```
{

"Effect": "Allow",

"Action": "ec2:Describe*",

"Resource": "*"

},

{

"Effect": "Allow"

"Action": [

"cloudwatch:ListMetrics",

"cloudwatch:GetMetricStatistics",

"cloudwatch:Describe*"

],

"Resource": "*"

},

{

"Effect": "Allow",

"Action": "autoscaling:Describe*",

"Resource": "*"

}

]

}
```

A. The policy will allow the user to perform all read only activities on the EC2 services
B. The policy will allow the user to list all the EC2 resources except EBS
C. The policy will allow the user to perform all read and write activities on the EC2 services
D. The policy will allow the user to perform all read only activities on the EC2 services except load Balancing

Correct Answer: D
Explanation:
AWS Identity and Access Management is a web service which allows organizations to manage users and user permissions for various AWS services. If an organization wants to setup read only access to EC2 for a particular user, they should mention the action in the IAM policy which entitles the user for Describe rights for EC2, CloudWatch, Auto Scaling and ELB. In the policy

shown below, the user will have read only access for EC2 and EBS, CloudWatch and Auto Scaling. Since ELB is not mentioned as a part of the list, the user will not have access to ELB.

```
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": "ec2:Describe*",
"Resource": "*"
},
{
"Effect": "Allow",
"Action": [
"cloudwatch:ListMetrics",
"cloudwatch:GetMetricStatistics",
"cloudwatch:Describe*"
],
"Resource": "*"
},
{
"Effect": "Allow",
"Action": "autoscaling:Describe*",
"Resource": "*"
}
]
}
```

QUESTION 182
An organization has configured two single availability zones. The Auto Scaling groups are configured in separate zones. The user wants to merge the groups such that one group spans across multiple zones. How can the user configure this?

A. Run the command as-join-auto-scaling-group to join the two groups
B. Run the command as-update-auto-scaling-group to configure one group to span across zones and delete the other group
C. Run the command as-copy-auto-scaling-group to join the two groups
D. Run the command as-merge-auto-scaling-group to merge the groups

Correct Answer: B
Explanation:
If the user has configured two separate single availability zone Auto Scaling groups and wants to merge them then he should update one of the groups and delete the other one. While updating the first group it is recommended that the user should increase the size of the minimum, maximum and desired capacity as a summation of both the groups.

QUESTION 183
Your mission is to create a lights-out datacenter environment, and you plan to use AWS OpsWorks to accomplish this. First you created a stack and added an App Server layer with an instance running in it. Next you added an application to the instance, and now you need to deploy a MySQL RDS database instance. Which of the following answers accurately describe how to add a backend database server to an OpsWorks stack? Choose 3 answers

A. Add a new database layer and then add recipes to the deploy actions of the database and App Server layers.

B. Use OpsWorks' "Clone Stack" feature to create a second RDS stack in another Availability Zone for redundancy in the event of a failure in the Primary AZ. To switch to the secondary RDS instance, set the [:database] attributes to values that are appropriate for your server which you can do by using custom JSON.
C. The variables that characterize the RDS database connection--host, user, and so on--are set using the corresponding values from the deploy JSON's [:depioy][:app_name][:database] attributes.
D. Cookbook attributes are stored in a repository, so OpsWorks requires that the "password": "your_password" attribute for the RDS instance must be encrypted using at least a 256-bit key.
E. Set up the connection between the app server and the RDS layer by using a custom recipe. The recipe configures the app server as required, typically by creating a configuration file. The recipe gets the connection data such as the host and database name from a set of attributes in the stack configuration and deployment JSON that AWS OpsWorks installs on every instance.

Correct Answer: BCE

QUESTION 184
A user has launched an RDS MySQL DB with the Multi AZ feature. The user has scheduled the scaling of instance storage during maintenance window. What is the correct order of events during maintenance window?

1. Perform maintenance on standby
2. Promote standby to primary
3. Perform maintenance on original primary
4. Promote original master back as primary

A. 1, 2, 3, 4
B. 1, 2, 3
C. 2, 3, 1, 4
D. None of the above

Correct Answer: B
Explanation:
Running MySQL on the RDS DB instance as a Multi-AZ deployment can help the user reduce the impact of a maintenance event, as the Amazon will conduct maintenance by following the steps in the below mentioned order:
Perform maintenance on standby
Promote standby to primary
Perform maintenance on original primary, which becomes the new standby.

QUESTION 185
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.

QUESTION 186
Which method can be used to prevent an IP address block from accessing public objects in an S3 bucket?

A. Create a bucket policy and apply it to the bucket
B. Create a NACL and attach it to the VPC of the bucket
C. Create an ACL and apply it to all objects in the bucket
D. Modify the IAM policies of any users that would access the bucket

Correct Answer: A
Explanation:
http://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies.html

QUESTION 187
A user has setup a CloudWatch alarm on the EC2 instance for CPU utilization. The user has setup to receive a notification on email when the CPU utilization is higher than 60%. The user is running a virus scan on the same instance at a particular time. The user wants to avoid receiving an email at this time. What should the user do?

A. Remove the alarm
B. Disable the alarm for a while using CLI
C. Modify the CPU utilization by removing the email alert
D. Disable the alarm for a while using the console

Correct Answer: B
Explanation:
Amazon CloudWatch alarm watches 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. When the user has setup an alarm and it is know that for some unavoidable event the status may change to Alarm, the user can disable the alarm using the DisableAlarmActions API or from the command line mon- disable-alarm-actions.

QUESTION 188
In AWS, which security aspects are the customer's responsibility? Choose 4 answers

A. Controlling physical access to compute resources
B. Patch management on the EC2 instance s operating system
C. Encryption of EBS (Elastic Block Storage) volumes
D. Life-cycle management of IAM credentials
E. Decommissioning storage devices
F. Security Group and ACL (Access Control List) settings

Correct Answer: BCEF

QUESTION 189
A user is using the AWS SQS to decouple the services. Which of the below mentioned operations is not supported by SQS?

A. SendMessageBatch
B. DeleteMessageBatch
C. CreateQueue
D. DeleteMessageQueue

Correct Answer: D
Explanation:
Amazon Simple Queue Service (SQS. is a fast, reliable, scalable, and fully managed message queuing service. SQS provides a simple and cost-effective way to decouple the components of an application. The user can perform the following set of operations using the Amazon SQS: CreateQueue, ListQueues, DeleteQueue, SendMessage, SendMessageBatch, ReceiveMessage, DeleteMessage, DeleteMessageBatch, ChangeMessageVisibility, ChangeMessageVisibilityBatch, SetQueueAttributes, GetQueueAttributes, GetQueueUrl, AddPermission and RemovePermission. Operations can be performed only by the AWS account owner or an AWS account that the account owner has delegated to.

QUESTION 190
A user is planning to scale up an application by 8 AM and scale down by 7 PM daily using Auto Scaling. What should the user do in this case?

A. Setup the scaling policy to scale up and down based on the CloudWatch alarms
B. The user should increase the desired capacity at 8 AM and decrease it by 7 PM manually
C. The user should setup a batch process which launches the EC2 instance at a specific time
D. Setup scheduled actions to scale up or down at a specific time

Correct Answer: A
Explanation:
Auto Scaling based on a schedule allows the user to scale the application in response to predictable load changes. To configure the Auto Scaling group to scale based on a schedule, the user needs to create scheduled actions. A scheduled action tells Auto Scaling to perform a scaling action at a certain time in the future.

QUESTION 191
A user has enabled detailed CloudWatch monitoring with the AWS Simple Notification Service. Which of the below mentioned statements helps the user understand detailed monitoring better?

A. SNS will send data every minute after configuration
B. There is no need to enable since SNS provides data every minute
C. AWS CloudWatch does not support monitoring for SNS
D. SNS cannot provide data every minute

Correct Answer: D
Explanation:
CloudWatch is used to monitor AWS as well as the custom services. It provides either basic or detailed monitoring for the supported AWS products. In basic monitoring, a service sends data points to CloudWatch every five minutes, while in detailed monitoring a service sends data points to CloudWatch every minute. The AWS SNS service sends data every 5 minutes. Thus, it supports only the basic monitoring. The user cannot enable detailed monitoring with SNS.