



Amazon

Exam Questions AWS-Certified-Security-Specialty

Amazon AWS Certified Security - Specialty

About ExamBible

Your Partner of IT Exam

Found in 1998

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

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

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

NEW QUESTION 1

- (Exam Topic 1)

A company has an encrypted Amazon S3 bucket. An Application Developer has an IAM policy that allows access to the S3 bucket, but the Application Developer is unable to access objects within the bucket.

What is a possible cause of the issue?

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

Answer: C

NEW QUESTION 2

- (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 3

- (Exam Topic 1)

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

What should the company do to meet these requirements?

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

Answer: C

NEW QUESTION 4

- (Exam Topic 1)

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

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

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

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

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

Answer: B

NEW QUESTION 5

- (Exam Topic 1)

A Developer is building a serverless application that uses Amazon API Gateway as the front end. The application will not be publicly accessible. Other legacy applications running on Amazon EC2 will make calls to the application. A Security Engineer has been asked to review the security controls for authentication and authorization of the application.

Which combination of actions would provide the MOST secure solution? (Select TWO)

- A. Configure an IAM policy that allows the least permissive actions to communicate with the API Gateway. Attach the policy to the role used by the legacy EC2 instances.
- B. Enable AWS WAF for API Gateway. Configure rules to explicitly allow connections from the legacy EC2 instances.
- C. Create a VPC endpoint for API Gateway. Attach an IAM resource policy that allows the role of the legacy EC2 instances to call specific APIs.
- D. Create a usage plan. Generate a set of API keys for each application that needs to call the API.
- E. Configure cross-origin resource sharing (CORS) in each API. Share the CORS information with the applications that call the API.

Answer: AE

NEW QUESTION 6

- (Exam Topic 1)

A company had one of its Amazon EC2 key pairs compromised. A Security Engineer must identify which current Linux EC2 instances were deployed and used the compromised key pair.

How can this task be accomplished?

- A. Obtain the list of instances by directly querying Amazon EC2 using: `aws ec2 describe-instances --filters "Name=key-name,Values=KEYNAMEHERE"`.
- B. Obtain the fingerprint for the key pair from the AWS Management Console, then search for the fingerprint in the Amazon Inspector logs.
- C. Obtain the output from the EC2 instance metadata using: `curl http://169.254.169.254/latest/meta-data/public-keys/0/`.
- D. Obtain the fingerprint for the key pair from the AWS Management Console, then search for the fingerprint in Amazon CloudWatch Logs using: `aws logs filter-log-events`.

Answer: A

NEW QUESTION 7

- (Exam Topic 1)

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

Assuming that AWS Certificate Manager is used, how many certificates will need to be generated?

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

Answer: B

NEW QUESTION 8

- (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 9

- (Exam Topic 1)

An organization policy states that all encryption keys must be automatically rotated every 12 months. Which AWS Key Management Service (KMS) key type should be used to meet this requirement?

- A. AWS managed Customer Master Key (CMK)
- B. Customer managed CMK with AWS generated key material
- C. Customer managed CMK with imported key material
- D. AWS managed data key

Answer: B

NEW QUESTION 10

- (Exam Topic 1)

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

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

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

Answer: C

NEW QUESTION 10

- (Exam Topic 1)

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

What should the security engineer do to meet these requirements?

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

Answer: A

NEW QUESTION 12

- (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 15

- (Exam Topic 1)

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

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

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

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

Answer: D

NEW QUESTION 19

- (Exam Topic 1)

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

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

Answer: ACD

NEW QUESTION 24

- (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 25

- (Exam Topic 1)

A security engineer needs to ensure their company's uses of AWS meets AWS security best practices. As part of this, the AWS account root user must not be used for daily work. The root user must be monitored for use, and the Security team must be alerted as quickly as possible if the root user is used. Which solution meets these requirements?

- A. Set up an Amazon CloudWatch Events rule that triggers an Amazon SNS notification.
- B. Set up an Amazon CloudWatch Events rule that triggers an Amazon SNS notification logs from S3 and generate notifications using Amazon SNS.
- C. Set up a rule in AWS config to trigger root user event
- D. Trigger an AWS Lambda function and generate notifications using Amazon SNS.
- E. Use Amazon Inspector to monitor the usage of the root user and generate notifications using Amazon SNS

Answer: A

NEW QUESTION 27

- (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 30

- (Exam Topic 1)

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

Which solution should the security engineer recommend?

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

Answer: B

NEW QUESTION 33

- (Exam Topic 1)

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

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

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

Answer: BCE

NEW QUESTION 38

- (Exam Topic 1)

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

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

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

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

Answer: ABE

NEW QUESTION 40

- (Exam Topic 1)

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

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

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

Answer: ABF

NEW QUESTION 44

- (Exam Topic 1)

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

```
2 123456789010 eni-1235b8ca 203.0.113.12 172.31.16.139 0 0 1 4 336 1432917027 1432917142 ACCEPT OK
2 123456789010 eni-1235b8ca 172.31.16.139 203.0.113.12 0 0 1 4 336 1432917094 1432917142 REJECT OK
```

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

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

Answer: D

NEW QUESTION 48

- (Exam Topic 1)

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

What should the Security Engineer do to meet these requirements?

- A. Use AWS Resource Access Manager (AWS RAM) to monitor the AWS CloudTrail configuration
- B. Send notifications using Amazon SNS.

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

Answer: B

NEW QUESTION 53

- (Exam Topic 1)

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

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

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

Answer: D

NEW QUESTION 55

- (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 56

- (Exam Topic 1)

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

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

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

Answer: A

NEW QUESTION 59

- (Exam Topic 1)

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

What is the likely cause of this access denial?

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

Answer: D

NEW QUESTION 61

- (Exam Topic 1)

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

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

- A. Disable the EC2 instance metadata service.

- B. Log all student SSH interactive session activity.
- C. Implement ip tables-based restrictions on the instances.
- D. Install the Amazon Inspector agent on the instances.

Answer: A

Explanation:

"To turn off access to instance metadata on an existing instance....." <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/configuring-instance-metadata-service.html> You can disable the service for existing (running or stopped) ec2 instances. <https://docs.aws.amazon.com/cli/latest/reference/ec2/modify-instance-metadata-options.html>

NEW QUESTION 66

- (Exam Topic 1)

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

How should a security engineer resolve these issues?

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

Answer: A

NEW QUESTION 68

- (Exam Topic 1)

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

What should the Security Engineer do to achieve this?

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

Answer: B

Explanation:

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

NEW QUESTION 71

- (Exam Topic 2)

A company hosts a popular web application that connects to an Amazon RDS MySQL DB instance running in a private VPC subnet that was created with default ACL settings. The IT Security department has a suspicion that a DDos attack is coming from a suspecting IP. How can you protect the subnets from this attack?

Please select:

- A. Change the Inbound Security Groups to deny access from the suspecting IP
- B. Change the Outbound Security Groups to deny access from the suspecting IP
- C. Change the Inbound NACL to deny access from the suspecting IP
- D. Change the Outbound NACL to deny access from the suspecting IP

Answer: C

Explanation:

Option A and B are invalid because by default the Security Groups already block traffic. You can use NACL's as an additional security layer for the subnet to deny traffic.

Option D is invalid since just changing the Inbound Rules is sufficient The AWS Documentation mentions the following

A network access control list (ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC.

The correct answer is: Change the Inbound NACL to deny access from the suspecting IP

NEW QUESTION 73

- (Exam Topic 2)

A Software Engineer wrote a customized reporting service that will run on a fleet of Amazon EC2 instances. The company security policy states that application logs for the reporting service must be centrally collected.

What is the MOST efficient way to meet these requirements?

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

Answer: D

Explanation:

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

NEW QUESTION 77

- (Exam Topic 2)

You have a web site that is sitting behind AWS Cloudfront. You need to protect the web site against threats such as SQL injection and Cross site scripting attacks. Which of the following service can help in such a scenario

Please select:

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

Answer: B

Explanation:

The AWS Documentation mentions the following

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

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

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

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

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

The correct answer is: AWS WAF

Submit your Feedback/Queries to our Experts

NEW QUESTION 78

- (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 82

- (Exam Topic 2)

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

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

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

Answer: ACE

Explanation:

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

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

NEW QUESTION 83

- (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 86

- (Exam Topic 2)

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

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

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

Answer: BEF

NEW QUESTION 89

- (Exam Topic 2)

An application makes calls to AWS services using the AWS SDK. The application runs on Amazon EC2 instances with an associated IAM role. When the application attempts to access an object within an Amazon S3 bucket; the Administrator receives the following error message: HTTP 403: Access Denied.

Which combination of steps should the Administrator take to troubleshoot this issue? (Select three.)

- A. Confirm that the EC2 instance's security group authorizes S3 access.
- B. Verify that the KMS key policy allows decrypt access for the KMS key for this IAM principle.
- C. Check the S3 bucket policy for statements that deny access to objects.
- D. Confirm that the EC2 instance is using the correct key pair.
- E. Confirm that the IAM role associated with the EC2 instance has the proper privileges.
- F. Confirm that the instance and the S3 bucket are in the same Region.

Answer: BCE

NEW QUESTION 91

- (Exam Topic 2)

A company is hosting a website that must be accessible to users for HTTPS traffic. Also port 22 should be open for administrative purposes. The administrator's workstation has a static IP address of 203.0.113.1/32. Which of the following security group configurations are the MOST secure but still functional to support these requirements? Choose 2 answers from the options given below

Please select:

- A. Port 443 coming from 0.0.0.0/0
- B. Port 443 coming from 10.0.0.0/16

- C. Port 22 coming from 0.0.0.0/0
- D. Port 22 coming from 203.0.113.1/32

Answer: AD

Explanation:

Since HTTPS traffic is required for all users on the Internet, Port 443 should be open on all IP addresses. For port 22, the traffic should be restricted to an internal subnet.

Option B is invalid, because this only allow traffic from a particular CIDR block and not from the internet Option C is invalid because allowing port 22 from the internet is a security risk

For more information on AWS Security Groups, please visit the following UR <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/usins-network-security.html>
The correct answers are: Port 443 coming from 0.0.0.0/0, Port 22 coming from 203.0.113.1 /32 Submit your Feedback/Queries to our Experts

NEW QUESTION 96

- (Exam Topic 2)

The InfoSec team has mandated that in the future only approved Amazon Machine Images (AMIs) can be used. How can the InfoSec team ensure compliance with this mandate?

- A. Terminate all Amazon EC2 instances and relaunch them with approved AMIs.
- B. Patch all running instances by using AWS Systems Manager.
- C. Deploy AWS Config rules and check all running instances for compliance.
- D. Define a metric filter in Amazon CloudWatch Logs to verify compliance.

Answer: C

Explanation:

<https://docs.aws.amazon.com/config/latest/developerguide/approved-amis-by-id.html>

NEW QUESTION 101

- (Exam Topic 2)

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

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

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

Answer: CE

NEW QUESTION 103

- (Exam Topic 2)

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

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

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

Answer: C

Explanation:

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

NEW QUESTION 108

- (Exam Topic 2)

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

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

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

Answer: C

NEW QUESTION 113

- (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 118

- (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 dat
- B. Set up CloudWatch alerts based on the metrics.
- C. Install and configure the Amazon CloudWatch Logs agent on the application's EC2 instanc
- 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 CloudTrai
- G. Use S3 events to trigger Lambda functions that update CloudWatch metrics with the log dat
- 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 dat
- J. Set up CloudWatch alerts based on the metrics.

Answer: B

Explanation:

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

NEW QUESTION 123

- (Exam Topic 2)

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

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

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

Answer: BDE

Explanation:

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

NEW QUESTION 125

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 128

- (Exam Topic 2)

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

Please select:

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

Answer: A

Explanation:

The AWS Documentation mentions the following on AWS KMS

AWS Key Management Service (AWS KMS) is a managed service that makes it easy for you to create and control the encryption keys used to encrypt your data. AWS KMS is integrated with other AWS services including Amazon Elastic Block Store (Amazon EBS), Amazon Simple Storage Service (Amazon S3), Amazon Redshift Amazon Elastic Transcoder, Amazon WorkMail, Amazon Relational Database Service (Amazon RDS), and others to make it simple to encrypt your data with encryption keys that you manage

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

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

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

AWS KMS API

Submit your Feedback/Queries to our Experts

NEW QUESTION 129

- (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 134

- (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 138

- (Exam Topic 2)

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

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

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

Answer: BDE

NEW QUESTION 141

- (Exam Topic 2)

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

Which configuration will ensure continued connectivity between sites MOST securely?

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

Answer: C

Explanation:

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

NEW QUESTION 142

- (Exam Topic 2)

A company has complex connectivity rules governing ingress, egress, and communications between Amazon EC2 instances. The rules are so complex that they cannot be implemented within the limits of the maximum number of security groups and network access control lists (network ACLs).

What mechanism will allow the company to implement all required network rules without incurring additional cost?

- A. Configure AWS WAF rules to implement the required rules.
- B. Use the operating system built-in, host-based firewall to implement the required rules.
- C. Use a NAT gateway to control ingress and egress according to the requirements.
- D. Launch an EC2-based firewall product from the AWS Marketplace, and implement the required rules in that product.

Answer: B

NEW QUESTION 147

- (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 151

- (Exam Topic 2)

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

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

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

Answer: D

NEW QUESTION 155

- (Exam Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 156

- (Exam Topic 2)

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

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

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

Answer: A

NEW QUESTION 161

- (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 166

- (Exam Topic 3)

You have a set of application, database and web servers hosted in AWS. The web servers are placed behind an ELB. There are separate security groups for the application, database and web servers. The network security groups have been defined accordingly. There is an issue with the communication between the application and database servers. In order to troubleshoot the issue between just the application and database server, what is the ideal set of MINIMAL steps you would take?

Please select:

- A. Check the Inbound security rules for the database security group Check the Outbound security rules for the application security group
- B. Check the Outbound security rules for the database security group I Check the inbound security rules for the application security group
- C. Check the both the Inbound and Outbound security rules for the database security group Check the inbound security rules for the application security group
- D. Check the Outbound security rules for the database security group Check the both the Inbound and Outbound security rules for the application security group

Answer: A

Explanation:

Here since the communication would be established inward to the database server and outward from the application server, you need to ensure that just the Outbound rules for application server security groups are checked. And then just the Inbound rules for database server security groups are checked.

Option B can't be the correct answer. It says that we need to check the outbound security group which is not needed.

We need to check the inbound for DB SG and outbound of Application SG. Because, this two group need to communicate with each other to function properly.

Option C is invalid because you don't need to check for Outbound security rules for the database security group

Option D is invalid because you don't need to check for Inbound security rules for the application security group

For more information on Security Groups, please refer to below URL:

The correct answer is: Check the Inbound security rules for the database security group Check the Outbound security rules for the application security group

Submit your Feedback/Queries to our Experts

NEW QUESTION 167

- (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 171

- (Exam Topic 3)

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

Please select:

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

Answer: B

Explanation:

The AWS Documentation mentions the following:

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

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

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

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

NEW QUESTION 172

- (Exam Topic 3)

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

Please select:

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

Answer: D

Explanation:

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

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

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

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

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

NEW QUESTION 176

- (Exam Topic 3)

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

Please select:

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

Answer: A

Explanation:

Option B is partially correct but a big maintenance over head to create and maintain a script when the functionality is already available in S3
 Option C is invalid because snapshots are not available in S3 Option D is invalid because versioning will not replicate objects The AWS Documentation mentions the following

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

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

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

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

NEW QUESTION 180

- (Exam Topic 3)

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

Please select:

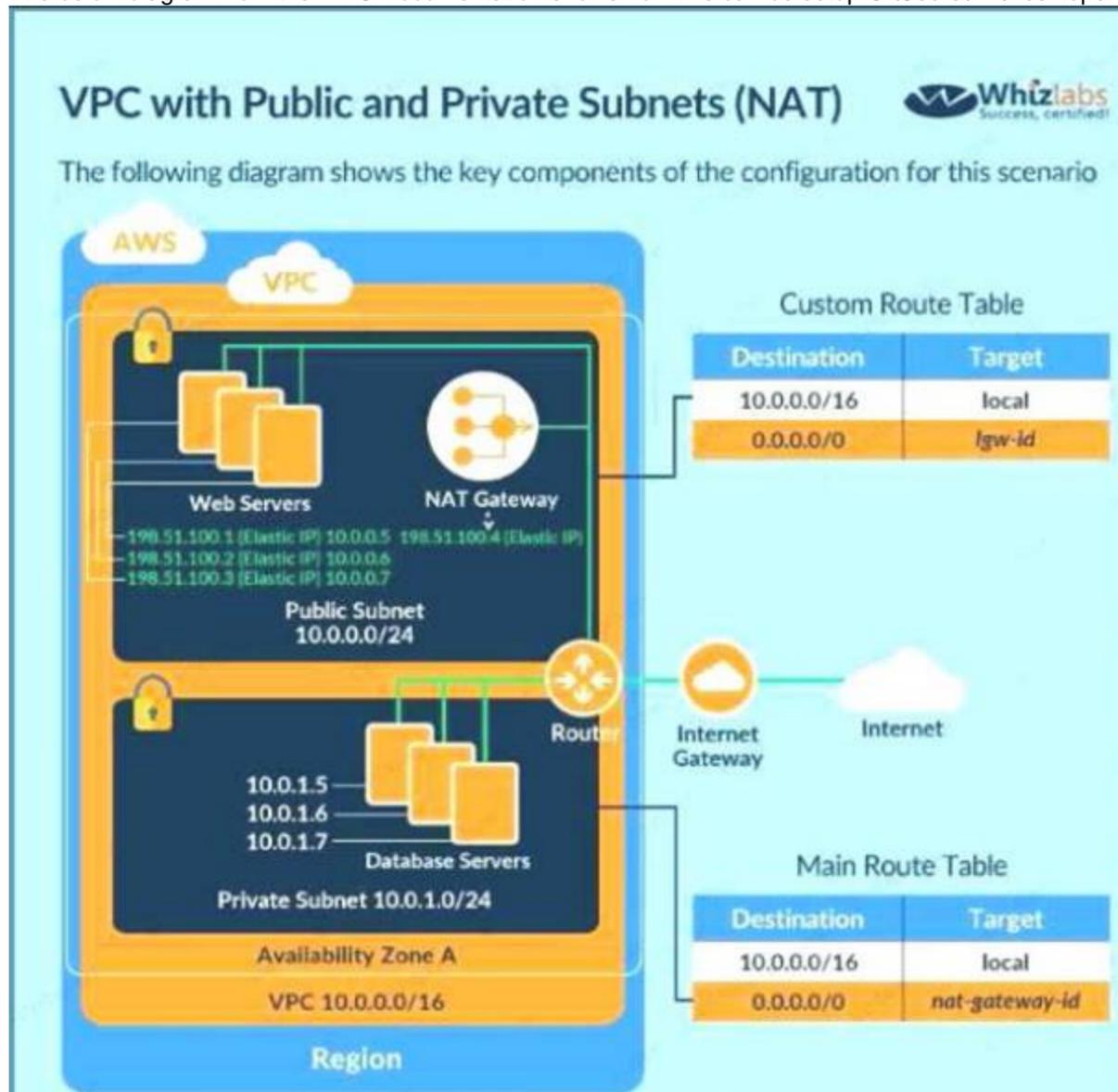
- A. Consider moving the web server to a private subnet
- B. Consider moving the database server to a private subnet
- C. Consider moving both the web and database server to a private subnet
- D. Consider creating a private subnet and adding a NAT instance to that subnet

Answer: B

Explanation:

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

The below diagram from the AWS Documentation shows how this can be setup C:\Users\wk\Desktop\mudassar\Untitled.jpg



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

For more information on public and private subnets in AWS, please visit the following url [com/AmazonVPC/latest/UserGuide/VPC_Scenario2](https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2).

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

NEW QUESTION 181

- (Exam Topic 3)

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

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

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

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

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

Answer: A

NEW QUESTION 184

- (Exam Topic 3)

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

Please select:

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

Answer: B

Explanation:

The AWS Documentation mentions the following

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

Option A is invalid because its the cluster that needs to be encrypted

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

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

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

NEW QUESTION 187

- (Exam Topic 3)

An ecommerce website was down for 1 hour following a DDoS attack Users were unable to connect to the website during the attack period. The ecommerce company's security team is worried about future potential attacks and wants to prepare for such events The company needs to minimize downtime in its response to similar attacks in the future.

Which steps would help achieve this9 (Select TWO)

- A. Enable Amazon GuardDuty to automatically monitor for malicious activity and block unauthorized access.
- B. Subscribe to AWS Shield Advanced and reach out to AWS Support in the event of an attack.
- C. Use VPC Flow Logs to monitor network: traffic and an AWS Lambda function to automatically block an attacker's IP using security groups.
- D. Set up an Amazon CloudWatch Events rule to monitor the AWS CloudTrail events in real time use AWS Config rules to audit the configuration, and use AWS Systems Manager for remediation.
- E. Use AWS WAF to create rules to respond to such attacks

Answer: CE

NEW QUESTION 191

- (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.AWSGuardDuty

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 (VNQ).

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 don't 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 196

- (Exam Topic 3)

A company is operating a website using Amazon CloudFront. CloudFront servers some content from Amazon S3 and other from web servers running EC2 instances behind an Application Load Balancer (ALB). Amazon DynamoDB is used as the data store. The company already uses AWS Certificate Manager (ACM) to store a public TLS certificate that can optionally secure connections between the website users and CloudFront. The company has a new requirement to enforce end-to-end encryption in transit.

Which combination of steps should the company take to meet this requirement? (Select THREE.)

- A. Update the CloudFront distribution
- B. configuring it to optionally use HTTPS when connecting to origins on Amazon S3
- C. Update the web application configuration on the web servers to use HTTPS instead of HTTP when connecting to DynamoDB
- D. Update the CloudFront distribution to redirect HTTP connections to HTTPS
- E. Configure the web servers on the EC2 instances to listen using HTTPS using the public ACM TLS certificate Update the ALB to connect to the target group using HTTPS
- F. Update the ALB listen to listen using HTTPS using the public ACM TLS certificate
- G. Update the CloudFront distribution to connect to the HTTPS listener.
- H. Create a TLS certificate Configure the web servers on the EC2 instances to use HTTPS only with that certificate
- I. Update the ALB to connect to the target group using HTTPS.

Answer: BCE

NEW QUESTION 200

- (Exam Topic 3)

A Security Architect has been asked to review an existing security architecture and identify why the application servers cannot successfully initiate a connection to the database servers. The following summary describes the architecture:

* 1 An Application Load Balancer, an internet gateway, and a NAT gateway are configured in the public subnet

* 2. Database, application, and web servers are configured on three different private subnets.

* 3 The VPC has two route tables: one for the public subnet and one for all other subnets The route table for the public subnet has a 0.0.0.0/0 route to the internet gateway The route table for all other subnets has a 0.0.0.0/0 route to the NAT gateway. All private subnets can route to each other

* 4 Each subnet has a network ACL implemented that limits all inbound and outbound connectivity to only the required ports and protocols

* 5 There are 3 Security Groups (SGs) database application and web Each group limits all inbound and outbound connectivity to the minimum required

Which of the following accurately reflects the access control mechanisms the Architect should verify?

- A. Outbound SG configuration on database servers Inbound SG configuration on application servers inbound and outbound network ACL configuration on the database subnet Inbound and outbound network ACL configuration on the application server subnet
- B. Inbound SG configuration on database servers Outbound SG configuration on application servers Inbound and outbound network ACL configuration on the database subnet Inbound and outbound network ACL configuration on the application server subnet
- C. Inbound and outbound SG configuration on database servers Inbound and outbound SG configuration on application servers Inbound network ACL configuration on the database subnet Outbound network ACL configuration on the application server subnet
- D. Inbound SG configuration on database servers Outbound SG configuration on application servers Inbound network ACL configuration on the database subnet Outbound network ACL configuration on the application server subnet.

Answer: A

NEW QUESTION 204

- (Exam Topic 3)

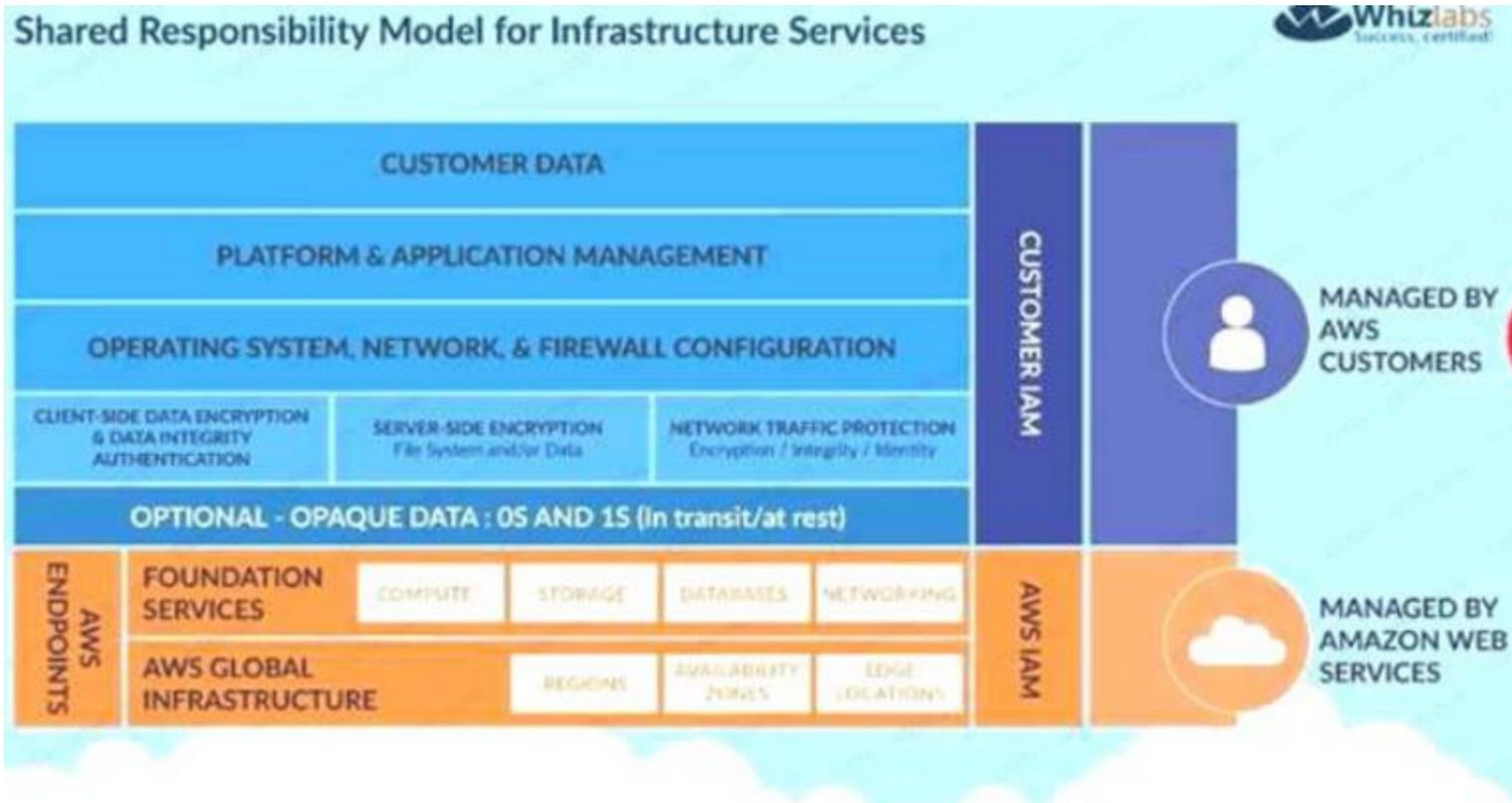
Which of the following is the responsibility of the customer? Choose 2 answers from the options given below. Please select:

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

Answer: BC

Explanation:

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



For more information on AWS Security best practises, please refer to below URL [awsstatic.com/whitepapers/Security/AWS Practices](https://awsstatic.com/whitepapers/Security/AWS%20Practices).
 The correct answers are: Encryption of data at rest Protection of data in transit Submit your Feedback/Queries to our Experts

NEW QUESTION 205

- (Exam Topic 3)

A company's Chief Security Officer has requested that a Security Analyst review and improve the security posture of each company AWS account The Security Analyst decides to do this by Improving AWS account root user security.

Which actions should the Security Analyst take to meet these requirements? (Select THREE.)

- A. Delete the access keys for the account root user in every account.
- B. Create an admin IAM user with administrative privileges and delete the account root user in every account.
- C. Implement a strong password to help protect account-level access to the AWS Management Console by the account root user.
- D. Enable multi-factor authentication (MFA) on every account root user in all accounts.
- E. Create a custom IAM policy to limit permissions to required actions for the account root user and attach the policy to the account root user.
- F. Attach an IAM role to the account root user to make use of the automated credential rotation in AWS STS.

Answer: ADE

NEW QUESTION 208

- (Exam Topic 3)

For compliance reasons a Security Engineer must produce a weekly report that lists any instance that does not have the latest approved patches applied. The Engineer must also ensure that no system goes more than 30 days without the latest approved updates being applied

What would the MOST efficient way to achieve these goals?

- A. Use Amazon inspector to determine which systems do not have the latest patches applied, and after 30 days, redeploy those instances with the latest AMI version
- B. Configure Amazon EC2 Systems Manager to report on instance patch compliance and enforce updates during the defined maintenance windows
- C. Examine AWS CloudTrail logs to determine whether any instances have not restarted in the last 30 days, and redeploy those instances
- D. Update the AMIs with the latest approved patches and redeploy each instance during the defined maintenance window

Answer: B

NEW QUESTION 209

- (Exam Topic 3)

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

- * sgLB - associated with the ELB
 - * sgWeb - associated with the EC2 instances.
 - * sgDB - associated with the database
 - * sgBastion - associated with the bastion host
- Which security group configuration will allow the application to be secure and functional?
 Please select:

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

Answer: D

Explanation:

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

NEW QUESTION 210

- (Exam Topic 3)

A company has been using the AWS KMS service for managing its keys. They are planning on carrying out housekeeping activities and deleting keys which are no longer in use. What are the ways that can be incorporated to see which keys are in use? Choose 2 answers from the options given below
Please select:

- A. Determine the age of the master key
- B. See who is assigned permissions to the master key
- C. See Cloudtrail for usage of the key
- D. Use AWS cloudwatch events for events generated for the key

Answer: BC

Explanation:

The direct ways that can be used to see how the key is being used is to see the current access permissions and cloudtrail logs
Option A is invalid because seeing how long ago the key was created would not determine the usage of the key
Option D is invalid because Cloudtrail Event is better for seeing for events generated by the key This is also mentioned in the AWS Documentation
Examining CMK Permissions to Determine the Scope of Potential Usage
Determining who or what currently has access to a customer master key (CMK) might help you determine how widely the CM was used and whether it is still needed. To learn how to determine who or what currently has access to a CMK, go to Determining Access to an AWS KMS Customer Master Key.
Examining AWS CloudTrail Logs to Determine Actual Usage
AWS KMS is integrated with AWS CloudTrail, so all AWS KMS API activity is recorded in CloudTrail log files. If you have CloudTrail turned on in the region where your customer master key (CMK) is located, you can examine your CloudTrail log files to view a history of all AWS KMS API activity for a particular CMK, and thus its usage history. You might be able to use a CMK's usage history to help you determine whether or not you still need it
For more information on determining the usage of CMK keys, please visit the following URL:

> <https://docs.aws.amazon.com/kms/latest/developerguide/deleting-keys-determining-usage.html>

The correct answers are: See who is assigned permissions to the master key. See Cloudtrail for usage of the key Submit your Feedback/Queries to our Experts

NEW QUESTION 214

- (Exam Topic 3)

You have a requirement to conduct penetration testing on the AWS Cloud for a couple of EC2 Instances. How could you go about doing this? Choose 2 right answers from the options given below.
Please select:

- A. Get prior approval from AWS for conducting the test
- B. Use a pre-approved penetration testing tool.
- C. Work with an AWS partner and no need for prior approval request from AWS
- D. Choose any of the AWS instance type

Answer: AB

Explanation:

You can use a pre-approved solution from the AWS Marketplace. But till date the AWS Documentation still mentions that you have to get prior approval before conducting a test on the AWS Cloud for EC2 Instances.
Option C and D are invalid because you have to get prior approval first. AWS Docs Provides following details:
"For performing a penetration test on AWS resources first of all we need to take permission from AWS and complete a requisition form and submit it for approval. The form should contain information about the instances you wish to test identify the expected start and end dates/times of your test and requires you to read and agree to Terms and Conditions specific to penetration testing and to the use of appropriate tools for testing. Note that the end date may not be more than 90 days from the start date."

(
At this time, our policy does not permit testing small or micro RDS instance types. Testing of ml .small, t1 .micro or t2.nano EC2 instance types is not permitted.

For more information on penetration testing please visit the following URL: <https://aws.amazon.com/security/penetration-testing/>

The correct answers are: Get prior approval from AWS for conducting the test Use a pre-approved penetration testing tool. Submit your Feedback/Queries to our Experts

NEW QUESTION 219

- (Exam Topic 3)

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

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

Answer: B

Explanation:

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

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

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

<http://docs.aws.amazon.com/IAM/latest/UserGuide/access>

pol-examples.htm#iam-policy-example-ec2-two-condition!

The correct answer is: Create an IAM policy with a condition which denies access when the IP address range is not from the organization

Submit your Feedback/Queries to our Experts

NEW QUESTION 224

- (Exam Topic 3)

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

Please select:

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

Answer: B

Explanation:

The AWS Documentation mentions the following

Amazon S3 is integrated with AWS CloudTrail. CloudTrail is a service that captures specific API calls made to Amazon S3 from your AWS account and delivers the log files to an Amazon S3 bucket that you specify. It captures API calls made from the Amazon S3 console or from the Amazon S3 API.

Using the information collected by CloudTrail, you can determine what request was made to Amazon S3, the source IP address from which the request was made, who made the request when it was made, and so on Options A,C and D are invalid because these services cannot be used to get the source IP address of the calls to S3 buckets

For more information on Cloudtrail logging, please refer to the below Link: <https://docs.aws.amazon.com/AmazonS3/latest/dev/cloudtrail-loggings.html>

The correct answer is: Monitor the S3 API calls by using Cloudtrail logging Submit your Feedback/Queries to our Experts

NEW QUESTION 227

- (Exam Topic 3)

A company has resources hosted in their AWS Account. There is a requirement to monitor all API activity for all regions. The audit needs to be applied for future regions as well. Which of the following can be used to fulfil this requirement.

Please select:

- A. Ensure Cloudtrail for each regio
- B. Then enable for each future region.
- C. Ensure one Cloudtrail trail is enabled for all regions.
- D. Create a Cloudtrail for each regio
- E. Use Cloudformation to enable the trail for all future regions.
- F. Create a Cloudtrail for each regio
- G. Use AWS Config to enable the trail for all future regions.

Answer: B

Explanation:

The AWS Documentation mentions the following

You can now turn on a trail across all regions for your AWS account. CloudTrail will deliver log files from all regions to the Amazon S3 bucket and an optional CloudWatch Logs log group you specified. Additionally, when AWS launches a new region, CloudTrail will create the same trail in the new region. As a result you will receive log files containing API activity for the new region without taking any action.

Option A and C is invalid because this would be a maintenance overhead to enable cloudtrail for every region Option D is invalid because this AWS Config cannot be used to enable trails

For more information on this feature, please visit the following URL:

<https://aws.amazon.com/about-aws/whats-new/2015/12/turn-on-cloudtrail-across-all-reeions-and-support-for-mul> The correct answer is: Ensure one Cloudtrail trail is enabled for all regions. Submit your Feedback/Queries to our Experts

NEW QUESTION 229

- (Exam Topic 3)

Your company is planning on developing an application in AWS. This is a web based application. The application users will use their facebook or google identities for authentication. You want to have the ability to manage user profiles without having to add extra coding to manage this. Which of the below would assist in this.

Please select:

- A. Create an OIDC identity provider in AWS
- B. Create a SAML provider in AWS
- C. Use AWS Cognito to manage the user profiles
- D. Use IAM users to manage the user profiles

Answer: B

Explanation:

The AWS Documentation mentions the following The AWS Documentation mentions the following

OIDC identity providers are entities in IAM that describe an identity provider (IdP) service that supports the OpenID Connect (OIDC) standard. You use an OIDC identity provider when you want to establish trust between an OIDC-compatible IdP—such as Google, Salesforce, and many others—and your AWS account This is useful if you are creating a mobile app or web application that requires access to AWS resources, but you don't want to create custom sign-in code or manage your own user identities

Option A is invalid because in the security groups you would not mention this information/ Option C is invalid because SAML is used for federated authentication

Option D is invalid because you need to use the OIDC identity provider in AWS For more information on ODIC identity providers, please refer to the below Link: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_create_oidc.html The correct answer is: Create an OIDC identity provider in AWS

NEW QUESTION 232

- (Exam Topic 3)

Example.com is hosted on Amazon EC2 instances behind an Application Load Balancer (ALB). Third-party host intrusion detection system (HIDS) agents that capture the traffic of the EC2 instance are running on each host. The company must ensure they are using privacy enhancing technologies for users, without losing the assurance the third-party solution offers.

What is the MOST secure way to meet these requirements?

- A. Enable TLS pass through on the ALB, and handle decryption at the server using Elliptic Curve Diffie-Hellman (ECDHE) cipher suites.
- B. Create a listener on the ALB that uses encrypted connections with Elliptic Curve Diffie-Hellman (ECDHE) cipher suites, and pass the traffic in the clear to the server.
- C. Create a listener on the ALB that uses encrypted connections with Elliptic Curve Diffie-Hellman (ECDHE) cipher suites, and use encrypted connections to the servers that do not enable Perfect Forward Secrecy (PFS).
- D. Create a listener on the ALB that does not enable Perfect Forward Secrecy (PFS) cipher suites, and use encrypted connections to the servers using Elliptic Curve Diffie-Hellman (ECDHE) cipher suites.

Answer: D

NEW QUESTION 235

- (Exam Topic 3)

Your company has just set up a new central server in a VPC. There is a requirement for other teams who have their servers located in different VPC's in the same region to connect to the central server. Which of the below options is best suited to achieve this requirement.

Please select:

- A. Set up VPC peering between the central server VPC and each of the teams VPCs.
- B. Set up AWS DirectConnect between the central server VPC and each of the teams VPCs.
- C. Set up an IPsec Tunnel between the central server VPC and each of the teams VPCs.
- D. None of the above options will work.

Answer: A

Explanation:

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account within a single region.

Options B and C are invalid because you need to use VPC Peering Option D is invalid because VPC Peering is available

For more information on VPC Peering please see the below Link:

<http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-peering.html>

The correct answer is: Set up VPC peering between the central server VPC and each of the teams VPCs. Submit your Feedback/Queries to our Experts

NEW QUESTION 237

- (Exam Topic 3)

A company plans to create individual child accounts within an existing organization in AWS Organizations for each of its DevOps teams. AWS CloudTrail has been enabled and configured on all accounts to write audit logs to an Amazon S3 bucket in a centralized AWS account. A security engineer needs to ensure that DevOps team members are unable to modify or disable this configuration.

How can the security engineer meet these requirements?

- A. Create an IAM policy that prohibits changes to the specific CloudTrail trail and apply the policy to the AWS account root user.
- B. Create an S3 bucket policy in the specified destination account for the CloudTrail trail that prohibits configuration changes from the AWS account root user in the source account.
- C. Create an SCP that prohibits changes to the specific CloudTrail trail and apply the SCP to the appropriate organizational unit or account in Organizations.
- D. Create an IAM policy that prohibits changes to the specific CloudTrail trail and apply the policy to a new IAM group
- E. Have team members use individual IAM accounts that are members of the new IAM group.

Answer: D

NEW QUESTION 239

- (Exam Topic 3)

A company's policy requires that all API keys be encrypted and stored separately from source code in a centralized security account. This security account is managed by the company's security team However, an audit revealed that an API key is stored with the source code of an AWS Lambda function in an AWS CodeCommit repository in the DevOps account

How should the security team securely store the API key?

- A. Create a CodeCommit repository in the security account using AWS Key Management Service (AWS KMS) for encryption Require the development team to migrate the Lambda source code to this repository
- B. Store the API key in an Amazon S3 bucket in the security account using server-side encryption with Amazon S3 managed encryption keys (SSE-S3) to encrypt the key Create a signed URL for the S3 key
- C. and specify the URL in a Lambda environmental variable in the AWS CloudFormation template Update the Lambda function code to retrieve the key using the URL and call the API
- D. Create a secret in AWS Secrets Manager in the security account to store the API key using AWS Key Management Service (AWS KMS) for encryption Grant access to the IAM role used by the Lambda function so that the function can retrieve the key from Secrets Manager and call the API
- E. Create an encrypted environment variable for the Lambda function to store the API key using AWS Key Management Service (AWS KMS) for encryption Grant access to the IAM role used by the Lambda function so that the function can decrypt the key at runtime

Answer: C

NEW QUESTION 243

- (Exam Topic 3)

You need to create a Linux EC2 instance in AWS. Which of the following steps is used to ensure secure authentication the EC2 instance from a windows machine. Choose 2 answers from the options given below.

Please select:

- A. Ensure to create a strong password for logging into the EC2 Instance
- B. Create a key pair using putty
- C. Use the private key to log into the instance
- D. Ensure the password is passed securely using SSL

Answer: BC

Explanation:

The AWS Documentation mentions the following

You can use Amazon EC2 to create your key pair. Alternatively, you could use a third-party tool and then import the public key to Amazon EC2. Each key pair requires a name. Be sure to choose a name that is easy to remember. Amazon EC2 associates the public key with the name that you specify as the key name. Amazon EC2 stores the public key only, and you store the private key. Anyone who possesses your private key can decrypt login information, so it's important that you store your private keys in a secure place.

Options A and D are incorrect since you should use key pairs for secure access to Ec2 Instances For more information on EC2 key pairs, please refer to below URL: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html>

The correct answers are: Create a key pair using putty. Use the private key to log into the instance Submit your Feedback/Queries to our Experts

NEW QUESTION 248

- (Exam Topic 3)

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

Please select:

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

Answer: D

Explanation:

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

The following is an example of an S3 bucket policy that restricts access to a specific bucket, examplebucket only from the VPC endpoint with the ID vpce-1a2b3c4d. The policy denies all access to the bucket if the specified endpoint is not being used. The aws:sourceVpce condition is used to specify the endpoint. The aws:sourceVpce condition does not require an ARN for the VPC endpoint resource, only the VPC endpoint ID. For more information about using conditions in a policy, see Specifying Conditions in a Policy.

```
{
  "Version": "2012-10-17",
  "Id": "Policy1415115909152",
  "Statement": [
    {
      "Sid": "Access-to-specific-VPCE-only",
      "Principal": "*",
      "Action": "s3:*",
      "Effect": "Deny",
      "Resource": ["arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"],
      "Condition": {
        "StringNotEquals": {
          "aws:sourceVpce": "vpce-1a2b3c4d"
        }
      }
    }
  ]
}
```

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

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

Option C is incorrect because it is the bucket policy that needs to be changed and not the IAM policy.

For more information on example bucket policies for VPC endpoints, please refer to below URL:

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

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

NEW QUESTION 252

- (Exam Topic 3)

A user has enabled versioning on an S3 bucket. The user is using server side encryption for data at Rest. If the user is supplying his own keys for encryption SSE-C, which of the below mentioned statements is true?

Please select:

- A. The user should use the same encryption key for all versions of the same object
- B. It is possible to have different encryption keys for different versions of the same object
- C. AWS S3 does not allow the user to upload his own keys for server side encryption
- D. The SSE-C does not work when versioning is enabled

Answer: B

Explanation:

Managing your own encryption keys, you

You can encrypt the object and send it across to S3

Option A is invalid because ideally you should use different encryption keys Option C is invalid because you can use your own encryption keys Option D is invalid because encryption works even if versioning is enabled For more information on client side encryption please visit the below Link:

""Keys.html <https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingClientSideEncryption.html>

The correct answer is: It is possible to have different encryption keys for different versions of the same object Submit your Feedback/Queries to our Experts

NEW QUESTION 257

- (Exam Topic 3)

You need to ensure that the CloudTrail logs which are being delivered in your AWS account is encrypted. How can this be achieved in the easiest way possible?

Please select:

- A. Don't do anything since CloudTrail logs are automatically encrypted.
- B. Enable S3-SSE for the underlying bucket which receives the log files
- C. Enable S3-KMS for the underlying bucket which receives the log files
- D. Enable KMS encryption for the logs which are sent to Cloudwatch

Answer: A

Explanation:

The AWS Documentation mentions the following

By default the log files delivered by CloudTrail to your bucket are encrypted by Amazon server-side encryption with Amazon S3-managed encryption keys (SSE-S3)

Option B,C and D are all invalid because by default all logs are encrypted when they are sent by CloudTrail to S3 buckets

For more information on AWS CloudTrail log encryption, please visit the following URL: <https://docs.aws.amazon.com/awscloudtrail/latest/userguide/encrypting-cloudtrail-log-files-with-aws-kms.html> The correct answer is: Don't do anything since CloudTrail logs are automatically encrypted. Submit your

Feedback/Queries to our Experts

NEW QUESTION 261

- (Exam Topic 3)

Your company uses AWS to host its resources. They have the following requirements

- 1) Record all API calls and Transitions
- 2) Help in understanding what resources are there in the account
- 3) Facility to allow auditing credentials and logins Which services would suffice the above requirements Please select:

- A. AWS Inspector, CloudTrail, IAM Credential Reports
- B. CloudTrail
- C. IAM Credential Reports, AWS SNS
- D. CloudTrail, AWS Config, IAM Credential Reports
- E. AWS SQS, IAM Credential Reports, CloudTrail

Answer: C

Explanation:

You can use AWS CloudTrail to get a history of AWS API calls and related events for your account. This history includes calls made with the AWS Management Console, AWS Command Line Interface, AWS SDKs, and other AWS services.

Options A,B and D are invalid because you need to ensure that you use the services of CloudTrail, AWS Config, IAM Credential Reports

For more information on CloudTrail, please visit the below URL:

<http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html>

AWS Config is a service that enables you to assess, audit and evaluate the configurations of your AWS resources. Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. With Config, you can review changes in configurations and relationships between AWS resources, dive into detailed resource configuration histories, and determine your overall compliance against the configurations specified in your internal guidelines. This enables you to simplify compliance auditing, security analysis, change management and operational troubleshooting.

For more information on the config service, please visit the below URL <https://aws.amazon.com/config/>

You can generate and download a credential report that lists all users in your account and the status of their various credentials, including passwords, access keys, and MFA devices. You can get a credential report from the AWS Management Console, the AWS SDKs and Command Line Tools, or the IAM API.

For more information on Credentials Report, please visit the below URL: http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_getting-report.html

The correct answer is: CloudTrail, AWS Config, IAM Credential Reports Submit your Feedback/Queries to our Experts

NEW QUESTION 264

- (Exam Topic 3)

You are planning on using the AWS KMS service for managing keys for your application. For which of the following can the KMS CMK keys be used for encrypting? Choose 2 answers from the options given below

Please select:

- A. Image Objects
- B. Large files
- C. Password
- D. RSA Keys

Answer: CD

Explanation:

The CMK keys themselves can only be used for encrypting data that is maximum 4KB in size. Hence it can be used for encrypting information such as passwords and RSA keys.

Option A and B are invalid because the actual CMK key can only be used to encrypt small amounts of data and not large amount of data. You have to generate the data key from the CMK key in order to encrypt high amounts of data

For more information on the concepts for KMS, please visit the following URL: <https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html>

The correct answers are: Password, RSA Keys Submit your Feedback/Queries to our Experts

NEW QUESTION 268

- (Exam Topic 3)

Your company has a set of EC2 Instances defined in AWS. These EC2 Instances have strict security groups attached to them. You need to ensure that changes to the Security groups are noted and acted on accordingly. How can you achieve this?

Please select:

- A. Use Cloudwatch logs to monitor the activity on the Security Group
- B. Use filters to search for the changes and use SNS for the notification.
- C. Use Cloudwatch metrics to monitor the activity on the Security Group
- D. Use filters to search for the changes and use SNS for the notification.
- E. Use AWS inspector to monitor the activity on the Security Group
- F. Use filters to search for the changes and use SNS for the notification.
- G. Use Cloudwatch events to be triggered for any changes to the Security Group
- H. Configure the Lambda function for email notification as well.

Answer: D

Explanation:

The below diagram from an AWS blog shows how security groups can be monitored <C:\Users\wk\Desktop\mudassar\Untitled.jpg>



Option A is invalid because you need to use Cloudwatch Events to check for changes, Option B is invalid because you need to use Cloudwatch Events to check for changes

Option C is invalid because AWS inspector is not used to monitor the activity on Security Groups For more information on monitoring security groups, please visit the below URL:

<https://aws.amazon.com/blogs/security/how-to-automatically-revert-and-receive-notifications-about-changes-to-vpc-security-groups/>

The correct answer is: Use Cloudwatch events to be triggered for any changes to the Security Groups. Configure the Lambda function for email notification as well. Submit your Feedback/Queries to our Experts

NEW QUESTION 273

- (Exam Topic 3)

Your company looks at the gaming domain and hosts several EC2 Instances as game servers. The servers each experience user loads in the thousands. There is a concern of DDoS attacks on the EC2 Instances which could cause a huge revenue loss to the company. Which of the following can help mitigate this security concern and also ensure minimum downtime for the servers.

Please select:

- A. Use VPC Flow logs to monitor the VPC and then implement NACL's to mitigate attacks
- B. Use AWS Shield Advanced to protect the EC2 Instances
- C. Use AWS Inspector to protect the EC2 Instances
- D. Use AWS Trusted Advisor to protect the EC2 Instances

Answer: B

Explanation:

Below is an excerpt from the AWS Documentation on some of the use cases for AWS Shield C:\Users\wk\Desktop\mudassar\Untitled.jpg

Example AWS Shield Advanced Use Cases		
You can use Shield Advanced to protect your resources in many types of scenarios. However, in some cases you should use other services or combine other services with Shield Advanced to offer the best protection. Following are examples of how to use Shield Advanced or other AWS services to help protect your resources.		
Goal	Suggested services	Related service documentation
Protect a web application and RESTful APIs against a DDoS attack	Shield Advanced protecting an Amazon CloudFront distribution and an Application Load Balancer	Amazon Elastic Load Balancing Documentation , Amazon CloudFront Documentation
Protect a TCP-based application against a DDoS attack	Shield Advanced protecting a Network Load Balancer attached to an Elastic IP address	Amazon Elastic Load Balancing Documentation
Protect a UDP-based game server against a DDoS attack	Shield Advanced protecting an Amazon EC2 instance attached to an Elastic IP address	Amazon Elastic Compute Cloud Documentation

NEW QUESTION 276

- (Exam Topic 3)

A Security Engineer receives alerts that an Amazon EC2 instance on a public subnet is under an SFTP brute force attack from a specific IP address, which is a known malicious bot. What should the Security Engineer do to block the malicious bot?

- A. Add a deny rule to the public VPC security group to block the malicious IP
- B. Add the malicious IP to AWS WAF backhsted IPs
- C. Configure Linux iptables or Windows Firewall to block any traffic from the malicious IP
- D. Modify the hosted zone in Amazon Route 53 and create a DNS sinkhole for the malicious IP

Answer: D

NEW QUESTION 280

- (Exam Topic 3)

A company continually generates sensitive records that it stores in an S3 bucket. All objects in the bucket are encrypted using SSE-KMS using one of the company's CMKs. Company compliance policies require that no more than one month of data be encrypted using the same encryption key. What solution below will meet the company's requirements?

Please select:

- A. Trigger a Lambda function with a monthly CloudWatch event that creates a new CMK and updates the S3 bucket to use the new CMK.
- B. Configure the CMK to rotate the key material every month.
- C. Trigger a Lambda function with a monthly CloudWatch event that creates a new CMK, updates the S3 bucket to use thfl new CMK, and deletes the old CMK.
- D. Trigger a Lambda function with a monthly CloudWatch event that rotates the key material in the CMK.

Answer: A

Explanation:

You can use a Lambda function to create a new key and then update the S3 bucket to use the new key. Remember not to delete the old key, else you will not be able to decrypt the documents stored in the S3 bucket using the older key.

Option B is incorrect because AWS KMS cannot rotate keys on a monthly basis

Option C is incorrect because deleting the old key means that you cannot access the older objects Option D is incorrect because rotating key material is not possible.

For more information on AWS KMS keys, please refer to below URL: <https://docs.aws.amazon.com/kms/latest/developereuide/concepts.html>

The correct answer is: Trigger a Lambda function with a monthly CloudWatch event that creates a new CMK and updates the S3 bucket to use the new CMK.

Submit your Feedback/Queries to our Experts

NEW QUESTION 284

- (Exam Topic 3)

You are building a system to distribute confidential training videos to employees. Using CloudFront, what method could be used to serve content that is stored in S3, but not publicly accessible from S3 directly?

Please select:

- A. Create an Origin Access Identity (OAI) for CloudFront and grant access to the objects in your S3 bucket to that OAI.
- B. Add the CloudFront account security group "amazon-cf/amazon-cf-sg" to the appropriate S3 bucket policy.
- C. Create an Identity and Access Management (IAM) User for CloudFront and grant access to the objects in your S3 bucket to that IAM User.
- D. Create a S3 bucket policy that lists the CloudFront distribution ID as the Principal and the target bucket as the Amazon Resource Name (ARN).

Answer: A

Explanation:

You can optionally secure the content in your Amazon S3 bucket so users can access it through CloudFront but cannot access it directly by using Amazon S3 URLs. This prevents anyone from bypassing CloudFront and using the Amazon S3 URL to get content that you want to restrict access to. This step isn't required to use signed URLs, but we recommend it

To require that users access your content through CloudFront URLs, you perform the following tasks: Create a special CloudFront user called an origin access identity.

Give the origin access identity permission to read the objects in your bucket. Remove permission for anyone else to use Amazon S3 URLs to read the objects.

Option B,C and D are all automatically invalid, because the right way is to ensure to create Origin Access Identity (OAI) for CloudFront and grant access accordingly.

For more information on serving private content via Cloudfront, please visit the following URL:

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

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

You can optionally secure the content in your Amazon S3 bucket so users can access it through CloudFront but cannot access it directly by using Amazon S3 URLs. This prevents anyone from bypassing CloudFront and using the Amazon S3 URL to get content that you want to restrict access to. This step isn't required to use signed URLs, but we recommend it

To require that users access your content through CloudFront URLs, you perform the following tasks: Create a special CloudFront user called an origin access identity.

Give the origin access identity permission to read the objects in your bucket. Remove permission for anyone else to use Amazon S3 URLs to read the objects. Option B,C and D are all automatically invalid, because the right way is to ensure to create Origin Access Identity (OAI) for CloudFront and grant access accordingly.

For more information on serving private content via Cloudfront, please visit the following URL:

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

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

Submit your Feedback/Queries to our Experts Submit your Feedback/Queries to our Experts

NEW QUESTION 288

- (Exam Topic 3)

A company's application team wants to replace an internal application with a new AWS architecture that consists of Amazon EC2 instances, an AWS Lambda function, and an Amazon S3 bucket in a single AWS Region. After an architecture review, the security team mandates that no application network traffic can traverse the public internet at any point. The security team already has an SCP in place for the company's organization in AWS Organizations to restrict the creation of internet gateways, NAT gateways, and egress-only gateways.

Which combination of steps should the application team take to meet these requirements? (Select THREE.)

- A. Create an S3 endpoint that has a full-access policy for the application's VPC.
- B. Create an S3 access point for the S3 bucket
- C. Include a policy that restricts the network origin to VPCs.
- D. Launch the Lambda function
- E. Enable the block public access configuration.
- F. Create a security group that has an outbound rule over port 443 with a destination of the S3 endpoint. Associate the security group with the EC2 instances.
- G. Create a security group that has an outbound rule over port 443 with a destination of the S3 access point. Associate the security group with the EC2 instances.
- H. Launch the Lambda function in a VPC.

Answer: ADF

NEW QUESTION 293

- (Exam Topic 3)

Your company has mandated that all data in AWS be encrypted at rest. How can you achieve this for EBS volumes? Choose 2 answers from the options given below

Please select:

- A. Use Windows bit locker for EBS volumes on Windows instances
- B. Use TrueEncrypt for EBS volumes on Linux instances
- C. Use AWS Systems Manager to encrypt the existing EBS volumes
- D. Boot EBS volume can be encrypted during launch without using custom AMI

Answer: AB

Explanation:

EBS encryption can also be enabled when the volume is created and not for existing volumes. One can use existing tools for OS level encryption.

Option C is incorrect.

AWS Systems Manager is a management service that helps you automatically collect software inventory, apply OS patches, create system images, and configure Windows and Linux operating systems.

Option D is incorrect

You cannot choose to encrypt a non-encrypted boot volume on instance launch. To have encrypted boot volumes during launch, your custom AMI must have its boot volume encrypted before launch.

For more information on the Security Best practices, please visit the following URL: [com/whit Security Practices](https://aws.amazon.com/whit).

The correct answers are: Use Windows bit locker for EBS volumes on Windows instances. Use TrueEncrypt for EBS volumes on Linux instances

Submit your Feedback/Queries to our Experts

NEW QUESTION 298

- (Exam Topic 3)

A company is hosting multiple applications within a single VPC in its AWS account. The applications are running behind an Application Load Balancer that is associated with an AWS WAF web ACL. The company's security team has identified that multiple port scans are originating from a specific range of IP addresses on the internet.

A security engineer needs to deny access from the offending IP addresses. Which solution will meet these requirements?

- A. Modify the AWS WAF web ACL with an IP set match rule statement to deny incoming requests from the IP address range.
- B. Add a rule to all security groups to deny the incoming requests from the IP address range.
- C. Modify the AWS WAF web ACL with a rate-based rule statement to deny the incoming requests from the IP address range.
- D. Configure the AWS WAF web ACL with regex match condition
- E. Specify a pattern set to deny the incoming requests based on the match condition

Answer: D

NEW QUESTION 301

- (Exam Topic 3)

An EC2 Instance hosts a Java based application that accesses a DynamoDB table. This EC2 Instance is currently serving production based users. Which of the following is a secure way of ensuring that the EC2 Instance accesses the Dynamo table

Please select:

- A. Use IAM Roles with permissions to interact with DynamoDB and assign it to the EC2 Instance
- B. Use KMS keys with the right permissions to interact with DynamoDB and assign it to the EC2 Instance
- C. Use IAM Access Keys with the right permissions to interact with DynamoDB and assign it to the EC2 Instance
- D. Use IAM Access Groups with the right permissions to interact with DynamoDB and assign it to the EC2 Instance

Answer: A

Explanation:

To always ensure secure access to AWS resources from EC2 Instances, always ensure to assign a Role to the EC2 Instance Option B is invalid because KMS keys are not used as a mechanism for providing EC2 Instances access to AWS services. Option C is invalid Access keys is not a safe mechanism for providing EC2 Instances access to AWS services. Option D is invalid because there is no way access groups can be assigned to EC2 Instances. For more information on IAM Roles, please refer to the below URL:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html

The correct answer is: Use IAM Roles with permissions to interact with DynamoDB and assign it to the EC2 Instance Submit your Feedback/Queries to our Experts

NEW QUESTION 306

- (Exam Topic 3)

A company is building an application on AWS that will store sensitive Information. The company has a support team with access to the IT infrastructure, including databases. The company's security engineer must introduce measures to protect the sensitive data against any data breach while minimizing management overhead. The credentials must be regularly rotated.

What should the security engineer recommend?

- A. Enable Amazon RDS encryption to encrypt the database and snapshot
- B. Enable Amazon Elastic Block Store (Amazon EBS) encryption on Amazon EC2 instance
- C. Include the database credential in the EC2 user data field
- D. Use an AWS Lambda function to rotate database credential
- E. Set up TLS for the connection to the database.
- F. Install a database on an Amazon EC2 Instance
- G. Enable third-party disk encryption to encrypt the Amazon Elastic Block Store (Amazon EBS) volume
- H. Store the database credentials in AWS CloudHSM with automatic rotation
- I. Set up TLS for the connection to the database.
- J. Enable Amazon RDS encryption to encrypt the database and snapshot
- K. Enable Amazon Elastic Block Store (Amazon EBS) encryption on Amazon EC2 instance
- L. Store the database credentials in AWS Secrets Manager with automatic rotation
- M. Set up TLS for the connection to the RDS hosted database.
- N. Set up an AWS CloudHSM cluster with AWS Key Management Service (AWS KMS) to store KMS key
- O. Set up Amazon RDS encryption using AWS KMS to encrypt the database
- P. Store database credentials in the AWS Systems Manager Parameter Store with automatic rotation
- Q. Set up TLS for the connection to the RDS hosted database.

Answer: C

NEW QUESTION 308

.....

Relate Links

100% Pass Your AWS-Certified-Security-Specialty Exam with Exambible Prep Materials

<https://www.exambible.com/AWS-Certified-Security-Specialty-exam/>

Contact us

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

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