

[Download Full Version AWS-SysOps Exam Dumps\(Updated in Feb/2023\)](#)

A user has launched an EC2 instance store backed instance in the US-East-1a zone. The user created AMI #1 and copied it to the Europe region. After that, the user made a few updates to the application running in the US-East-1a zone. The user makes an AMI#2 after the changes. If the user launches a new instance in Europe from the AMI #1 copy, which of the below mentioned statements is true?

- A. The new instance will have the changes made after the AMI copy as AWS just copies the reference of the original AMI during the copying. Thus, the copied AMI will have all the updated data.
- B. The new instance will have the changes made after the AMI copy since AWS keeps updating the AMI.
- C. It is not possible to copy the instance store backed AMI from one region to another.
- D. The new instance in the EU region will not have the changes made after the AMI copy.

Correct Answer: D

Explanation:

Within EC2, when the user copies an AMI, the new AMI is fully independent of the source AMI; there is no link to the original (source) AMI. The user can modify the source AMI without affecting the new AMI and vice versa. Therefore, in this case even if the source AMI is modified, the copied AMI of the EU region will not have the changes. Thus, after copy the user needs to copy the new source AMI to the destination region to get those changes.

QUESTION 170

An AWS account owner has setup multiple IAM users. One IAM user only has CloudWatch access. He has setup the alarm action which stops the EC2 instances when the CPU utilization is below the threshold limit. What will happen in this case?

- A. It is not possible to stop the instance using the CloudWatch alarm
- B. CloudWatch will stop the instance when the action is executed
- C. The user cannot set an alarm on EC2 since he does not have the permission
- D. The user can setup the action but it will not be executed if the user does not have EC2 rights

Correct Answer: D

Explanation:

Amazon CloudWatch alarms watch a single metric over a time period that the user specifies and performs one or more actions based on the value of the metric relative to a given threshold over a number of time periods. The user can setup an action which stops the instances when their CPU utilization is below a certain threshold for a certain period of time. The EC2 action can either terminate or stop the instance as part of the EC2 action. If the IAM user has read/write permissions for Amazon CloudWatch but not for Amazon EC2, he can still create an alarm. However, the stop or terminate actions will not be performed on the Amazon EC2 instance.

QUESTION 171

When an EC2 instance that is backed by an S3-based AMI is terminated, what happens to the data on the root volume?

- A. Data is automatically deleted
- B. Data is automatically saved as an EBS snapshot.
- C. Data is unavailable until the instance is restarted

[Download Full Version AWS-SysOps Exam Dumps\(Updated in Feb/2023\)](#)

D. Data is automatically saved as an EBS volume.

Correct Answer: A

QUESTION 172

A user has setup a VPC with CIDR 20.0.0.0/16. The VPC has a private subnet (20.0.1.0/24. and a public subnet (20.0.0.0/24.. The user's data centre has CIDR of 20.0.54.0/24 and 20.1.0.0/24. If the private subnet wants to communicate with the data centre, what will happen?

- A. It will allow traffic communication on both the CIDRs of the data centre
- B. It will not allow traffic with data centre on CIDR 20.1.0.0/24 but allows traffic communication on 20.0.54.0/24
- C. It will not allow traffic communication on any of the data centre CIDRs
- D. It will allow traffic with data centre on CIDR 20.1.0.0/24 but does not allow on 20.0.54.0/24

Correct Answer: D

Explanation:

VPC allows the user to set up a connection between his VPC and corporate or home network data centre. If the user has an IP address prefix in the VPC that overlaps with one of the networks' prefixes, any traffic to the network's prefix is dropped. In this case CIDR 20.0.54.0/24 falls in the VPC's CIDR range of 20.0.0.0/16. Thus, it will not allow traffic on that IP. In the case of 20.1.0.0/24, it does not fall in the VPC's CIDR range. Thus, traffic will be allowed on it.

QUESTION 173

A user has launched two EBS backed EC2 instances in the US-East-1a region. The user wants to change the zone of one of the instances. How can the user change it?

- A. The zone can only be modified using the AWS CLI
- B. It is not possible to change the zone of an instance after it is launched
- C. Stop one of the instances and change the availability zone
- D. From the AWS EC2 console, select the Actions - > Change zones and specify the new zone

Correct Answer: B

Explanation:

With AWS EC2, when a user is launching an instance he can select the availability zone (AZ) at the time of launch. If the zone is not selected, AWS selects it on behalf of the user. Once the instance is launched, the user cannot change the zone of that instance unless he creates an AMI of that instance and launches a new instance from it.

QUESTION 174

A system admin wants to add more zones to the existing ELB. The system admin wants to perform this activity from CLI. Which of the below mentioned command helps the system admin to add new zones to the existing ELB?

- A. elb-enable-zones-for-lb
- B. elb-add-zones-for-lb
- C. It is not possible to add more zones to the existing ELB
- D. elb-configure-zones-for-lb

Correct Answer: A

Explanation:

The user has created an Elastic Load Balancer with the availability zone and wants to add more

[AWS-SysOps Exam Dumps](#) [AWS-SysOps PDF Dumps](#) [AWS-SysOps VCE Dumps](#) [AWS-SysOps Q&As](#)

<https://www.ensurepass.com/AWS-SysOps.html>

[Download Full Version AWS-SysOps Exam Dumps\(Updated in Feb/2023\)](#)

zones to the existing ELB. The user can do so in two ways:
From the console or CLI, add new zones to ELB;

QUESTION 175

A user is sending the data to CloudWatch using the CloudWatch API. The user is sending data 90 minutes in the future. What will CloudWatch do in this case?

- A. CloudWatch will accept the data
- B. It is not possible to send data of the future
- C. It is not possible to send the data manually to CloudWatch
- D. The user cannot send data for more than 60 minutes in the future

Correct Answer: A

Explanation:

With Amazon CloudWatch, each metric data point must be marked with a time stamp. The user can send the data using CLI but the time has to be in the UTC format. If the user does not provide the time, CloudWatch will take the data received time in the UTC timezone. The time stamp sent by the user can be up to two weeks in the past and up to two hours into the future.

QUESTION 176

A system admin is planning to encrypt all objects being uploaded to S3 from an application. The system admin does not want to implement his own encryption algorithm; instead he is planning to use server side encryption by supplying his own key (SSE-C.. Which parameter is not required while making a call for SSE-C?

- A. x-amz-server-side-encryption-customer-key-AES-256
- B. x-amz-server-side-encryption-customer-key
- C. x-amz-server-side-encryption-customer-algorithm
- D. x-amz-server-side-encryption-customer-key-MD5

Correct Answer: A

Explanation:

AWS S3 supports client side or server side encryption to encrypt all data at rest. The server side encryption can either have the S3 supplied AES-256 encryption key or the user can send the key along with each API call to supply his own encryption key (SSE-C.. When the user is supplying his own encryption key, the user has to send the below mentioned parameters as a part of the API calls:

x-amz-server-side-encryption-customer-algorithm: Specifies the encryption algorithm

x-amz-server-side-encryption-customer-key: To provide the base64-encoded encryption key

x-amz-server-side-encryption-customer-key-MD5: To provide the base64-encoded 128-bit MD5 digest of the encryption key

QUESTION 177

A user has created a subnet in VPC and launched an EC2 instance within it. The user has not selected the option to assign the IP address while launching the instance. Which of the below mentioned statements is true with respect to this scenario?

- A. The instance will always have a public DNS attached to the instance by default
- B. The user can directly attach an elastic IP to the instance
- C. The instance will never launch if the public IP is not assigned

[AWS-SysOps Exam Dumps](#) [AWS-SysOps PDF Dumps](#) [AWS-SysOps VCE Dumps](#) [AWS-SysOps Q&As](#)

<https://www.ensurepass.com/AWS-SysOps.html>

[Download Full Version AWS-SysOps Exam Dumps\(Updated in Feb/2023\)](#)

- D. The user would need to create an internet gateway and then attach an elastic IP to the instance to connect from internet

Correct Answer: D

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. When the user is launching an instance he needs to select an option which attaches a public IP to the instance. If the user has not selected the option to attach the public IP then it will only have a private IP when launched. The user cannot connect to the instance from the internet. If the user wants an elastic IP to connect to the instance from the internet he should create an internet gateway and assign an elastic IP to instance.

QUESTION 178

Which of the following statements about this S3 bucket policy is true?

```
{
  "Id": "IPAllowPolicy",
  "Statement": [
    {
      "Sid": "IPAllow",
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::mybucket/*",
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": "192.168.100.0/24"
        },
        "NotIpAddress": {
          "aws:SourceIp": "192.168.100.188/32"
        }
      }
    }
  ],
  "Principal": {
    "AWS": [
      "*"
    ]
  }
}
```

- A. Denies the server with the IP address 192.166 100.0 full access to the "mybucket" bucket

[Download Full Version AWS-SysOps Exam Dumps\(Updated in Feb/2023\)](#)

- B. Denies the server with the IP address 192.166 100.188 full access to the "mybucket bucket
- C. Grants all the servers within the 192 168 100 0/24 subnet full access to the "mybucket" bucket
- D. Grants all the servers within the 192 168 100 188/32 subnet full access to the "mybucket" bucket

Correct Answer: C

QUESTION 179

A user has created an Auto Scaling group with default configurations from CLI. The user wants to setup the CloudWatch alarm on the EC2 instances, which are launched by the Auto Scaling group. The user has setup an alarm to monitor the CPU utilization every minute. Which of the below mentioned statements is true?

- A. It will fetch the data at every minute but the four data points [corresponding to 4 minutes] will not have value since the EC2 basic monitoring metrics are collected every five minutes.
- B. It will fetch the data at every minute as detailed monitoring on EC2 will be enabled by the default launch configuration of Auto Scaling.
- C. The alarm creation will fail since the user has not enabled detailed monitoring on the EC2 instances.
- D. The user has to first enable detailed monitoring on the EC2 instances to support alarm monitoring at every minute.

Correct Answer: B

Explanation:

CloudWatch is used to monitor AWS as well as the custom services. To enable detailed instance monitoring for a new Auto Scaling group, the user does not need to take any extra steps. When the user creates an Auto Scaling launch config using CLI, each launch configuration contains a flag named InstanceMonitoring.Enabled. The default value of this flag is true. Thus, by default detailed monitoring will be enabled for Auto Scaling as well as for all the instances launched by that Auto Scaling group.

QUESTION 180

You have a business-to-business web application running in a VPC consisting of an Elastic Load Balancer (ELB), web servers, application servers and a database. Your web application should only accept traffic from pre-defined customer IP addresses. Which two options meet this security requirement? Choose 2 answers

- A. Configure web server VPC security groups to allow traffic from your customers' IPs
- B. Configure your web servers to filter traffic based on the ELB's "X-forwarded-for" header
- C. Configure ELB security groups to allow traffic from your customers' IPs and deny all outbound traffic
- D. Configure a VPC NACL to allow web traffic from your customers' IPs and deny all outbound traffic

Correct Answer: AB

QUESTION 181

An organization has created one IAM user and applied the below mentioned policy to the user. What entitlements do the IAM users avail with this policy?

{

"Version": "2012-10-17",

"Statement": [

[AWS-SysOps Exam Dumps](#) [AWS-SysOps PDF Dumps](#) [AWS-SysOps VCE Dumps](#) [AWS-SysOps Q&As](#)
<https://www.ensurepass.com/AWS-SysOps.html>