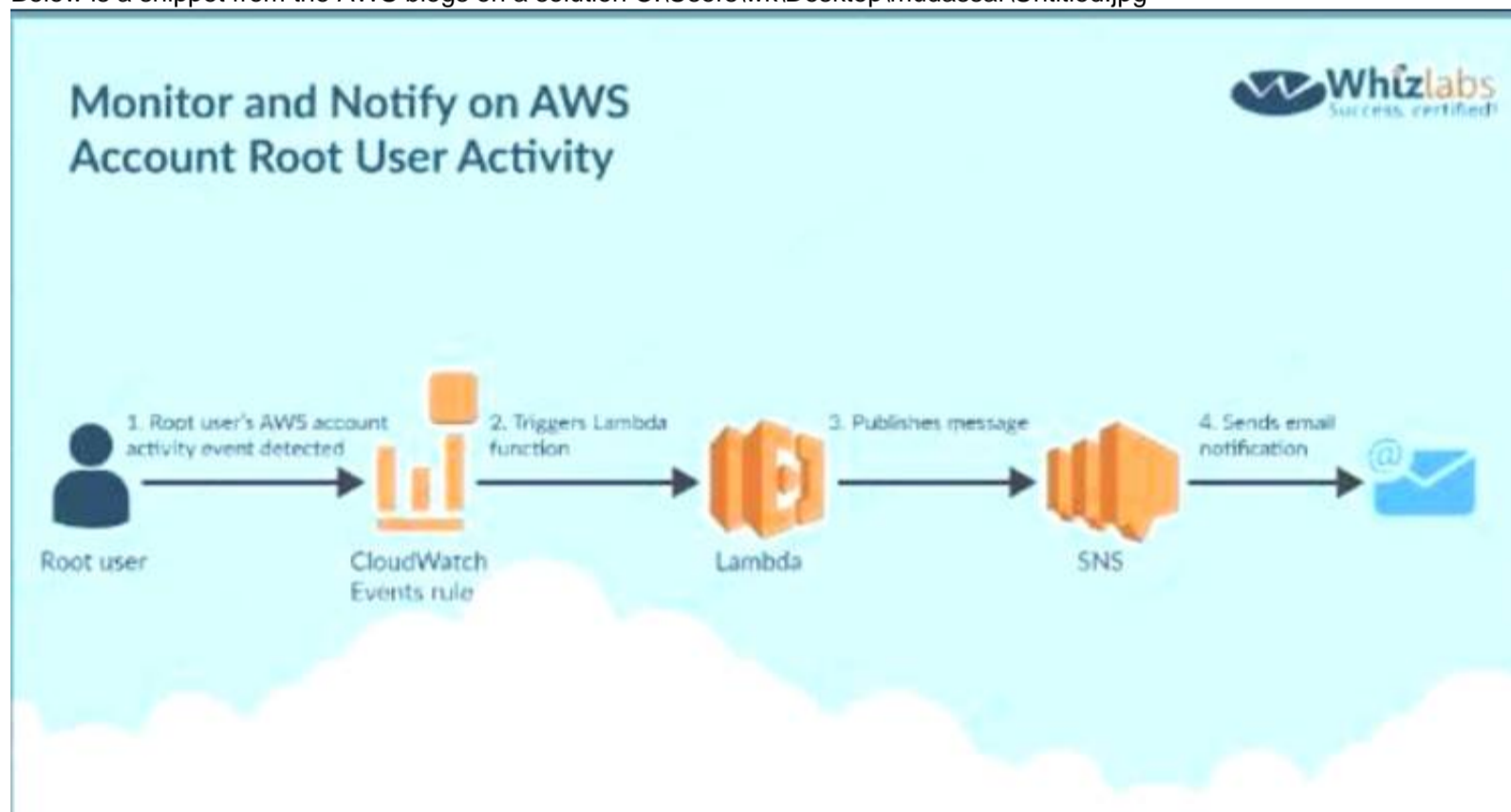
Your company has a requirement to monitor all root user activity by notification. How can this best be achieved? Choose 2 answers from the options given below.
 Each answer forms part of the solution
 Please select:

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

Answer: AC

Explanation:

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



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

NEW QUESTION 140

- (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/awscloudtrail/latest/useruide/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 145

- (Exam Topic 2)

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

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

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

Answer: B

Explanation:

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

NEW QUESTION 150

- (Exam Topic 2)

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

Please select:

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

Answer: AB

Explanation:

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

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

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

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/usins-network-security.html>

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

Submit your Feedback/Queries to our Experts

NEW QUESTION 152

- (Exam Topic 2)

You have just received an email from AWS Support stating that your AWS account might have been compromised. Which of the following steps would you look to carry out immediately. Choose 3 answers from the options below.

Please select:

- A. Change the root account password.
- B. Rotate all IAM access keys
- C. Keep all resources running to avoid disruption
- D. Change the password for all IAM users.

Answer: ABD

Explanation:

One of the articles from AWS mentions what should be done in such a scenario

If you suspect that your account has been compromised, or if you have received a notification from AWS that the account has been compromised, perform the following tasks:

Change your AWS root account password and the passwords of any IAM users.

Delete or rotate all root and AWS Identity and Access Management (IAM) access keys.

Delete any resources on your account you didn't create, especially running EC2 instances, EC2 spot bids, or IAM users.

Respond to any notifications you received from AWS Support through the AWS Support Center.

Option C is invalid because there could be compromised instances or resources running on your environment. They should be shutdown or stopped immediately.

For more information on the article, please visit the below URL: <https://aws.amazon.com/premiumsupport/knowledge-center/potential-account-compromise>

The correct answers are: Change the root account password. Rotate all IAM access keys. Change the password for all IAM users. Submit your Feedback/Queries to our Experts

NEW QUESTION 154

- (Exam Topic 2)

You are hosting a web site via website hosting on an S3 bucket - <http://demo.s3-website-us-east-1.amazonaws.com>. You have some web pages that use Javascript that access resources in another bucket which has web site hosting also enabled. But when users access the web pages, they are getting a blocked Javascript error. How can you rectify this?

Please select:

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

Answer: A

Explanation:

Your answer is incorrect Answer-A

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

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

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

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

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

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

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

Submit your Feedback/Queries to our Experts

NEW QUESTION 155

- (Exam Topic 2)

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

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

Please select:

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

Answer: BD

Explanation:

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

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

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

- * <https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/Working>

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

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

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

Submit your Feedback/Queries to our Experts

NEW QUESTION 159

- (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 162

- (Exam Topic 2)

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

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

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

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

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

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

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

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

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

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

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

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

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

Answer: A

NEW QUESTION 167

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 169

- (Exam Topic 2)

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

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

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

Answer: D

Explanation:

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

NEW QUESTION 170

- (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 173

- (Exam Topic 2)

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

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

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

Answer: A

Explanation:

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

References:

NEW QUESTION 176

- (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 177

- (Exam Topic 2)

The Security team believes that a former employee may have gained unauthorized access to AWS resources sometime in the past 3 months by using an identified access key.

What approach would enable the Security team to find out what the former employee may have done within AWS?

- A. Use the AWS CloudTrail console to search for user activity.
- B. Use the Amazon CloudWatch Logs console to filter CloudTrail data by user.
- C. Use AWS Config to see what actions were taken by the user.
- D. Use Amazon Athena to query CloudTrail logs stored in Amazon S3.

Answer: A

Explanation:

You can use CloudTrail to search event history for the last 90 days. You can use CloudWatch queries to search API history beyond the last 90 days. You can use Athena to query CloudTrail logs over the last 90 days. <https://aws.amazon.com/premiumsupport/knowledge-center/view-iam-history/>

NEW QUESTION 181

- (Exam Topic 2)

An Amazon S3 bucket is encrypted using an AWS KMS CMK. An IAM user is unable to download objects from the S3 bucket using the AWS Management Console; however, other users can download objects from the S3 bucket.

Which policies should the Security Engineer review and modify to resolve this issue? (Select three.)

- A. The CMK policy
- B. The VPC endpoint policy
- C. The S3 bucket policy
- D. The S3 ACL
- E. The IAM policy

Answer: CDE

NEW QUESTION 186

- (Exam Topic 2)

A company has contracted with a third party to audit several AWS accounts. To enable the audit, cross-account IAM roles have been created in each account targeted for audit. The Auditor is having trouble accessing some of the accounts. Which of the following may be causing this problem? (Choose three.)

- A. The external ID used by the Auditor is missing or incorrect.
- B. The Auditor is using the incorrect password.
- C. The Auditor has not been granted sts:AssumeRole for the role in the destination account.
- D. The Amazon EC2 role used by the Auditor must be set to the destination account role.
- E. The secret key used by the Auditor is missing or incorrect.

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

Answer: ACF

Explanation:

Using IAM to grant access to a Third-Party Account 1) Create a role to provide access to the require resources 1.1) Create a role policy that specifies the AWS Account ID to be accessed, "sts:AssumeRole" as action, and "sts:ExternalID" as condition 1.2) Create a role using the role policy just created 1.3) Assign a resource policy to the role. This will provide permission to access resource ARNs to the auditor 2) Repeat steps 1 and 2 on all AWS accounts 3) The auditor connects to the AWS account AWS Security Token Service (STS). The auditor must provide its ExternalID from step 1.2, the ARN of the role he is trying to assume from step 1.3, sts:ExternalID 4) STS provide the auditor with temporary credentials that provides the role access from step 1

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

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

NEW QUESTION 187

- (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 190

- (Exam Topic 2)

A Security Engineer is defining the logging solution for a newly developed product. Systems Administrators and Developers need to have appropriate access to event log files in AWS CloudTrail to support and troubleshoot the product.

Which combination of controls should be used to protect against tampering with and unauthorized access to log files? (Choose two.)

- A. Ensure that the log file integrity validation mechanism is enabled.
- B. Ensure that all log files are written to at least two separate Amazon S3 buckets in the same account.
- C. Ensure that Systems Administrators and Developers can edit log files, but prevent any other access.
- D. Ensure that Systems Administrators and Developers with job-related need-to-know requirements only are capable of viewing—but not modifying—the log files.
- E. Ensure that all log files are stored on Amazon EC2 instances that allow SSH access from the internal corporate network only.

Answer: AD

NEW QUESTION 195

- (Exam Topic 3)

A company has an existing AWS account and a set of critical resources hosted in that account. The employee who was in-charge of the root account has left the company. What must be now done to secure the account. Choose 3 answers from the options given below.

Please select:

- A. Change the access keys for all IAM users.
- B. Delete all custom created IAM policies
- C. Delete the access keys for the root account
- D. Confirm MFA to a secure device
- E. Change the password for the root account
- F. Change the password for all IAM users

Answer: CDE

Explanation:

Now if the root account has a chance to be compromised, then you have to carry out the below steps

* 1. Delete the access keys for the root account

* 2. Confirm MFA to a secure device

* 3. Change the password for the root account

This will ensure the employee who has left has no change to compromise the resources in AWS. Option A is invalid because this would hamper the working of the current IAM users

Option B is invalid because this could hamper the current working of services in your AWS account Option F is invalid because this would hamper the working of the current IAM users

For more information on IAM root user, please visit the following URL: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_root-user.html

The correct answers are: Delete the access keys for the root account Confirm MFA to a secure device. Change the password for the root account

Submit Your Feedback/Queries to our Experts

NEW QUESTION 198

- (Exam Topic 3)

There is a set of EC2 Instances in a private subnet. The application hosted on these EC2 Instances need to access a DynamoDB table. It needs to be ensured that traffic does not flow out to the internet. How can this be achieved?

Please select:

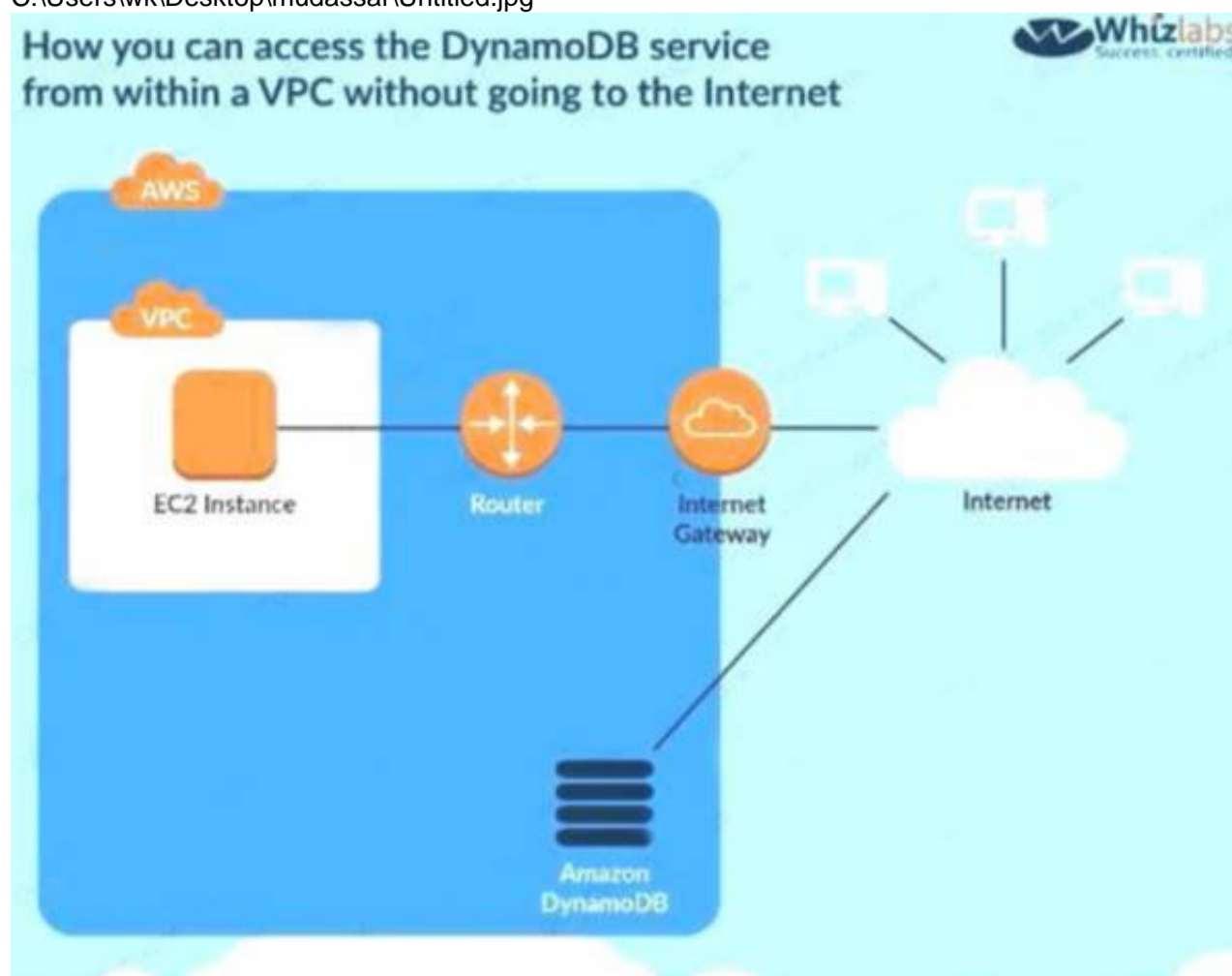
- A. Use a VPC endpoint to the DynamoDB table
- B. Use a VPN connection from the VPC
- C. Use a VPC gateway from the VPC
- D. Use a VPC Peering connection to the DynamoDB table

Answer: A

Explanation:

The following diagram from the AWS Documentation shows how you can access the DynamoDB service from within a V without going to the Internet This can be done with the help of a VPC endpoint

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



Option B is invalid because this is used for connection between an on-premise solution and AWS Option C is invalid because there is no such option

Option D is invalid because this is used to connect 2 VPCs

For more information on VPC endpoints for DynamoDB, please visit the URL:

The correct answer is: Use a VPC endpoint to the DynamoDB table Submit your Feedback/Queries to our Experts

NEW QUESTION 199

- (Exam Topic 3)

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

Please select:

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

Answer: A

Explanation:

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

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

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

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

Submit your Feedback/Queries to our Experts

NEW QUESTION 202

- (Exam Topic 3)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "NotAction": [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws:TagKeys/Team": "2 (aws:PrincipalTag/Team)"
        }
      }
    }
  ]
}
```

Answer: A

NEW QUESTION 206

- (Exam Topic 3)

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

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

Answer: C

Explanation:

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

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

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

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

NEW QUESTION 209

- (Exam Topic 3)

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

Please select:

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

Answer: AB

Explanation:

Tags enable you to categorize your 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 211

- (Exam Topic 3)

You have an S3 bucket defined in AWS. You want to ensure that you encrypt the data before sending it across the wire. What is the best way to achieve this. Please select:

- A. Enable server side encryption for the S3 bucke
- B. This request will ensure that the data is encrypted first.
- C. Use the AWS Encryption CLI to encrypt the data first
- D. Use a Lambda function to encrypt the data before sending it to the S3 bucket.
- E. Enable client encryption for the bucket

Answer: B

Explanation:

One can use the AWS Encryption CLI to encrypt the data before sending it across to the S3 bucket. Options A and C are invalid because this would still mean that data is transferred in plain text Option D is invalid because you cannot just enable client side encryption for the S3 bucket For more information on Encrypting and Decrypting data, please visit the below URL:

<https://aws.amazon.com/blogs/security/how-to-encrypt-and-decrypt-your-data-with-the-aws-encryption-cli>

The correct answer is: Use the AWS Encryption CLI to encrypt the data first Submit your Feedback/Queries to our Experts

NEW QUESTION 215

- (Exam Topic 3)

You currently have an S3 bucket hosted in an AWS Account. It holds information that needs be accessed by a partner account. Which is the MOST secure way to allow the partner account to access the S3 bucket in your account? Select 3 options.

Please select:

- A. Ensure an IAM role is created which can be assumed by the partner account.
- B. Ensure an IAM user is created which can be assumed by the partner account.
- C. Ensure the partner uses an external id when making the request
- D. Provide the ARN for the role to the partner account
- E. Provide the Account Id to the partner account
- F. Provide access keys for your account to the partner account

Answer: ACD

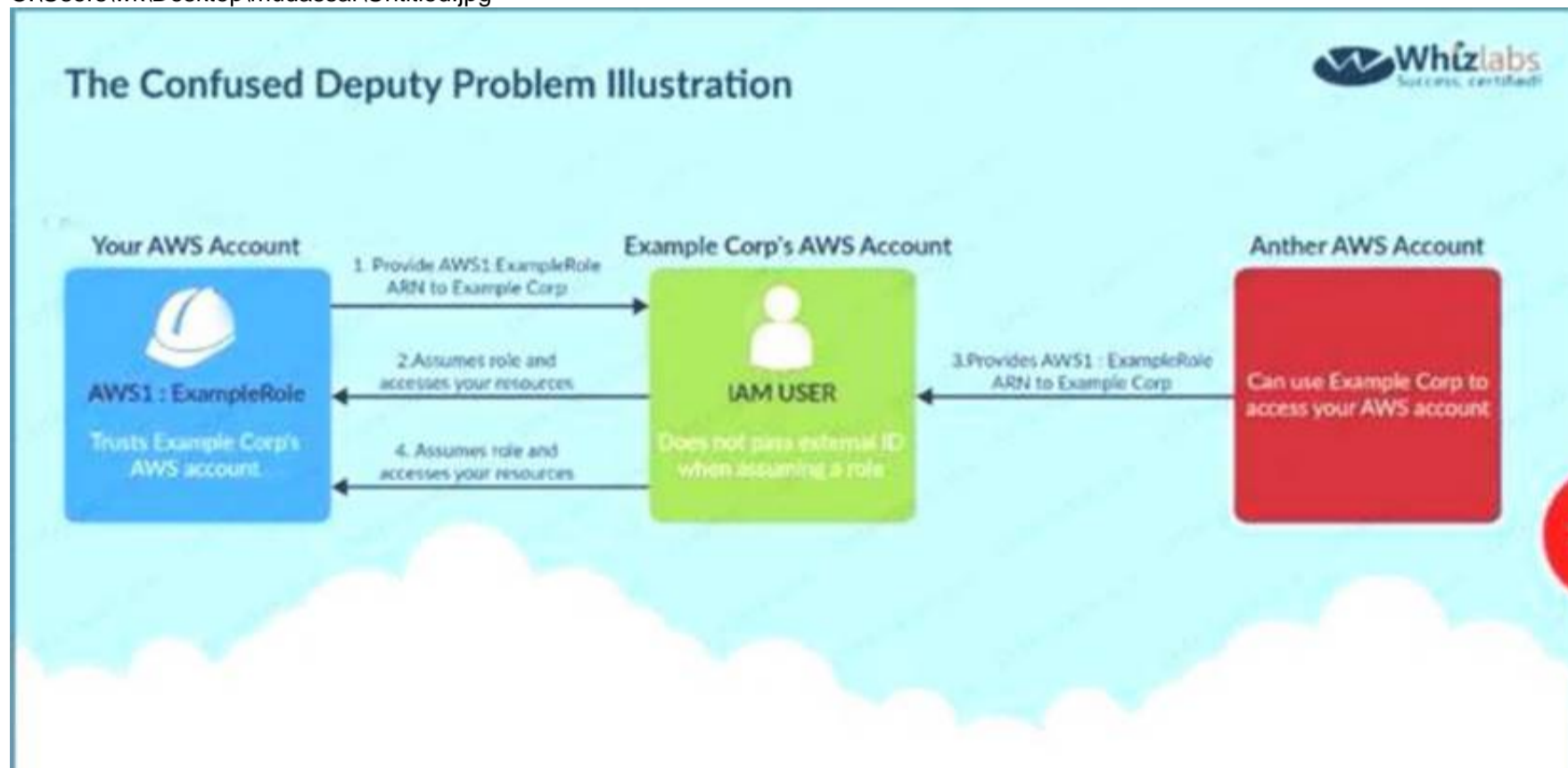
Explanation:

Option B is invalid because Roles are assumed and not IAM users

Option E is invalid because you should not give the account ID to the partner Option F is invalid because you should not give the access keys to the partner

The below diagram from the AWS documentation showcases an example on this wherein an IAM role and external ID is used to access an AWS account resources

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



For more information on creating roles for external ID'S please visit the following URL:

The correct answers are: Ensure an IAM role is created which can be assumed by the partner account. Ensure the partner uses an external id when making the request Provide the ARN for the role to the partner account

Submit your Feedback/Queries to our Experts

NEW QUESTION 220

- (Exam Topic 3)

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

Please select:

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

Answer: BD

Explanation:

The AWS Documentation mentions the following on AWS Inspector

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

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

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

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

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

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

(

NEW QUESTION 221

- (Exam Topic 3)

You have a set of Keys defined using the AWS KMS service. You want to stop using a couple of keys, but are not sure of which services are currently using the keys. Which of the following would be a safe option to stop using the keys from further usage. Please select:

- A. Delete the keys since anyway there is a 7 day waiting period before deletion
- B. Disable the keys
- C. Set an alias for the key
- D. Change the key material for the key

Answer: B

Explanation:

Option A is invalid because once you schedule the deletion and waiting period ends, you cannot come back from the deletion process.

Option C and D are invalid because these will not check to see if the keys are being used or not. The AWS Documentation mentions the following

Deleting a customer master key (CMK) in AWS Key Management Service (AWS KMS) is destructive and potentially dangerous. It deletes the key material and all metadata associated with the CMK, and is irreversible. After a CMK is deleted you can no longer decrypt the data that was encrypted under that CMK, which means that data becomes unrecoverable. You should delete a CMK only when you are sure that you don't need to use it anymore. If you are not sure, consider disabling the CMK instead of deleting it. You can re-enable a disabled CMK if you need to use it again later, but you cannot recover a deleted CMK.

For more information on deleting keys from KMS, please visit the below URL: <https://docs.aws.amazon.com/kms/latest/developerguide/deleting-keys.html>

The correct answer is: Disable the keys. Submit your Feedback/Queries to our Experts

NEW QUESTION 222

- (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 226

- (Exam Topic 3)

How can you ensure that an instance in a VPC does not use AWS DNS for routing DNS requests. You want to use your own managed DNS instance. How can this be achieved?

Please select:

- A. Change the existing DHCP options set
- B. Create a new DHCP options set and replace the existing one.
- C. Change the route table for the VPC
- D. Change the subnet configuration to allow DNS requests from the new DNS Server

Answer: B

Explanation:

In order to use your own DNS server, you need to ensure that you create a new custom DHCP options set with the IP of the custom DNS server. You cannot modify the existing set, so you need to create a new one.

Option A is invalid because you cannot make changes to an existing DHCP options set.

Option C is invalid because this can only be used to work with Routes and not with a custom DNS solution. Option D is invalid because this needs to be done at the VPC level and not at the Subnet level.

For more information on DHCP options set, please visit the following URL: <https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC-DHCP-Options.html>

The correct answer is: Create a new DHCP options set and replace the existing one. Submit your Feedback/Queries to our Experts

NEW QUESTION 231

- (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 236

- (Exam Topic 3)

An organization has launched 5 instances: 2 for production and 3 for testing. The organization wants that one particular group of IAM users should only access the test instances and not the production ones. How can the organization set that as a part of the policy?

Please select:

- A. Launch the test and production instances in separate regions and allow region wise access to the group
- B. Define the IAM policy which allows access based on the instance ID
- C. Create an IAM policy with a condition which allows access to only small instances
- D. Define the tags on the test and production servers and add a condition to the IAM policy which allows access to specification tags

Answer: D

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

Option A is invalid because this is not a recommended practice

Option B is invalid because this is an overhead to maintain this in policies Option C is invalid because the instance type will not resolve the requirement For information on resource tagging, please visit the below URL: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Usine_Tags.html

The correct answer is: Define the tags on the test and production servers and add a condition to the IAM policy which allows access to specific tags

Submit your Feedback/Queries to our Experts

NEW QUESTION 240

- (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 encryptio 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 243

- (Exam Topic 3)

A company's on-premises networks are connected to VPCs using an AWS Direct Connect gateway. The company's on-premises application needs to stream data using an existing Amazon Kinesis Data Firehose delivery stream. The company's security policy requires that data be encrypted in transit using a private network. How should the company meet these requirements?

- A. Create a VPC endpoint for Kinesis Data Firehos
- B. Configure the application to connect to the VPC endpoint.
- C. Configure an IAM policy to restrict access to Kinesis Data Firehose using a source IP condition. Configure the application to connect to the existing Firehose delivery stream.
- D. Create a new TLS certificate in AWS Certificate Manager (ACM). Create a public-facing Network Load Balancer (NLB) and select the newly created TLS certificat
- E. Configure the NLB to forward all traffic to Kinesis Data Firehos
- F. Configure the application to connect to the NLB.
- G. Peer the on-premises network with the Kinesis Data Firehose VPC using Direct Connec
- H. Configure the application to connect to the existing Firehose delivery stream.

Answer: A

NEW QUESTION 244

- (Exam Topic 3)

An organization wants to log all AWS API calls made within all of its AWS accounts, and must have a central place to analyze these logs. What steps should be taken to meet these requirements in the MOST secure manner? (Select TWO)

- A. Turn on AWS CloudTrail in each AWS account
- B. Turn on CloudTrail in only the account that will be storing the logs
- C. Update the bucket ACL of the bucket in the account that will be storing the logs so that other accounts can log to it
- D. Create a service-based role for CloudTrail and associate it with CloudTrail in each account
- E. Update the bucket policy of the bucket in the account that will be storing the logs so that other accounts can log to it

Answer: AE

NEW QUESTION 245

- (Exam Topic 3)

Company policy requires that all insecure server protocols, such as FTP, Telnet, HTTP, etc be disabled on all servers. The security team would like to regularly check all servers to ensure compliance with this requirement by using a scheduled CloudWatch event to trigger a review of the current infrastructure. What process will check compliance of the company's EC2 instances?

Please select:

- A. Trigger an AWS Config Rules evaluation of the restricted-common-ports rule against every EC2 instance.
- B. Query the Trusted Advisor API for all best practice security checks and check for "action recommended" status.
- C. Enable a GuardDuty threat detection analysis targeting the port configuration on every EC2 instance.
- D. Run an Amazon inspector assessment using the Runtime Behavior Analysis rules package against every EC2 instance.

Answer: D

Explanation:

Option B is incorrect because querying Trusted Advisor API's are not possible

Option C is incorrect because GuardDuty should be used to detect threats and not check the compliance of security protocols.

Option D states that Run Amazon Inspector using runtime behavior analysis rules which will analyze the behavior of your instances during an assessment run, and provide guidance about how to make your EC2 instances more secure.

Insecure Server Protocols

This rule helps determine whether your EC2 instances allow support for insecure and unencrypted ports/services such as FTP, Telnet HTTP, IMAP, POP version 3, SMTP, SNMP versions 1 and 2, rsh, and rlogin.

For more information, please refer to below URL: https://docs.aws.amazon.com/mspector/latest/userguide/inspector_runtime-behavior-analysis.html#insecure-prot

(The correct answer is: Run an Amazon Inspector assessment using the Runtime Behavior Analysis rules package against every EC2 instance.

Submit your Feedback/Queries to our Experts

NEW QUESTION 248

- (Exam Topic 3)

Your company makes use of S3 buckets for storing data. There is a company policy that all services should have logging enabled. How can you ensure that logging is always enabled for created S3 buckets in the AWS Account?

Please select:

- A. Use AWS Inspector to inspect all S3 buckets and enable logging for those where it is not enabled
- B. Use AWS Config Rules to check whether logging is enabled for buckets
- C. Use AWS Cloudwatch metrics to check whether logging is enabled for buckets
- D. Use AWS Cloudwatch logs to check whether logging is enabled for buckets

Answer: B

Explanation:

This is given in the AWS Documentation as an example rule in AWS Config Example rules with triggers Example rule with configuration change trigger

* 1. You add the AWS Config managed rule, S3_BUCKET_LOGGING_ENABLED, to your account to check whether your Amazon S3 buckets have logging enabled.

* 2. The trigger type for the rule is configuration changes. AWS Config runs the evaluations for the rule when an Amazon S3 bucket is created, changed, or deleted.

* 3. When a bucket is updated, the configuration change triggers the rule and AWS Config evaluates whether the bucket is compliant against the rule.

Option A is invalid because AWS Inspector cannot be used to scan all buckets

Option C and D are invalid because Cloudwatch cannot be used to check for logging enablement for buckets. For more information on Config Rules please see the below Link:

➤ <https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config-rules.html>

The correct answer is: Use AWS Config Rules to check whether logging is enabled for buckets Submit your Feedback/Queries to our Experts

NEW QUESTION 249

- (Exam Topic 3)

Your company has been using AWS for hosting EC2 Instances for their web and database applications. They want to have a compliance check to see the following

Whether any ports are left open other than admin ones like SSH and RDP

Whether any ports to the database server other than ones from the web server security group are open Which of the following can help achieve this in the easiest way possible. You don't want to carry out an extra configuration changes?

Please select:

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

Answer: B

Explanation:

Trusted Advisor checks for compliance with the following security recommendations:

Limited access to common administrative ports to only a small subset of addresses. This includes ports 22 (SSH), 23 (Telnet) 3389 (RDP), and 5500 (VNC).

Limited access to common database ports. This includes ports 1433 (MSSQL Server), 1434 (MSSQL Monitor), 3306 (MySQL), Oracle (1521) and 5432 (PostgreSQL).

Option A is partially correct but then you would need to write custom rules for this. The AWS trusted advisor can give you all o these checks on its dashboard

Option C is incorrect. Amazon Inspector needs a software agent to be installed on all EC2 instances that are included in th.

assessment target, the security of which you want to evaluate with Amazon Inspector. It monitors the behavior of the EC2 instance on which it is installed,

including network, file system, and process activity, and collects a wide set of behavior and configuration data (telemetry), which it then passes to the Amazon Inspector service.

Our question's requirement is to choose a choice that is easy to implement. Hence Trusted Advisor is more appropriate for this question.

Options D is invalid because this service dont provide these details.

For more information on the Trusted Advisor, please visit the following URL <https://aws.amazon.com/premiumsupport/trustedadvisor>>

The correct answer is: AWS Trusted Advisor Submit your Feedback/Queries to our Experts

NEW QUESTION 254

- (Exam Topic 3)

You are planning on hosting a web application on AWS. You create an EC2 Instance in a public subnet. This instance needs to connect to an EC2 Instance that will host an Oracle database. Which of the following steps should be followed to ensure a secure setup is in place? Select 2 answers.

Please select:

A. Place the EC2 Instance with the Oracle database in the same public subnet as the Web server for faster communication

B. Place the EC2 Instance with the Oracle database in a separate private subnet

C. Create a database security group and ensure the web security group to allowed incoming access

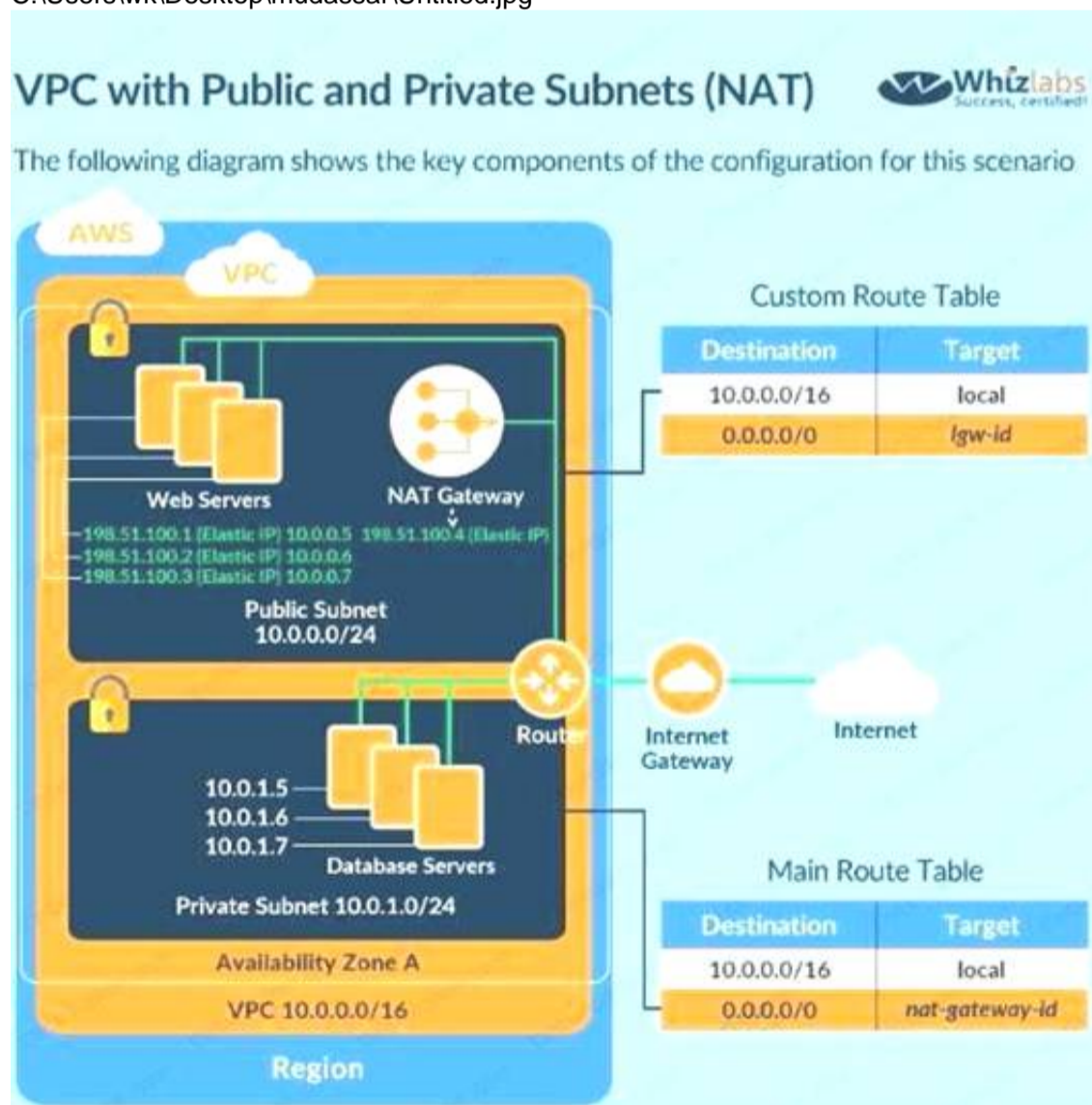
D. Ensure the database security group allows incoming traffic from 0.0.0.0/0

Answer: BC

Explanation:

The best secure option is to place the database in a private subnet. The below diagram from the AWS Documentation shows this setup. Also ensure that access is not allowed from all sources but just from the web servers.

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



Option A is invalid because databases should not be placed in the public subnet

Option D is invalid because the database security group should not allow traffic from the internet For more information on this type of setup, please refer to the below URL:

https://docs.aws.amazon.com/AmazonVPC/latest/UserGuideA/PC_Scenario2.

The correct answers are: Place the EC2 Instance with the Oracle database in a separate private subnet Create a database security group and ensure the web security group to allowed incoming access

Submit your Feedback/Queries to our Experts

NEW QUESTION 257

- (Exam Topic 3)

Which of the below services can be integrated with the AWS Web application firewall service. Choose 2 answers from the options given below

Please select:

A. AWS Cloudfront

- B. AWS Lambda
- C. AWS Application Load Balancer
- D. AWS Classic Load Balancer

Answer: AC

Explanation:

The AWS documentation mentions the following on the Application Load Balancer

AWS WAF can be deployed on Amazon CloudFront and the Application Load Balancer (ALB). As part of Amazon CloudFront it can be part of your Content Distribution Network (CDN) protecting your resources and content at the Edge locations and as part of the Application Load Balancer it can protect your origin web servers running behind the ALBs.

Options B and D are invalid because only Cloudfront and the Application Load Balancer services are supported by AWS WAF.

For more information on the web application firewall please refer to the below URL: <https://aws.amazon.com/waf/faq>;

The correct answers are: AWS Cloudfront AWS Application Load Balancer Submit your Feedback/Queries to our Experts

NEW QUESTION 261

- (Exam Topic 3)

A company deployed AWS Organizations to help manage its increasing number of AWS accounts. A security engineer wants to ensure only principals in the Organization structure can access a specific Amazon S3 bucket. The solution must also minimize operational overhead

Which solution will meet these requirements?

- A. 1 Put all users into an IAM group with an access policy granting access to the J bucket.
- B. Have the account creation trigger an AWS Lambda function that manages the bucket policy, allowing access to accounts listed in the policy only.
- C. Add an SCP to the Organizations master account, allowing all principals access to the bucket.
- D. Specify the organization ID in the global key condition element of a bucket policy, allowing all principals access.

Answer: D

NEW QUESTION 265

.....

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](#)