



- [🏠 \(https://www.whizlabs.com/learn\)](https://www.whizlabs.com/learn) > [My Courses \(https://www.whizlabs.com/learn/my-courses\)](https://www.whizlabs.com/learn/my-courses)
- > [AWS Certified SysOps Administrator Associate \(https://www.whizlabs.com/learn/course/aws-csyopaa-practice-tests#section-1\)](https://www.whizlabs.com/learn/course/aws-csyopaa-practice-tests#section-1)
- > [Practice Test II \(https://www.whizlabs.com/learn/course/aws-csyopaa-practice-tests/quiz/12745\)](https://www.whizlabs.com/learn/course/aws-csyopaa-practice-tests/quiz/12745) > **Report**

## PRACTICE TEST II

**Attempt** 1

**Marks Obtained** 1 / 60

**Your score is** 1.67%

**Completed on** Tuesday , 29 January 2019 , 02:11 PM

**Time Taken** 00 H 00 M 04 S

**Result** Fail

### Domains / Topics wise Quiz Performance Report

S.No.	Topic	Total Questions	Correct	Incorrect	Unattempted
1	Other	60	1	0	59

<b>60</b> Questions	<b>1</b> Correct	<b>0</b> Incorrect	<b>59</b> Unattempted
------------------------	---------------------	-----------------------	--------------------------

Show Answers

All	▼
-----	---

QUESTION 1      CORRECT

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?

- ☒ 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

### Explanation :

Answer – A

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.

#### 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 wrong because you need to assign rules for the WebSecurity Group.

Option C and D are invalid because you don't need to worry about Outbound rules based on the question.

For more information on security groups please visit the below link:

- [http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC\\_Scenario2.html](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2.html)  
([http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC\\_Scenario2.html](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2.html))

Ask our Experts



QUESTION 2 UNATTEMPTED

A root account owner is trying to understand the S3 bucket ACL. Choose one of the following group which cannot be used to set up an ACL permission on the objects.

- ☐ A. Authenticated user group
- ☐ B. All users group
- ☐ C. Log Delivery Group
- ☐ D. Canonical user group ✓

**Explanation :**

Answer – D

If you look at the bucket ACL permissions in S3, you can see the below options. Hence option A,B and C are right.

## ▼ Permissions

You can control access to the bucket and its contents using access policies. [Learn more.](#)

[What's new in Amazon S3](#) [Amazon S3](#) [Amazon S3](#) [Amazon S3](#) [Amazon S3](#) [Amazon S3](#) [Amazon S3](#) [Amazon S3](#) [Amazon S3](#) [Amazon S3](#)

Grantee:  ☒ List ☒ Upload/Delete ☐ View Permissions ☐ Edit Permissions X

Grantee:   ☐ List ☐ Upload/Delete ☐ View Permissions ☐ Edit Permissions X

Everyone

Any Authenticated AWS User



Add more

Log Delivery

Me

Policy



Add CORS Configuration

For more information on S3 ACL, please visit the link:

- <http://docs.aws.amazon.com/AmazonS3/latest/dev/acl-overview.html>  
(<http://docs.aws.amazon.com/AmazonS3/latest/dev/acl-overview.html>)

Ask our Experts



QUESTION 3 UNATTEMPTED

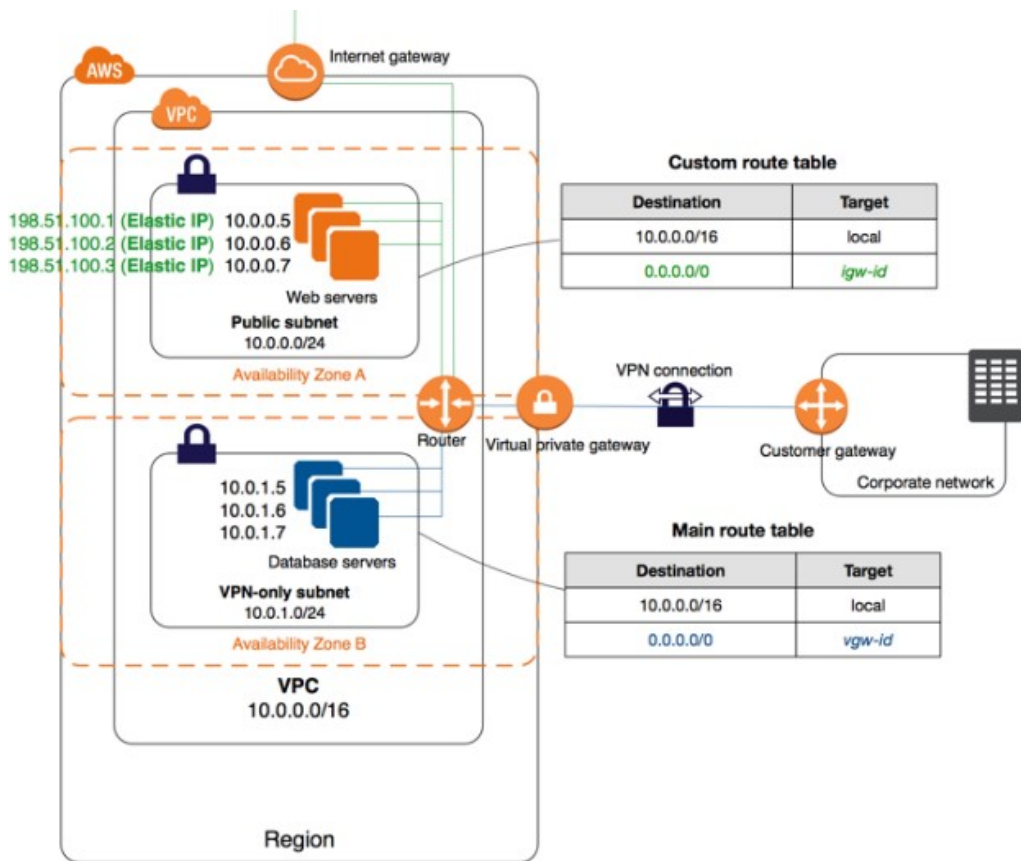
A user has created a VPC with CIDR 20.0.0.0/16 using the wizard. The user has created a public subnet CIDR (20.0.0.0/24) and VPN only subnets CIDR (20.0.1.0/24) along with the VPN gateway (vgw-12345) to connect to the user's data centre. The user's data centre has CIDR 172.28.0.0/12. The user has also setup a NAT instance (i-12345) to allow traffic to the internet from the VPN subnet. Which of the below mentioned options is not a valid entry for the main route table in this scenario?

- ☐ A. Destination: 20.0.1.0/24 and Target: i-12345 ✓
- ☐ B. Destination: 0.0.0.0/0 and Target: i-12345
- ☐ C. Destination: 172.28.0.0/12 and Target: vgw-12345
- ☐ D. Destination: 20.0.0.0/16 and Target: local

**Explanation :**

Answer – A

The below diagram shows how a typical setup for a VPC with VPN and Internet gateway would look like. The only routing option which should have access to the internet gateway should be the 0.0.0.0/0 address. So Option A is the right answer.



For more information on VPC with the option of VPN, please visit the link:

- [http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC\\_Scenario3.html](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario3.html)  
([http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC\\_Scenario3.html](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario3.html))

Ask our Experts



#### QUESTION 4 UNATTEMPTED

A user has created a VPC with public and private subnets using the VPC wizard. The VPC has CIDR 20.0.0.0/16. The private subnet uses CIDR 20.0.0.0/24. The NAT instance ID is i-a12345. Which of the below mentioned entries are created in the main route table attached with the private subnet to allow instances to connect with the internet?

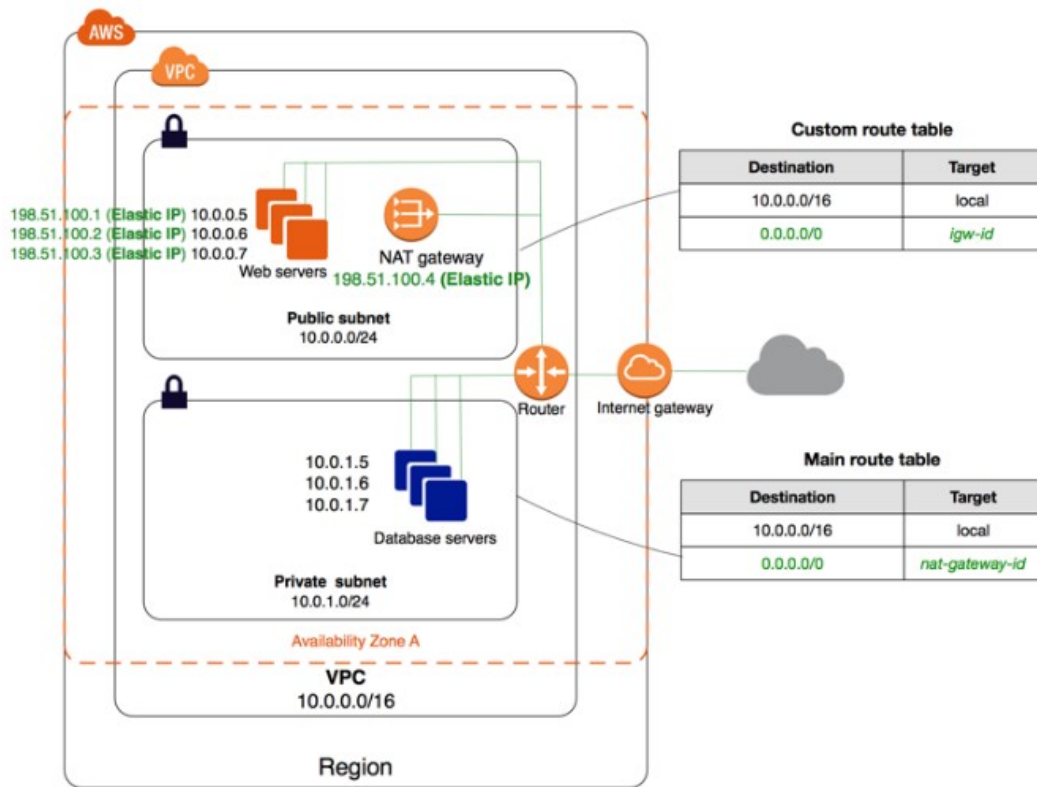
- ☐ A. Destination: 0.0.0.0/0 and Target: i-a12345 ✓

- ☐ B. Destination: 20.0.0.0/0 and Target: 80
- ☐ C. Destination: 20.0.0.0/0 and Target: i-a12345
- ☐ D. Destination: 20.0.0.0/24 and Target: i-a12345

### Explanation :

Answer – A

The below diagram shows how a typical setup for a VPC with a NAT would look like. It clear shows that the CIDR 0.0.0.0/0 should be attached to the internet gateway.



For more information on VPC with the NAT option, please visit the link:

- [https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC\\_Route\\_Tables.html](https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Route_Tables.html)  
([https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC\\_Route\\_Tables.html](https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Route_Tables.html))
- [http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC\\_Scenario2.html](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2.html)  
([http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC\\_Scenario2.html](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2.html))

Ask our Experts



QUESTION 5 UNATTEMPTED

A root account owner has given full access of his S3 bucket to one of the IAM users using the bucket ACL. When the IAM user logs in to the S3 console, which actions can he perform?

- ☐ A. He can just view the content of the bucket
- ☐ B. He can do all the operations on the bucket
- ☒ C. It is not possible to give access to an IAM user using ACL ✓
- ☐ D. The IAM user can perform all operations on the bucket using only API/SDK

**Explanation :**

Answer – C

Amazon S3 access control lists (ACLs) enable you to manage access to buckets and objects. When you create a bucket or an object, Amazon S3 creates a default ACL that grants the resource owner full control over the resource.

You can grant permission to an AWS account using the email address or the canonical user ID. However, if you provide an email address in your grant request, Amazon S3 finds the canonical user ID for that account and adds it to the ACL.

The diagram below shows how you can add an email address or a User ID to grant permission to an AWS account.

Permissions

You can control access to the bucket and its contents using access policies. [Learn more.](#)

Grantee	List	Upload/Delete	View Permissions	Edit Permissions
Everyone	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Grantee: [dropdown]	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Buttons: Add more..., policy, Add CORS Configuration

The table given below gives a full description of the permissions that can be set on the ACL of S3 bucket.



For more information please visit:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/acl-overview.html>  
 (https://docs.aws.amazon.com/AmazonS3/latest/dev/acl-overview.html)

Since the user has been provided with Full Access he can do all the operations on the bucket.

**Note:** As per AWS, You can use ACLs to grant basic read/write permissions to other AWS accounts. There are limits to managing permissions using ACLs. For example, **you can grant permissions only to other AWS accounts; you cannot grant permissions to users in your account.** You cannot grant conditional permissions, nor can you explicitly deny permissions.

For more information please visit:

[https://docs.aws.amazon.com/AmazonS3/latest/dev/S3\\_ACLs\\_UsingACLs.html](https://docs.aws.amazon.com/AmazonS3/latest/dev/S3_ACLs_UsingACLs.html)  
 (https://docs.aws.amazon.com/AmazonS3/latest/dev/S3\_ACLs\_UsingACLs.html)

Ask our Experts



## QUESTION 6 UNATTEMPTED

An organization has configured Auto Scaling with ELB. There is a memory issue in the application which is causing CPU utilization to go above 90%. The higher CPU usage triggers an event for Auto Scaling as per the scaling policy. If the user wants to find the root cause inside the application without triggering a scaling activity, how can he achieve this?

- ☐ A. Stop the scaling process until research is completed
- ☐ B. It is not possible to find the root cause from that instance without triggering scaling
- ☐ C. Delete Auto Scaling until research is completed
- ☒ D. Suspend the scaling process until research is completed ✓

**Explanation :**

Answer – D

From the AWS documentation it is very clear that the suspending process for Autoscaling can be used to debug root causes with the application.

Auto Scaling enables you to suspend and then resume one or more of the Auto Scaling processes in your Auto Scaling group. This can be very useful when you want to investigate a configuration problem or other issue with your web application and then make changes to your application, without triggering the Auto Scaling process.

For more information on suspending autoscaling processes, please visit the link:

- <http://docs.aws.amazon.com/autoscaling/latest/userguide/as-suspend-resume-processes.html> (<http://docs.aws.amazon.com/autoscaling/latest/userguide/as-suspend-resume-processes.html>)

**Note:** The terminology used for this scenario is "suspended processes" not stop by AWS. Hence, option D would be the correct answer.

Please check the below link to know more about it.

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-suspend-resume-processes.html#as-suspend-resume>  
(<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-suspend-resume-processes.html#as-suspend-resume>)

Ask our Experts



A user has launched an EC2 instance. The instance got terminated as soon as it was launched. Which of the below mentioned options is not a possible reason for this?

- ☐ A. The user account has reached the maximum EC2 instance limit ✓
- ☐ B. The snapshot is corrupt
- ☐ C. The AMI is missing a required part
- ☐ D. The user account has reached the maximum volume limit

### Explanation :

Answer – A

For more information on this particular issue, please visit the link:

- [http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using\\_InstanceStraightToTerminated.html](http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_InstanceStraightToTerminated.html)  
([http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using\\_InstanceStraightToTerminated.html](http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_InstanceStraightToTerminated.html))

The AWS documentation makes it very clear as to why an instance might terminate immediately.

After you launch an instance, we recommend that you check its status to confirm that it goes from the *pending* state to the *running* state, not the *terminated* state.

The following are a few reasons why an instance might immediately terminate:

- You've reached your EBS volume limit. For information about the volume limit, and to submit a request to increase your volume limit, see [Request to Increase the Amazon EBS Volume Limit](#).
- An EBS snapshot is corrupt.
- The instance store-backed AMI you used to launch the instance is missing a required part (an image.part.xx file).

When the user account has reached the maximum number of EC2 instances, it will not be allowed to launch an instance. AWS will throw an 'InstanceLimitExceeded' error. For all other reasons, such as "AMI is missing part", "Corrupt Snapshot" or "Volume limit has reached" it will launch an EC2 instance and then terminate it.

### Note:

The question states that the instance got terminated as soon as it is launched.

Options B,C,and D can be a reason for this.

But we need to know which **one of these is not a reason** for this behaviour.

Option A is the answer. Because if we have reached the maximum number of EC2 instance it won't even launch the instance.

Ask our Experts



QUESTION 8 UNATTEMPTED

A user is trying to understand the detailed CloudWatch monitoring concept. Which of the below mentioned services does not provide detailed monitoring with CloudWatch?

- ☐ A. AWSEMR ✓
- ☐ B. AWSRDS
- ☐ C. AWSELB
- ☐ D. AWS Route53

**Explanation :**

Answer – A

If you look at the AWS documentation you will see that the cloudwatch metrics for EMR is 5 minutes and cannot be configured beyond this.

Metrics are updated every five minutes. This interval is not configurable. Metrics are archived for two weeks; after that period, the data is discarded.

These metrics are automatically collected and pushed to CloudWatch for every Amazon EMR cluster. There is no charge for the Amazon EMR metrics reported in CloudWatch; they are provided as part of the Amazon EMR service.

For more information on metrics for EMR, please visit the link:

- [http://docs.aws.amazon.com/emr/latest/ManagementGuide/UsingEMR\\_ViewingMetrics.html](http://docs.aws.amazon.com/emr/latest/ManagementGuide/UsingEMR_ViewingMetrics.html)  
([http://docs.aws.amazon.com/emr/latest/ManagementGuide/UsingEMR\\_ViewingMetrics.html](http://docs.aws.amazon.com/emr/latest/ManagementGuide/UsingEMR_ViewingMetrics.html))

Ask our Experts



QUESTION 9 UNATTEMPTED

A user is measuring the CPU utilization of a private data centre machine every minute. The machine provides the aggregate of data every hour, such as Sum of data", "Min value", "Max value, and "Number of Data points". The user wants to send these values to CloudWatch. How can the user achieve this?

- ☐ A. Send the data using the put-metric-data command with the aggregate-values parameter
- ☐ B. Send the data using the put-metric-data command with the average-values parameter
- ☐ C. Send the data using the put-metric-data command with the statistic-values parameter ✓
- ☐ D. Send the data using the put-metric-data command with the aggregate -data parameter

#### Explanation :

Answer – C

You can aggregate your data before you publish to CloudWatch. When you have multiple data points per minute, aggregating data minimizes the number of calls to **put-metric-data**.

An example of the command is given below

```
AWS cloudwatch put-metric-data --metric-name PageViewCount --namespace MyService --
statistic-value Sum=11,Minimum=2,Maximum=5,SampleCount=3 --timestamp 2016-10-
14T12:00:00.000Z
```

For more information on the command, please visit the link:

- <http://docs.aws.amazon.com/cli/latest/reference/cloudwatch/put-metric-data.html>  
(<http://docs.aws.amazon.com/cli/latest/reference/cloudwatch/put-metric-data.html>)

Ask our Experts



QUESTION 10

UNATTEMPTED

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 ✓

#### Explanation :

Answer – D

If you look at the AWS documentation you will see that the cloudwatch metrics for SNS is 5 minutes and cannot be configured beyond this.

The metrics you configure with CloudWatch for your Amazon SNS topics are automatically collected and pushed to CloudWatch every five minutes. These metrics are gathered on all topics that meet the CloudWatch guidelines for being active. A topic is considered active by CloudWatch for up to six hours from the last activity (i.e., any API call) on the topic.

For more information on the SNS monitoring, please visit the link:

- <http://docs.aws.amazon.com/sns/latest/dg/MonitorSNSwithCloudWatch.html>  
(<http://docs.aws.amazon.com/sns/latest/dg/MonitorSNSwithCloudWatch.html>)

**Note:** Detailed monitoring, or one-minute metrics, is currently unavailable for Amazon Simple Notification Service.

Ask our Experts



QUESTION 11 UNATTEMPTED

A user wants to find the particular error that occurred on a certain date in the AWS MySQL RDS DB. Which of the below mentioned activities may help the user to get the data easily?

- ☐ A. It is not possible to get the log files for MySQL RDS
- ☐ B. Find all the transaction logs and query on those records

- ☐ C. Direct the logs to the DB table and then query that table ✓
- ☐ D. Download the log file to DynamoDB and search for the record

#### Explanation :

Answer – C

You can monitor the MySQL error log, slow query log, and the general log. The MySQL error log is generated by default; you can generate the slow query and general logs by setting parameters in your DB parameter group. Amazon RDS rotates all of the MySQL log files; the intervals for each type are given following.

You can monitor the MySQL logs directly through the Amazon RDS console, Amazon RDS API, Amazon RDS CLI, or AWS SDKs. You can also access MySQL logs by directing the logs to a database table in the main database and querying that table. You can use the mysqlbinlog utility to download a binary log.

Since AWS rotates the logs, it's better to store the logs in a DB to ensure you archive all the logs and you can then have the ability to find the errors in the log based on the date.

For more information on the MySQL logs, please visit the link:

- [http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER\\_LogAccess.Concepts.MySQL.html](http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_LogAccess.Concepts.MySQL.html)  
([http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER\\_LogAccess.Concepts.MySQL.html](http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_LogAccess.Concepts.MySQL.html))

Ask our Experts



#### QUESTION 12 UNATTEMPTED

A user has created a VPC with CIDR 20.0.0.0/16 using the wizard. The user has created public and VPN only subnets along with hardware VPN access to connect to the user's data centre. The user has not yet launched an instance, nor modified, or deleted any of the original setup. Now he wants to delete this VPC from the console. Will the console allow the user to delete the VPC?

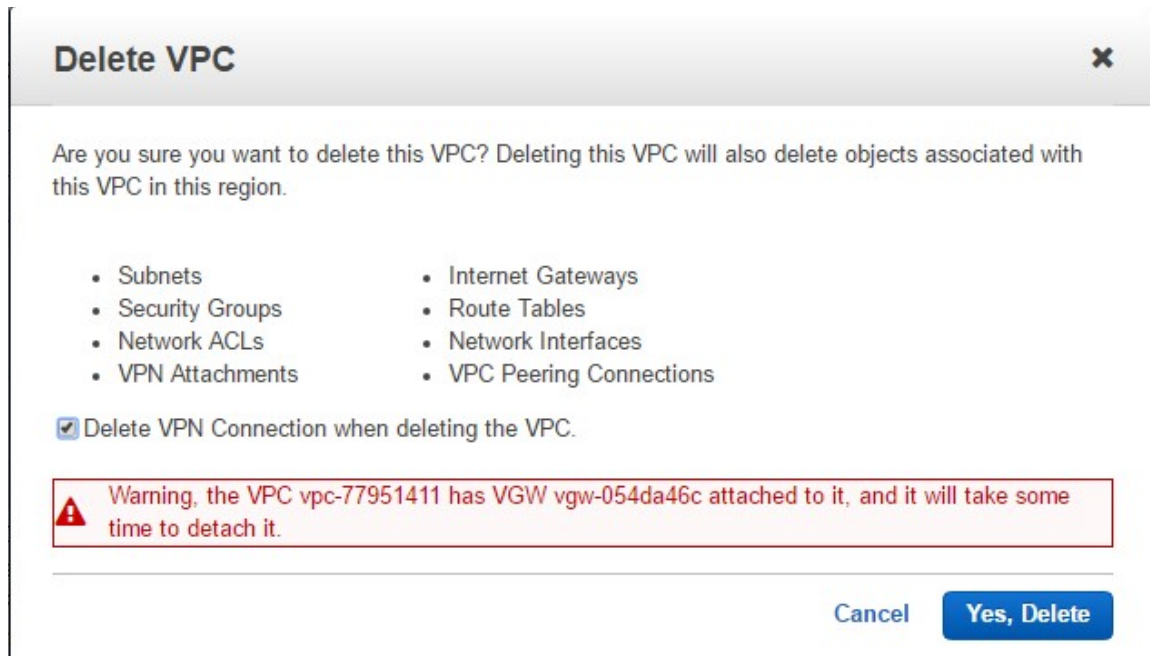
- ☐ A. Yes, the console will delete all the setups and also delete the virtual private gateway
- ☐ B. No, the console will ask the user to manually detach the virtual private gateway first and then allow deleting the VPC

- ☐ C. Yes, the console will delete all the setups and detach the virtual private gateway ✓
- ☐ D. No, since the NAT instance is running

**Explanation :**

Answer – C

The below screenshot shows the deletion of a VPC that has a VPN connection. You will be prompted with a warning, but in the end the VPC will delete it along with all the related components.



For more information on VPC and subnets please visit the below link:

- [http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC\\_Subnets.html](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html)  
([http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC\\_Subnets.html](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html))

Ask our Experts



QUESTION 13 UNATTEMPTED

A user is trying to send custom metrics to CloudWatch using the PutMetricData APIs. What is the limit for sending this data to CloudWatch?



- ☐ A. The size of the request is limited to 40 KB in size for HTTP POST requests. ✓
- ☐ B. The size of the request is limited to 40 KB in size for HTTP PUT requests.
- ☐ C. The size of the request is limited to 40 KB in size for HTTP GET requests.
- ☐ D. The size of the request is limited to 256 KB in size for HTTP POST requests.

Explanation :

Answer – A

## put-metric-data

### Description

Publishes metric data points to Amazon CloudWatch. Amazon CloudWatch associates the data points with the specified metric. If the specified metric does not exist, Amazon CloudWatch creates the metric. When Amazon CloudWatch creates a metric, it can take up to fifteen minutes for the metric to appear in calls to list-metrics .

Each put-metric-data request is limited to 8 KB in size for HTTP GET requests and is limited to 40 KB in size for HTTP POST requests.

- <https://docs.aws.amazon.com/sdkfornet/v3/apidocs/index.html?page=CloudWatch/MCloudWatchPutMetricDataPutMetricDataRequest.html>  
(<https://docs.aws.amazon.com/sdkfornet/v3/apidocs/index.html?page=CloudWatch/MCloudWatchPutMetricDataPutMetricDataRequest.html>)

Ask our Experts



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

#### Explanation :

Answer – C

For more information on cloudwatch access, please visit the link:

- <http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/auth-and-access-control-cw.html> (<http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/auth-and-access-control-cw.html>)

If you have read/write permissions for Amazon CloudWatch **you can create an alarm with out any EC2 actions associated with it.** When **you try to add an EC2 action with the alarm** you will not be able to save the alarm and **you will receive the following error message.**

**"A system administrator must provision SWF permissions for your IAM user so that the IAM user can perform this action."**

Please find the observations from the scenario mentioned in the question.

user -dptest, IAM permission -cloudwatchfullaccess

Logged in as dptest and created an alarm with out any actions and the user was able to save the alarm. Please see the diagram below.

Create Alarm

Add to Dashboard

Actions ▾

Filter: All alarms ▾

Search Alarms

X

Hide all AutoScaling alarms ⓘ

1 to 1 of 1 alarms

< >

State ▾	Name ▾	Threshold ▾	Config Status ▾
INSUFFICIENT_DATA	testdp-alarm1	CPUUtilization >= 80 for 1 datapoints within 5 minutes	No actions

State Details:

State changed to INSUFFICIENT DATA at 2018/06/20. Reason: Unchecked: Initial alarm creation

Description:

testdp-alarm on ec2

Threshold:

CPUUtilization >= 80 for 1 datapoints within 5 minutes

Actions:

This alarm has no associated actions. For example it will not notify or auto-scale when it triggers. Please modify this alarm to add actions.

Namespace:

AWS/EC2

Metric Name:

CPUUtilization

Dimensions:

InstanceId = i-0ab7f3179f11e244b (Tag loading not authorized)

Statistic:

Average

Period:

5 minutes

Treat missing data as:

missing

Percentiles with evaluate low samples:

testdp-alarm1

CPUUtilization >= 80 for 1 datapoints within 5...

Time	CPU Utilization (%)
6/20 07:00	80
6/20 08:00	80
6/20 09:00	80

Next step

Then the user modified the alarm to add an EC2 action to stop the instance, then the user received the following error message.

**"A system administrator must provision SWF permissions for your IAM user so that the IAM user can perform this action."**

## Actions

Define what actions are taken when your alarm changes state.

EC2 Action Delete

**Whenever this alarm:** State is ALARM

**Take this action:**  
☐ Recover this instance ⓘ  
☒ Stop this instance ⓘ  
☐ Terminate this instance ⓘ  
☐ Reboot this instance ⓘ

This will stop your EC2 instance (i-0ab7f3179f11e244b).  
You can only stop an instance if it is backed by an EBS volume.

A system administrator must provision SWF permissions for your IAM user so that the IAM user can perform this action.

+ Notification

+ AutoScaling Action

+ EC2 Action

Period: 5 Minutes

Statistic: ☒ Standard ☐ Custom

Average

So based on these findings Option C is correct.

As per AWS documentation,

"If you have read/write permissions for Amazon CloudWatch but not for Amazon EC2, you can still create an alarm but the stop or terminate actions won't be performed on the instance.

- <https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/UsingAlarmActions.html>  
(<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/UsingAlarmActions.html>)

We can interpret the above AWS documentation as,

If you have read/write permissions for Amazon CloudWatch you can create an alarm with out any EC2 actions associated with it. When you try to add an EC2 action with the alarm you will not be able to save the alarm and you will receive the following error message.

"A system administrator must provision SWF permissions for your IAM user so that the IAM user can perform this action."



QUESTION 15 UNATTEMPTED

A user has configured ELB with Auto Scaling. The user suspended the Auto Scaling terminate process only for a while. What will happen to the availability zone rebalancing process AZRebalance during this period?

- ☐ A. Auto Scaling will not launch or terminate any instances
- ☒ B. Auto Scaling will allow the instances to grow more than the maximum size ✓
- ☐ C. Auto Scaling will keep launching instances till the maximum instance size
- ☐ D. It is not possible to suspend the terminate process while keeping the launch active

**Explanation :**

Answer – B

The AWS documentation clearly says that if you suspend the terminate process, there is a chance that the instances can grow more than the maximum size due to AZRebalance.

If you suspend *Launch*, *AZRebalance* neither launches new instances nor terminates existing instances. This is because *AZRebalance* terminates instances only after launching the replacement instances. If you suspend *Terminate*, your Auto Scaling group can grow up to ten percent larger than its maximum size, because Auto Scaling allows this temporarily during rebalancing activities. If Auto Scaling cannot terminate instances, your Auto Scaling group could remain above its maximum size until you resume the *Terminate* process.

For more information on Suspend and Resume process, please visit the link:

- <http://docs.aws.amazon.com/autoscaling/latest/userguide/as-suspend-resume-processes.html> (<http://docs.aws.amazon.com/autoscaling/latest/userguide/as-suspend-resume-processes.html>)

Ask our Experts



QUESTION 16 UNATTEMPTED

A user has created a mobile application which makes calls to DynamoDB to fetch certain data

The application is using the DynamoDB SDK and root account access/secret access key to connect to DynamoDB from mobile. Which of the below mentioned statements is true with respect to the best practice for security in this scenario?

- ☐ A. The user should create a separate IAM user for each mobile application and provide DynamoDB access with it
- ☐ B. The user should create an IAM role with DynamoDB and EC2 access. Attach the role with EC2 and route all calls from the mobile through EC2
- ☐ C. The application should use an IAM role with web identity federation which validates calls to DynamoDB with identity providers, such as Google, Amazon, and Facebook ✓
- ☐ D. Create an IAM Role with DynamoDB access and attach it with the mobile application

#### Explanation :

Answer – C

With web identity federation, you don't need to create custom sign-in code or manage your own user identities. Instead, users of your app can sign in using a well-known identity provider (IdP) —such as Login with Amazon, Facebook, Google, or any other OpenID Connect (OIDC) (<http://openid.net/connect/>)-compatible IdP, receive an authentication token, and then exchange that token for temporary security credentials in AWS that map to an IAM role with permissions to use the resources in your AWS account

And always the best way to authenticate is to ensure that you create an IAM role which can then be assigned to the EC2 instance.

For more information on Web Identity Federation, please visit the link:

- [http://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_roles\\_providers\\_oidc.html](http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_oidc.html)  
([http://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_roles\\_providers\\_oidc.html](http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_oidc.html))

Ask our Experts



A user is configuring the Multi AZ feature of an RDS DB. The user came to know that this

RDS DB does not use the AWS technology, but uses server mirroring to achieve HA.

Which DB is the user using right now?

- ☐ A. My SQL
- ☐ B. Oracle
- ☒ C. MS SQL ✓
- ☐ D. PostgreSQL

#### Explanation :

Answer – C

As per the AWS documentation it is very clear that MultiAZ is supported for MySQL, MariaDb, Oracle and PostgreSQL. With Microsoft SQL server, you need to use the native mirroring to achieve High Availability.

Multi-AZ deployments for the MySQL, MariaDB, Oracle, and PostgreSQL engines utilize synchronous physical replication to keep data on the standby up-to-date with the primary. Multi-AZ deployments for the SQL Server engine use synchronous logical replication to achieve the same result, employing SQL Server-native Mirroring technology. Both approaches safeguard your data in the event of a DB Instance failure or loss of an Availability Zone.

For more information on RDS MultiAZ, please visit the link:

- <https://aws.amazon.com/rds/details/multi-az/> (<https://aws.amazon.com/rds/details/multi-az/>)

Ask our Experts



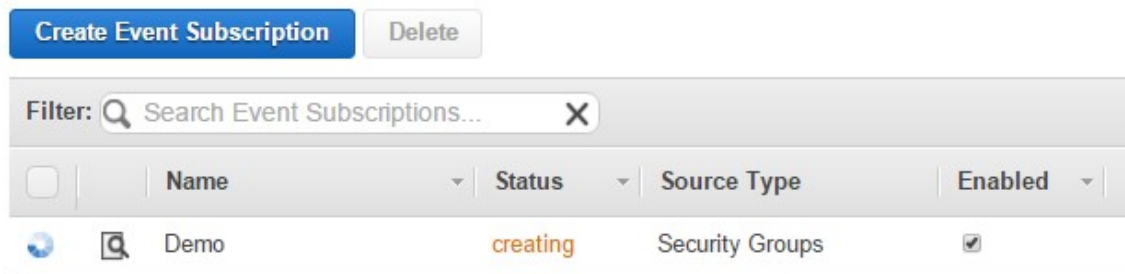
A user is receiving a notification from the RDS DB whenever there is a change in the DB security group. The user does not want to receive these notifications for only a month. Thus, he does not want to delete the notification. How can the user configure this?

- ☐ A. Change the Disable button for notification to “Yes” in the RDS console
- ☐ B. Set the send mail flag to false in the DB event notification console
- ☐ C. The only option is to delete the notification from the console
- ☐ D. Change the Enable button for notification to “No” in the RDS console ✓

#### Explanation :

Answer – D

When you have an Event subscription, you can simply disable it by de-selecting on the Enabled option.



For more information on RDS Event subscriptions, please visit the link:

- [http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER\\_Events.html](http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_Events.html)  
([http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER\\_Events.html](http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_Events.html))

Ask our Experts





A user has created a VPC with CIDR 20.0.0.0/16. The user has created one subnet with CIDR 20.0.0.0/16 by mistake. The user is trying to create another subnet of CIDR 20.0.1.0/24. How can the user create the second subnet?

- ☐ A. There is no need to update the subnet as VPC automatically adjusts the CIDR of the first subnet based on the second subnet's CIDR
- ☐ B. The user can modify the first subnet CIDR from the console
- ☐ C. It is not possible to create a second subnet as one subnet with the same CIDR as the VPC has been created ✓
- ☐ D. The user can modify the first subnet CIDR with AWS CLI

#### Explanation :

Answer – C

Once you create a subnet, you cannot modify it, you have to delete it. Hence option B and D are wrong.

Also the VPC will not create the second subnet because of the overlapping CIDR and hence you need to delete and recreate the subnet again.

Below is the screenshot of what happens when you try to create a subnet of CIDR 20.0.0.1/24 on an existing subnet of 20.0.0.0/16

The screenshot shows the 'Create Subnet' dialog box in the AWS Management Console. It includes fields for 'Name tag' (20.0.0.1/24), 'VPC' (vpc-0624a460 | 20.0.0.0/16), and 'Availability Zone' (No Preference). The 'CIDR block' field is set to 20.0.0.1/24, which is highlighted in red with an error message: 'CIDR block 20.0.0.1/24 overlaps with pre-existing CIDR block 20.0.0.0/16 from subnet-78664d31 | 20.0.0.0/16.' The dialog has 'Cancel' and 'Yes, Create' buttons at the bottom right.

For more information on VPC and subnets, please visit the link:

- [http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC\\_Subnets.html](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html)  
([http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC\\_Subnets.html](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html))

Ask our Experts



QUESTION 20 UNATTEMPTED

A user is trying to understand the detailed CloudWatch monitoring concept. Which of the below mentioned services provides detailed monitoring with CloudWatch without charging the user extra?

- ☐ A. AWS ELB ✓
- ☐ B. AWSEC2
- ☐ C. AWSEMR
- ☐ D. AWS SNS

**Explanation :**

Answer – A

If you look at the product details for Amazon Cloudwatch, it clearly mentions that detailed monitoring is by default enabled for ELB for certain metrics with no additional charge.

Compute & Networking   Storage & Content Delivery   Databases & Analytics   Other

No additional software needs to be installed.

- **Auto Scaling groups:** seven pre-selected metrics at one-minute frequency, optional and for no additional charge.
- **Elastic Load Balancers:** thirteen pre-selected metrics at one-minute frequency, for no additional charge.
- **Amazon Route 53 health checks:** One pre-selected metric at one-minute frequency, for no additional charge.

For more information on Cloudwatch, please visit the link:

- <https://aws.amazon.com/cloudwatch/details/>  
(<https://aws.amazon.com/cloudwatch/details/>)
- <https://www.amazonaws.cn/en/cloudwatch/details/>  
(<https://www.amazonaws.cn/en/cloudwatch/details/>)

Ask our Experts



QUESTION 21

UNATTEMPTED

A user is trying to understand the CloudWatch metrics for the AWS services. It is required that the user should first understand the namespace for the AWS services. Which of the below mentioned is not a valid namespace for the AWS services?

- ☐ A. AWS/StorageGateway
- ☒ B. AWS/CloudTrail ✓
- ☐ C. AWS/ElastiCache
- ☐ D. AWS/SWF

**Explanation :**

Answer – B

As per Amazon, below are the list of valid namespaces and Cloudtrail is not present in this list.

AWS Product	Namespace
Amazon API Gateway	AWS/ApiGateway
AppStream 2.0	AWS/AppStream
Amazon EC2 Auto Scaling	AWS/AutoScaling
AWS Billing	AWS/Billing
Amazon CloudFront	AWS/CloudFront
Amazon CloudSearch	AWS/CloudSearch
Amazon CloudWatch Events	AWS/Events
Amazon CloudWatch Logs	AWS/Logs
Amazon Connect	AWS/Connect
AWS Database Migration Service	AWS/DMS
AWS Direct Connect	AWS/DX
Amazon DynamoDB	AWS/DynamoDB
Amazon EC2	AWS/EC2
Amazon EC2	AWS/EC2Spot (Spot Instances)
Amazon Elastic Container Service	AWS/ECS
AWS Elastic Beanstalk	AWS/ElasticBeanstalk
Amazon Elastic Block Store	AWS/EBS
Amazon Elastic File System	AWS/EFS
Elastic Load Balancing	AWS/ELB (Classic Load Balancers)
Elastic Load Balancing	AWS/ApplicationELB (Application Load Balancers)
Elastic Load Balancing	AWS/NetworkELB (Network Load Balancers)
Amazon Elastic Transcoder	AWS/ElasticTranscoder
Amazon ElastiCache	AWS/ElastiCache

Amazon Elasticsearch Service	AWS/ES
Amazon EMR	AWS/ElasticMapReduce
Amazon GameLift	AWS/GameLift
Amazon Inspector	AWS/Inspector
AWS IoT	AWS/IoT
AWS Key Management Service	AWS/KMS
Amazon Kinesis Data Analytics	AWS/KinesisAnalytics
Amazon Kinesis Data Firehose	AWS/Firehose
Amazon Kinesis Data Streams	AWS/Kinesis
Amazon Kinesis Video Streams	AWS/KinesisVideo
AWS Lambda	AWS/Lambda
Amazon Lex	AWS/Lex
Amazon Machine Learning	AWS/ML
AWS OpsWorks	AWS/OpsWorks
Amazon Polly	AWS/Polly
Amazon Redshift	AWS/Redshift
Amazon Relational Database Service	AWS/RDS
Amazon Route 53	AWS/Route53
Amazon SageMaker	AWS/SageMaker
AWS Shield Advanced	AWS/DDoSProtection
Amazon Simple Email Service	AWS/SES
Amazon Simple Notification Service	AWS/SNS
Amazon Simple Queue Service	AWS/SQS
Amazon Simple Storage Service	AWS/S3
Amazon Simple Workflow Service	AWS/SWF
AWS Step Functions	AWS/States
AWS Storage Gateway	AWS/StorageGateway
Amazon VPC	AWS/NATGateway (NAT gateway)
Amazon VPC	AWS/VPN (VPN)
AWS WAF	WAF
Amazon WorkSpaces	AWS/WorkSpaces

For more information on Cloudwatch namespaces, please visit the link:

- <http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/aws-namespaces.html> (<http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/aws-namespaces.html>)

Ask our Experts



## QUESTION 22 UNATTEMPTED

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 valid 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

### Explanation :

Answer – A

As per the AWS documentation, below are the parameters passed for SSE-C encryption for S3. And in this list x-amz-server-side-encryption-customer-key-AES-256 is not present.

Name	Description
<code>x-amz-server-side-encryption-customer-algorithm</code>	Use this header to specify the encryption algorithm. The header value must be "AES256".
<code>x-amz-server-side-encryption-customer-key</code>	Use this header to provide the 256-bit, base64-encoded encryption key for Amazon S3 to use to encrypt or decrypt your data.
<code>x-amz-server-side-encryption-customer-key-MD5</code>	Use this header to provide the base64-encoded 128-bit MD5 digest of the encryption key according to <a href="#">RFC 1321</a> . Amazon S3 uses this header for a message integrity check to ensure the encryption key was transmitted without error.

For more information on S3 SSE-C encryption, please visit the link:

- <http://docs.aws.amazon.com/AmazonS3/latest/dev/ServerSideEncryptionCustomerKeys.html>  
(<http://docs.aws.amazon.com/AmazonS3/latest/dev/ServerSideEncryptionCustomerKeys.html>)

Ask our Experts



QUESTION 23

UNATTEMPTED

A user is trying to create a PIOPS EBS volume with 5000 IOPS and 17000 GiB size. AWS does not allow the user to create this volume. What is the possible root cause of this?

- ☐ A. The ratio between IOPS and the EBS volume is higher than 30
- ☐ B. The maximum IOPS supported by EBS is 3000
- ☐ C. The ratio between IOPS and the EBS volume is lower than 50
- ☐ D. PIOPS does not support a size higher than 16384GiB ✓

**Explanation :**

Answer – D

The below screenshot shows what happens when you try to create a volume with the above specification. You will get the below error which shows that Option D is the right answer.

### Create Volume ✕

Volume Type ⓘ

Provisioned IOPS SSD (IO1) ▾

Size (GiB) ⓘ

17000 (Min: 4 GiB, Max: 16384 GiB)

⚠ Size can't exceed 16384 GiB

IOPS ⓘ

5000 (Min: 100 IOPS, Max: 20000 IOPS)

Throughput (MB/s) ⓘ

Not Applicable

Availability Zone ⓘ

us-east-1a ▾

Snapshot ID ⓘ

Search (case-insensitive)

Encryption ⓘ

☐ Encrypt this volume

Cancel

Create

For more information on the EBS storage types please visit the below link:

- <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html>  
(<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html>)

Ask our Experts



#### QUESTION 24 UNATTEMPTED

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 ✓

#### Explanation :

Answer – D

Below are the various operations provided by AWS on SQS. In this list DeleteMessageQueue is not present.



## Basic Message Operations

- **SendMessage:** Send messages to a specified queue.
- **ReceiveMessage:** Return one or more messages from a specified queue.
- **DeleteMessage:** Remove a previously received message from a specified queue.
- **ChangeMessageVisibility:** Change the visibility timeout of a previously received message.

## Batch Message Operations

- **SendMessageBatch:** Send multiple messages to a specified queue.
- **DeleteMessageBatch:** Remove multiple previously received messages from a specified queue.
- **ChangeMessageVisibilityBatch:** Change the visibility timeout of multiple previously received messages.

## Basic Queue Management

- **CreateQueue:** Create queues for use with your AWS account.
- **ListQueues:** List your existing queues.
- **DeleteQueue:** Delete one of your queues.
- **PurgeQueue:** Delete all the messages in a queue.

## Advanced Queue Management

- **SetQueueAttributes:** Control queue settings such as the visibility timeout (amount of time that messages are locked after being read so they cannot be read again), a delay value, or dead letter queue parameters.
- **GetQueueAttributes:** Get information about a queue such as the visibility timeout, number of messages in the queue, or the maximum message size.
- **GetQueueUrl:** Get the queue URL.
- **AddPermission:** Add queue sharing for another AWS account for a specified queue.
- **RemovePermission:** Remove an AWS account from queue sharing for a specified queue.
- **ListDeadLetterSourceQueues:** List the queues attached to a dead letter queue.

For more information on SQS please visit the link:

- <https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-api-permissions-reference.html>  
(<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-api-permissions-reference.html>)
- <https://aws.amazon.com/sqs/faqs/> (<https://aws.amazon.com/sqs/faqs/>)

Ask our Experts



## QUESTION 25

## UNATTEMPTED

A user has configured Auto Scaling with 3 instances. The user had created a new AMI after updating one of the instances. If the user wants to terminate two specific instances to ensure that Auto Scaling launches an instances with the new launch configuration, which command should he run?

- ☐ A. `delete-instance-in-auto-scaling-group <Instance ID> --no-decrement-desired-capacity`
- ☐ B. `terminate-instance-in-auto-scaling-group <Instance ID> --update-desired-capacity`
- ☐ C. `terminate-instance-in-auto-scaling-group <Instance ID> --decrement-desired-capacity`
- ☒ D. `terminate-instance-in-auto-scaling-group <Instance ID> --no-should-decrement-desired-capacity` ✓

**Explanation :**

Answer – D

To terminate an instance using the CLI you need to use the `terminate-instance-in-auto-scaling-group` command. In this command , the user can specify the instance id which needs to be deleted. They need to mention the `--no-should-decrement-desired-capacity` option so that Autoscaling will launch instances with the new AMI configuration.

**Syntax:** `AWS autoscaling terminate-instance-in-auto-scaling-group --instance-id i-88563d9c --no-should-decrement-desired-capacity`.

**NOTE:** `*--no*` (It's a double code)

For more information on the `terminate-instance-in-auto-scaling-group` command visit the link:

- <https://docs.aws.amazon.com/cli/latest/reference/autoscaling/terminate-instance-in-auto-scaling-group.html> (<https://docs.aws.amazon.com/cli/latest/reference/autoscaling/terminate-instance-in-auto-scaling-group.html>)

Ask our Experts



A user has launched an EC2 instance. However, due to some reason the instance was terminated. If the user wants to find out the reason for termination, where can he find the details?

- ☐ A. It is not possible to find the details after the instance is terminated
- ☐ B. The user can get information from the AWS console, by checking the Instance description under the State transition reason label ✓
- ☐ C. The user can get information from the AWS console, by checking the Instance description under the Instance Status Change reason label
- ☐ D. The user can get information from the AWS console, by checking the Instance description under the Instance Termination reason label

### Explanation :

Answer – B

For each instance there is a property called State transition reason. This will show the user the reason as to why an EC2 instance would have been terminated.

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS
	i-00acbc26037124...	t2.micro	us-east-1a	running	2/2 checks ...	None	

Alarm status	None
Kernel ID	-
RAM disk ID	-
Placement group	-
Virtualization	hvm
Reservation	r-0ac5bc9f794ef3afc
AMI launch index	0
Tenancy	default
Host ID	-
Affinity	-
State transition reason	-

For more information on this topic visit the link:

- [http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using\\_InstanceStraightToTerminated.html](http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_InstanceStraightToTerminated.html)  
([http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using\\_InstanceStraightToTerminated.html](http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_InstanceStraightToTerminated.html))

Ask our Experts



QUESTION 27

UNATTEMPTED

A user has created a VPC with CIDR 20.0.0.0/24. The user has used all the IPs of CIDR and wants to increase the size of the VPC. The user has two subnets: public (20.0.0.0/25. and private (20.0.0.128/25). How can the user change the size of the VPC?

- ☐ A. The user can delete all the instances of the subnet. Change the size of the subnets to 20.0.0.0/32 and 20.0.1.0/32, respectively. Then the user can increase the size of the VPC using CLI
- ☐ B. It is not possible to change the size of the VPC once it has been created
- ☐ C. The user can add a subnet with a higher range so that it will automatically increase the size of the VPC
- ☐ D. You can expand your existing VPC by adding four (4) secondary IPv4 IP ranges (CIDRs) to your VPC ✓

#### Explanation :

Answer – D

You can expand your existing VPC by adding four (4) secondary IPv4 IP ranges (CIDRs) to your VPC. You can shrink your VPC by deleting the secondary CIDR blocks you have added to your VPC. You cannot however change the size of the IPv6 address range of your VPC.

#### Q. Can I change a VPC's size?

Yes. You can expand your existing VPC by adding four (4) secondary IPv4 IP ranges (CIDRs) to your VPC. You can shrink your VPC by deleting the secondary CIDR blocks you have added to your VPC. You cannot however change the size of the IPv6 address range of your VPC.

For more information on VPC's visit the link:

- <https://aws.amazon.com/vpc/faqs/> (<https://aws.amazon.com/vpc/faqs/>)

The correct answer is: You can expand your existing VPC by adding four (4) secondary IPv4 IP ranges (CIDRs) to your VPC

**Note:**

We can have up to 4 secondary CIDR block associated with a VPC. So in total 5 CIDR blocks. (1 primary and 4 secondary). If you try to associate a 5th secondary CIDR block it will give you an error.

Q. Can I change a VPC's size?

No. To change the size of a VPC you must terminate your existing VPC and create a new one.

CIDR ①	Status	Status reason	
10.1.0.0/16	associated	-	⊗
10.2.0.0/16	associated	-	⊗
10.3.0.0/16	associated	-	⊗
10.4.0.0/16	associated	-	⊗
10.5.0.0/16	associated	-	⊗
⚠ This network vpc-dbb70eb3 has met its maximum number of allowed CIDRs: 5			
10.10.0.0/16	-	-	⊗ ✓

Ask our Experts



A user has configured ELB with SSL using a security policy for secure negotiation between the client and load balancer. Which of the below mentioned security policies is supported by ELB?

- ☐ A. Dynamic Security Policy
- ☐ B. All the other options
- ☒ C. Predefined Security Policy ✓
- ☐ D. Default Security Policy

**Explanation :**

Answer – C

A security policy determines which ciphers and protocols are supported during SSL negotiations between a client and a load balancer. Elastic Load Balancing supports configuring your load balancer to use either predefined or custom security policies.

For more information on ELB security policies visit the link:

- <http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-security-policy-options.html> (<http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-security-policy-options.html>)

Ask our Experts



QUESTION 29 UNATTEMPTED

A user has configured an ELB to distribute the traffic among multiple instances. The user instances are facing some issues due to the back-end servers. Which of the below mentioned CloudWatch metrics helps the user understand the issue with the instances?

- ☐ A. HTTPCode\_Backend\_3XX
- ☐ B. HTTPCode\_Backend\_4XX
- ☐ C. HTTPCode\_Backend\_2XX

☐ D. HTTPCode\_Backend\_5XX ✓

**Explanation :**

Answer – D

The Either HTTPCode\_Backend\_5XX for the load balancer is caused by issues in the backend servers. The different sort of errors are given below

- HTTP 502: Bad Gateway
- HTTP 503: Service Unavailable
- HTTP 504: Gateway Timeout

Option A is wrong because this indicates a redirect response sent from the registered instances.

Option B is wrong because this indicates a client error response sent from the registered instances.

Option C is wrong because this indicates a normal, successful response from the registered instances.

For more information on ELB errors visit the link:

- <http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/ts-elb-http-errors.html>  
(<http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/ts-elb-http-errors.html>)

Ask our Experts



QUESTION 30 UNATTEMPTED

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 ✓

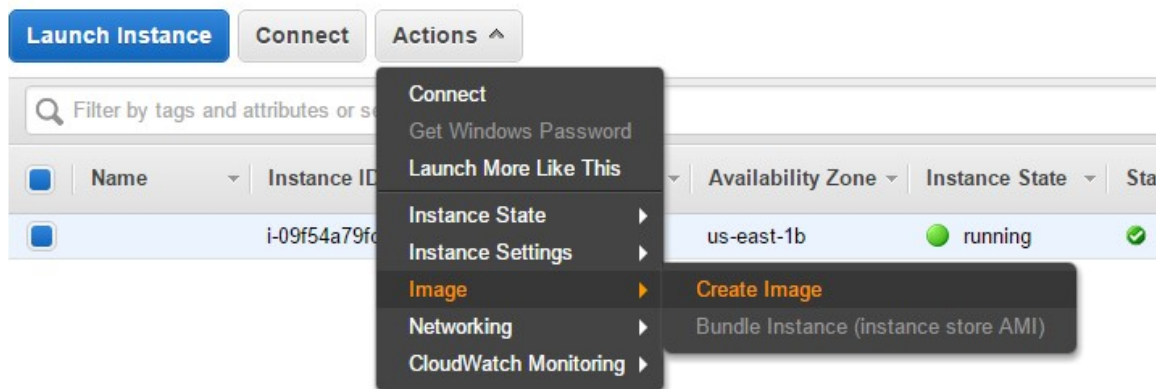
### Explanation :

Answer – D

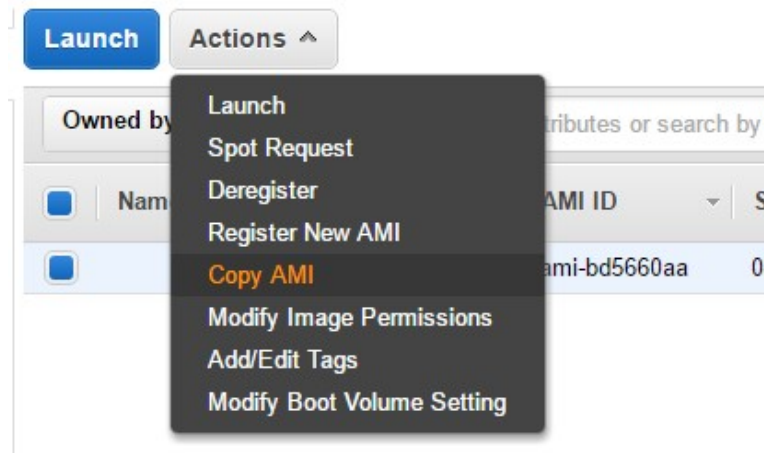
Everytime you make a change to the instance you need to make an AMI out of it and copy it to the desired region. Only then will the instance created out of that AMI have the required changes.

To copy AMI's , follow the below steps

Step 1) The first step is to create an AMI from your running instance by choosing on Image->Create Image.



Step 2) Once the Image has been created, go to the AMI section in the EC2 dashboard and click on the Copy AMI option.



Step 3) In the next screen , you can specify where to copy the AMI to.





- ☒ C. Initializing the EBS volume ✓
- ☐ D. Formatting the EBS volume

### Explanation :

Answer – C

New EBS volumes receive their maximum performance the moment that they are available and do not require initialization (formerly known as pre-warming). However, storage blocks on volumes that were restored from snapshots must be initialized (pulled down from Amazon S3 and written to the volume) before you can access the block. This preliminary action takes time and can cause a significant increase in the latency of an I/O operation the first time each block is accessed

The dd command is installed by default on Linux systems and is used to read all of the blocks on the device.

[dd] The if (input file) parameter should be set to the drive you wish to initialize. The of (output file) parameter should be set to the Linux null virtual device, /dev/xvdf (Based on the question). The bs parameter sets the block size of the read operation; for optimal performance, this should be set to 1 MB.

In order to Pre-warm existing data and un-used space with a read and write back operation where a command reads your blocks and writes them back to the same location. This pre-warms your complete volume and existing data won't be erased.

Ask our Experts



### QUESTION 32 UNATTEMPTED

A user has created a VPC with a public subnet. The user has terminated all the instances which are part of the subnet. Which of the below mentioned statements is true with respect to this scenario?

- ☐ A. The user cannot delete the VPC since the subnet is not deleted
- ☒ B. All network interface attached with the instances have been deleted ✓

- ☐ C. When the user launches a new instance it cannot use the same subnet
- ☐ D. The subnet to which the instances were launched with will be deleted

**Explanation :**

Answer – B

When you delete an instance the elastic network interface which in the below example of eth0 will also be deleted.

Filter by tags and attributes or search by keyword	
<input type="checkbox"/>	Name
<input type="checkbox"/>	Instance ID
<input type="checkbox"/>	Instance Type
<input type="checkbox"/>	i-00acbc260371247b7
<input type="checkbox"/>	t2.micro
Secondary private IPs	
VPC ID	
vpc-3e6dde58	
Subnet ID	
subnet-dfd2a5f2	
Network interfaces	
eth0	
Source/dest. check	
True	
EBS-optimized	
False	
Root device type	
ebs	
Root device	
/dev/xvda	
Block devices	
/dev/xvda	

For information on elastic network interfaces , please visit the link:

- <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html>  
(<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html>)

Ask our Experts



A user has configured ELB with SSL using a security policy for secure negotiation between the client and load balancer. The ELB security policy supports various ciphers. Which of the below mentioned options helps identify the matching cipher at the client side to the ELB cipher list when client is requesting ELB DNS over SSL?

- ☐ A. Cipher Protocol
- ☐ B. Client Configuration Preference
- ☒ C. Server Order Preference ✓
- ☐ D. Load Balancer Preference

#### Explanation :

Answer – C

If you select a policy that is enabled for Server Order Preference, the load balancer uses the ciphers in the order that they are specified in this table to negotiate connections between the client and load balancer. Otherwise, the load balancer uses the ciphers in the order that they are presented by the client.

Security Policy	2016-08	2015-05	2015-03	2015-02	2014-10	2014-01	2011-08
<b>SSL Protocols</b>							
Protocol-SSLv3						♦	♦
Protocol-TLSv1	♦	♦	♦	♦	♦	♦	♦
Protocol-TLSv1.1	♦	♦	♦	♦	♦	♦	
Protocol-TLSv1.2	♦	♦	♦	♦	♦	♦	
<b>SSL Options</b>							
Server Order Preference	♦	♦	♦	♦	♦	♦	

For information on ELB security , please visit the link:

- <http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-security-policy-table.html> (<http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-security-policy-table.html>)

Ask our Experts



A user has setup a custom application which generates a number in decimals. The user wants to track that number and setup the alarm whenever the number is above a certain limit. The application is sending the data to CloudWatch at regular intervals for this purpose.

Which of the below mentioned statements is not true with respect to the above scenario?

- ☐ A. The user can get the aggregate data of the numbers generated over a minute and send it to CloudWatch
- ☐ B. The user has to supply the Timestamp with each data point ✓
- ☐ C. CloudWatch will not truncate the number until it has an exponent larger than 126.
- ☐ D. The user can create a file in the JSON format with the metric name and value and supply it to CloudWatch

#### Explanation :

Answer – B

The statement you have provided is more on recommendation rather than requirement. Time stamp is not a compulsory parameter, if we don't specify the timestamp, Cloudwatch will automatically create a time stamp for the data point. I have extracted the documentation for your convenience:

#####

#### Time Stamps

Each metric data point must be marked with a time stamp. The time stamp can be up to two weeks in the past and up to two hours into the future. If you do not provide a time stamp, CloudWatch creates a time stamp for you based on the time the data point was received.

Time stamps are ***dateTime*** objects, with the complete date plus hours, minutes, and seconds (for example, 2016-10-31T23:59:59Z). For more information, see [dateTime](http://www.w3.org/TR/xmlschema-2/#dateTime) (<http://www.w3.org/TR/xmlschema-2/#dateTime>). Although it is not required, we recommend that you use Coordinated Universal Time (UTC). When you retrieve statistics from CloudWatch, all times are in UTC.

CloudWatch alarms check metrics based on the current time in UTC. Custom metrics sent to CloudWatch with time stamps other than the current UTC time can cause alarms to display the **Insufficient Data** state or result in delayed alarms.

####

Please refer to the link below for more info:

- [https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/cloudwatch\\_concepts.html](https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/cloudwatch_concepts.html)  
([https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/cloudwatch\\_concepts.html](https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/cloudwatch_concepts.html))

As per the AWS documentation below are the required parameters when using the put metric data command.

### Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

#### **MetricData.member.N**

The data for the metric.

Type: array of [MetricDatum](#) objects

Required: Yes

#### **Namespace**

The namespace for the metric data.

You cannot specify a namespace that begins with "AWS/". Namespaces that begin with "AWS/" are reserved for use by Amazon Web Services products.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 255.

Pattern: `[^:]*`

Required: Yes

For more information on publishing custom metrics, please visit the link:

- <http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/publishingMetrics.html>  
(<http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/publishingMetrics.html>)

Ask our Experts



A user has created a VPC with public and private subnets. The VPC has CIDR 20.0.0.0/16. The private subnet uses CIDR 20.0.1.0/24 and the public subnet uses CIDR 20.0.0.0/24. The user is planning to host a web server in the public subnet (port 80) and a DB server in the private subnet (port 3306). The user is configuring a security group of the NAT instance. Which of the below mentioned entries is not required for the NAT security group?

- ☐ A. For Inbound allow Source: 20.0.1.0/24 on port 80
- ☐ B. For Outbound allow Destination: 0.0.0.0/0 on port 80
- ☒ C. For Inbound allow Source: 20.0.0.0/24 on port 80 ✓
- ☐ D. For Outbound allow Destination: 0.0.0.0/0 on port 443

#### Explanation :

Answer – C

As per AWS below are the recommended rules for a NAT instance. Hence based on the best practice, Option C is a correct statement.

#### NATSG: Recommended Rules

Inbound			
Source	Protocol	Port Range	Comments
10.0.1.0/24	TCP	80	Allow inbound HTTP traffic from servers in the private subnet
10.0.1.0/24	TCP	443	Allow inbound HTTPS traffic from servers in the private subnet
Public IP address range of your home network	TCP	22	Allow inbound SSH access to the NAT instance from your home network (over the Internet gateway)
Outbound			
Destination	Protocol	Port Range	Comments
0.0.0.0/0	TCP	80	Allow outbound HTTP access to the Internet
0.0.0.0/0	TCP	443	Allow outbound HTTPS access to the Internet

For information on NAT security , please visit the link:

- [http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC\\_NAT\\_Instance.html](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_NAT_Instance.html)  
([http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC\\_NAT\\_Instance.html](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_NAT_Instance.html))

**Note:**

The Question says that "Which of the below mentioned entries **is not required** for the NAT security group?"

20.0.0.0/24 is on the public subnet, hence not required to be mentioned in NAT security group.

Hence, the answer would be option C.

Ask our Experts



QUESTION 36 UNATTEMPTED

An organization (Account ID 123412341234). has attached the below mentioned IAM policy to a user. What does this policy statement entitle the user to perform?

{

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

"Statement": [{

"Sid": "AllowUsersAllActionsForCredentials",

"Effect": "Allow",

"Action": [

"iam:\*LoginProfile",

"iam:\*AccessKey\*",

"iam:\*SigningCertificate"

],

"Resource": ["arn:AWS:iam::123412341234:user/\${AWS:username}"]

}]

}

- ☐ A. The policy allows the IAM user to modify all IAM user's credentials using the console, SDK, CLI or APIs



- ☐ B. The policy will give an invalid resource error
- ☐ C. The policy allows the IAM user to modify all credentials using only the console
- ☐ D. The policy allows the user to modify the IAM user's password, sign in certificates and access keys using only CLI, SDK or APIs ✓

#### Explanation :

Answer – D

First in order to give a user a certain set of policies , you need to mention the following line. The AWS:username will apply to the AWS logged in user.

Resource": "arn:AWS:iam::account-id-without-hyphens:user/\${AWS:username}

Next the policies will give the permissions to modify IAM user password, sign in certificates and access keys using only CLI, SDK or APIs

"iam:\*LoginProfile",

"iam:\*AccessKey\*",

"iam:\*SigningCertificate\*"

For information on IAM security policies , please visit the link:

- [http://docs.aws.amazon.com/IAM/latest/UserGuide/access\\_policies.html](http://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html)  
([http://docs.aws.amazon.com/IAM/latest/UserGuide/access\\_policies.html](http://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html))
- [https://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_credentials\\_delegate-permissions\\_examples.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_delegate-permissions_examples.html)  
([https://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_credentials\\_delegate-permissions\\_examples.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_delegate-permissions_examples.html))

Ask our Experts



#### QUESTION 37 UNATTEMPTED

A system admin is trying to understand the sticky session algorithm. Please select the correct sequence of steps, both when the cookie is present and when it is not, to help the admin understand the implementation of the sticky session:

1. ELB inserts the cookie in the response
2. ELB chooses the instance based on the load balancing algorithm

3. Check the cookie in the service request

4. The cookie is found in the request

5. The cookie is not found in the request

- ☐ A. 3,1,4,2 [Cookie is not Present] & 3,1,5,2 [Cookie is Present]
- ☐ B. 3,4,1,2 [Cookie is not Present] & 3,5,1,2 [Cookie is Present]
- ☐ C. 3,5,2,1 [Cookie is not Present] & 3,4,2,1 [Cookie is Present] ✓
- ☐ D. 3,2,5,4 [Cookie is not Present] & 3,2,4,5 [Cookie is Present]

#### Explanation :

Answer – C

This is how the ELB algorithm works in general when Cookie is not present

- First it checks the cookie is present in the service request
- Since the cookie is not found in the request it will then decide which instance the service request should be routed to.
- Finally the cookie is inserted in the response

This is how the ELB algorithm works in general when Cookie is present

- First it checks the cookie is present in the service request
- Since the cookie is found in the request it will then decide which instance the service request should be routed to based on the already present cookie.
- Finally the cookie is inserted in the response

For information on ELB sticky sessions, please visit the link:

- <http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-sticky-sessions.html>  
(<http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-sticky-sessions.html>)

Ask our Experts



A user has a weighing plant. The user measures the weight of some goods every 5 minutes and sends data to AWS CloudWatch for monitoring and tracking. Which of the below mentioned parameters is mandatory for the user to include in the request list?

- ☐ A. Value
- ☒ B. Namespace ✓
- ☐ C. Metric Name
- ☐ D. Timezone

#### Explanation :

Answer – B

A general syntax of the put-metric-data command which is used to publish the data on to cloudwatch is given below.

```
AWS cloudwatch put-metric-data --metric-name PageViewCount --namespace MyService --value 2 --timestamp 2016-10-14T12:00:00.000Z
```

For more details please check AWS Docs for put-metric below:

- <https://docs.aws.amazon.com/cli/latest/reference/cloudwatch/put-metric-data.html>  
(<https://docs.aws.amazon.com/cli/latest/reference/cloudwatch/put-metric-data.html>)

If you go to the below link you will see the mandatory parameters for this command which is namespace and metricname URL:

- [http://docs.aws.amazon.com/AmazonCloudWatch/latest/APIReference/API\\_PutMetricData.html](http://docs.aws.amazon.com/AmazonCloudWatch/latest/APIReference/API_PutMetricData.html)  
([http://docs.aws.amazon.com/AmazonCloudWatch/latest/APIReference/API\\_PutMetricData.html](http://docs.aws.amazon.com/AmazonCloudWatch/latest/APIReference/API_PutMetricData.html))

For information on publishing custom metrics, please visit the link:

- <http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/publishingMetrics.html>  
(<http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/publishingMetrics.html>)

Ask our Experts



An organization has configured Auto Scaling for hosting their application. The system admin wants to understand the Auto Scaling health check process. If the instance is unhealthy, Auto Scaling launches an instance and terminates the unhealthy instance. What is the order execution?

- ☐ A. Auto Scaling launches a new instance first and then terminates the unhealthy instance
- ☐ B. Auto Scaling performs the launch and terminate processes in a random order
- ☐ C. Auto Scaling launches and terminates the instances simultaneously
- ☒ D. Auto Scaling terminates the instance first and then launches a new instance ✓

#### Explanation :

Answer – D

The AWS documentation clearly mentions that if the an instance becomes unhealthy as part of a health check then the instance is first terminated and then a new one is launched.

### Maintaining the Number of Instances in Your Auto Scaling Group

After you have created your launch configuration and Auto Scaling group, the Auto Scaling group starts by launching the minimum number of EC2 instances (or the desired capacity, if specified). If there are no other scaling conditions attached to the Auto Scaling group, the Auto Scaling group maintains this number of running instances at all times.

To maintain the same number of instances, Auto Scaling performs a periodic health check on running instances within an Auto Scaling group. When it finds that an instance is unhealthy, it terminates that instance and launches a new one.

All instances in your Auto Scaling group start in the healthy state. Instances are assumed to be healthy unless Auto Scaling receives notification that they are unhealthy. This notification can come from one or more of the following sources: Amazon EC2, Elastic Load Balancing, or your customized health check.

For information on Autoscaling groups and managing instances, please visit the link:

- <http://docs.aws.amazon.com/autoscaling/latest/userguide/as-maintain-instance-levels.html> (<http://docs.aws.amazon.com/autoscaling/latest/userguide/as-maintain-instance-levels.html>)

Ask our Experts



## QUESTION 40

UNATTEMPTED

A user is trying to connect to a running EC2 instance using SSH. However, the user gets an Unprotected Private Key File error. Which of the below mentioned options can be a possible reason for rejection?

- ☒ A. The private key file has the wrong file permission ✓
- ☐ B. The ppk file used for SSH is read only
- ☐ C. The public key file has the wrong permission
- ☐ D. The user has provided the wrong user name for the OS login

**Explanation :**

Answer – A

Your private key file must be protected from read and write operations from any other users. If your private key can be read or written to by anyone but you, then SSH ignores your key and you see the error as shown in the question. This error can be resolved by changing the permissions on your key.  
`chmod 0400 .ssh/my_private_key.pem`

For information on EC2 troubleshooting, please visit the link:

- <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/TroubleshootingInstancesConnecting.html>  
(<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/TroubleshootingInstancesConnecting.html>)

Ask our Experts



## QUESTION 41

UNATTEMPTED

A user has provisioned 2000 IOPS to the EBS volume. The application hosted on that EBS is experiencing less IOPS than provisioned. Which of the below mentioned options does not affect the IOPS of the volume?

- ☐ A. The application does not have enough IO for the volume
- ☐ B. The instance is EBS optimized
- ☐ C. The EC2 instance has 10 Gigabit Network connectivity

☐ D. The volume size is too large ✓

**Explanation :**

Answer – D

The question states that the user has provision 2000 IOPS to the EBS volume. However the application is not making use of it. A few options are listed in the question and we need to select the option which won't affect the IOPS.

If the application itself is not having enough I/O operation then it can be a cause. Hence option A is not the right option.

If the instance is not EBS optimized then this can effect it. Hence option B is not the right choice.

EC2 instance with 10Gigabit Network connectivity is good enough for EBS volume to work efficiently. So it is not causing this issue. Hence Option C is also not the right choice.

AWS says that "Whatever your EBS volume type, if you are not experiencing the IOPS or throughput you expect in your configuration, ensure that your EC2 instance bandwidth is not the limiting factor. You should always use a current-generation, EBS-optimized instance (or one that includes 10 Gb/s network connectivity) for optimal performance. Another possible cause for not experiencing the expected IOPS is that you are not driving enough I/O to the EBS volumes."

The volume size is not an attribute that need to be considered for this issue. The only choice that **does not affect the IOPS** is Option D.

For information on the various EBS volumes, please visit the link:

- <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html>  
(<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html>)
- <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-io-characteristics.html>  
(<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-io-characteristics.html>)

Ask our Experts



QUESTION 42 UNATTEMPTED

A storage admin wants to encrypt all the objects stored in S3 using server side encryption. The user does not want to use the AES 256 encryption key provided by S3. How can the user achieve this?

- ☐ A. The admin should upload his secret key to the AWS console and let S3 decrypt the objects
- ☐ B. The admin should use CLI or API to upload the encryption key to the S3 bucket. When making a call to the S3 API mention the encryption key URL in each request
- ☐ C. S3 does not support client supplied encryption keys for server side encryption
- ☐ D. The admin should send the keys and encryption algorithm with each API call ✓

**Explanation :**

Answer – D

Server-side encryption is about protecting data at rest. Using server-side encryption with customer-provided encryption keys (SSE-C) allows you to set your own encryption keys. With the encryption key you provide as part of your request, Amazon S3 manages both the encryption, as it writes to disks, and decryption, when you access your objects. Therefore, you don't need to maintain any code to perform data encryption and decryption. The only thing you do is manage the encryption keys you provide.

For information on S3 server side encryption, please visit the link:

- <http://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html>  
(<http://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html>)

Ask our Experts



QUESTION 43 UNATTEMPTED

A user has scheduled a maintenance window of an RDS DB on Monday at 3 AM. Which of the below events may force to take the DB instance offline during the maintenance window?

- ☐ A. Enabling Read Replica
- ☐ B. Making the DB Multi AZ
- ☐ C. DB password change
- ☐ D. Security patching ✓

### Explanation :

Answer – D

As per the AWS documentation it is clearly given that the maintenance window is only for scale operations or security patching.

The only maintenance events that require Amazon RDS to take your DB instance offline are scale compute operations (which generally take only a few minutes from start-to-finish) or required software patching. Required patching is automatically scheduled only for patches that are security and durability related. Such patching occurs infrequently (typically once every few months) and should seldom require more than a fraction of your maintenance window. If you do not specify a preferred weekly maintenance window when creating your DB instance, a 30 minute default value is assigned. If you wish to modify when maintenance is performed on your behalf, you can do so by modifying your DB instance in the [AWS Management Console](#), the [ModifyDBInstance API](#) or the [modify-db-instance command](#). Each of your DB instances can have different preferred maintenance windows, if you so choose.

For information on AWS rds, please visit the link:

- <https://aws.amazon.com/rds/faqs/> (<https://aws.amazon.com/rds/faqs/>)

Ask our Experts



### QUESTION 44 UNATTEMPTED

An organization has launched 5 instances: 2 for production and 3 for testing. The organization wants that one particular group of IAM users should only access the test instances and not the production ones. How can the organization set that as a part of the policy?

- ☐ A. Launch the test and production instances in separate regions and allow region wise access to the group
- ☐ B. Define the IAM policy which allows access based on the instance ID
- ☐ C. Create an IAM policy with a condition which allows access to only small instances
- ☐ D. Define the tags on the test and production servers and add a condition to the IAM policy which allows access to specific tags ✓

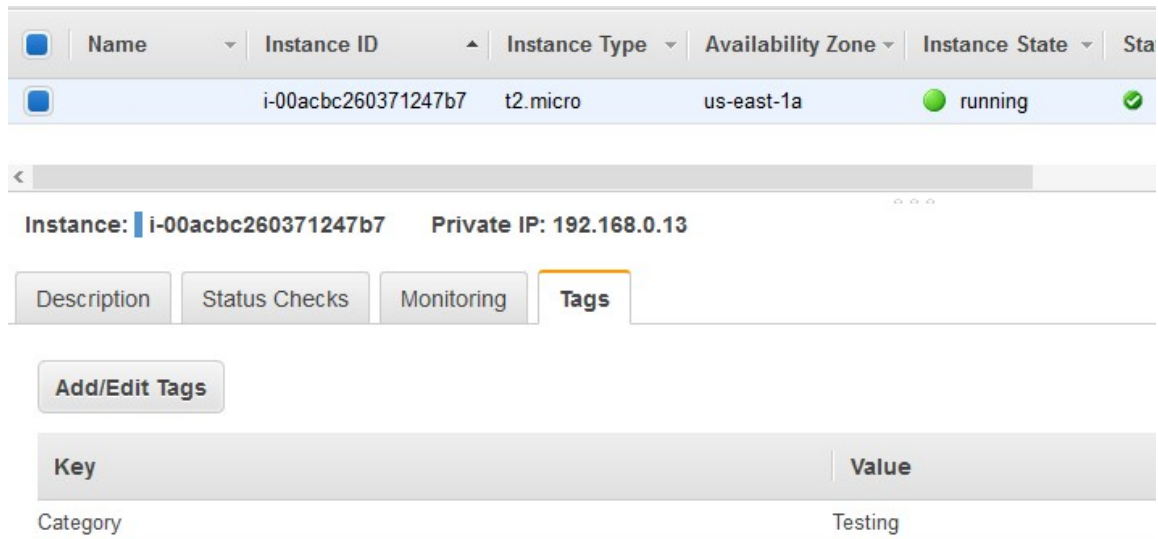
### Explanation :

Answer – D



Tags enable you to categorize your AWS resources in different ways, for example, by purpose, owner, or environment. This is useful when you have many resources of the same type – you can quickly identify a specific resource based on the tags you've assigned to it.

So as shown as an example below you can assign a Key name as Category and the value of Testing for all instances in your testing environment. And the same goes for the production instances which can carry a value of production.



The screenshot shows the AWS Management Console interface for an EC2 instance. At the top, there's a table with columns: Name, Instance ID, Instance Type, Availability Zone, Instance State, and Status. The first row shows an instance with ID i-00acbc260371247b7, type t2.micro, in us-east-1a, with a state of running and a green checkmark in the status column.

Below the table, the instance details for i-00acbc260371247b7 are shown, including the Private IP: 192.168.0.13. There are tabs for Description, Status Checks, Monitoring, and Tags. The Tags tab is selected, showing an 'Add/Edit Tags' button and a table with the following content:

Key	Value
Category	Testing

For information on resource tagging, please visit the link:

- [http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using\\_Tags.html](http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html)  
([http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using\\_Tags.html](http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html))

Ask our Experts



#### QUESTION 45 UNATTEMPTED

A user has launched an EC2 Windows instance from an instance store backed AMI. The user has also set the Instance initiated shutdown behavior to stop. What will happen when the user shuts down the OS?

- ☐ A. It will not allow the user to shutdown the OS when the shutdown behavior is set to Stop
- ☐ B. It is not possible to set the termination behavior to Stop for an Instance store backed AMI instance ✓

- ☐ C. The instance will stay running but the OS will be shutdown
- ☐ D. The instance will be terminated

### Explanation :

Answer – B

As per the AWS documentation, you cannot place an Instance store backed instance in a stopped state. Hence B is the right option.

Characteristic	Amazon EBS-Backed	Amazon Instance Store-Backed
Boot time	Usually less than 1 minute	Usually less than 5 minutes
Size limit	16 TiB	10 GiB
Root device volume	Amazon EBS volume	Instance store volume
Data persistence	By default, the root volume is deleted when the instance terminates.* Data on any other Amazon EBS volumes persists after instance termination by default. Data on any instance store volumes persists only during the life of the instance.	Data on any instance store volumes persists only during the life of the instance. Data on any Amazon EBS volumes persists after instance termination by default.
Upgrading	The instance type, kernel, RAM disk, and user data can be changed while the instance is stopped.	Instance attributes are fixed for the life of an instance.
Charges	You're charged for instance usage, Amazon EBS volume usage, and storing your AMI as an Amazon EBS snapshot.	You're charged for instance usage and storing your AMI in Amazon S3.
AMI creation/bundling	Uses a single command/call	Requires installation and use of AMI tools
Stopped state	Can be placed in stopped state where instance is not running, but the root volume is persisted in Amazon EBS	Cannot be in stopped state; instances are running or terminated

For more information on Instance store AMI's, please visit the link:

- <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ComponentsAMIs.html>  
(<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ComponentsAMIs.html>)

Ask our Experts



A user is collecting 1000 records per second. The user wants to send the data to CloudWatch using the custom namespace. Which of the below mentioned options is recommended for this activity?

- ☐ A. Aggregate the data with statistics, such as Min, max, Average, Sum and Sample data and send the data to CloudWatch ✓
- ☐ B. Send all the data values to CloudWatch in a single command by separating them with a comma. CloudWatch will parse automatically
- ☐ C. Create one csv file of all the data and send a single file to CloudWatch
- ☐ D. It is not possible to send all the data in one call. Thus, it should be sent one by one. CloudWatch will aggregate the data automatically

#### Explanation :

Answer – A

You can aggregate your data before you publish to CloudWatch. When you have multiple data points per minute, aggregating data minimizes the number of calls to **put-metric-data**. For example, instead of calling **put-metric-data** multiple times for three data points that are within three seconds of each other, you can aggregate the data into a statistic set that you publish with one call

An example of the call is given below

```
AWS cloudwatch put-metric-data --metric-name PageViewCount --namespace MyService --  
statistic-value Sum=11,Minimum=2,Maximum=5,SampleCount=3 --timestamp 2016-10-  
14T12:00:00.000Z
```

For information on publishing custom metrics, please visit the link:

- <http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/publishingMetrics.html>  
(<http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/publishingMetrics.html>)

Ask our Experts



A user has configured Auto Scaling with the minimum capacity as 2 and the desired capacity as 2. The user is trying to terminate one of the existing instance with the command:

```
terminate-instance-in-auto-scaling-group<Instance ID> --decrement-desired-capacity
```

What will Auto Scaling do in this scenario?

- ☐ A. Terminates the instance and does not launch a new instance
- ☐ B. Terminates the instance and updates the desired capacity to 1
- ☐ C. Terminates the instance and updates the desired capacity and minimum size to 1
- ☒ D. Throws an error ✓

#### Explanation :

Answer – D

This command will throw since the desired capacity cannot be less than the minimum capacity. The below diagram shows an autoscaling group in AWS which has the configuration of Desired capacity of 2, minimum capacity of 2 and maximum capacity of 3. Now if you try to decrement the value of the desired capacity to below the minimum capacity you will get an error.

Filter: <input type="text" value="Filter Auto Scaling groups..."/>					
<input type="checkbox"/>	Name	Launch Configuration	Instances	Desired	Min
<input type="checkbox"/>	Demo	New	0 ⓘ	2	2

Target Groups

Desired

*Desired capacity must be between minimum and maximum group size, inclusive*

Min

Max

Health Check Type

Health Check Grace

Period

For information on Manual scaling, please visit the link:

- <http://docs.aws.amazon.com/autoscaling/latest/userguide/as-manual-scaling.html>  
(<http://docs.aws.amazon.com/autoscaling/latest/userguide/as-manual-scaling.html>)

Ask our Experts



QUESTION 48 UNATTEMPTED

An organization is trying to create various IAM users. Which of the below mentioned options is not a valid IAM username?

- ☐ A. John.cloud
- ☐ B. john@cloud
- ☐ C. John=cloud
- ☐ D. john#cloud ✓

### Explanation :

Answer – D

When creating user names on AWS , the following conditions need to be met. Hence based on the below conditions the user name john#cloud is invalid.

User names can be a combination of up to 64 letters, digits, and these characters: plus (+), equal (=), comma (,), period (.), at sign (@), and hyphen (-). Names must be unique within an account.

They are not distinguished by case.

For information on IAM users, please visit the link:

- [http://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_users\\_create.html](http://docs.aws.amazon.com/IAM/latest/UserGuide/id_users_create.html)  
([http://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_users\\_create.html](http://docs.aws.amazon.com/IAM/latest/UserGuide/id_users_create.html))

Ask our Experts



### QUESTION 49 UNATTEMPTED

A user is having data generated randomly based on a certain event. The user wants to upload that data to CloudWatch. It may happen that event may not have data generated for some period due to randomness. Which of the below mentioned options is a recommended option for this case?

- ☐ A. For the period when there is no data, the user should not send the data at all
- ☐ B. For the period when there is no data the user should send a blank value
- ☐ C. For the period when there is no data the user should send the value as 0 ✓
- ☐ D. The user must upload the data to CloudWatch as having no data for some period will cause an error at CloudWatch monitoring

### Explanation :

Answer – C

When your data is more sporadic and you have periods that have no associated data, you can choose to publish the value zero (0) for that period or no value at all. You might want to publish zero instead of no value if you use periodic calls to PutMetricData to monitor the health of your application. For example, you can set a CloudWatch alarm to notify you if your application fails to publish metrics every five minutes. You want such an application to publish zeros for periods with no associated data.

For information on publishing custom metrics, please visit the link:

- <http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/publishingMetrics.html>  
(<http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/publishingMetrics.html>)

Ask our Experts



QUESTION 50 UNATTEMPTED

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

**Explanation :**

Answer – A

As per the AWS documentation, you can send cloudwatch metrics up to 2 hours in the future.

**Time Stamps**

Each metric data point must be marked with a time stamp. The time stamp can be up to two weeks in the past and up to two hours into the future. If you do not provide a time stamp, CloudWatch creates a time stamp for you based on the time the data point was received.

For information on custom metrics, please visit the link:

- [http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/cloudwatch\\_concepts.html](http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/cloudwatch_concepts.html)  
([http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/cloudwatch\\_concepts.html](http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/cloudwatch_concepts.html))

Ask our Experts



Which of the below mentioned AWS RDS logs cannot be viewed from the console for MySQL?

- ☐ A. Error Log
- ☐ B. Slow Query Log
- ☒ C. Transaction Log ✓
- ☐ D. General Log

#### Explanation :

Answer – C

As per AWS, below are the logs available for the various databases. And in this you cannot see the mention of Transaction logs.

Database Engine	Relevant Documentation
MariaDB	You can access the error log, the slow query log, and the general log. For more information, see <a href="#">MariaDB Database Log Files</a> .
Microsoft SQL Server	You can access SQL Server error logs, agent logs, and trace files. For more information, see <a href="#">Microsoft SQL Server Database Log Files</a> .
MySQL	You can access the error log, the slow query log, and the general log. For more information, see <a href="#">MySQL Database Log Files</a> .
Oracle	You can access Oracle alert logs, audit files, and trace files. For more information, see <a href="#">Oracle Database Log Files</a> .
PostgreSQL	You can access query logs and error logs. Error logs can contain auto-vacuum and connection information, as well as rds_admin actions. For more information, see <a href="#">PostgreSQL Database Log Files</a> .

For information on rds logs, please visit the link:

- [http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER\\_LogAccess.html](http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_LogAccess.html)  
([http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER\\_LogAccess.html](http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_LogAccess.html))

Ask our Experts





A user has launched an EBS backed EC2 instance in the US-East-1a region. The user stopped the instance and started it back after 20 days. AWS throws up an 'InsufficientInstanceCapacity' error. What can be the possible reason for this?

- ☐ A. AWS does not have sufficient capacity in that availability zone ✓
- ☐ B. AWS zone mapping is changed for that user account
- ☐ C. There is some issue with the host capacity on which the instance is launched
- ☐ D. The user account has reached the maximum EC2 instance limit

#### Explanation :

Answer – A

In the AWS documentation it is clearly mentioned that if you get the below error that means AWS does not have sufficient capacity in that availability zone.

#### Error: InsufficientInstanceCapacity

If you get an *InsufficientInstanceCapacity* error when you try to launch an instance or start a stopped instance, AWS does not currently have enough available capacity to service your request. Try the following:

- Wait a few minutes and then submit your request again; capacity can shift frequently.
- Submit a new request with a reduced number of instances. For example, if you're making a single request to launch 15 instances, try making 3 requests for 5 instances, or 15 requests for 1 instance instead.
- If you're launching an instance, submit a new request without specifying an Availability Zone.
- If you're launching an instance, submit a new request using a different instance type (which you can resize at a later stage). For more information, see [Resizing Your Instance](#).
- Try purchasing Reserved Instances. Reserved Instances are a long-term capacity reservation. For more information, see: [Amazon EC2 Reserved Instances](#).

For information on this topic, please visit the link:

- <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instance-capacity.html>  
(<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instance-capacity.html>)

Ask our Experts



QUESTION 53

UNATTEMPTED

A user has created a VPC with public and private subnets using the VPC wizard.

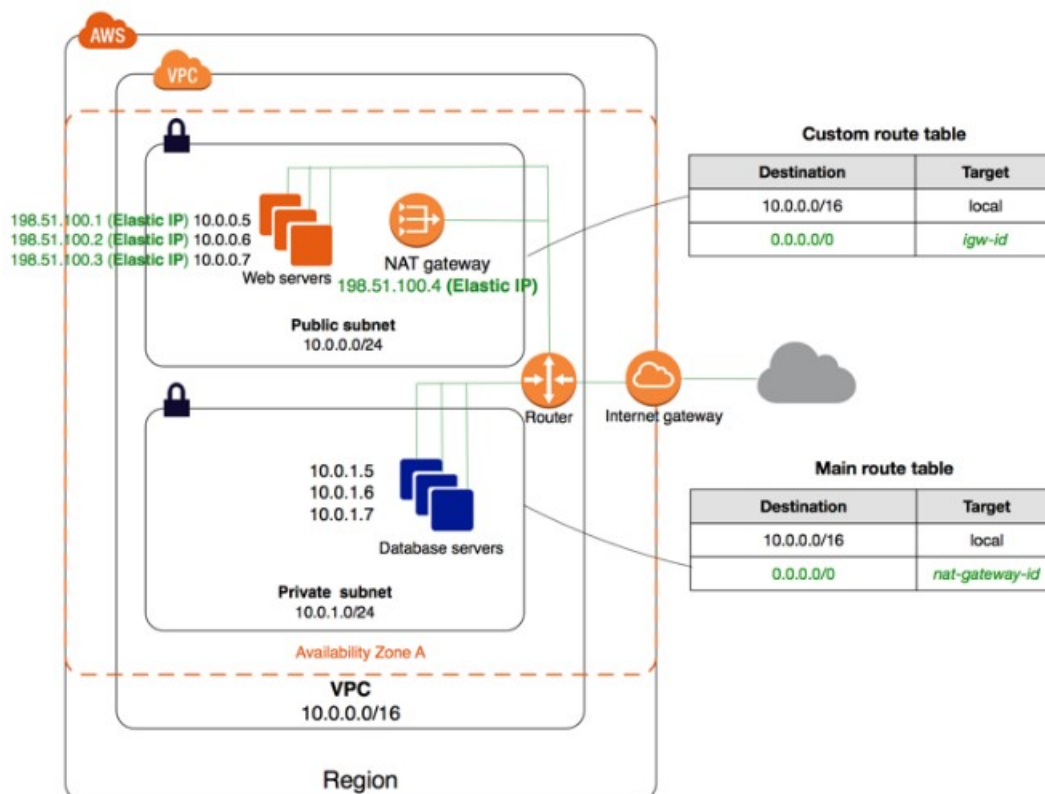
Which of the below mentioned statements is true in this scenario?

- ☐ 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

### Explanation :

Answer – B

From the AWS documentation, below you can see the configuration of the route tables when you have a private and public subnet. It clearly shows that the main route table is associated with the private subnet and the custom route table with the public subnet.



For information on Public and private subnets, please visit the link:

- [http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC\\_Scenario2.html](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2.html)  
([http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC\\_Scenario2.html](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2.html))

Ask our Experts



QUESTION 54 UNATTEMPTED

The CFO of a company wants to allow one of his employees to view only the AWS usage report page. Which of the below mentioned IAM policy statements allows the user to have access to the AWS usage report page?

- ☐ A. "Effect": "Allow", "Action": ["Describe"], "Resource": "Billing"
- ☐ B. "Effect": "Allow", "Action": ["AccountUsage"], "Resource": "\*"
- ☐ C. "Effect": "Allow", "Action": ["aws-portal:ViewUsage", "aws-portal:ViewBilling"], "Resource": "\*" ✓
- ☐ D. "Effect": "Allow", "Action": ["aws-portal:ViewBilling"], "Resource": "\*"

**Explanation :**

Answer – C

As per the AWS documentation, below is the access required for a user to access the Usage reports page and as per this, Option C is the right answer.

**Example 2: Allow IAM users to access the Reports console page**

To allow an IAM user to access the **Reports** console page and to view the usage reports that contain account activity information, you would use a policy similar to this example policy.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "aws-portal:ViewUsage",
        "aws-portal:ViewBilling"
      ],
      "Resource": "*"
    }
  ]
}
```

For information on IAM policies, please visit the link:

- [http://docs.aws.amazon.com/IAM/latest/UserGuide/access\\_policies.html](http://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html)  
([http://docs.aws.amazon.com/IAM/latest/UserGuide/access\\_policies.html](http://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html))

Ask our Experts



QUESTION 55

UNATTEMPTED

A user has configured an HTTPS listener on an ELB. The user has not configured any security policy which can help to negotiate SSL between the client and ELB. What will ELB do in this scenario?

- ☐ A. By default ELB will select the first version of the security policy
- ☐ B. By default ELB will select the latest version of the policy ✓
- ☐ C. ELB creation will fail without a security policy
- ☐ D. It is not required to have a security policy since SSL is already installed

**Explanation :**

Answer – B

AWS ELB has the following pre-defined security policies. If there no security policy defined by the user, the last 2 default policy's will be picked up.

- ELBSecurityPolicy-2016-08
- ELBSecurityPolicy-2015-05
- ELBSecurityPolicy-2015-03
- ELBSecurityPolicy-2015-02
- ELBSecurityPolicy-2014-10
- ELBSecurityPolicy-2014-01
- ELBSecurityPolicy-2011-08
- ELBSample-ELBDefaultNegotiationPolicy or ELBSample-ELBDefaultCipherPolicy
- ELBSample-OpenSSLDefaultNegotiationPolicy or ELBSample-OpenSSLDefaultCipherPolicy

For information on ELB security policies, please visit the link:

- <http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-security-policy-options.html> (<http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-security-policy-options.html>)

Ask our Experts



QUESTION 56 UNATTEMPTED

A user has enabled versioning on an S3 bucket. The user is using server side encryption for data at Rest. If the user is supplying his own keys for encryption SSE-C., which of the below mentioned statements is true?

- ☐ A. The user should use the same encryption key for all versions of the same object
- ☐ B. It is possible to have different encryption keys for different versions of the same object ✓
- ☐ C. AWS S3 does not allow the user to upload his own keys for server side encryption
- ☐ D. The SSE-C does not work when versioning is enabled

**Explanation :**

Answer – B

Server-side encryption is about protecting data at rest. Using server-side encryption with customer-provided encryption keys (SSE-C) allows you to set your own encryption keys. With the encryption key you provide as part of your request, Amazon S3 manages both the encryption, as it writes to disks, and decryption, when you access your objects. Therefore, you don't need to maintain any code to perform data encryption and decryption. The only thing you do is manage the encryption keys you provide.

Option C and D is wrong as per the below snippet from AWS documentation

- You manage a mapping of which encryption key was used to encrypt which object. Amazon S3 does not store encryption keys. You are responsible for tracking which encryption key you provided for which object.
  - If your bucket is versioning-enabled, each object version you upload using this feature can have its own encryption key. You are responsible for tracking which encryption key was used for which object version.
  - Because you manage encryption keys on the client side, you manage any additional safeguards, such as key rotation, on the client side.

**Caution**

If you lose the encryption key any GET request for an object without its encryption key will fail, and you lose the object.

Option A is wrong because it is not a good security practice to have the same keys for each version

of the same object.

For more information on server side encryption, please visit the link:

- <http://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html>  
(<http://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html>)

Ask our Experts



## QUESTION 57 UNATTEMPTED

In an IAM policy , there are the basic elements that make up the policy. Which in the below list does not come up in the IAM policy.

- ☒ A. Permission ✓
- ☐ B. Actions
- ☐ C. Resources
- ☐ D. Effect

### Explanation :

Answer – A

In its most basic sense, a policy lets you specify the following:

- **Actions:** what actions you will allow. Each AWS service has its own set of actions. For example, you might allow a user to use the Amazon S3 ListBucket action, which returns information about the items in a bucket. Any actions that you don't explicitly allow are denied.
- **Resources:** which resources you allow the action on. For example, what specific Amazon S3 buckets will you allow the user to perform the ListBucket action on? Users cannot access any resources that you have not explicitly granted permissions to.
- **Effect:** what the effect will be when the user requests access—either allow or deny. Because the default is that resources are denied to users, you typically specify that you will allow users access to resource.

For information on IAM policies, please visit the link:

- [http://docs.aws.amazon.com/IAM/latest/UserGuide/access\\_policies.html](http://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html)  
([http://docs.aws.amazon.com/IAM/latest/UserGuide/access\\_policies.html](http://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html))

Ask our Experts



QUESTION 58

UNATTEMPTED

A user has created a VPC with CIDR 20.0.0.0/16. The user has created one subnet with CIDR 20.0.0.0/16 in this VPC. The user is trying to create another subnet with the same VPC for CIDR 20.0.1.0/24. What will happen in this scenario?

- ☐ A. The VPC will modify the first subnet CIDR automatically to allow the second subnet IP range
- ☐ B. It is not possible to create a subnet with the same CIDR as VPC
- ☐ C. The second subnet will be created
- ☒ D. It will throw a CIDR overlaps error ✓

### Explanation :

Answer – D

Below is an example of what happens when you define a VPC with a CIDR block of 20.0.0.0/16 and then first create a subnet of CIDR block of 20.0.0.0/16 and then a second one of 20.0.1.0/24. Since the second block conflicts with the first one, there will be a clash and will throw an error.

**Create Subnet** ✕

Use the CIDR format to specify your subnet's IP address block (e.g., 10.0.0.0/24). Note that block sizes must be between a /16 netmask and /28 netmask. Also, note that a subnet can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag  ?

VPC  ?

VPC CIDRs		
CIDR	Status	Status Reason
20.0.0.0/16	associated	

Availability Zone  ?

IPv4 CIDR block  ?

⚠ CIDR block 20.0.0.1/24 overlaps with pre-existing CIDR block 20.0.0.0/16 from subnet-2f01f354 | 20.0.0.0/16.

Cancel Yes, Create

For more information on VPC and subnets please visit the below link:

- [http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC\\_Subnets.html](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html)  
([http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC\\_Subnets.html](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html))

Ask our Experts



QUESTION 59 UNATTEMPTED

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

**Explanation :**

Answer – B

In the AWS documentation, it is clearly mentioned that the patching or changes are first done to the standby instance. Once done, the standby will be promoted to the primary and then the patching is done on the primary. Please note that the “Promote original master back as primary” will not be carried out.



### Multi-AZ Deployments for RDS DB Instances

Running a DB instance as a Multi-AZ deployment can further reduce the impact of a maintenance event, because Amazon RDS will conduct maintenance by following these steps:

1. Perform maintenance on the standby.
2. Promote the standby to primary.
3. Perform maintenance on the old primary, which becomes the new standby.

For more information on MultiAZ RDS please visit the link:

- <https://aws.amazon.com/rds/faqs/> (<https://aws.amazon.com/rds/faqs/>)

Ask our Experts



QUESTION 60 UNATTEMPTED

A system admin is using server side encryption with AWS S3. Which of the below mentioned statements helps the user understand the S3 encryption functionality?

- ☒ A. The server side encryption with the user supplied key works when versioning is enabled ✓
- ☐ B. The user can use the AWS console, SDK and APIs to encrypt or decrypt the content for server side encryption with the user supplied key
- ☐ C. The user must send an AES-128 encrypted key
- ☐ D. The user can upload his own encryption key to the S3 console

#### Explanation :

Answer – A

As per the AWS documentation it is very clear that Option B and D are wrong because u cannot use the AWS console when using server side encryption keys.

#### Note

You cannot use the Amazon S3 console to upload an object and request SSE-C. You also cannot use the console to update (for example, change the storage class or add metadata) an existing object stored using SSE-C.

Option C is wrong because from the below snippet from the AWS documentation it mentions that you need to use 256 bit encryption.

Server-side encryption is about protecting data at rest. Using server-side encryption with customer-provided encryption keys (SSE-C) allows you to set your own encryption keys. With the encryption key you provide as part of your request, Amazon S3 manages both the encryption, as it writes to disks, and decryption, when you access your objects. Therefore, you don't need to maintain any code to perform data encryption and decryption. The only thing you do is manage the encryption keys you provide.

When you upload an object, Amazon S3 uses the encryption key you provide to apply AES-256 encryption to your data and removes the encryption key from memory.

For more information on server side encryption, please visit the link:

- <http://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html>  
(<http://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html>)

Ask our Experts



Finish Review (<https://www.whizlabs.com/learn/course/aws-csyopaa-practice-tests/quiz/12745>)

## Certification

- ➔ Cloud Certification  
(<https://www.whizlabs.com/cloud-certification-training-courses/>)
- ➔ Java Certification  
(<https://www.whizlabs.com/oracle-java-certifications/>)
- ➔ PM Certification  
(<https://www.whizlabs.com/project-management-certifications/>)

## Company

- ➔ Support (<https://help.whizlabs.com/hc/en-us>)
- ➔ Discussions (<http://ask.whizlabs.com/>)
- ➔ Blog (<https://www.whizlabs.com/blog/>)

➔ Big Data Certification  
(<https://www.whizlabs.com/big-data-certifications/>)

## Mobile App

 Android Coming Soon

 iOS Coming Soon

## Follow us



(<https://www.facebook.com/whizlabs.software/>)



(<https://in.linkedin.com/company/whizlabs-software>)



(<https://twitter.com/whizlabs?lang=en>)



(<https://plus.google.com/+WhizlabsSoftware>)