SOA-C01 Q&As

AWS Certified SysOps Administrator - Associate (SOA-C01)

Pass Amazon SOA-C01 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/aws-sysops.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Amazon Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Application developers are reporting Access Denied errors when trying to list the contents of an Amazon S3 bucket by using the IAM user "arn:aws:iam::111111111111:user/application". The following S3 bucket policy is in use: How should a SysOps Administrator modify the S3 bucket policy to fix the issue?

```
{
  "Id": "S3BucketPolicy",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "List",
      "Action": [
        "s3:List*"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::bucketname/*"
      ],
      "Principal": {
        "AWS": [
          "arn:aws:iam::111111111111:user/application"
      ]
    }
  }
]
}
```

A. Change the "Effect" from "Allow" to "Deny"

B. Change the "Action" from "s3:List*" to "s3:ListBucket"

C. Change the "Resource" from "arn:aws:s3:::bucketname/*" to "arn:aws:s3:::bucketname"

D. Change the "Principal" from "arn:aws:iam::111111111111:user/application" to "arn:aws:iam::111111111111:role/application"

Correct Answer: C

QUESTION 2

A user is trying to create a list of IAM users with the AWS console. When the IAM users are creat-ed which of the below mentioned credentials will be enabled by default for the user?

A. IAM X.509 certificates

B. Nothing. Everything is disabled by default

C. IAM passwords

D. IAM access key and secret access key

Correct Answer: B

Explanation: Newly created IAM users have no password and no access key (access key ID and secret access key). If the user needs to administer your AWS resources using the AWS Management Console, you can create a password for the user. If the user needs to interact with AWS programmatically (using the command line interface (CLI), the AWS SDK, or service-specific APIs), you can create an access key for that user. The credentials you create for users are what they use to uniquely identi-fy themselves to AWS. Reference:

http://docs.aws.amazon.com/IAM/latest/UserGuide/Using_WorkingWithGroupsAndUsers.html

QUESTION 3

You have set up Individual AWS accounts for each project. You have been asked to make sure your AWS

Infrastructure costs do not exceed the budget set per project for each month.

Which of the following approaches can help ensure that you do not exceed the budget each month?

A. Consolidate your accounts so you have a single bill for all accounts and projects

B. Set up auto scaling with CloudWatch alarms using SNS to notify you when you are running too many Instances in a given account

C. Set up CloudWatch billing alerts for all AWS resources used by each project, with a notification occurring when the amount for each resource tagged to a particular project matches the budget allocated to the project.

D. Set up CloudWatch billing alerts for all AWS resources used by each account, with email notifications when it hits 50%. 80% and 90% of its budgeted monthly spend

Correct Answer: D

Explanation: Consolidate your accounts so you have a single bill for all accounts and projects (Consolidation will not help limit per account) Set up auto scaling with CloudWatch alarms using SNS to notify you when you are running too many Instances in a given account (many instances do not directly map to cost and would not give exact cost). Set up CloudWatch billing alerts for all AWS resources used by each project, with a notification occurring when the amount for each resource tagged to a particular project matches the budget allocated to the project. (as each project already has an account, no need for resource tagging).

QUESTION 4

A SysOps Administrator needs Amazon EC2 instances in two different VPCs in private subnets to be able to communicate. A peering connection between the two VPCs has been created using the AWS Management Console and shows a status of Active. The instances are still unable to send traffic to each other.

Why are the EC2 instances unable to communicate?

A. One or both of the VPCs do not have an Internet Gateway attached

B. The route tables have not been updated

C. The peering connection has not been properly tagged

D. One or both of the instances do not have an Elastic IP address assigned

Correct Answer: B

QUESTION 5

A user has created a VPC with public and private subnets using the VPC wizard. Which of the below mentioned statements is true in this scenario?

A. The AWS VPC will automatically create a NAT instance with the micro size

B. VPC bounds the main route table with a private subnet and a custom route table with a public subnet

C. The user has to manually create a NAT instance D. VPC bounds the main route table with a public subnet and a custom route table with a private subnet

Correct Answer: B

Explanation: A Virtual Private Cloud (VPC) is a virtual network dedicated to the user\\'s AWS account. A user can create a subnet with VPC and launch instances inside that subnet. If the user has created a public private subnet, the instances in the public subnet can receive inbound traffic directly from the internet, whereas the instances in the private subnet cannot. If these subnets are created with Wizard, AWS will create a NAT instance of a smaller or higher size, respectively. The VPC has an implied router and the VPC wizard updates the main route table used with the private subnet, creates a custom route table and associates it with the public subnet.