hotcerts

DESIRE FOR CERTS

WAS NEVER HOTTER

AWS certified Security Speciality

Exam: AWS-SECURITY-SPECIALTY

Demo Edition

QUESTION: 1
A company hosts a popular web application that connects to an Amazon RDS MySQL DB instance running in a private VPC subnet that was created with default ACL settings. The IT Security department has a suspicion that a DDos attack is coming from a suspecting IP. How can you protect the subnets from this attack?Please select:

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

Answer: C

Explanation:
Option A and B are invalid because by default the Security Groups already block traffic. You can use NACL's as an additional security layer for the subnet to deny traffic. Option D is invalid since just changing the Inbound Rules is sufficient The AWS Documentation mentions the followingA network access control list (ACLJ is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC.The correct answer is: Change the Inbound NACL to deny access from the suspecting IP

QUESTION: 2
You are designing a custom 1AM policy that would allow uses to list buckets in S3 only if they are MFA authenticated. Which of the following would best match this requirement?

A.

```
"Version":"2012-10-17",
"Statement": {
  "Effect": "Allow",
  "Action": [
      "s3:ListAllMyBuckets",
      "s3:GetBucketLocation"
   ],
  "Resource": "Resource": "arn:aws:s3:::*",
  "Condition": {
   "Bool": {"aws:MultiFactorAuthPresent": true}
  }
 }
}
```

B.

```
"Version": "2012-10-17",
"Statement": {
  "Effect": "Allow",
  "Action": [
      "s3:ListAllMyBuckets",
      "s3:GetBucketLocation"
   ],
  "Resource": "Resource": "arn:aws:s3:::*",
  "Condition": {
   "Bool": {"aws:MultiFactorAuthPresent":false}
  }
 }
```

C.

```
 "Version": "2012-10-17",
 "Statement": {
  "Effect": "Allow",
  "Action": [
       "s3:ListAllMyBuckets",
       "s3:GetBucketLocation"
   ],
  "Resource": "Resource": "arn:aws:s3:::*",
  "Condition": {
   "aws:MultiFactorAuthPresent":false
  }
 }
}
```

D.

```
 "Version": "2012-10-17",
 "Statement": {
  "Effect": "Allow",
  "Action": [
       "s3:ListAllMyBuckets",
       "s3:GetBucketLocation"
   ],
  "Resource": "Resource": "arn:aws:s3:::*",
  "Condition": {
   "aws:MultiFactorAuthPresent":true
  }
 }
}
```

Answer: A

Explanation:
The Condition clause can be used to ensure users can only work with resources if they are MFA authenticated.Option B and C are wrong since the aws:MultiFactorAuthPresent clause should be marked as true. Here you are saying that onl if the user has been MFA activated, that means it is true, then allow access.Option D is invalid because the "boor clause is missing in the evaluation for the condition clause. Boolean conditions let you construct Condition elements that restrict access based on comparing a key to "true" or "false."Here in this scenario

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

Answer: A

Explanation:
Your answer is incorrect Answer-ASuch a scenario is also given in the AWS Documentation Cross-Origin Resource Sharing: Use-case ScenariosThe following are example scenarios for using CORS:• Scenario 1: Suppose that you are hosting a website in an Amazon S3 bucket named website as described in Hosting a Static Website on Amazon S3. Your users load the website endpoint Now you want to use JavaScript on the webpages that are stored in this bucket to be able to make authenticated GET and PUT requests against the same bucket by using the Amazon S3 API endpoint for the bucket website.s3.amazonaws.com. A browser would normally block JavaScript from allowing those requests, but with CORS you can configure your bucket to explicitly enable cross-origin requests from website.s3-website-us-east-1 .amazonaws.com.
• Scenario 2: Suppose that you want to host a web font from your S3 bucket. Again, browsers require a CORS check (also called a preflight check) for loading web fonts. You would configure the bucket that is hosting the web font to allow any origin to make these requests.Option Bis invalid because versioning is only to create multiple versions of an object and can help in accidental deletion of objectsOption C is invalid because this is used as an extra measure of caution for deletion of objects Option D is invalid because this is used for Cross region replication of objectsFor more information on Cross Origin Resource sharing, please visit the following
URL• ittps://docs.aws.amazon.com/AmazonS3/latest/dev/cors.html The correct answer is: Enable CORS for the bucketSubmit your Feedback/Queries to our Experts

QUESTION: 4
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 perio D. 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

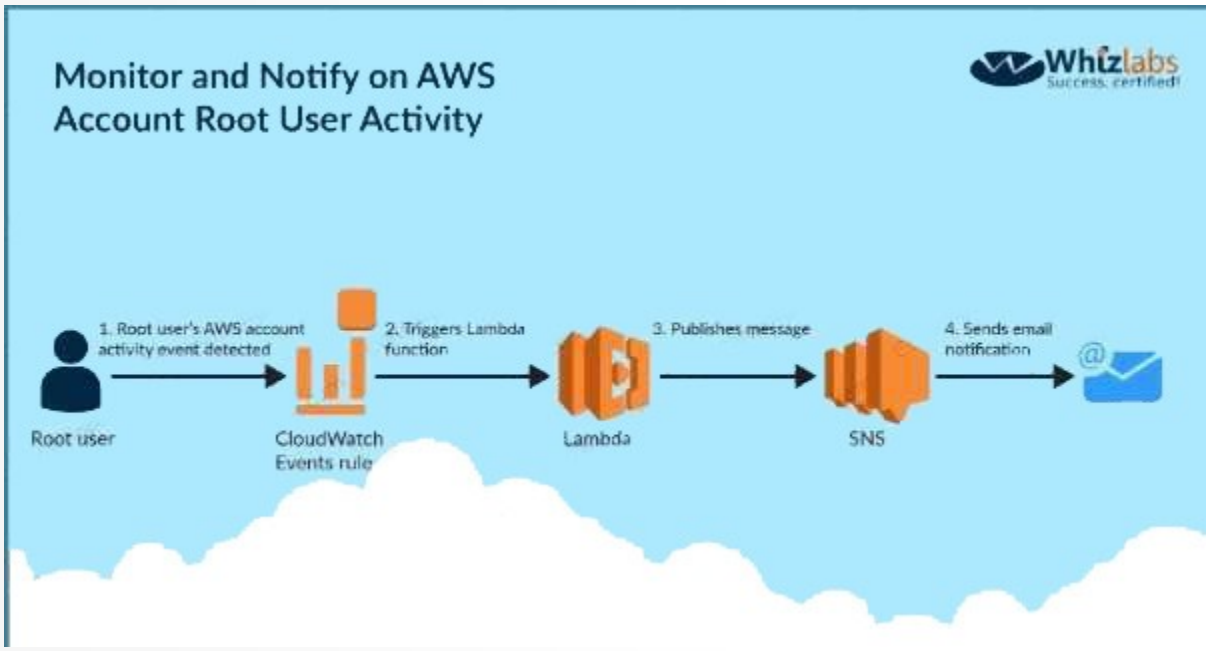
Explanation:
The AWS Documentation gives an example on such a caseInline policies are useful if you want to maintain a strict one-to-one relationship between a policy and the principal entity that if s applied to. For example, you want to be sure that the permissions in a policy are not inadvertently 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 entit 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 Polices 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-inlineThe correct answer is: An Inline Policy Submit your Feedback/Queries to our Experts

QUESTION: 5
Your company has a requirement to monitor all root user activity by notification. How can this best be achieved? Choose 2 answers from the options given below. Each answer forms part of the solutionPlease select:

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

Answer: A, C

Explanation:
Below is a snippet from the AWS blogs on a solution



Option B is invalid because you need to create a Cloudwatch Events Rule and there is such thing as a Cloudwatch Logs Rule Option D is invalid because Cloud Trail API calls can be recorded but cannot be used to send across notifications For more information on this blog article, please visit the following The correct answers are: Create a Cloudwatch Events Rule, Use a Lambda function Submit your Feedback/Queries to our Experts