

SCS-C01 Dumps

AWS Certified Security- Specialty

<https://www.certleader.com/SCS-C01-dumps.html>



NEW QUESTION 1

A Security Engineer has been asked to create an automated process to disable IAM user access keys that are more than three months old. Which of the following options should the Security Engineer use?

- A. In the AWS Console, choose the IAM service and select “Users”. Review the “Access Key Age” column.
- B. Define an IAM policy that denies access if the key age is more than three months and apply to all users.
- C. Write a script that uses the GenerateCredentialReport, GetCredentialReport, and UpdateAccessKey APIs.
- D. Create an Amazon CloudWatch alarm to detect aged access keys and use an AWS Lambda function to disable the keys older than 90 days.

Answer: C

NEW QUESTION 2

An application uses Amazon Cognito to manage end users’ permissions when directly accessing AWS resources, including Amazon DynamoDB. A new feature request reads as follows:

Provide a mechanism to mark customers as suspended pending investigation or suspended permanently. Customers should still be able to log in when suspended, but should not be able to make changes.

The priorities are to reduce complexity and avoid potential for future security issues. Which approach will meet these requirements and priorities?

- A. Create a new database field “suspended_status” and modify the application logic to validate that field when processing requests.
- B. Add suspended customers to second Cognito user pool and update the application login flow to check both user pools.
- C. Use Amazon Cognito Sync to push out a “suspension_status” parameter and split the IAM policy into normal users and suspended users.
- D. Move suspended customers to a second Cognito group and define an appropriate IAM access policy for the group.

Answer: D

NEW QUESTION 3

A company has a customer master key (CMK) with imported key materials. Company policy requires that all encryption keys must be rotated every year. What can be done to implement the above policy?

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

Answer: D

NEW QUESTION 4

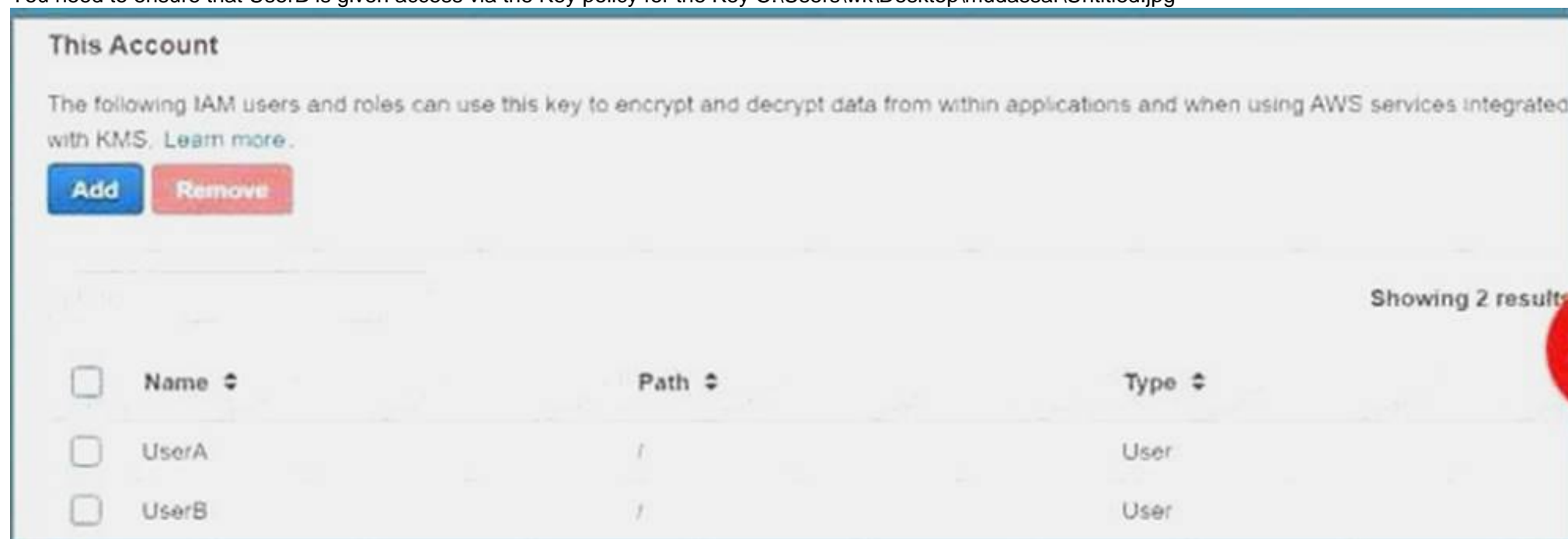
Your developer is using the KMS service and an assigned key in their Java program. They get the below error when running the code
arn:aws:iam::113745388712:user/UserB is not authorized to perform: kms:DescribeKey Which of the following could help resolve the issue?
Please select:

- A. Ensure that UserB is given the right IAM role to access the key
- B. Ensure that UserB is given the right permissions in the IAM policy
- C. Ensure that UserB is given the right permissions in the Key policy
- D. Ensure that UserB is given the right permissions in the Bucket policy

Answer: C

Explanation:

You need to ensure that UserB is given access via the Key policy for the Key C:\Users\wk\Desktop\mudassar\Untitled.jpg



Option is invalid because you don't assign roles to IAM users

For more information on Key policies please visit the below Link: <https://docs.aws.amazon.com/kms/latest/developerguide/key-poli>

The correct answer is: Ensure that UserB is given the right permissions in the Key policy

NEW QUESTION 5

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

Please select:

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

Answer: ACD

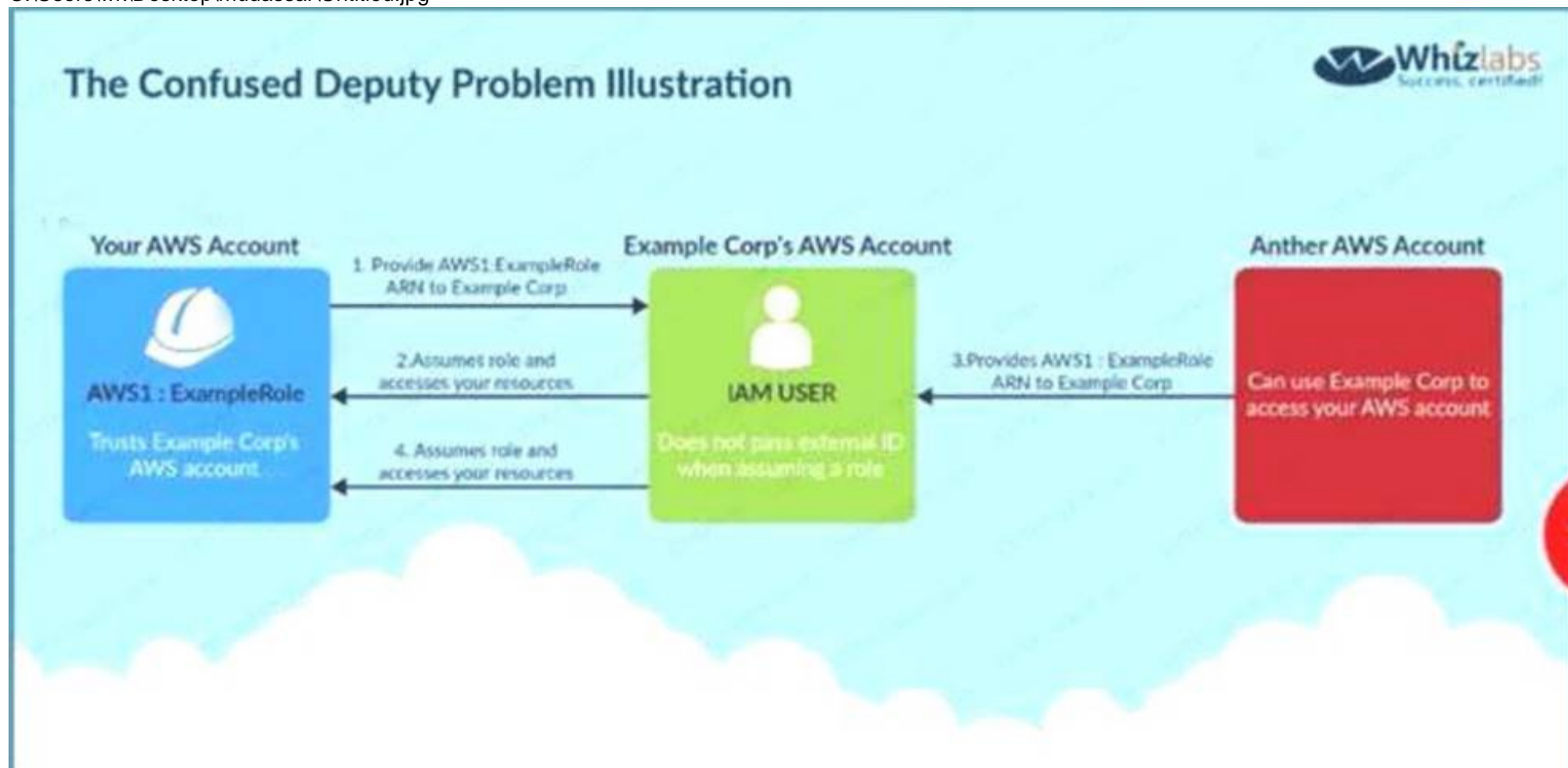
Explanation:

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

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

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

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



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

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

Submit your Feedback/Queries to our Experts

NEW QUESTION 6

A Development team has asked for help configuring the IAM roles and policies in a new AWS account. The team using the account expects to have hundreds of master keys and therefore does not want to manage access control for customer master keys (CMKs).

Which of the following will allow the team to manage AWS KMS permissions in IAM without the complexity of editing individual key policies?

- A. The account's CMK key policy must allow the account's IAM roles to perform KMS EnableKey.
- B. Newly created CMKs must have a key policy that allows the root principal to perform all actions.
- C. Newly created CMKs must allow the root principal to perform the kms CreateGrant API operation.
- D. Newly created CMKs must mirror the IAM policy of the KMS key administrator.

Answer: C

NEW QUESTION 7

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

Please select:

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

Answer: B

Explanation:

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

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

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

The AWS Documentation mentions the following

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

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

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

NEW QUESTION 8

Your company is planning on using AWS EC2 and ELB for deployment for their web applications. The security policy mandates that all traffic should be encrypted. Which of the following options will ensure that this requirement is met. Choose 2 answers from the options below.

Please select:

- A. Ensure the load balancer listens on port 80
- B. Ensure the load balancer listens on port 443
- C. Ensure the HTTPS listener sends requests to the instances on port 443
- D. Ensure the HTTPS listener sends requests to the instances on port 80

Answer: BC

Explanation:

The AWS Documentation mentions the following

You can create a load balancer that listens on both the HTTP (80) and HTTPS (443) ports. If you specify that the HTTPS listener sends requests to the instances on port 80, the load balancer terminates the requests and communication from the load balancer to the instances is not encrypted, if the HTTPS listener sends requests to the instances on port 443, communication from the load balancer to the instances is encrypted.

Option A is invalid because there is a need for secure traffic, so port 80 should not be used Option D is invalid because for the HTTPS listener you need to use port 443

For more information on HTTPS with ELB, please refer to the below Link: <https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-create-https-ssl-load-balancer.html>

The correct answers are: Ensure the load balancer listens on port 443, Ensure the HTTPS listener sends requests to the instances on port 443

Submit your Feedback/Queries to our Experts

NEW QUESTION 9

A distributed web application is installed across several EC2 instances in public subnets residing in two Availability Zones. Apache logs show several intermittent brute-force attacks from hundreds of IP addresses at the layer 7 level over the past six months.

What would be the BEST way to reduce the potential impact of these attacks in the future?

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

Answer: C

NEW QUESTION 10

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

Please select:

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

Answer: BD

Explanation:

The AWS Documentation mentions the following on AWS Inspector

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

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

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

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

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

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

NEW QUESTION 10

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

Which of the following solutions will meet these requirements?

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

Answer: B

NEW QUESTION 13

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 16

You have a set of 100 EC2 Instances in an AWS account. You need to ensure that all of these instances are patched and kept to date. All of the instances are in a private subnet. How can you achieve this. Choose 2 answers from the options given below

Please select:

- A. Ensure a NAT gateway is present to download the updates
- B. Use the Systems Manager to patch the instances
- C. Ensure an internet gateway is present to download the updates
- D. Use the AWS inspector to patch the updates

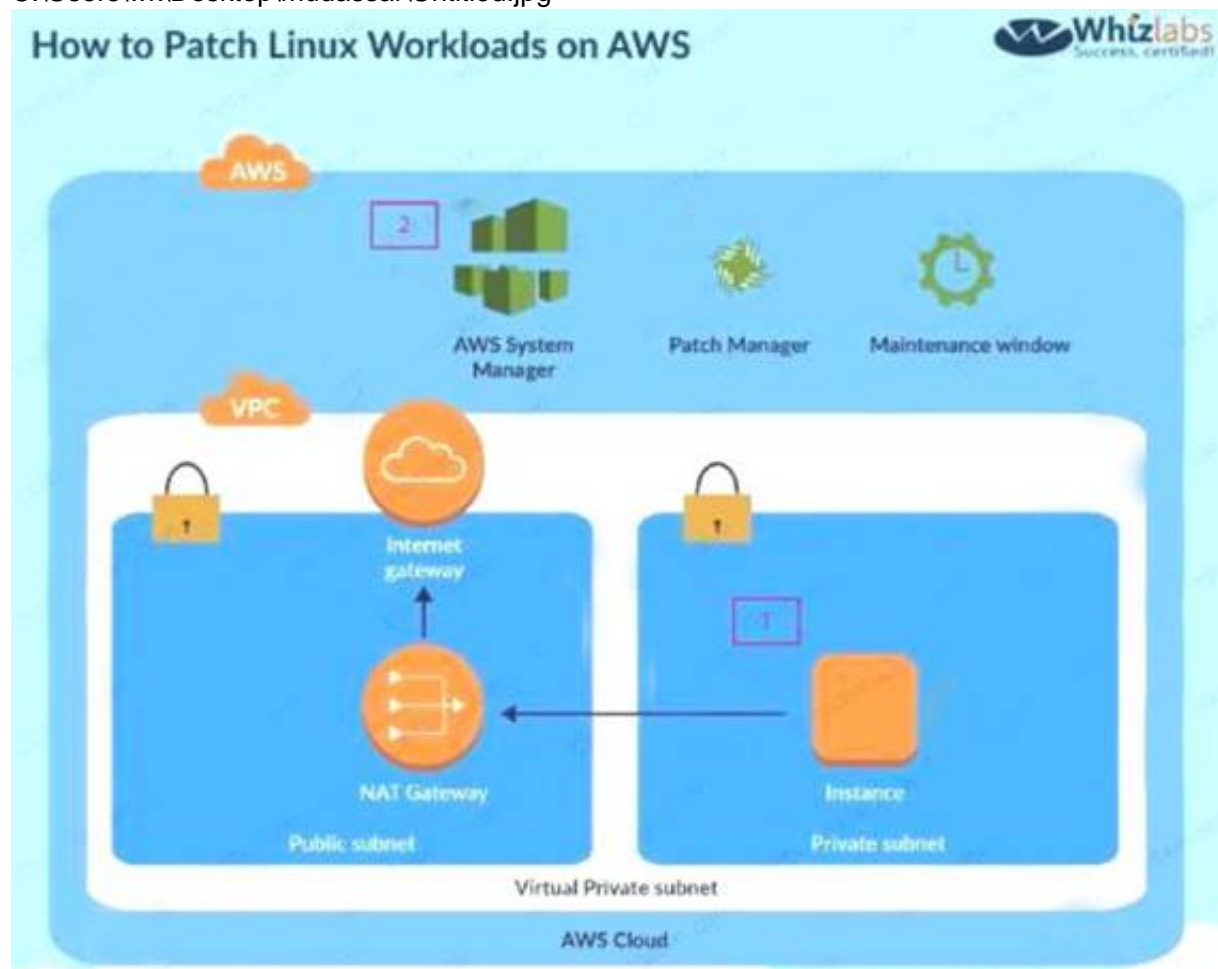
Answer: AB

Explanation:

Option C is invalid because the instances need to remain in the private: Option D is invalid because AWS inspector can only detect the patches

One of the AWS Blogs mentions how patching of Linux servers can be accomplished. Below is the diagram representation of the architecture setup

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



For more information on patching Linux workloads in AWS, please refer to the Lin. <https://aws.amazon.com/blogs/security/how-to-patch-linux-workloads-on-aws/>

The correct answers are: Ensure a NAT gateway is present to download the updates. Use the Systems Manager to patch the instances

Submit your Feedback/Queries to our Experts

NEW QUESTION 17

You are devising a policy to allow users to have the ability to access objects in a bucket called appbucket. You define the below custom bucket policy

```
{ "ID": "Policy1502987489630",  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "Stmt1502987487640",  
      "Action": [  
        "s3:GetObject",  
        "s3:GetObjectVersion"  
      ],  
      "Effect": "Allow",  
      "Resource": "arn:aws:s3:::appbucket",  
      "Principal": "*"   
    }  
  ]  
}
```

But when you try to apply the policy you get the error "Action does not apply to any resource(s) in statement." What should be done to rectify the error Please select:

- A. Change the 1AM permissions by applying PutBucketPolicy permissions.
- B. Verify that the policy has the same name as the bucket nam
- C. If no
- D. make it the same.
- E. Change the Resource section to "arn:aws:s3:::appbucket/*".
- F. Create the bucket "appbucket" and then apply the policy.

Answer: C

Explanation:

When you define access to objects in a bucket you need to ensure that you specify to which objects in the bucket access needs to be given to. In this case, the * can be used to assign the permission to all objects in the bucket

Option A is invalid because the right permissions are already provided as per the question requirement Option B is invalid because it is not necessary that the policy has the same name as the bucket

Option D is invalid because this should be the default flow for applying the policy For more information on bucket policies please visit the below URL:

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

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

NEW QUESTION 21

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

- Storage is accessible by using only VPCs.
- Service has tamper-evident controls.
- Access logging is enabled.
- Storage has high availability.

Which of the following services meets these requirements?

- A. Amazon S3 with default encryption
- B. AWS CloudHSM
- C. Amazon DynamoDB with server-side encryption
- D. AWS Systems Manager Parameter Store

Answer: B

NEW QUESTION 26

An application running on EC2 instances in a VPC must call an external web service via TLS (port 443). The instances run in public subnets.

Which configurations below allow the application to function and minimize the exposure of the instances? Select 2 answers from the options given below

Please select:

- A. A network ACL with a rule that allows outgoing traffic on port 443.
- B. A network ACL with rules that allow outgoing traffic on port 443 and incoming traffic on ephemeral ports
- C. A network ACL with rules that allow outgoing traffic on port 443 and incoming traffic on port 443.
- D. A security group with a rule that allows outgoing traffic on port 443
- E. A security group with rules that allow outgoing traffic on port 443 and incoming traffic on ephemeralports.
- F. A security group with rules that allow outgoing traffic on port 443 and incoming traffic on port 443.

Answer: BD

Explanation:

Since here the traffic needs to flow outbound from the Instance to a web service on Port 443, the outbound rules on both the Network and Security Groups need to allow outbound traffic. The Incoming traffic should be allowed on ephemeral ports for the Operating System on the Instance to allow a connection to be established on any desired or available port.

Option A is invalid because this rule alone is not enough. You also need to ensure incoming traffic on ephemeral ports

Option C is invalid because need to ensure incoming traffic on ephemeral ports and not only port 443 Option E and F are invalid since here you are allowing additional ports on Security groups which are not required

For more information on VPC Security Groups, please visit the below URL:

https://docs.aws.amazon.com/AmazonVPC/latest/UserGuideA/PC_SecurityGroups.html

The correct answers are: A network ACL with rules that allow outgoing traffic on port 443 and incoming traffic on ephemeral ports, A security group with a rule that allows outgoing traffic on port 443

Submit your Feedback/Queries to our Experts

NEW QUESTION 31

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

NEW QUESTION 32

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

Please select:

- A. Check to see if the right role has been assigned to the EC2 instances
- B. Check to see if the 1AM user has the right permissions for EC2
- C. Ensure that agent is running on the instances.
- D. Check the Instance status by using the Health API.

Answer: ACD

Explanation:

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

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

The operating system

The version of the EC2Config service (Windows) The status of the EC2Config service (Windows)

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

<https://docs.aws.amazon.com/systems-manager/latest/userguide/troubleshooting-remote-commands.html>

The correct answers are: Check to see if the right role has been assigned to the EC2 Instances, Ensure that agent is running on the Instances., Check the Instance status by using the Health API.

Submit your Feedback/Queries to our Experts

NEW QUESTION 37

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

NEW QUESTION 41

Your company has a set of 1000 EC2 Instances defined in an AWS Account. They want to effectively automate several administrative tasks on these instances. Which of the following would be an effective way to achieve this?

Please select:

- A. Use the AWS Systems Manager Parameter Store
- B. Use the AWS Systems Manager Run Command
- C. Use the AWS Inspector
- D. Use AWS Config

Answer: B

Explanation:

The AWS Documentation mentions the following

AWS Systems Manager Run Command lets you remotely and securely manage the configuration of your managed instances. A managed instance is any Amazon EC2 instance or on-premises machine in your hybrid environment that has been configured for Systems Manager. Run Command enables you to automate common administrative tasks and perform ad hoc configuration changes at scale. You can use Run Command from the AWS console, the AWS Command Line Interface, AWS Tools for Windows PowerShell, or the AWS SDKs. Run Command is offered at no additional cost.

Option A is invalid because this service is used to store parameter Option C is invalid because this service is used to scan vulnerabilities in an EC2 Instance.

Option D is invalid because this service is used to check for configuration changes For more information on executing remote commands, please visit the below U

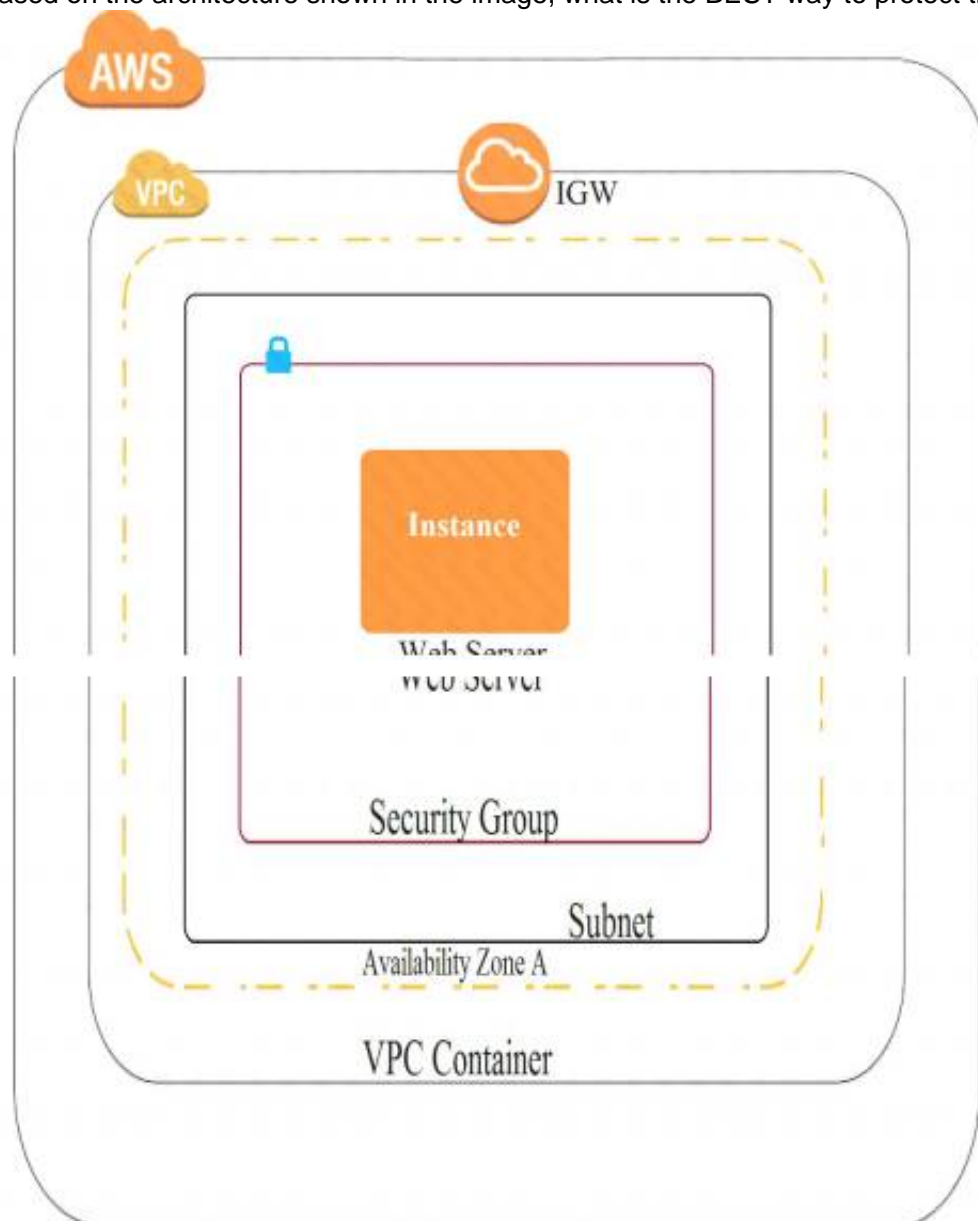
<https://docs.aws.amazon.com/systems-manageer/latest/userguide/execute-remote-commands.html> (

The correct answer is: Use the AWS Systems Manager Run Command Submit your Feedback/Queries to our Experts

NEW QUESTION 42

A company recently experienced a DDoS attack that prevented its web server from serving content. The website is static and hosts only HTML, CSS, and PDF files that users download.

Based on the architecture shown in the image, what is the BEST way to protect the site against future attacks while minimizing the ongoing operational overhead?

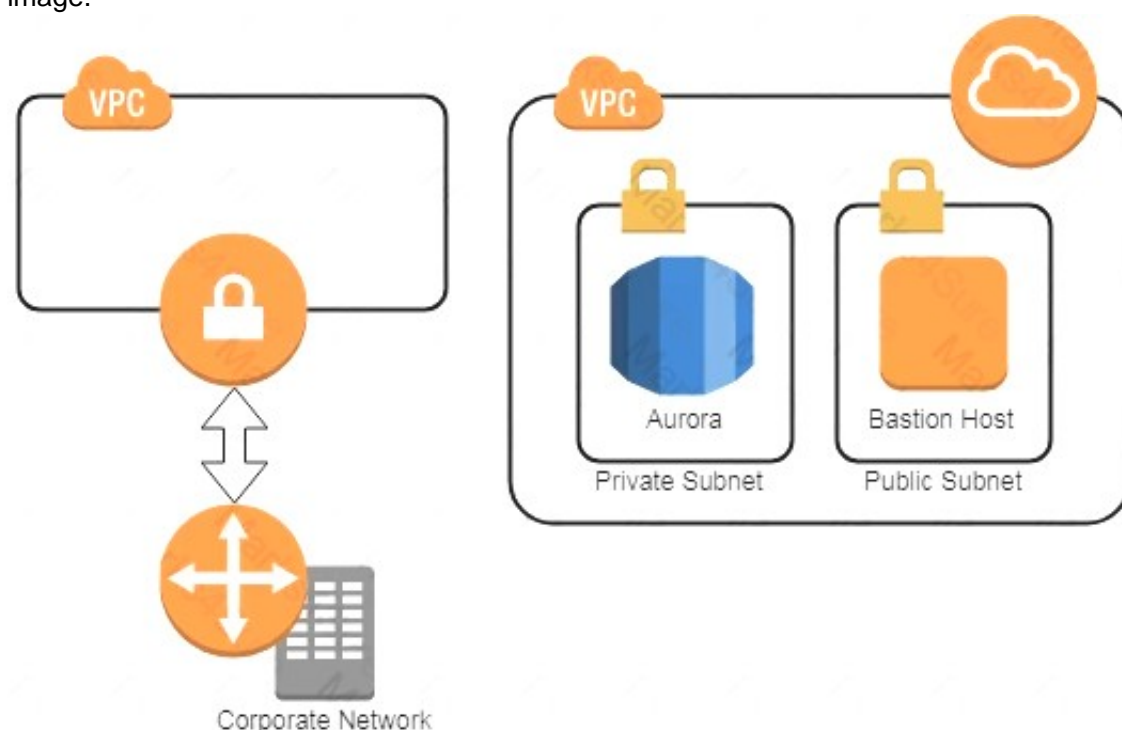


- A. Move all the files to an Amazon S3 bucket
- B. Have the web server serve the files from the S3 bucket.
- C. Launch a second Amazon EC2 instance in a new subne
- D. Launch an Application Load Balancer in front of both instances.
- E. Launch an Application Load Balancer in front of the EC2 instanc
- F. Create an Amazon CloudFront distribution in front of the Application Load Balancer.
- G. Move all the files to an Amazon S3 bucke
- H. Create a CloudFront distribution in front of the bucket and terminate the web server.

Answer: D

NEW QUESTION 47

A company has two AWS accounts, each containing one VPC. The first VPC has a VPN connection with its corporate network. The second VPC, without a VPN, hosts an Amazon Aurora database cluster in private subnets. Developers manage the Aurora database from a bastion host in a public subnet as shown in the image.



A security review has flagged this architecture as vulnerable, and a Security Engineer has been asked to make this design more secure. The company has a short deadline and a second VPN connection to the Aurora account is not possible. How can a Security Engineer securely set up the bastion host?

- A. Move the bastion host to the VPC with VPN connectivity
- B. Create a VPC peering relationship between the bastion host VPC and Aurora VPC.
- C. Create a SSH port forwarding tunnel on the Developer's workstation to the bastion host to ensure that only authorized SSH clients can access the bastion host.
- D. Move the bastion host to the VPC with VPN connectivity
- E. Create a cross-account trust relationship between the bastion VPC and Aurora VPC, and update the Aurora security group for the relationship.
- F. Create an AWS Direct Connect connection between the corporate network and the Aurora account, and adjust the Aurora security group for this connection.

Answer: C

NEW QUESTION 51

A company has a set of EC2 instances hosted in AWS. These instances have EBS volumes for storing critical information. There is a business continuity requirement and in order to boost the agility of the business and to ensure data durability which of the following options are not required. Please select:

- A. Use lifecycle policies for the EBS volumes
- B. Use EBS Snapshots
- C. Use EBS volume replication
- D. Use EBS volume encryption

Answer: CD

Explanation:

Data stored in Amazon EBS volumes is redundantly stored in multiple physical locations as part of normal operation of those services and at no additional charge. However, Amazon EBS replication is stored within the same availability zone, not across multiple zones; therefore, it is highly recommended that you conduct regular snapshots to Amazon S3 for long-term data durability.

You can use Amazon Data Lifecycle Manager (Amazon DLM) to automate the creation, retention, and deletion of snapshots taken to back up your Amazon EBS volumes.

With lifecycle management, you can be sure that snapshots are cleaned up regularly and keep costs under control.

EBS Lifecycle Policies

A lifecycle policy consists of these core settings:

- Resource type—The AWS resource managed by the policy, in this case, EBS volumes.
- Target tag—The tag that must be associated with an EBS volume for it to be managed by the policy.
- Schedule—Defines how often to create snapshots and the maximum number of snapshots to keep. Snapshot creation starts within an hour of the specified start time. If creating a new snapshot exceeds the maximum number of snapshots to keep for the volume, the oldest snapshot is deleted.

Option C is correct. Each Amazon EBS volume is automatically replicated within its Availability Zone to protect you from component failure, offering high availability and durability. But it does not have an explicit feature like that.

Option D is correct Encryption does not ensure data durability

For information on security for Compute Resources, please visit the below URL <https://d1.awsstatic.com/whitepapers/Security/Security Compute Services Whitepaper.pdf>

The correct answers are: Use EBS volume replication. Use EBS volume encryption Submit your Feedback/Queries to our Experts

NEW QUESTION 55

An IAM user with full EC2 permissions could not start an Amazon EC2 instance after it was stopped for a maintenance task. Upon starting the instance, the instance state would change to "Pending", but after a few seconds, it would switch back to "Stopped".

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

The IAM user policy is as follows:

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

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

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

Answer: CE

NEW QUESTION 56

A company's database developer has just migrated an Amazon RDS database credential to be stored and managed by AWS Secrets Manager. The developer

has also enabled rotation of the credential within the Secrets Manager console and set the rotation to change every 30 days. After a short period of time, a number of existing applications have failed with authentication errors. What is the MOST likely cause of the authentication errors?

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

Answer: B

NEW QUESTION 60

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:

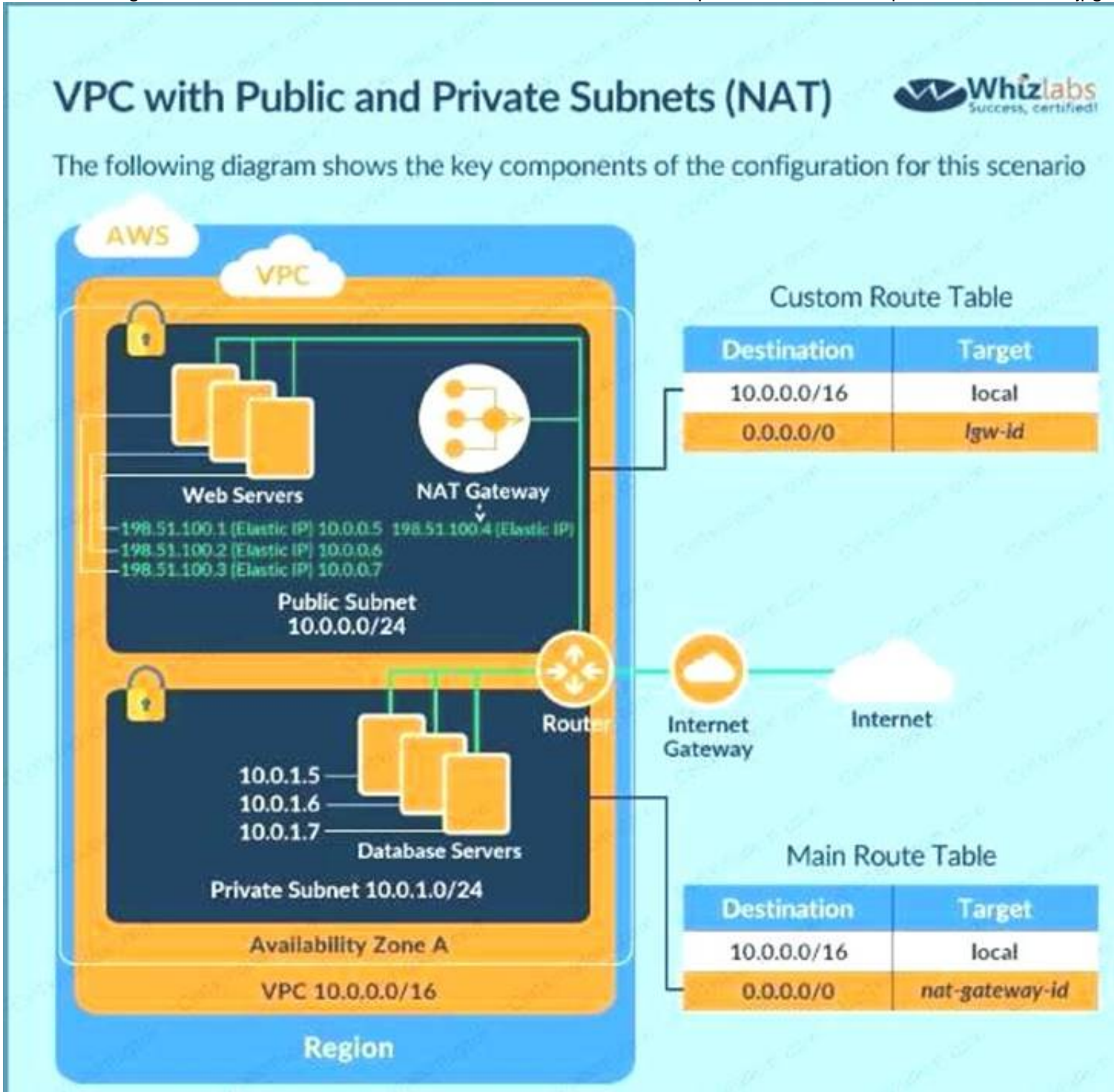
- A. Consider moving the web server to a private subnet
- B. Consider moving the database server to a private subnet
- C. Consider moving both the web and database server to a private subnet
- D. Consider creating a private subnet and adding a NAT instance to that subnet

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 61

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: ABC

NEW QUESTION 63

Your team is designing a web application. The users for this web application would need to sign in via an external ID provider such as Facebook or Google. Which of the following AWS service would you use for authentication?

Please select:

- A. AWS Cognito
- B. AWS SAML
- C. AWS IAM
- D. AWS Config

Answer: A

Explanation:

The AWS Documentation mentions the following

Amazon Cognito provides authentication, authorization, and user management for your web and mobile apps. Your users can sign in directly with a user name and password, or through a third party such as Facebook, Amazon, or Google.

Option B is incorrect since this is used for identity federation

Option C is incorrect since this is pure Identity and Access management Option D is incorrect since AWS is a configuration service

For more information on AWS Cognito please refer to the below Link: <https://docs.aws.amazon.com/cognito/latest/developerguide/what-is-amazon-cognito.html>

The correct answer is: AWS Cognito

Submit your Feedback/Queries to our Experts

NEW QUESTION 67

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

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

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

Answer: CDE

NEW QUESTION 69

You need to establish a secure backup and archiving solution for your company, using AWS. Documents should be immediately accessible for three months and available for five years for compliance reasons. Which AWS service fulfills these requirements in the most cost-effective way? Choose the correct answer

Please select:

- A. Upload data to S3 and use lifecycle policies to move the data into Glacier for long-term archiving.
- B. Upload the data on EBS, use lifecycle policies to move EBS snapshots into S3 and later into Glacier for long-term archiving.
- C. Use Direct Connect to upload data to S3 and use IAM policies to move the data into Glacier for long-term archiving.
- D. Use Storage Gateway to store data to S3 and use lifecycle policies to move the data into Redshift for long-term archiving.

Answer: A

Explanation:

Amazon Glacier is a secure, durable, and extremely low-cost cloud storage service for data archiving and long-term backup. Customers can reliably store large or small amounts of data for as little as \$0,004 per gigabyte per month, a significant savings compared to on-premises solutions.

With Amazon lifecycle policies you can create transition actions in which you define when objects transition to another Amazon S3 storage class. For example, you may choose to transition objects to the STANDARD_IA (IA, for infrequent access) storage class 30 days after creation, or archive objects to the GLACIER storage class one year after creation.

Option B is invalid because lifecycle policies are not available for EBS volumes Option C is invalid because IAM policies cannot be used to move data to Glacier

Option D is invalid because lifecycle policies are not used to move data to Redshift For more information on S3 lifecycle policies, please visit the URL:

<http://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html>

The correct answer is: Upload data to S3 and use lifecycle policies to move the data into Glacier for long-term archiving.

Submit your Feedback/Queries to our Experts

NEW QUESTION 71

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

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

Answer: A

NEW QUESTION 75

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

Please select:

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

Answer: BD

Explanation:

The AWS Documentation mentions the following

All AWS accounts have root user credentials (that is, the credentials of the account owner). These credentials allow full access to all resources in the account.

Because you can't restrict permissions for root user credentials, we recommend that you delete your root user access keys. Then create AWS Identity and Access Management (IAM) user credentials for everyday interaction with AWS.

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

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

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

NEW QUESTION 76

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 80

An application running on EC2 instances in a VPC must access sensitive data in the data center. The access must be encrypted in transit and have consistent low latency. Which hybrid architecture will meet these requirements?

Please select:

- A. Expose the data with a public HTTPS endpoint.
- B. A VPN between the VPC and the data center over a Direct Connect connection
- C. A VPN between the VPC and the data center.
- D. A Direct Connect connection between the VPC and data center

Answer: B

Explanation:

Since this is required over a consistency low latency connection, you should use Direct Connect. For encryption, you can make use of a VPN

Option A is invalid because exposing an HTTPS endpoint will not help all traffic to flow between a VPC and the data center.

Option C is invalid because low latency is a key requirement Option D is invalid because only Direct Connect will not suffice

For more information on the connection options please see the below Link: <https://aws.amazon.com/answers/networking/aws-multiple-vpc-vpn-connection-sharint>

The correct answer is: A VPN between the VPC and the data center over a Direct Connect connection Submit your Feedback/Queries to our Experts

NEW QUESTION 84

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 85

A Security Engineer must implement mutually authenticated TLS connections between containers that communicate inside a VPC.

Which solution would be MOST secure and easy to maintain?

- A. Use AWS Certificate Manager to generate certificates from a public certificate authority and deploy them to all the containers.
- B. Create a self-signed certificate in one container and use AWS Secrets Manager to distribute the certificate to the other containers to establish trust.
- C. Use AWS Certificate Manager Private Certificate Authority (ACM PCA) to create a subordinate certificate authority, then create the private keys in the containers and sign them using the ACM PCA API.
- D. Use AWS Certificate Manager Private Certificate Authority (ACM PCA) to create a subordinate certificate authority, then use AWS Certificate Manager to generate the private certificates and deploy them to all the containers.

Answer: C

NEW QUESTION 86

A company is deploying a new web application on AWS. Based on their other web applications, they anticipate being the target of frequent DDoS attacks. Which steps can the company use to protect their application? Select 2 answers from the options given below.

Please select:

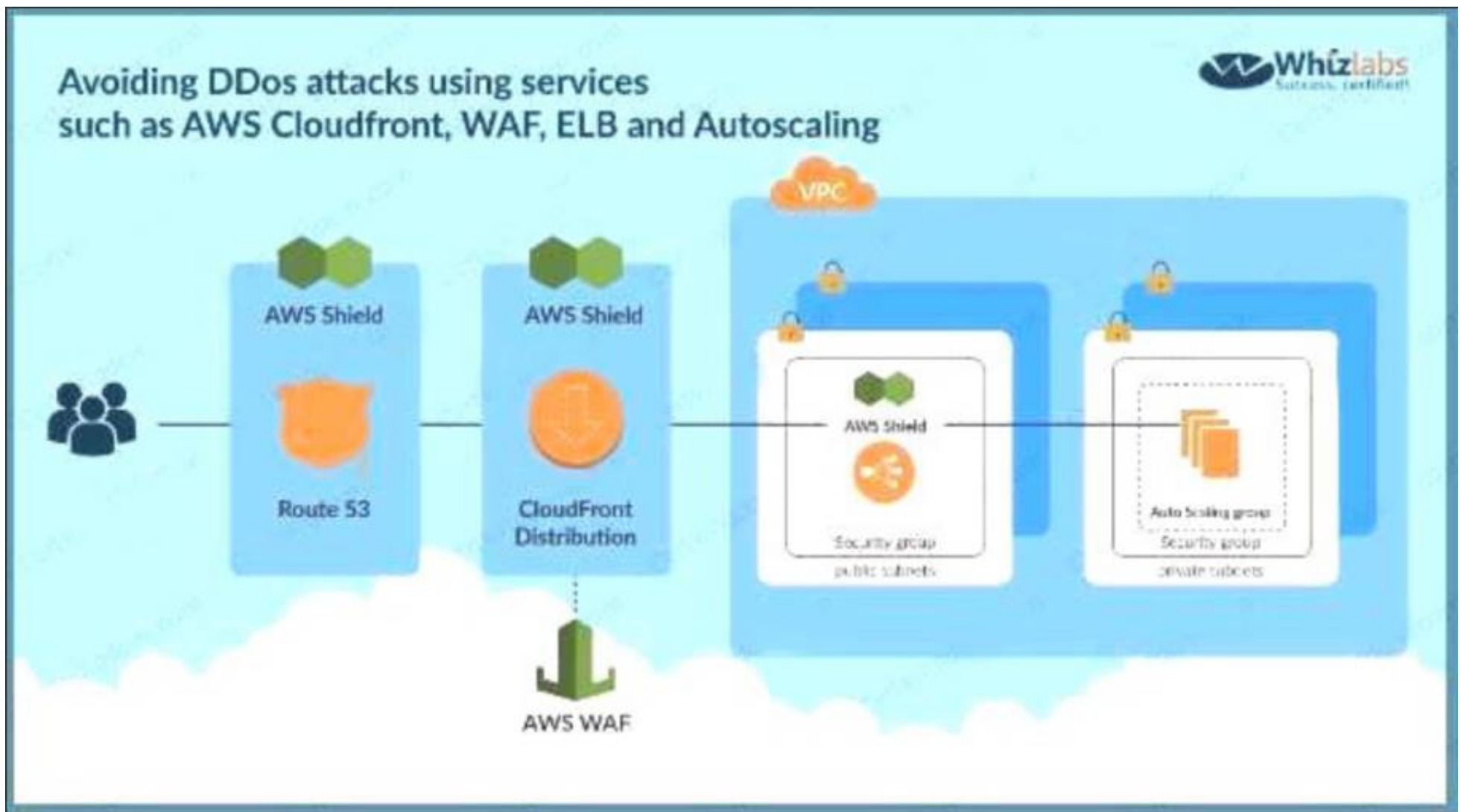
- A. Associate the EC2 instances with a security group that blocks traffic from blacklisted IP addresses.
- B. Use an ELB Application Load Balancer and Auto Scaling group to scale to absorb application layer traffic.
- C. Use Amazon Inspector on the EC2 instances to examine incoming traffic and discard malicious traffic.
- D. Use CloudFront and AWS WAF to prevent malicious traffic from reaching the application.
- E. Enable GuardDuty to block malicious traffic from reaching the application.

Answer: BD

Explanation:

The below diagram from AWS shows the best case scenario for avoiding DDoS attacks using services such as AWS CloudFront WAF, ELB and Autoscaling

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



Option A is invalid because by default security groups don't allow access Option C is invalid because AWS Inspector cannot be used to examine traffic Option E is invalid because this can be used for attacks on EC2 Instances but not against DDos attacks on the entire application For more information on DDos mitigation from AWS, please visit the below URL:

<https://aws.amazon.com/answers/networking/aws-ddos-attack-mitigation/>

The correct answers are: Use an ELB Application Load Balancer and Auto Scaling group to scale to absorb application layer traffic., Use CloudFront and AWS WAF to prevent malicious traffic from reaching the application

Submit your Feedback/Queries to our Experts

NEW QUESTION 88

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: B

NEW QUESTION 93

Which of the following bucket policies will ensure that objects being uploaded to a bucket called 'demo' are encrypted.

Please select:

A.

```
"Version":"2012-10-17",
"Id":"PutObj",
"Statement":[{
  "Sid":"DenyUploads",
  "Effect":"Deny",
  "Principal":"*",
  "Action":"s3:PutObject",
  "Resource":"arn:aws:s3:::demo/*",
  "Condition":{"
    "StringNotEquals":{"
      "s3:x-amz-server-side-encryption":"aws:kms"
    }
  }
}]
}
```

B.

```
"Version": "2012-10-17",
"Id": "PutObj",
"Statement": [{
  "Sid": "DenyUploads",
  "Effect": "Deny",
  "Principal": "*",
  "Action": "s3:PutObject",
  "Resource": "arn:aws:s3:::demo/*",
  "Condition": {
    "StringEquals": {
      "s3:x-amz-server-side-encryption": "aws:kms"
    }
  }
}]
```

C.

```
"Version": "2012-10-17",
"Id": "PutObj",
"Statement": [{
  "Sid": "DenyUploads",
  "Effect": "Deny",
  "Principal": "*",
  "Action": "s3:PutObject",
  "Resource": "arn:aws:s3:::demo/*"
}]
```

D.

```
"Version": "2012-10-17",
"Id": "PutObj",
"Statement": [{
  "Sid": "DenyUploads",
  "Effect": "Deny",
  "Principal": "*",
  "Action": "s3:PutObjectEncrypted",
  "Resource": "arn:aws:s3:::demo/*"
}]
```

A.

Answer: A**Explanation:**

The condition of "s3:x-amz-server-side-encryption":"aws:kms" ensures that objects uploaded need to be encrypted.

Options B,C and D are invalid because you have to ensure the condition of "s3:x-amz-server-side-encryption":"aws:kms" is present

For more information on AWS KMS best practices, just browse to the below URL: <https://dl.awsstatic.com/whitepapers/aws-kms-best-practices.pdf>


```
The correct answer is: {  
  "Version": "2012-10-17",  
  "Id": "PutObj",  
  "Statement": [{  
    "Sid": "DenyUploads",  
    "Effect": "Deny",  
    "Principal": "*",  
    "Action": "s3:PutObject",  
    "Resource": "arn:aws:s3:::demo/*",  
    "Condition": {  
      "StringNotEquals": {  
        "s3:x-amz-server-side-encryption": "aws:kms"  
      }  
    }  
  }  
}
```

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

Submit your Feedback/Queries to our Expert

NEW QUESTION 97

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

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

Please select:

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

Answer: D

Explanation:

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

The AWS Documentation additionally mentions the following:

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

If your Lambda function code accesses other AWS resources, such as to read an object from an S3 bucket or write logs to CloudWatch Logs, you need to grant permissions for relevant Amazon S3 and CloudWatch actions to the role.

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

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

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

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

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

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

Submit your Feedback/Queries to our Expert

NEW QUESTION 102

A threat assessment has identified a risk whereby an internal employee could exfiltrate sensitive data from production host running inside AWS (Account 1). The threat was documented as follows:

Threat description: A malicious actor could upload sensitive data from Server X by configuring credentials for an AWS account (Account 2) they control and uploading data to an Amazon S3 bucket within their control.

Server X has outbound internet access configured via a proxy server. Legitimate access to S3 is required so that the application can upload encrypted files to an S3 bucket. Server X is currently using an IAM instance role. The proxy server is not able to inspect any of the server communication due to TLS encryption.

Which of the following options will mitigate the threat? (Choose two.)

- A. Bypass the proxy and use an S3 VPC endpoint with a policy that whitelists only certain S3 buckets within Account 1.
- B. Block outbound access to public S3 endpoints on the proxy server.

- C. Configure Network ACLs on Server X to deny access to S3 endpoints.
- D. Modify the S3 bucket policy for the legitimate bucket to allow access only from the public IP addresses associated with the application server.
- E. Remove the IAM instance role from the application server and save API access keys in a trusted and encrypted application config file.

Answer: AD

NEW QUESTION 106

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 t 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 t that OAI.

Submit your Feedback/Queries to our Experts

Submit your Feedback/Queries to our Experts

NEW QUESTION 110

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

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

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

Answer: CE

NEW QUESTION 114

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 l#iam-policy-example-ec2-two-condition!
The correct answer is: Create an 1AM 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 115

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

NEW QUESTION 117

A company runs an application on AWS that needs to be accessed only by employees. Most employees work from the office, but others work remotely or travel. How can the Security Engineer protect this workload so that only employees can access it?

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

Answer: C

NEW QUESTION 121

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

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

Answer: A

Explanation:

The AWS Documentation mentions the following

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

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

<https://aws.amazon.com/blogs/security/control-access-to-aws-resources-by-using-the-aws-organization-of-iam-p/> (

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

NEW QUESTION 122

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

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

Answer: B

NEW QUESTION 123

You need to create a policy and apply it for just an individual user. How could you accomplish this in the right way?
Please select:

- A. Add an AWS managed policy for the user
- B. Add a service policy for the user
- C. Add an IAM role for the user
- D. Add an inline policy for the user

Answer: D

Explanation:

Options A and B are incorrect since you need to add an inline policy just for the user Option C is invalid because you don't assign an IAM role to a user

The AWS Documentation mentions the following

An inline policy is a policy that's embedded in a principal entity (a user, group, or role)—that is, the policy is an inherent part of the principal entity. You can create a policy and embed it in a principal entity, either when you create the principal entity or later.

For more information on 1AM Access and Inline policies, just browse to the below URL: <https://docs.aws.amazon.com/IAM/latest/UserGuide/access>
The correct answer is: Add an inline policy for the user Submit your Feedback/Queries to our Experts

NEW QUESTION 128

Which of the following are valid event sources that are associated with web access control lists that trigger AWS WAF rules? (Choose two.)

- A. Amazon S3 static web hosting
- B. Amazon CloudFront distribution
- C. Application Load Balancer
- D. Amazon Route 53
- E. VPC Flow Logs

Answer: BC

Explanation:

A web access control list (web ACL) gives you fine-grained control over the web requests that your Amazon API Gateway API, Amazon CloudFront distribution or Application Load Balancer responds to.

NEW QUESTION 132

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

NEW QUESTION 134

An organization is using Amazon CloudWatch Logs with agents deployed on its Linux Amazon EC2 instances. The agent configuration files have been checked and the application log files to be pushed are configured correctly. A review has identified that logging from specific instances is missing. Which steps should be taken to troubleshoot the issue? (Choose two.)

- A. Use an EC2 run command to confirm that the "awslogs" service is running on all instances.
- B. Verify that the permissions used by the agent allow creation of log groups/streams and to put log events.
- C. Check whether any application log entries were rejected because of invalid time stamps by reviewing /var/cwlogs/rejects.log.
- D. Check that the trust relationship grants the service "cwlogs.amazonaws.com" permission to write objects to the Amazon S3 staging bucket.
- E. Verify that the time zone on the application servers is in UTC.

Answer: AB

NEW QUESTION 136

During a security event, it is discovered that some Amazon EC2 instances have not been sending Amazon CloudWatch logs. Which steps can the Security Engineer take to troubleshoot this issue? (Select two.)

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

Answer: AE

NEW QUESTION 138

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. CloudTrai
- 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, 1AM 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, char 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 1AM API.

For more information on Credentials Report, please visit the below URL:

[http://docs.aws.amazon.com/IAM/latest/UserGuide/id](http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_getting-report.html)

[credentials_getting-report.html](http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_getting-report.html)

The correct answer is: CloudTrail, AWS Config, 1AM Credential Reports Submit your Feedback/Queries to our Experts

NEW QUESTION 142

You have a set of Customer keys created using the AWS KMS service. These keys have been used for around 6 months. You are now trying to use the new KMS features for the existing set of key's but are not able to do so. What could be the reason for this.

Please select:

- A. You have not explicitly given access via the key policy
- B. You have not explicitly given access via the 1AM policy
- C. You have not given access via the 1AM roles
- D. You have not explicitly given access via 1AM users

Answer: A

Explanation:

By default, keys created in KMS are created with the default key policy. When features are added to KMS, you need to explii update the default key policy for these keys.

Option B,C and D are invalid because the key policy is the main entity used to provide access to the keys

For more information on upgrading key policies please visit the following URL: <https://docs.aws.ama20n.com/kms/latest/developerguide/key-policy-upgrading.html> (

The correct answer is: You have not explicitly given access via the key policy Submit your Feedback/Queries to our Experts

NEW QUESTION 144

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: A

NEW QUESTION 148

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 bucke
- 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 bucke
- 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 bucke
- G. Use server-side encryption with AWS KMS-managed keys (SSE-KMS) to encrypt the data

Answer: D

NEW QUESTION 149

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 152

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

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

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

Answer: BC

NEW QUESTION 156

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 160

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 164

A company has set up the following structure to ensure that their S3 buckets always have logging enabled



If there are any changes to the configuration to an S3 bucket, a config rule gets checked. If logging is disabled, then Lambda function is invoked. This Lambda function will again enable logging on the S3 bucket. Now there is an issue being encountered with the entire flow. You have verified that the Lambda function is being invoked. But when logging is disabled for the bucket, the lambda function does not enable it again. Which of the following could be an issue Please select:

- A. The AWS Config rule is not configured properly
- B. The AWS Lambda function does not have appropriate permissions for the bucket
- C. The AWS Lambda function should use Node.js instead of python.
- D. You need to also use the API gateway to invoke the lambda function

Answer: B

Explanation:

The most probable cause is that you have not allowed the Lambda functions to have the appropriate permissions on the S3 bucket to make the relevant changes. Option A is invalid because this is more of a permission instead of a configuration rule issue. Option C is invalid because changing the language will not be the core solution.

Option D is invalid because you don't necessarily need to use the API gateway service

For more information on accessing resources from a Lambda function, please refer to below URL <https://docs.aws.amazon.com/lambda/latest/ds/accessing-resources.html>

The correct answer is: The AWS Lambda function does not have appropriate permissions for the bucket Submit your Feedback/Queries to our Experts

NEW QUESTION 169

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 174

For compliance reasons, an organization limits the use of resources to three specific AWS regions. It wants to be alerted when any resources are launched in unapproved regions.

Which of the following approaches will provide alerts on any resources launched in an unapproved region?

- A. Develop an alerting mechanism based on processing AWS CloudTrail logs.
- B. Monitor Amazon S3 Event Notifications for objects stored in buckets in unapproved regions.
- C. Analyze Amazon CloudWatch Logs for activities in unapproved regions.
- D. Use AWS Trusted Advisor to alert on all resources being created.

Answer: A

NEW QUESTION 179

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

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

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

Answer: A

NEW QUESTION 182

A Security Administrator is restricting the capabilities of company root user accounts. The company uses AWS Organizations and has enabled it for all feature

sets, including consolidated billing. The top-level account is used for billing and administrative purposes, not for operational AWS resource purposes. How can the Administrator restrict usage of member root user accounts across the organization?

- A. Disable the use of the root user account at the organizational root
- B. Enable multi-factor authentication of the root user account for each organizational member account.
- C. Configure IAM user policies to restrict root account capabilities for each Organizations member account.
- D. Create an organizational unit (OU) in Organizations with a service control policy that controls usage of the root user
- E. Add all operational accounts to the new OU.
- F. Configure AWS CloudTrail to integrate with Amazon CloudWatch Logs and then create a metric filter for RootAccountUsage.

Answer: C

NEW QUESTION 183

An application is designed to run on an EC2 Instance. The application needs to work with an S3 bucket. From a security perspective, what is the ideal way for the EC2 instance/ application to be configured?

Please select:

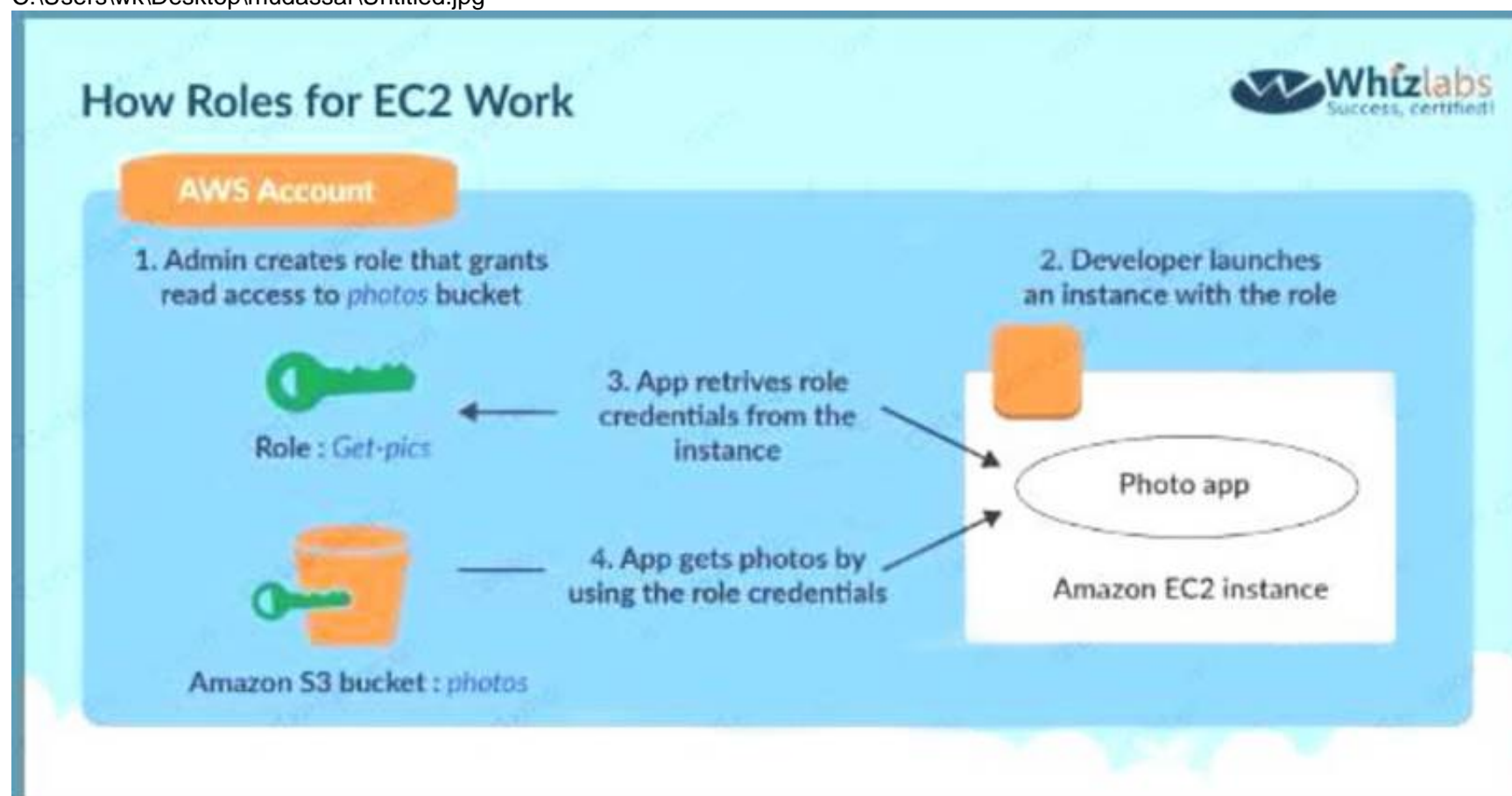
- A. Use the AWS access keys ensuring that they are frequently rotated.
- B. Assign an IAM user to the application that has specific access to only that S3 bucket
- C. Assign an IAM Role and assign it to the EC2 Instance
- D. Assign an IAM group and assign it to the EC2 Instance

Answer: C

Explanation:

The below diagram from the AWS whitepaper shows the best security practice of allocating a role that has access to the S3 bucket

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



Options A,B and D are invalid because using users, groups or access keys is an invalid security practice when giving access to resources from other AWS resources.

For more information on the Security Best practices, please visit the following URL: [https://d1.awsstatic.com/whitepapers/Security/AWS Security Best Practices.pdf](https://d1.awsstatic.com/whitepapers/Security/AWS%20Security%20Best%20Practices.pdf)

The correct answer is: Assign an IAM Role and assign it to the EC2 Instance Submit your Feedback/Queries to our Experts

NEW QUESTION 188

Your application currently uses AWS Cognito for authenticating users. Your application consists of different types of users. Some users are only allowed read access to the application and others are given contributor access. How would you manage the access effectively?

Please select:

- A. Create different Cognito endpoints, one for the readers and the other for the contributors.
- B. Create different Cognito groups, one for the readers and the other for the contributors.
- C. You need to manage this within the application itself
- D. This needs to be managed via Web security tokens

Answer: B

Explanation:

The AWS Documentation mentions the following

You can use groups to create a collection of users in a user pool, which is often done to set the permissions for those users. For example, you can create separate groups for users who are readers, contributors, and editors of your website and app.

Option A is incorrect since you need to create Cognito groups and not endpoints

Options C and D are incorrect since these would be overheads when you can use AWS Cognito. For more information on AWS Cognito user groups, please refer to the below link: <https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-user-pools-user-groups.html>

The correct answer is: Create different Cognito groups, one for the readers and the other for the contributors. Submit your Feedback/Queries to our Experts

NEW QUESTION 189

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: A

NEW QUESTION 190

A Security Engineer must enforce the use of only Amazon EC2, Amazon S3, Amazon RDS, Amazon DynamoDB, and AWS STS in specific accounts. What is a scalable and efficient approach to meet this requirement?

- A** Set up an AWS Organizations hierarchy, and replace the FullAWSAccess policy with the following Service Control Policy for the governed organization units:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "dynamodb:*", "rds:*", "ec2:*",
        "s3:*", "sts:*"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

- B** Create multiple IAM users for the regulated accounts, and attach the following policy statement to restrict services as required:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": *
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "NotAction": [
        "dynamodb:*", "rds:*", "ec2:*",
        "s3:*", "sts:*"
      ],
      "Effect": "Deny ",
      "Resource": "*"
    }
  ]
}
```


- c Set up an Organizations hierarchy, replace the global FullAWSAccess with the following Service Control Policy at the top level:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "dynamodb:*", "rds:*", "ec2:*",
        "s3:*", "sts:*"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

- D Set up all users in the Active Directory for federated access to all accounts in the company. Associate Active Directory groups with IAM groups, and attach the following policy statement to restrict services as required:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": *
      "Effect": "Allow",
      "Resource": "*"
    }
    {
      "NotAction": [
        "dynamodb:*", "rds:*", "ec2:*",
        "s3:*", "sts:*"
      ],
      "Effect": "Deny ",
      "Resource": "*"
    }
  ]
}
```

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

Answer: A

NEW QUESTION 194

A company has a large set of keys defined in AWS KMS. Their developers frequently use the keys for the applications being developed. What is one of the ways that can be used to reduce the cost of accessing the keys in the AWS KMS service.

Please select:

- A. Enable rotation of the keys
- B. Use Data key caching
- C. Create an alias of the key
- D. Use the right key policy

Answer: B

Explanation:

The AWS Documentation mentions the following

Data key caching stores data keys and related cryptographic material in a cache. When you encrypt or decrypt data, the AWS Encryption SDK looks for a matching data key in the cache. If it finds a match, it uses the cached data key rather than generating a new one. Data key caching can improve performance, reduce cost, and help you stay within service limits as your application scales.

Option A,C and D are all incorrect since these options will not impact how the key is used. For more information on data key caching, please refer to below URL:
<https://docs.aws.amazon.com/encryption-sdk/latest/developer-guide/data-key-cache.html> The correct answer is: Use Data key caching Submit your Feedback/Queries to our Experts

NEW QUESTION 199

A user has created a VPC with the public and private subnets using the VPC wizard. The VPC has CIDR 20.0.0.0/16. The public subnet uses CIDR 20.0.1.0/24. The user is planning to host a web server in the public subnet with port 80 and a Database server in the private subnet with port 3306. The user is configuring a security group for the public subnet (WebSecGrp) and the private subnet (DBSecGrp). which of the below mentioned entries is required in the private subnet database security group DBSecGrp?
Please select:

- A. Allow Inbound on port 3306 for Source Web Server Security Group WebSecGrp.
- B. Allow Inbound on port 3306 from source 20.0.0.0/16
- C. Allow Outbound on port 3306 for Destination Web Server Security Group WebSecGrp.
- D. Allow Outbound on port 80 for Destination NAT Instance IP

Answer: A

Explanation:

Since the Web server needs to talk to the database server on port 3306 that means that the database server should allow incoming traffic on port 3306. The below table from the aws documentation shows how the security groups should be set up.

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

DBServerSG: Recommended Rules			
Inbound			
Source	Protocol	Port Range	Comments
The ID of your WebServerSG security group	TCP	1433	Allow inbound Microsoft SQL Server access from the web servers associated with the WebServerSG security group
The ID of your WebServerSG security group	TCP	3306	Allow inbound MySQL Server access from the web servers associated with the WebServerSG security group.
Outbound			
Destination	Protocol	Port Range	Comments
0.0.0.0/0	TCP	80	Allow outbound HTTP access to the Internet over IPv4 (for example, for software updates)
0.0.0.0/0	TCP	443	Allow outbound HTTPS access to the Internet over IPv4 (for example, for software updates)

Option B is invalid because you need to allow incoming access for the database server from the WebSecGrp security group.
Options C and D are invalid because you need to allow Outbound traffic and not inbound traffic For more information on security groups please visit the below Link:
<http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPCScenario2.html>

The correct answer is: Allow Inbound on port 3306 for Source Web Server Security Group WebSecGrp. Submit your Feedback/Queries to our Experts

NEW QUESTION 203

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

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

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

Answer: B

NEW QUESTION 208

Your company is planning on using bastion hosts for administering the servers in AWS. Which of the following is the best description of a bastion host from a security perspective? Please select:

- A. A Bastion host should be on a private subnet and never a public subnet due to security concerns
- B. A Bastion host sits on the outside of an internal network and is used as a gateway into the private network and is considered the critical strong point of the network
- C. Bastion hosts allow users to log in using RDP or SSH and use that session to S5H into internal network to access private subnet resources.
- D. A Bastion host should maintain extremely tight security and monitoring as it is available to the public

Answer: C

Explanation:

A bastion host is a special purpose computer on a network specifically designed and configured to withstand attacks. The computer generally hosts a single application, for example a proxy server, and all other services are removed or limited to reduce the threat to the computer.

In AWS, A bastion host is kept on a public subnet. Users log on to the bastion host via SSH or RDP and then use that session to manage other hosts in the private subnets.

Options A and B are invalid because the bastion host needs to sit on the public network. Option D is invalid because bastion hosts are not used for monitoring. For more information on bastion hosts, just browse to the below URL:

<https://docsaws.amazon.com/quickstart/latest/linux-bastion/architecture.html>

The correct answer is: Bastion hosts allow users to log in using RDP or SSH and use that session to SSH into internal network to access private subnet resources. Submit your Feedback/Queries to our Experts

NEW QUESTION 213

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

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

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

Answer: D

NEW QUESTION 217

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 220

You have a vendor that needs access to an AWS resource. You create an AWS user account. You want to restrict access to the resource using a policy for just that user over a brief period. Which of the following would be an ideal policy to use?

Please select:

- A. An AWS Managed Policy
- B. An Inline Policy
- C. A Bucket Policy
- D. A bucket ACL

Answer: B

Explanation:

The AWS Documentation gives an example on such a case

Inline policies are useful if you want to maintain a strict one-to-one relationship between a policy and the principal entity that it is applied to. For example, you want to be sure that the permissions in a policy are not inadvertently assigned to a principal entity other than the one they're intended for. When you use an inline policy, the permissions in the policy cannot be inadvertently attached to the wrong principal entity. In addition, when you use the AWS Management Console to delete that principal entity the policies embedded in the principal entity are deleted as well. That's because they are part of the principal entity.

Option A is invalid because AWS Managed Policies are OK for a group of users, but for individual users, inline policies are better.

Option C and D are invalid because they are specifically meant for access to S3 buckets. For more information on policies, please visit the following URL:

<https://docs.aws.amazon.com/IAM/latest/UserGuide/access-managed-vs-inline>

The correct answer is: An Inline Policy. Submit your Feedback/Queries to our Experts

NEW QUESTION 225

A company hosts data in S3. There is a requirement to control access to the S3 buckets. Which are the 2 ways in which this can be achieved?

Please select:

- A. Use Bucket policies
- B. Use the Secure Token service
- C. Use IAM user policies
- D. Use AWS Access Keys

Answer: AC

Explanation:

The AWS Documentation mentions the following

Amazon S3 offers access policy options broadly categorized as resource-based policies and user policies. Access policies you attach to your resources (buckets and objects) are referred to as resource-based policies. For example, bucket policies and access control lists (ACLs) are resource-based policies. You can also attach access policies to users in your account. These are called user policies. You may choose to use resource-based policies, user policies, or some combination of these to manage permissions to your Amazon S3 resources.

Option B and D are invalid because these cannot be used to control access to S3 buckets. For more information on S3 access control, please refer to the below

Link: <https://docs.aws.amazon.com/AmazonS3/latest/dev/s3-access-control.html>

The correct answers are: Use Bucket policies. Use IAM user policies. Submit your Feedback/Queries to our Experts

NEW QUESTION 230

In response to the past DDoS attack experiences, a Security Engineer has set up an Amazon CloudFront distribution for an Amazon S3 bucket. There is concern that some users may bypass the CloudFront distribution and access the S3 bucket directly. What must be done to prevent users from accessing the S3 objects directly by using URLs?

- A. Change the S3 bucket/object permission so that only the bucket owner has access.
- B. Set up a CloudFront origin access identity (OAI), and change the S3 bucket/object permission so that only the OAI has access.
- C. Create IAM roles for CloudFront, and change the S3 bucket/object permission so that only the IAM role has access.
- D. Redirect S3 bucket access to the corresponding CloudFront distribution.

Answer: B

NEW QUESTION 234

One of your company's EC2 Instances have been compromised. The company has strict po thorough investigation on finding the culprit for the security breach. What would you do in from the options given below. Please select:

- A. Take a snapshot of the EBS volume
- B. Isolate the machine from the network
- C. Make sure that logs are stored securely for auditing and troubleshooting purpose
- D. Ensure all passwords for all 1AM users are changed
- E. Ensure that all access kevs are rotated.

Answer: ABC

Explanation:

Some of the important aspects in such a situation are

- 1) First isolate the instance so that no further security harm can occur on other AWS resources
- 2) Take a snapshot of the EBS volume for further investigation. This is incase if you need to shutdown the initial instance and do a separate investigation on the data
- 3) Next is Option C. This indicates that we have already got logs and we need to make sure that it is stored securely so that n unauthorised person can access it and manipulate it.

Option D and E are invalid because they could have adverse effects for the other 1AM users. For more information on adopting a security framework, please refer to below URL [https://d1.awsstatic.com/whitepapers/compliance/NIST Cybersecurity Framework](https://d1.awsstatic.com/whitepapers/compliance/NIST%20Cybersecurity%20Framework.pdf)

Note:

In the question we have been asked to take actions to find the culprit and to help the investigation or to further reduce the damage that has happened due to the security breach. So by keeping logs secure is one way of helping the investigation.

The correct answers are: Take a snapshot of the EBS volume. Isolate the machine from the network. Make sure that logs are stored securely for auditing and troubleshooting purpose

Submit your Feedback/Queries to our Experts

NEW QUESTION 239

Your company has the following setup in AWS

- a:. A set of EC2 Instances hosting a web application
- b: An application load balancer placed in front of the EC2 Instances

There seems to be a set of malicious requests coming from a set of IP addresses. Which of the following can be used to protect against these requests?

Please select:

- A. Use Security Groups to block the IP addresses
- B. Use VPC Flow Logs to block the IP addresses
- C. Use AWS inspector to block the IP addresses
- D. Use AWS WAF to block the IP addresses

Answer: D

Explanation:

Your answer is incorrect Answer -D

The AWS Documentation mentions the following on AWS WAF which can be used to protect Application Load Balancers and Cloud front

A web access control list (web ACL) gives you fine-grained control over the web requests that your Amazon CloudFront distributions or Application Load Balancers respond to. You can allow or block the following types of requests:

Originate from an IP address or a range of IP addresses Originate from a specific country or countries

Contain a specified string or match a regular expression (regex) pattern in a particular part of requests Exceed a specified length

Appear to contain malicious SQL code (known as SQL injection) Appear to contain malicious scripts (known as cross-site scripting)

Option A is invalid because by default Security Groups have the Deny policy

Options B and C are invalid because these services cannot be used to block IP addresses For information on AWS WAF, please visit the below URL:

<https://docs.aws.amazon.com/waf/latest/developerguide/web-acl.html>

The correct answer is: Use AWS WAF to block the IP addresses Submit your Feedback/Queries to our Experts

NEW QUESTION 244

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

.m icro 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 246

You are building a large-scale confidential documentation web server on AWS and all of the documentation for it will be stored on S3. One of the requirements is that it cannot be publicly accessible from S3 directly, and you will need to use Cloud Front to accomplish this. Which of the methods listed below would satisfy the requirements as outlined? Choose an answer from the options below

Please select:

- A. Create an Identity and Access Management (IAM) user for CloudFront and grant access to the objects in your S3 bucket to that IAM User.
- B. Create an Origin Access Identity (OAI) for CloudFront and grant access to the objects in your S3 bucket to that OAI.
- C. Create individual policies for each bucket the documents are stored in and in that policy grant access to only CloudFront.
- D. Create an S3 bucket policy that lists the CloudFront distribution ID as the Principal and the target bucket as the Amazon Resource Name (ARN).

Answer: B

Explanation:

If you want to use CloudFront signed URLs or signed cookies to provide access to objects in your Amazon S3 bucket you probably also want to prevent users from accessing your Amazon S3 objects using Amazon S3 URLs. If users access your objects directly in Amazon S3, they bypass the controls provided by CloudFront signed URLs or signed cookies, for example, control over the date and time that a user can no longer access your content and control over which IP addresses can be used to access content. In addition, if user's access objects both through CloudFront and directly by using Amazon S3 URLs, CloudFront access logs are less useful because they're incomplete.

Option A is invalid because you need to create a Origin Access Identity for Cloudfront and not an IAM user Option C and D are invalid because using policies will not help fulfil the requirement

For more information on Origin Access Identity please see the below Link:

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

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

NEW QUESTION 250

A security alert has been raised for an Amazon EC2 instance in a customer account that is exhibiting strange behavior. The Security Engineer must first isolate the EC2 instance and then use tools for further investigation.

What should the Security Engineer use to isolate and research this event? (Choose three.)

- A. AWS CloudTrail
- B. Amazon Athena
- C. AWS Key Management Service (AWS KMS)
- D. VPC Flow Logs
- E. AWS Firewall Manager
- F. Security groups

Answer: ADF

NEW QUESTION 251

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

Please select:

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

Answer: B

Explanation:

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

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

For more information on authorizing access to an instance, please visit the below URL: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/authorizing-access-to-an-instance.html>

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

NEW QUESTION 255

DDoS attacks that happen at the application layer commonly target web applications with lower volumes of traffic compared to infrastructure attacks. To mitigate these types of attacks, you should probably want to include a WAF (Web Application Firewall) as part of your infrastructure. To inspect all HTTP requests, WAFs

sit in-line with your application traffic. Unfortunately, this creates a scenario where WAFs can become a point of failure or bottleneck. To mitigate this problem, you need the ability to run multiple WAFs on demand during traffic spikes. This type of scaling for WAF is done via a "WAF sandwich." Which of the following statements best describes what a "WAF sandwich" is? Choose the correct answer from the options below
Please select:

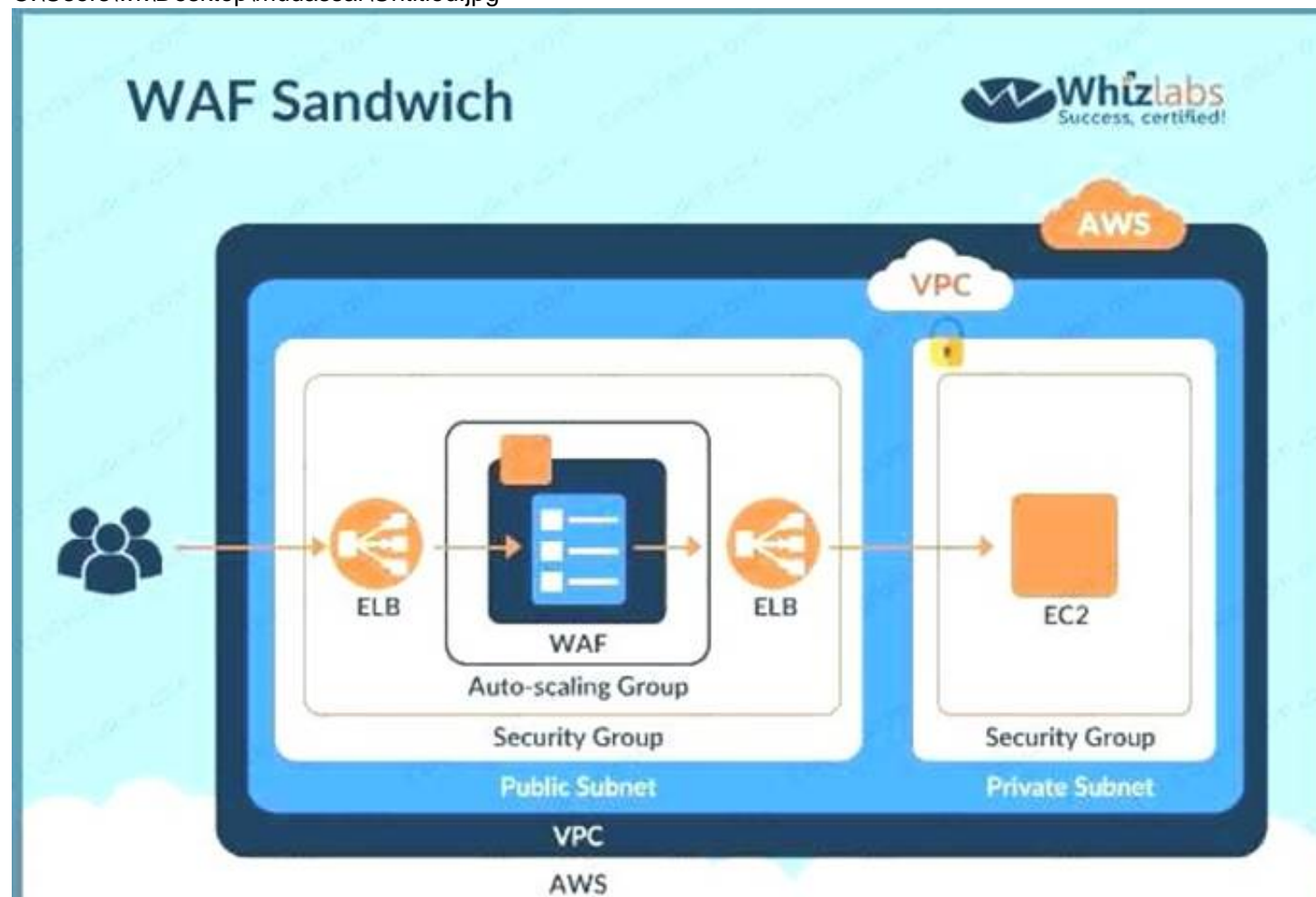
- A. The EC2 instance running your WAF software is placed between your private subnets and any NATed connections to the internet.
- B. The EC2 instance running your WAF software is placed between your public subnets and your Internet Gateway.
- C. The EC2 instance running your WAF software is placed between your public subnets and your private subnets.
- D. The EC2 instance running your WAF software is included in an Auto Scaling group and placed in between two Elastic load balancers.

Answer: D

Explanation:

The below diagram shows how a WAF sandwich is created. Its the concept of placing the Ec2 instance which hosts the WAF software in between 2 elastic load balancers.

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



Option A,B and C are incorrect since the EC2 Instance with the WAF software needs to be placed in an Autoscaling Group For more information on a WAF sandwich please refer to the below Link:

<https://www.cloudaxis.com/2016/11/21/waf-sandwich/>

The correct answer is: The EC2 instance running your WAF software is included in an Auto Scaling group and placed in between two Elastic load balancers. Submit your Feedback/Queries to our Experts

NEW QUESTION 258

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

Please select:

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

Answer: C

Explanation:

This concept is given in the AWS Documentation

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

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

Resolution

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

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

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

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

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

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

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

(

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

NEW QUESTION 261

A security team is creating a response plan in the event an employee executes unauthorized actions on AWS infrastructure. They want to include steps to determine if the employee's 1AM permissions changed as part of the incident. What steps should the team document in the plan? Please select:

- A. Use AWS Config to examine the employee's 1AM permissions prior to the incident and compare them to the employee's current 1AM permissions.
- B. Use Made to examine the employee's 1AM permissions prior to the incident and compare them to the employee's A current 1AM permissions.
- C. Use CloudTrail to examine the employee's 1AM permissions prior to the incident and compare them to the employee's current 1AM permissions.
- D. Use Trusted Advisor to examine the employee's 1AM permissions prior to the incident and compare them to the employee's current 1AM permissions.

Answer: A

Explanation:

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

The below snapshot shows an example configuration for a user in AWS Config



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

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

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

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

The correct answer is: Use AWS Config to examine the employee's 1AM permissions prior to the incident and compare them the employee's current 1AM permissions.

Submit your Feedback/Queries to our Experts

NEW QUESTION 263

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

Which of the following actions would resolve this issue?

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

Answer: B

NEW QUESTION 264

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

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

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

Answer: B

NEW QUESTION 265

You are designing a connectivity solution between on-premises infrastructure and Amazon VPC. Your server's on-premises will be communicating with your VPC instances. You will be establishing IPSec tunnels over the internet. Yo will be using VPN gateways and terminating the IPsec tunnels on AWS-supported customer gateways. Which of the following objectives would you achieve by implementing an IPSec tunnel as outlined above? Choose 4 answers form the options below Please select:

- A. End-to-end protection of data in transit
- B. End-to-end Identity authentication
- C. Data encryption across the internet
- D. Protection of data in transit over the Internet
- E. Peer identity authentication between VPN gateway and customer gateway
- F. Data integrity protection across the Internet

Answer: CDEF

Explanation:

IPSec is a widely adopted protocol that can be used to provide end to end protection for data

NEW QUESTION 269

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: BCE

NEW QUESTION 272

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

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

Answer: AB

NEW QUESTION 274

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-regions-and-support-for-multiple-regions/> The correct answer is: Ensure one Cloudtrail trail is enabled for all regions. Submit your Feedback/Queries to our Experts

NEW QUESTION 276

A company has a set of EC2 Instances hosted in AWS. The EC2 Instances have EBS volumes which is used to store critical information. There is a business continuity requirement to ensure high availability for the EBS volumes. How can you achieve this?

- A. Use lifecycle policies for the EBS volumes
- B. Use EBS Snapshots
- C. Use EBS volume replication
- D. Use EBS volume encryption

Answer: B

Explanation:

Data stored in Amazon EBS volumes is redundantly stored in multiple physical locations as part of normal operation of those services and at no additional charge. However, Amazon EBS replication is stored within the same availability zone, not across multiple zones; therefore, it is highly recommended that you conduct regular snapshots to Amazon S3 for long-term data durability Option A is invalid because there is no lifecycle policy for EBS volumes Option C is invalid because there is no EBS volume replication Option D is invalid because EBS volume encryption will not ensure business continuity For information on security for Compute Resources, please visit the below URL: https://d1.awsstatic.com/whitepapers/Security/Security_Compute_Services_Whitepaper.pdf

NEW QUESTION 278

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

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

Security Engineer

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

Lambda function execution role

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

What is causing the error?

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

Answer: D

NEW QUESTION 281

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 283

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 288

A company's AWS account consists of approximately 300 IAM users. Now there is a mandate that an access change is required for 100 IAM users to have unlimited privileges to S3.As a system administrator, how can you implement this effectively so that there is no need to apply the policy at the individual user level? Please select:

- A. Create a new role and add each user to the IAM role
- B. Use the IAM groups and add users, based upon their role, to different groups and apply the policy to group

- C. Create a policy and apply it to multiple users using a JSON script
- D. Create an S3 bucket policy with unlimited access which includes each user's AWS account ID

Answer: B

Explanation:

Option A is incorrect since you don't add a user to the 1AM Role Option C is incorrect since you don't assign multiple users to a policy Option D is incorrect since this is not an ideal approach

An 1AM group is used to collectively manage users who need the same set of permissions. By having groups, it becomes easier to manage permissions. So if you change the permissions on the group scale, it will affect all the users in that group

For more information on 1AM Groups, just browse to the below URL: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_eroups.html

The correct answer is: Use the 1AM groups and add users, based upon their role, to different groups and apply the policy to group

Submit your Feedback/Queries to our Experts

NEW QUESTION 292

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your SCS-C01 Exam with Our Prep Materials Via below:

<https://www.certleader.com/SCS-C01-dumps.html>