

Whizlabs Learning Center

[HOME](#) > [AWS CSAA PRACTICE TESTS](#) > [FULL TEST\(S\)](#) > [NEW PRACTICE TEST V](#)**Started on** Wednesday, 5 July 2017, 3:31 AM**State** Finished**Completed on** Wednesday, 5 July 2017, 3:31 AM**Time taken** 12 secs**Grade** 0.00 out of 60.00 (0%)**Result** FAIL**Question 1**

Not answered



A company AWS account consist of approximately 300 IAM users. Now there is a mandate that an access change is required for 100 IAM users to have unlimited privileges to S3.As a system administrator, how can you implement this effectively so that there is no need to apply the policy at the individual user level?

Please select :

- ☐ A. Create a new role and add each user to the IAM role
- ☐ B. Use the IAM groups and add users, based upon their role, to different groups and apply the policy to group
- ☐ C. Create a policy and apply it to multiple users using a JSON script
- ☐ D. Create an S3 bucket policy with unlimited access which includes each user's AWS account ID

Your answer is incorrect.

Answer:- B

An IAM group is used to collectively manage users who need the same set of permissions. By having groups, it becomes easier to manage permissions. So if you change the permissions on the group scale, it will affect all the users in that group. Please find the steps below for the group creation.

Step 1) Go to IAM and click on the Groups section. Click on Create New Group.

Search IAM

Dashboard

Groups

Users

Roles

Policies

Identity providers

Create New Group

Group Actions ▾

Filter

<input type="checkbox"/>	Group Name ↕	Users
No records found.		

Step 2) Provide a name for the Group

Set Group Name

Specify a group name. Group names can be edited any time.




Group Name:

Example: Developers or ProjectAlpha
Maximum 128 characters

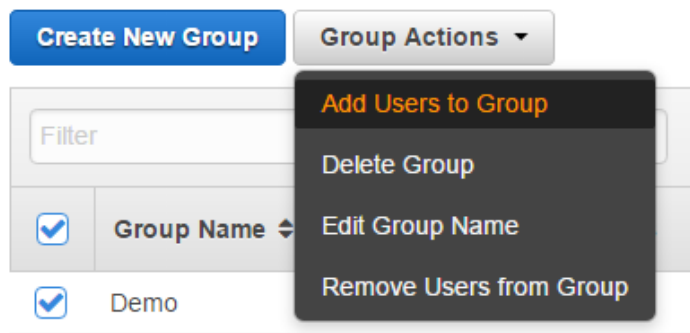
Step 3) Next you need to attach a policy. Since the question asks that this group needs full access to S3 , choose the AmazonS3FullAccess role.

Attach Policy

Select one or more policies to attach. Each group can have up to 10 policies

Filter: Policy Type ▾ S3			
		Policy Name ↕	Attached Entities ↕
<input type="checkbox"/>		AmazonDMSRedshiftS3Role	0
<input checked="" type="checkbox"/>		AmazonS3FullAccess	0
<input type="checkbox"/>		AmazonS3ReadOnlyAccess	0

Step 4) Once the group is created, you can then add the 50 users to the group



For more information on users and groups, please visit the url - <http://docs.aws.amazon.com/IAM/latest/UserGuide/id.html>

The correct answer is: Use the IAM groups and add users, based upon their role, to different groups and apply the policy to group

Question 2

Not answered



You are a consultant tasked with migrating an on-premise application architecture to AWS. During your design process you have to give consideration to current on-premise security and determine which security attributes you are responsible for on AWS. Which of the following does AWS provide for you as part of the shared responsibility model? Choose the 2 correct options

Please select :

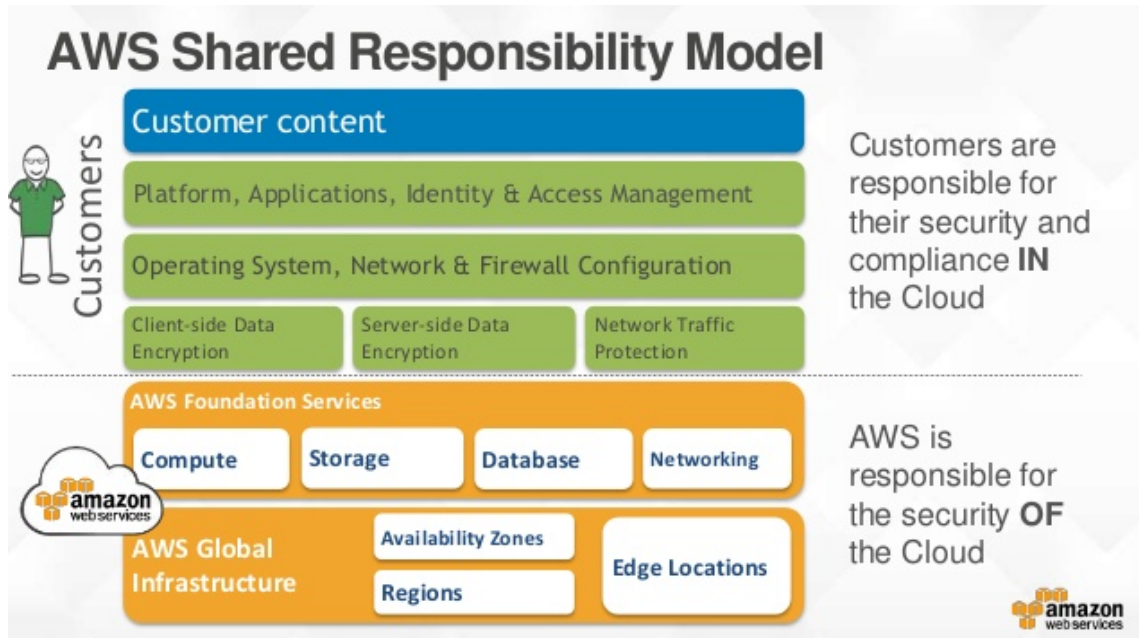
- ☐ A. EC2 Instance security
- ☐ B. Physical network infrastructure
- ☐ C. User access to the AWS environment via IAM.
- ☐ D. Virtualization infrastructure

Your answer is incorrect.

Answer:- B and D.

As per the shared responsibility shown below, the users are required to control the EC2 security via security groups and network access control layers.

Also it is the user's responsibility model, aws takes care of the physical components and the infrastructure to provide Virtualization.



For more information on aws shared responsibility model, please visit the link -

<https://aws.amazon.com/blogs/security/tag/shared-responsibility-model/>

The correct answer is: Physical network infrastructure, Virtualization infrastructure

Question 3

Not answered



There is a requirement to host an application in aws that requires access to a NoSQL database. But there are no human resources available who can take care of the database infrastructure. Which Amazon service provides a fully-managed and highly available NoSQL service? Choose the correct option

Please select :

- ☐ A. DynamoDB
- ☐ B. ElasticMap Reduce
- ☐ C. Amazon RDS
- ☐ D. SimpleDB

Your answer is incorrect.

Answer:- A

DynamoDB is an aws service that provides a NoSQL database option to users. DynamoDB is a hosted solution by aws , there is no requirement to manage the environment for DynamoDB. And the question clearly states there are no resources in place to manage the DynamoDB environment.

DynamoDB lets you offload the administrative burdens of operating and scaling a distributed database, so that you don't have to worry about hardware provisioning, setup and configuration, replication, software patching, or cluster scaling.

ElasticMapReduce is not a NoSQL solution.

SimpleDB is a simplified DB solution given by aws and hence is not a solution.

For more information on DynamoDB, please visit the link -

<http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Introduction.html>

The correct answer is: DynamoDB

Question 4

Not answered



As a AWS Solution architect , you have been tasked to put the organization data on the cloud. But there is a concern from a security perspective on what can be put on the cloud. What are the best security options from the ones listed below which can be used from a security perspective. Please choose the 3 correct answers from the below options.

Please select :

- ☐ A. Enable EBS Encryption
- ☐ B. Enable S3 Encryption
- ☐ C. Encrypt the file system on an EBS volume using Linux tools
- ☐ D. In AWS , you dont need to worry as it encrypts all data

Your answer is incorrect.

Answer:- A, B and C

Encryption in aws needs to be done by the users and can be done on different levels.

For EBS , we can enable encryption at the volume level. This can be done when the volume is created, this is shown in the screenshot below.

Create Volume

Volume Type ⓘ

General Purpose SSD (GP2) ▼

Size (GiB) ⓘ

100

(Min: 1 GiB, Max: 16384 GiB)

IOPS ⓘ

300 / 3000

(Baseline of 3 IOPS per GiB with a minimum of 100 IOPS, burstable to 3000 IOPS)

Throughput (MB/s) ⓘ

Not Applicable

Availability Zone ⓘ

us-east-1a ▼

Snapshot ID ⓘ

Search (case-insensitive)

Encryption ⓘ

☒ Encrypt this volume

Master Key ⓘ

(default) aws/eks ▼

Key Details

Description	Default master key that protects my EBS volumes when no other key is defined
Account	This account (085363624145)
KMS Key ID	ca4e8a5f-8b4e-43f0-97f7-2c3583d57dd0
KMS Key ARN	arn:aws:kms:us-east-1:085363624145:key/ca4e8a5f-8b4e-43f0-97f7-2c3583d57dd0

Cancel

Create

On S3, For any object you can enable server side encryption by going to the Permissions section of the object in S3 and enable the server side encryption option.

Object: aws-programmatic-access-test-object ×

Bucket: shakinstev
Name: aws-programmatic-access-test-object
Link: <https://s3-ap-southeast-1.amazonaws.com/shakinstev/aws-programmatic-access-test-object>
Size: 4
Last Modified: Wed Jul 27 12:40:02 GMT+400 2016
ETag: 098f6bcd4621d373cade4e832627b4f6
Expiry Date: None
Expiration Rule: N/A

▼ Details

Storage Class: ☒ Standard ☐ Standard - Infrequent Access ☐ Reduced Redundancy

Server Side Encryption: ☐ None ☒ AES-256

And finally , one can use Linux based tools to Encrypt a volume if it is not encrypted.

The correct answer is: Enable EBS Encryption, Enable S3 Encryption, Encrypt the file system on an EBS volume using Linux tools

Question 5

Not answered



AWS provides a storage option known as Amazon Glacier. What is this aws service designed for. Please specify 2 correct options.

Please select :

- ☐ A. Cached session data
- ☐ B. Infrequently accessed data
- ☐ C. Data archives
- ☐ D. Active database storage

Your answer is incorrect.

Answer – B and C

Amazon Glacier is an extremely low-cost storage service that provides secure, durable, and flexible storage for data backup and archival. So Amazon glacier is used for Infrequently accessed data and Data archives.

For Cached Data Session , the service provided by aws is known as elastic cache. So Amazon glacier is the wrong option.

For Active database storage , this is done via EBS volumes , so this option is also incorrect.

For more information on Amazon Glacier , please visit the link -

<https://aws.amazon.com/glacier/faqs/>

The correct answer is: Infrequently accessed data, Data archives

Question 6

Not answered



There is a requirement for a user to modify the configuration of one of your Elastic Load Balancers (ELB). This access is just required one time only. Which of the following choices would be the best way to allow this access?

Please select :

- ☐ A. Open up whichever port ELB uses in a security group and give the user access to that security group via a policy
- ☐ B. Create an IAM Role and attach a policy allowing modification access to the ELB
- ☐ C. Create a new IAM user who only has access to the ELB resources and delete that user when the work is completed.
- ☐ D. Give them temporary access to the root account for 12 hours only and change the password once the activity is completed

Your answer is incorrect.

Answer – B

The best practise for IAM is to create roles which has specific access to an AWS service and then give the user permission to the AWS service via the role.

To get the role in place , follow the below steps

Step 1) Create a role which has the required ELB access

Step 2) You need to provide permissions to the underlying EC2 instances in the Elastic Load Balancer

Select Role Type

Role Name	Permissions	Created	Last Used
<input type="checkbox"/> AmazonEC2ContainerService...	0	2015-04-09 20:14 UTC+0400	2016-08-11 17:08 UTC+0400
<input checked="" type="checkbox"/> AmazonEC2FullAccess	0	2015-02-06 22:40 UTC+0400	2015-02-06 22:40 UTC+0400

For the best practises on IAM policies, please visit the link:

- <http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html>
- http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-user.html

The correct answer is: Create an IAM Role and attach a policy allowing modification access to the ELB

Question 7

Not answered



You are an AWS Solution Architect and architecting an application environment on AWS. Which services or service features might you enable to take advantage of monitoring to ensure auditing the environment for compliance is easy and follows the strict security compliance requirements? Choose the correct option

Please select :

- ☐ A. CloudTrail for security logs
- ☐ B. S3 logging
- ☐ C. Encrypted data storage
- ☐ D. Multi Factor Authentication

Your answer is incorrect.

Answer – A

AWS Cloudtrail is the defacto service provided by aws for monitoring all API calls to AWS and is used for logging and monitoring purposes for compliance purposes. Amazon cloudtrail detects every call made to aws and creates a log which can then be further used for analysis.

For more information on Amazon Cloudtrail , please visit the link –

<https://aws.amazon.com/cloudtrail/>

The correct answer is: CloudTrail for security logs

Question 8

Not answered



An application has been migrated from on-premise to AWS in your company and you will not be responsible for the ongoing maintenance of packages. Which of the below services allows for access to the underlying infrastructure. Choose the 2 correct options

Please select :

- ☐ A. Elastic Beanstalk
- ☐ B. EC2
- ☐ C. DynamoDB
- ☐ D. RDS

Your answer is incorrect.

Answer – A and B

EC2 and Elastic Beanstalk are aws services that allow the developer access to the underlying infrastructure.

When you create an Elastic beanstalk environment as shown below , you will have access to the underlying EC2 instance. So in the below example , for the Elastic beanstalk environment , you will have access to the Windows Server 2012 environment.



Health
Grey
Causes

Running Version
Sample Application
Upload and Deploy

Windows Server 2012

Configuration

64bit Windows Server 2012 R2
v1.2.0 running IIS 8.5

Change

DynamoDB and RDS are services provided and the infrastructure is managed by aws.

The correct answer is: Elastic Beanstalk, EC2

Question 9

Not answered



To protect S3 data from both accidental deletion and accidental overwriting, you should

Please select :

- ☐ A. Enable Multi-Factor Authentication (MFA) protected access
- ☐ B. Disable S3 delete using an IAM bucket policy
- ☐ C. Access S3 data using only signed URLs
- ☐ D. Enable S3 versioning on the bucket

Your answer is incorrect.

Answer- D

To protect objects in S3 from both accidental deletion and accidental overwriting, the methodology adopted by aws is to Enable versioning on the bucket. Versioning allows to store every version of an object , so that if by mistake there is a version deleted , you can recover other versions, because the entire object is not deleted.

Enable Multi-Factor Authentication (MFA) protected access on S3 is only used to add an additional security layer to S3. So that users who are authenticated properly before having access to the bucket. But this is not what the question is asking.

To enable versioning on S3 , you need to go to the bucket , and in the properties , you can enable versioning.

The correct answer is: Enable S3 versioning on the bucket

Question 10

Not answered



By default is data in S3 encrypted?

Please select :

- ☐ A. Yes, S3 always encrypts data for security purposes.
- ☐ B. Yes, but only in government cloud data centers

- ☐ C. No, but it can be when the right APIs are called for SSE
- ☐ D. No, it must be encrypted before upload of any data to S3.

Your answer is incorrect.

Answer- C

Please note that, no , by default , Encryption is not enabled. So option A and B are incorrect.

Also note that it is not necessary to encrypt before every upload.

For any object you can enable server side encryption by going to the Permissions section of the object in S3 and enable the server side encryption option.

Object: aws-programmatic-access-test-object ×

Bucket: shakinstev
Name: aws-programmatic-access-test-object
Link: <https://s3-ap-southeast-1.amazonaws.com/shakinstev/aws-programmatic-access-test-object>
Size: 4
Last Modified: Wed Jul 27 12:40:02 GMT+400 2016
ETag: 098f6bcd4621d373cade4e832627b4f6
Expiry Date: None
Expiration Rule: N/A

▼ Details

Storage Class: ☒ Standard ☐ Standard - Infrequent Access ☐ Reduced Redundancy

Server Side Encryption: ☐ None ☒ AES-256

For more information on Encryption for S3 , please refer to the link -
<http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html>

The correct answer is: No, but it can be when the right APIs are called for SSE

Question 11

Not answered



Your AWS environment contains several reserved EC2 instances dedicated to a project that has just been cancelled. You need to stop incurring charges for the reserved instances immediately. What steps would you take to avoid taking the hit on the charge for these reserved instances? Choose 2 correct options

Please select :

- ☐ A. Stop the instances as soon as possible.
- ☐ B. Contact AWS and explain the situation to try and recover the costs.
- ☐ C. Sell the reserved instances on the AWS Reserved Instance Marketplace
- ☐ D. Terminate the instances as soon as possible.

Your answer is incorrect.

Answer: - C and D.

Reserved Instances provide a significant discount (up to 75%) compared to On-Demand instance pricing. There is a fixed quote of reserved power that it is given to the account. You have the Flexibility to change families, OS types, and tenancies while benefitting from Reserved Instance pricing.

Now reserved instances are bought upfront for a specified duration. Unlike On-demand instances, there is no cost difference if you stop the instances, so option A is incorrect. Since you have already bought the reserved instances, you cannot ask aws to recover the costs.

The only 2 options available are to terminate the instances immediately and sell them on AWS Reserved Instance Marketplace for a specified price.

Note that all Reserved Instances are grouped according to the duration of the term remaining and the hourly price in the market place. Hence, terminating the instance immediately would help to save remaining term.

You can purchase reserved instances from the reserved instances section in the EC2 dashboard.

In the next screen, you can choose the reserved instance to buy. But you are making an upfront commitment to buy the instances.

For more information on reserved instances please follow the link -

<https://aws.amazon.com/ec2/pricing/reserved-instances/>

The correct answer is: Sell the reserved instances on the AWS Reserved Instance Marketplace, Terminate the instances as soon as possible.

Question 12

Not answered



A company has been asked to comply with the HIPPA laws, and they have been told that all data being backed up or stored on Amazon S3 needs to be encrypted at rest. What is the best method for encryption for your data? Please choose 2 options.

Please select :

- ☐ A. Encrypt the data locally using your own encryption keys, then copy the data to Amazon S3 over HTTPS endpoints
- ☐ B. Store the data on EBS volumes with encryption enabled instead of using Amazon S3
- ☐ C. Store the data in encrypted EBS snapshots
- ☐ D. Enable SSE on an S3 bucket to make use of AES-256 encryption.

Your answer is incorrect.

Answer:- A and D.

The question asks for Encryption at rest for S3, so any answer related to EBS encryption does not correspond to the right answer.

For any object you can enable server side encryption by going to the Permissions section of the object in S3 and enable the server side encryption option.

And then for client side encryption, you can encrypt the object and send it to S3 when you program your application.

For the entire detailed description on Encryption strategies, please visit the link - <http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html>

The correct answer is: Encrypt the data locally using your own encryption keys, then copy the data to Amazon S3 over HTTPS endpoints, Enable SSE on an S3 bucket to make use of AES-256 encryption.

Question 13

Not answered



Which of the following is true of an SQS message? Choose the correct option

Please select :

- ☐ A. SQS messages are guaranteed to be delivered at least once
- ☐ B. SQS messages must be less than 32 KB in size
- ☐ C. SQS messages must be in JSON format
- ☐ D. SQS messages can live in the queue up to thirty days

Your answer is incorrect.

Answer - A

If you look at the SQS FAQ, it is clearly mentioned that SQS messages are guaranteed to be delivered at least once.

The message size for SQS can be 256KB in size.

The message formats can be in XML, JSON and unformatted text.

The messages can live in the queue for a maximum of 14 days.

For more information on SQS messages, please follow the link

<https://aws.amazon.com/sqs/faqs/>

The correct answer is: SQS messages are guaranteed to be delivered at least once

Question 14

Not answered



An EC2 instance has been running and data has been stored on the instance's volumes. The instance was shutdown over the weekend to save costs. The next week, after starting the instance, you notice that all data is lost and is no longer available on the EC2 instance. What might be the cause of this?

Please select :

- ☐ A. The EC2 instance was using instance store volumes, which are ephemeral and only lives for the life of the instance
- ☐ B. The EC2 instance was using EBS backed root volumes, which are ephemeral and only lives for the life of the instance
- ☐ C. The EBS volume was not big enough to handle all of the processing data.
- ☐ D. The instance has been compromised

Your answer is incorrect.

Answer - A

Anything that is stored on an instance store volume is destroyed when the instance is shutdown. Instance store volumes are ephemeral, which means that they only survive when the instance is active.

EBS backed Volumes are not ephemeral and exists even if the instance is stopped and started, so Option B is wrong.

Even if EBS volume is not big enough, it does not mean that it will not be present when the instance is stopped and started, so Option C is wrong.

If the instance is compromised, then the instance would not even start , so Option D is wrong.

For more information on instance store volumes, please visit

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/InstanceStorage.html>

The correct answer is: The EC2 instance was using instance store volumes, which are ephemeral and only lives for the life of the instance

Question 15

Not answered



What database services are provided by aws from the list mentioned below

Please select :

- ☐ A. Aurora
- ☐ B. MariaDB
- ☐ C. MySQL
- ☐ D. DB2

Your answer is incorrect.

Answer – A, B and C

DB2 is the only database service not provided by AWS. For the list of DB services , please visit the link <https://aws.amazon.com/rds/>

For more information on Aurora , please visit the link - <https://aws.amazon.com/rds/aurora/>

For more information on mySQL , please visit the link - <https://aws.amazon.com/rds/mysql/>

For more information on MariaDB , please visit the link - <https://aws.amazon.com/rds/mariadb/>

The correct answer is: Aurora, MariaDB, MySQL

Question 16

Not answered



There is a requirement to move 10 TB data warehouse to the cloud. With the current bandwidth allocation it would take 2 months to transfer the data. Which service would allow you to quickly get their data into AWS? Choose the correct option.

Please select :

- ☐ A. Amazon Import/Export
- ☐ B. Amazon Direct Connect
- ☐ C. Amazon S3 MultiPart Upload
- ☐ D. Amazon S3 Connector

Your answer is incorrect.

Answer – A

AWS Import/Export is a service that accelerates transferring large amounts of data into and out of AWS using physical storage appliances, bypassing the Internet.

For Amazon S3 Multipart Upload, there are the following restrictions, so then it's better to use the Amazon Import/Export.

For more information on aws import/export, please visit the link -

<https://aws.amazon.com/snowball/>

Amazon Direct Connect is used as a connection between AWS and On-premise so this is the wrong option.

The correct answer is: Amazon Import/Export

Question 17

Not answered



What is the difference between an availability zone and an edge location? Choose the correct option

Please select :

- ☐ A. An availability zone is a grouping of AWS resources in a specific region; an edge location is a specific resource within the AWS region
- ☐ B. An availability zone is an Amazon resource within an AWS region, whereas an edge location will deliver cached content to the closest location to reduce latency
- ☐ C. Edge locations are used as control stations for AWS resources
- ☐ D. None of the above

Your answer is incorrect.

Answer – B

In aws , there are regions with each region separated in a seperate geographic area. Each region has multiple, isolated locations known as Availability Zones. An availability zone is used to host resources in a specific region.

For more information on Regions and availability zone, please visit the url -

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html>

An edge location is used to deliver content depending on the location of the user. So if the user is located in Australia, the Australia region can be used to deliver content. If a user was in Australia and you delivered content in Asia , there would a delay in the relay of information to the user. Each edge location synchronizes data so that integrity of data is maintained across all edge locations.

For more information on Edge locations, please visit the url -

<https://aws.amazon.com/about-aws/global-infrastructure/>

The correct answer is: An availability zone is an Amazon resource within an AWS region, whereas an edge location will deliver cached content to the closest location to reduce latency

Question 18

Not answered



An order processing website is using EC2 instances to process messages from an SQS queue. A user reported an issue that their order was processed twice and hence charged twice. What action would you recommend to ensure this does not happen again? Choose the correct option

Please select :

- ☐ A. Insert code into the application to delete messages after processing
- ☐ B. Increase the visibility timeout for the queue
- ☐ C. Modify the order process to use SWF
- ☐ D. Use long polling rather than short polling

Your answer is incorrect.

Answer – C

This is a tricky question and note that Options A,B and D can be used to decrease the likelihood of duplicate messages , but cannot remove the change entirely.

For option A , even if the code is inserted , which should be the case already , if the EC2 instance goes down , the same issue can occur again. The message will not be deleted and when it comes in the SQS queue , it will be processed again.

For option B , even if you increase the visibility timeout , if the process has taken the message but not deleted the message , after the visibility timeout expires , the EC2 instance will again process the message and the same issue will happen again.

If you use long polling instead of short polling , you still have the same problem with Option A and B.

For more information on SQS , please visit the link -

<https://aws.amazon.com/sqs/faqs/>

The correct answer is: Modify the order process to use SWF

Question 19

Not answered



There is a connectivity issue reported on a client's Amazon Virtual Private Cloud and EC2 instances. After logging into the environment, you notice that the client is using two instances that all belong to a subnet with an attached internet gateway. The instances also belong to the same security group. However, one of the instances is not able to send or receive traffic like the other three. You see that there is no OS level issue and the instance is working as it should.

What could be the possible issue? Choose the correct option.

Please select :

- ☐ A. A proper route table configuration that sends traffic from the instance to the Internet through the internet gateway
- ☐ B. The EC2 instance is running in an availability zone that does not support Internet gateways
- ☐ C. The EC2 instance is not a member of the same Auto Scaling group/policy
- ☐ D. The EC2 instance does not have a public IP address associated with it

Your answer is incorrect.

Answer – D

Below is a sample VPC from the aws VPC guides. For an instance to be available from the internet , you need to ensure

- 1) The Internet gateway is in place – This has been confirmed in the question.
- 2) There is a route entry for the internet gateway – This should be in place , because out of the 2 instances , one is working.
- 3) The EC2 instance should have a public or Elastic IP – From the question , there is no mention of one being allocated to the problem instance.

Hence option D is the right answer.

For more information on VPC public subnets , please visit the url -

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario1.html

The correct answer is: The EC2 instance does not have a public IP address associated with it

Question 20

Not answered



Which of the following best describes what "bastion hosts" are? Choose the correct option.

Please select :

- ☐ A. Bastion hosts are instances that sit within a private subnet and are typically accessed using SSH or RDP. Once remote connectivity has been established with the bastion host, it then acts as a 'jump' server, allowing you to use SSH or RDP to log into other instances (within public subnets) deeper within your network.
- ☐ B. Bastion hosts are instances that sit within your public subnet and are typically accessed using SSH or RDP. Once remote connectivity has been established with the bastion host, it then acts as a 'jump' server,

allowing you to use HTTPS to log into other instances (within private subnets) deeper within your network.

- ☐ C. Bastion hosts are instances that sit within your public subnet and are typically accessed using SSH or RDP. Once remote connectivity has been established with a bastion host, it then acts as a 'jump' server, allowing you to use SSH or RDP to log into other instances (within private subnets) deeper within your network.
- ☐ D. Bastion hosts are instances that sit within your private subnet and are typically accessed using SSH or RDP. Once remote connectivity has been established with the bastion host, it then acts as a 'jump' server, allowing you to use HTTPS to log into other instances (within public subnets) deeper within your network.

Your answer is incorrect.

Answer - C

A bastion host is a special purpose computer on a network specifically designed and configured to withstand attacks. The computer generally hosts a single application, for example a proxy server, and all other services are removed or limited to reduce the threat to the computer.

In AWS , A bastion host is kept on a public subnet. Users log on to the bastion host via SSH or RDP and then use that session to manage other hosts in the private subnets.

This is a security practise adopted by many organization to secure the assets in their private subnets.

The correct answer is: Bastion hosts are instances that sit within your public subnet and are typically accessed using SSH or RDP. Once remote connectivity has been established with a bastion host, it then acts as a 'jump' server, allowing you to use SSH or RDP to log into other instances (within private subnets) deeper within your network.

Question 21

Not answered



A web application is hosted on EC2 instances and using SQS. Requests are saved as messages in the SQS queue. The SQS queue is configured with the maximum message retention period. After 10 days you notice that the application was in a hung state and 2000 messages are still lying in the queue unprocessed. You are going to resolve the issue but you need to send a communication to the users on the issue. What information will you provide?

Choose the correct option.

Please select :

- ☐ A. An apology for the delay in processing requests and telling them that unfortunately they have to resubmit all the requests.
- ☐ B. An apology for the delay in processing requests, assurance that the application will be operational shortly, and a note that requests greater than five days old will need to be resubmitted.
- ☐ C. An apology for the delay in processing requests, assurance that the application will be operational shortly, and a note that all received requests will be processed at that time.

- ☐ D. An apology for the delay in processing requests and telling them that unfortunately they have to resubmit all the requests since the queue would not be able to process the 2000 messages together.

Your answer is incorrect.

Answer – C

Since the question states that the SQS is configured with the maximum retention period , it means that messages can last for 14 days.

- So option A is invalid , since the messages will still be in the queue even after 10 days
- Option B is invalid for the same reason noted in Option B
- Option D is invalid because a queue can have up to 120,000 messages.

For more information on SQS , please visit the link:

- <https://aws.amazon.com/sqs/>

The correct answer is: An apology for the delay in processing requests, assurance that the application will be operational shortly, and a note that all received requests will be processed at that time.

Question **22**

Not answered



A Company provides an online service that utilizes SQS to decouple system components for scalability. The SQS consumer's EC2 instances poll the queue as often as possible to keep end-to-end throughput as high as possible. However, it is noticed that polling in tight loops is burning CPU cycles and increasing costs with empty responses. What can be done to reduce the number of empty responses? Choose the correct option.

Please select :

- ☐ A. Scale the component making the request using Auto Scaling based off the number of messages in the queue
- ☐ B. Enable long polling by setting the ReceiveMessageWaitTimeSeconds to a number > 0
- ☐ C. Enable short polling on the SQS queue by setting the ReceiveMessageWaitTimeSeconds to a number > 0
- ☐ D. Enable short polling on the SQS message by setting the ReceiveMessageWaitTimeSeconds to a number = 0

Your answer is incorrect.

Answer - B

By default an SQS queue is configured with Shortpolling , which means that the queue is polled every so often for new messages. There is an option of long polling which allows for a shorter poll time but taking in more messages during the long polling cycle. In order to reduce the number of polling cycles , it better to have bigger gaps by enabling long polling. And this can be done by setting the ReceiveMessageWaitTimeSeconds attribute of the queue to a value greater than 0.

You can do this by changing the queue attributes as shown below

Answer - B

For more information on polling, please visit the link -

<http://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-long-polling.html>

The correct answer is: Enable long polling by setting the ReceiveMessageWaitTimeSeconds to a number > 0

Question **23**

Not answered



You are asked to perform a security audit on a company's AWS environment. You log in to their AWS account with the root user credentials and discover that they are using a VPN to connect to and manage their private EC2 instances. Upon further inspection, you find that they are not regularly patching their RDS instances. Finally, you notice that they are using IAM policies rather than bucket policies to manage access to their S3 buckets. What do you cite as the most critical security risk in your report?

Please select :

- ☐ A. The company allows people to log in with their AWS account's root user
- ☐ B. The company's employees are not using a bastion host to connect to their private EC2 instances
- ☐ C. The company has not been patching their RDS instances
- ☐ D. The company is not using bucket policies to manage S3 bucket access

Your answer is incorrect.

Answer:- A.

The first key security rule is that the user needs to delete their root access keys. When you log into aws with your root account and see the IAM dashboard, you will see all the major security concerns with your account. The first major one as shown below is the deletion of the root access keys. You should create an IAM Admin user and manage the aws account.

For more information on security in aws please visit the link -

<https://aws.amazon.com/security/>

The correct answer is: The company allows people to log in with their AWS account's root user

Question **24**

Not answered



An application is currently configured such that it uses EC2 instances to poll an SQS queue. You have verified that the EC2 instances can correctly retrieve messages from the SQS queue. But your co-workers are complaining about not being able to manually retrieve any messages from the queue from their on-premises workstations. What is the most likely source of this problem? Choose the correct option.

Please select :

- ☐ A. Manual polling of SQS queues is not possible

- ☐ B. SQS queues only accept traffic from within AWS
- ☐ C. They are using short polling
- ☐ D. Your co-workers may not have permission to the SQS queue

Your answer is incorrect.

Answer – D

SQS queues have permissions attached to them. If a user does not have the necessary permission they cannot access the messages in the queue. For EC2 instances, they can access it via a role.

Option A is incorrect because Manual polling is possible.

Option B is incorrect because queues can be accessed from outside AWS as well.

Option C is incorrect, it does not matter if they are using short or long polling.

To give permissions to Queues, follow the below steps

Step 1) Select Permissions in the property of the queue.

Step 2) In the next screen add the necessary permission and choose the right user account.

The correct answer is: Your co-workers may not have permission to the SQS queue

Question 25

Not answered



As part of your application architecture requirements, the company you are working for has requested the ability to run analytics against all combined log files from the Elastic Load Balancer. Which services are used together to collect logs and process log file analysis in an AWS environment? Choose the correct option.

Please select :

- ☐ A. Amazon DynamoDB to store the logs and EC2 for running custom log analysis scripts
- ☐ B. Amazon EC2 for storing and processing the log files
- ☐ C. Amazon S3 for storing the ELB log files and EC2 for processing the log files in analysis
- ☐ D. Amazon S3 for storing ELB log files and Amazon EMR for processing the log files in analysis

Your answer is incorrect.

Answer – D

This question is not that complicated, even though if you don't understand the options. By default when you see "collection of logs and processing of logs", directly think of AWS EMR.

Amazon EMR provides a managed Hadoop framework that makes it easy, fast, and cost-effective to process vast amounts of data across dynamically scalable Amazon EC2 instances. You can also run other popular distributed frameworks such as Apache Spark, HBase, Presto, and Flink in Amazon EMR, and interact with data in other AWS data stores such as Amazon S3 and Amazon DynamoDB.

Amazon EMR securely and reliably handles a broad set of big data use cases, including log analysis, web indexing, data transformations (ETL), machine learning, financial analysis, scientific simulation, and bioinformatics.

For more information on EMR, please visit the link –

<https://aws.amazon.com/emr/>

The correct answer is: Amazon S3 for storing ELB log files and Amazon EMR for processing the log files in analysis

Question 26

Not answered



You have been told that you need to set up a bastion host by your manager in the cheapest, most secure way, and that you should be the only person that can access it via SSH. Which of the following setups would satisfy your manager's request?

Choose the correct option

Please select :

- ☐ A. A large EC2 instance and a security group which only allows access on port 22
- ☐ B. A large EC2 instance and a security group which only allows access on port 22 via your IP address
- ☐ C. A small EC2 instance and a security group which only allows access on port 22
- ☐ D. A small EC2 instance and a security group which only allows access on port 22 via your IP address

Your answer is incorrect.

Answer – D

A bastion host should always be a small EC2 instance, because there is no requirement of applications to run on it.

Also you should only open port 22 from your IP address and no other IP Address.

In AWS , A bastion host is kept on a public subnet. Users log on to the bastion host via SSH or RDP and then use that session to manage other hosts in the private subnets.

This is a security practise adopted by many organization to secure the assets in their private subnets.

The correct answer is: A small EC2 instance and a security group which only allows access on port 22 via your IP address

Question 27

Not answered



As a solution Architect you design an SQS queue and decide to test it out by creating a simple application which looks for messages in the queue. When a message is retrieved, the application is supposed to delete the message. Your team creates four test messages in your SQS queue and discover that messages 1 and 3 are quickly deleted but message 2 and 4 remains in the queue. What is a possible cause for this behaviour? Choose the 2 correct option

Please select :

- ☐ A. The order that messages are received in is not guaranteed in SQS
- ☐ B. You failed to set the correct permissions on message 2 and 4
- ☐ C. Message 2 and 4 uses JSON formatting
- ☐ D. Your application is using short polling

Your answer is incorrect.

Answer – A and D

Option C is incorrect because the type of formatting has not impact on the retrieval of messages.

Option B is not correct because there is no mention of different users polling the messages.

In SQS the order of messages is not guaranteed. And also if you use short polling, there can be a case that message 1 and 3 appeared to the user, but not messages 2 and 4. This is why normally applications opt for Long polling to retrieve all messages at once.

Option D is correct because, if you are using the short polling, the return of all the messages in single request may not happen. But, the subsequent request would return the remaining messages. You can read the clear explanation about short polling here:

- <http://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/standard-queues.html?shortFooter=true#standard-queues-message-sample>

The following figure shows the short-polling behavior of messages returned after one of your system components makes a receive request. Amazon SQS samples several of the servers (in gray) and returns the messages from those servers (Message A, C, D, and B). Message E isn't returned to this particular request, but is returned to a subsequent request.

For more information on SQS, please visit the link –

- <https://aws.amazon.com/sqs/faqs/>

The correct answer is: The order that messages are received in is not guaranteed in SQS, Your application is using short polling

Question 28

Not answered



Your supervisor asks you to create a highly available website which serves static content from EC2 instances. Which of the following is not a requirement to accomplish this goal? Choose the correct option

Please select :

- ☐ A. Multiple Availability Zones
- ☐ B. Multiple subnets
- ☐ C. An SQS queue
- ☐ D. An auto scaling group to recover from EC2 instance failures

Your answer is incorrect.

Answer – C

For highly available websites, yes Multiple Availability Zones and Multiple subnets are required. Below is a simple architecture of a highly available website consisting of an ELB and 2 AZ's. BY default each AZ should be located in a different subnet.

Also auto-scaling is used to add additional EC2 instances for fault tolerance.

SQS is not an option, because SQS is only used to decouple components in an architecture, it is not necessary for a high available web site.

The correct answer is: An SQS queue

Question **29**

Not answered



What is the maximum object size allowed for Multi-part file upload for S3.

Please select :

- ☐ A. 10 TB
- ☐ B. 5 TB
- ☐ C. 1 TB
- ☐ D. 5 GB

Your answer is incorrect.

Answer – B

Please refer to the below table which gives the restrictions for the Multi-part file upload for S3. From here it clearly shows that the right answer is 5TB.

For more information on Multi-part file upload for S3 , please visit the url - <http://docs.aws.amazon.com/AmazonS3/latest/dev/qfacts.html>

The correct answer is: 5 TB

Question **30**

Not answered



Which of the following statements about S3 are true. Please choose 2 options

Please select :

- ☐ A. The total volume of data and number of objects you can store are unlimited
- ☐ B. Individual Amazon S3 objects can range in size from a minimum of 0 bytes to a maximum of 1 terabytes
- ☐ C. You can use Multi-Object Delete to delete large numbers of objects from Amazon S3
- ☐ D. You can store only objects of a particular format in S3

Your answer is incorrect.

Answer – A and C

The below screenshots are from the S3 FAQ's of AWS.

Option B is incorrect, because as per the S3 definition, the maximum size of objects can be 5 TB

Option D is incorrect because you can virtually store objects of any type

For more information on S3 , please visit the URL –

<https://aws.amazon.com/s3/faqs/>

The correct answer is: The total volume of data and number of objects you can store are unlimited, You can use Multi-Object Delete to delete large numbers of objects from Amazon S3

Question 31

Not answered



What is a document that provides a formal statement of one or more permissions?

Please select :

- ☐ A. policy
- ☐ B. permission
- ☐ C. Role
- ☐ D. resource

Your answer is incorrect.

Answer – A

A policy is a JSON document that specifies what a user can do on AWS. This document consists of

- Actions: what actions you will allow. Each AWS service has its own set of actions.
- Resources: which resources you allow the action on.
- Effect: what the effect will be when the user requests access—either allow or deny.

Below is a sample snippet of a policy document that allows access to all users to Describe EC2 Instances. You can clearly see the Actions, Resources and Effect which define the policy document.

For more information on policies, please visit the url -

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

The correct answer is: policy

Question 32

Not answered

True or False: Automated backups are enabled by default for a new DB Instance.



Please select :

- ☐ A. TRUE
- ☐ B. FALSE

Your answer is incorrect.

Answer – A

This is one of the key features of aws RDS. AWS gives you less headache of maintaining your backups by creating the backup's for you.

When you create a database , by default you have a Backup retention period which can be defined during a backup window.

The correct answer is: TRUE

Question 33

Not answered



What are the two permission types used by AWS?

Please select :

- ☐ A. Resource-based and Product-based
- ☐ B. Product-based and Service-based
- ☐ C. Service-based
- ☐ D. User-based and Resource-based

Your answer is incorrect.

Answer – D

Permissions are defined via policies which consist of the following elements

- Actions: what actions you will allow. Each AWS service has its own set of actions.
- Resources: which resources you allow the action on.
- Effect: what the effect will be when the user requests access—either allow or deny.

Below is a sample snippet of a policy document that allows access to all users to Describe EC2 Instances. You can clearly see the Actions, Resources and Effect which define the policy document.

For more information on policies, please visit the url:

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

The correct answer is: User-based and Resource-based

Question 34

Not answered



In Auto scaling, where do you mention the AMI ID used in an Auto Scaling policy

Please select :

- ☐ A. Group policy
- ☐ B. Launch configuration
- ☐ C. Auto Scaling group
- ☐ D. Auto Scaling policy

Your answer is incorrect.

Answer:- B

The launch configuration is used to mention the details of the EC2 instances that will be launched during the auto scaling process. Please find the below steps

Step 1) In your EC2 dashboard, click on Auto scaling – Launch Configurations section.

Step 2) Click on Create Auto Scaling Group

Step 3) The first Step will be to create a launch Configuration.

Step 4) You will then be presented to choose the required AMI

For more information on auto scaling launch configuration , visit the link

<http://docs.aws.amazon.com/autoscaling/latest/userguide/LaunchConfiguration.html>

The correct answer is: Launch configuration

Question **35**

Not answered



Amazon RDS DB snapshots and automated backups are stored in

Please select :

- ☐ A. Amazon S3
- ☐ B. Amazon ECS Volume
- ☐ C. Amazon RDS
- ☐ D. Amazon EMR

Your answer is incorrect.

Answer – A

Automated backups automatically back up your DB instance during a specific, user-definable backup window. Amazon RDS keeps these backups for a limited period that you can specify. You can later recover your database to any point in time during this backup retention period. And all of these backups get stored to S3 by default.

Option B is not correct, because that is used to store data for EC2 instances

Option C is not correct because an RDS cannot be used to store snapshots

Option D because EMR is used for storing and processing logs.

For more information on DB instance backup's , go to the url -

<http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.BackingUpAndRestoringAmazonRDSInstances.html>

The correct answer is: Amazon S3

Question **36**

Not answered



Using Amazon CloudWatch's Free Tier, what is the frequency of metric updates which you receive?

Please select :

- ☐ A. 5 minutes
- ☐ B. 500 milliseconds.
- ☐ C. 30 seconds
- ☐ D. 1 minute

Your answer is incorrect.

Answer – A

AWS free tier gives you access to the basic metrics for Cloudwatch and by default the basic package gives 5 minutes of aggregation of Cloudwatch metrics. If you need a further shorter interval, the you need to pay extra.

For more information on the free tier , please feel free to visit the url - <https://aws.amazon.com/free/>

The correct answer is: 5 minutes

Question **37**

Not answered



What option from the below lets you categorize your EC2 resources in different ways, for example, by purpose, owner, or environment.

Please select :

- ☐ A. wildcards
- ☐ B. pointers
- ☐ C. Tags
- ☐ D. special filters

Your answer is incorrect.

Answer – C

Please note that this is an important concept, if you are pursuing further certifications in AWS. Tags in aws are used to segregate resources in aws , which can also be used for cost reporting and billing purposes. In EC2 dashboard , there is a separate section for Tags.

The correct answer is: Tags

Question **38**

Not answered



What acts as a firewall that controls the traffic allowed to reach one or more instances?

Please select :

- ☐ A. Security group
- ☐ B. ACL
- ☐ C. IAM
- ☐ D. Private IP Addresses

Your answer is incorrect.

Answer – A

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. When you launch an instance in a VPC, you can assign the instance to up to five security groups. Security groups act at the instance level. Below is an example of a security group which has inbound rules. The below rule states that users can only SSH into EC2 instances that are attached to this security group.

For more information on Security Groups , please visit the url -
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html

The correct answer is: Security group

Question **39**

Not answered



You design an application that checks for new items in an S3 bucket once per hour. If new items exist, a message is added to an SQS queue. You have several EC2 instances which retrieve messages from the SQS queue, parse the file, and send you an email containing the relevant information from the file. You upload one test file to the bucket, wait a couple hours and find that you have hundreds of emails from the application. What is the most likely cause for this volume of email? Choose the correct answer from the options given below

Please select :

- ☐ A. This is expected behavior when using short polling because SQS does not guarantee that there will not be duplicate messages processed
- ☐ B. You can only have one EC2 instance polling the SQS queue at a time
- ☐ C. This is expected behavior when using long polling because SQS does not guarantee that there will not be duplicate messages processed
- ☐ D. Your application does not issue a delete command to the SQS queue after processing the message

Your answer is incorrect.

Answer – D

You need to ensure that after a message is processed in SQS, the message is deleted.

For more information on SQS, please visit the below url

<https://aws.amazon.com/sqs/faqs/>

The correct answer is: Your application does not issue a delete command to the SQS queue after processing the message

Question **40**

Not answered



An application requires a minimum of 4 instances to run to ensure that it can cater to its users. You want to ensure fault tolerance and high availability. Which of the following is the best option.

Please select :

- ☐ A. Deploy 2 instances in each of 3 Availability Zones, add a load balancer and an Auto Scaling group to launch more instances if required.
- ☐ B. Deploy 2 instances in each of 2 Availability Zones, add a load balancer and an Auto Scaling group to launch more instances if required.
- ☐ C. Deploy 4 instances in one Availability Zone, add a load balancer and an Auto Scaling group to launch more instances if required.
- ☐ D. Deploy 1 instance in each of 3 Availability Zones, add a load balancer and an Auto Scaling group to launch more instances if required.

Your answer is incorrect.

Answer – A

Since there is a minimum of 4 instances required to run, if you deploy them in 3 AZ's and even if one AZ goes down , you will have at least 4 instances running.

For more information on fault tolerance and high availability, please visit the below URL:

- https://media.amazonwebservices.com/architecturecenter/AWS_ac_ra_ftha_04.pdf

The correct answer is: Deploy 2 instances in each of 3 Availability Zones, add a load balancer and an Auto Scaling group to launch more instances if required.

Question **41**

Not answered



Which of the following is true when it comes to hosting a database in VPC's using the AWS RDS service.

Please select :

- ☐ A. The VPC must have at least one subnet
- ☐ B. The VPC must have at least one subnet in one Availability Zone
- ☐ C. Your VPC must have at least one subnet in at least two of the Availability Zones
- ☐ D. None of the above

Your answer is incorrect.

Answer - C

One of the important aspects of hosting databases in VPC's is the following:

Your VPC must have at least one subnet in at least two of the Availability Zones in the region where you want to deploy your DB instance. A subnet is a segment of a VPC's IP address range that you can specify and that lets you group instances based on your security and operational needs.

Few important points about VPC:

- When you create a VPC, it spans all the Availability Zones in the region.
- After creating a VPC, you can add one or more subnets in each Availability Zone.

For more information on working with RDS instances , please refer to the below link:

- http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_VPC.WorkingWithRDSInstanceinaVPC.html

The correct answer is: Your VPC must have at least one subnet in at least two of the Availability Zones

Question 42

Not answered



There are currently multiple applications hosted in a VPC. During monitoring it has been noticed that multiple port scans are coming in from a specific IP Address block. The internal security team has requested that all offending IP Addresses be denied for the next 24 hours. Which of the following is the best method to quickly and temporarily deny access from the specified IP Address's.

Please select :

- ☐ A. Create an AD policy to modify the Windows Firewall settings on all hosts in the VPC to deny access from the IP Address block.
- ☐ B. Modify the Network ACLs associated with all public subnets in the VPC to deny access from the IP Address block.
- ☐ C. Add a rule to all of the VPC Security Groups to deny access from the IP Address block.
- ☐ D. Modify the Windows Firewall settings on all AMI's that your organization uses in that VPC to deny access from the IP address block.

Your answer is incorrect.

Answer – B

A network access control list (ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets.

Option A and D are wrong because this is a tedious task and it only works for Windows systems. You need something that will work for Linux systems as well.

Option C is only adequate for EC2 instances, but you need rules that will apply to the whole subnet. Otherwise the task of having this done for all servers becomes a tedious task.

For more information on Network ACL's, please visit the URL

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html

The correct answer is: Modify the Network ACLs associated with all public subnets in the VPC to deny access from the IP Address block.

Question **43**

Not answered



Which service allows one to issue temporary credentials in AWS? Choose one answer from the options below.

Please select :

- ☐ A. AWS SQS
- ☐ B. AWS STS
- ☐ C. AWS SES
- ☐ D. None of the above. You need to use a third party software to achieve this.

Your answer is incorrect.

Answer – B

You can use the AWS Security Token Service (AWS STS) to create and provide trusted users with temporary security credentials that can control access to your AWS resources. Temporary security credentials work almost identically to the long-term access key credentials that your IAM users can use.

Option A is wrong because this is the queuing service provided by AWS.

Option C is wrong because this is the emailing service provided by AWS.

Option D is wrong because there is a service which exists from AWS.

For more information on STS, please visit the below URL

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

The correct answer is: AWS STS

Question **44**

Not answered



You have two Elastic Compute Cloud (EC2) instances inside a Virtual Private Cloud (VPC) in the same Availability Zone (AZ) but in different subnets. One instance is running a database and the other instance an application that will interface with the database. You want to confirm that they can talk to each other for your application to work properly. Which two things do we need to confirm in the VPC settings so that these EC2 instances can communicate inside the VPC? Choose 2 answers.

Please select :

- ☐ A. A network ACL that allows communication between the two subnets.
- ☐ B. Both instances are the same instance class and using the same Key-pair.

- ☐ C. That the default route is set to a NAT instance or internet Gateway (IGW) for them to communicate.
- ☐ D. Security groups are set to allow the application host to talk to the database on the right port/protocol.

Your answer is incorrect.

Answer - A and D

When you design a web server and database server, the security groups must be defined so that the web server can talk to the database server. An example image from the AWS documentation is given below

Also when communicating between subnets you need to have the NACL's defined

Option B is wrong since the EC2 instances need not be of the same class or same key pair to communicate to each other.

Option C is wrong since there the NAT and Internet gateway is used for the subnet to communicate to the internet.

For more information on VPC and Subnets, please visit the below URL

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html

The correct answer is: A network ACL that allows communication between the two subnets., Security groups are set to allow the application host to talk to the database on the right port/protocol.

Question 45

Not answered



As a solution architect, you have been asked to design a cloud service based on AWS and choose to use RRS on S3 instead of S3 standard storage type. In such a case what type of trade-offs do you have to build your application around?

Please select :

- ☐ A. With RRS you have to copy data and extract data which can take up to 3 hours.
- ☐ B. RRS only has 99.99% availability
- ☐ C. With RRS, you don't need to worry since AWS will take care of the durability of RRS.
- ☐ D. RRS only has 99.99% durability and you have to design automation around replacing lost objects

Your answer is incorrect.

Answer:- D

RRS only has 99.99% durability and there is a chance that data can be lost. So you need to ensure you have the right steps in place to replace lost objects.

Even though RRS has 99.99% availability, all storage types have the same availability, so it does not answer the question on the specific trade-offs for RRS.

For more information on RRS , visit the link

<https://aws.amazon.com/s3/reduced-redundancy/>

The correct answer is: RRS only has 99.99% durability and you have to design automation around replacing lost objects

Question 46

Not answered



You are running a web-application on AWS consisting of the following components an Elastic Load Balancer (ELB) an Auto-Scaling Group of EC2 instances running Linux/PHP/Apache, and Relational DataBase Service (RDS) MySQL. Which security measures fall into AWS's responsibility?

Please select :

- ☐ A. Protect the EC2 instances against unsolicited access by enforcing the principle of least-privilege access
- ☐ B. Protect against IP spoofing or packet sniffing
- ☐ C. Assure all communication between EC2 instances and ELB is encrypted
- ☐ D. Install latest security patches on ELB, RDS and EC2 instances

Your answer is incorrect.

Answer – B

As per the shared responsibility shown below, the users are required to control the EC2 security via security groups and network access control layers.

For more information on the Shared Responsibility model

<https://aws.amazon.com/compliance/shared-responsibility-model/>

The correct answer is: Protect against IP spoofing or packet sniffing

Question 47

Not answered



What would happen to an RDS (Relational Database Service) multi-Availability Zone deployment of the primary DB instance fails?

Please select :

- ☐ A. The IP of the primary DB instance is switched to the standby DB instance
- ☐ B. The RDS (Relational Database Service) DB instance reboots
- ☐ C. A new DB instance is created in the standby availability zone
- ☐ D. The canonical name record (CNAME) is changed from primary to standby

Your answer is incorrect.

Answer – D

Amazon RDS Multi-AZ deployments provide enhanced availability and durability for Database (DB) Instances, making them a natural fit for production database workloads. When you provision a Multi-AZ DB Instance, Amazon RDS automatically creates a primary DB Instance and synchronously replicates the data to a standby instance in a different Availability Zone (AZ). Each AZ runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure (for example, instance hardware failure, storage failure, or network disruption), Amazon RDS performs an automatic failover to the standby, so that you can resume database operations as soon as the failover is complete. And as per the AWS documentation, the cname is changed to the standby DB when the primary one fails.

For more information on Multi-AZ RDS, please visit the link –

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

The correct answer is: The canonical name record (CNAME) is changed from primary to standby

Question **48**

Not answered



An organization is planning to use AWS for their production roll out. The organization wants to implement automation for deployment such that it will automatically create a LAMP stack, download the latest PHP installable from S3 and setup the ELB. Which of the below mentioned AWS services meets the requirement for making an orderly deployment of the software?

Please select :

- ☐ A. AWS Elastic Beanstalk
- ☐ B. AWS Cloudfront
- ☐ C. AWS Cloudformation
- ☐ D. AWS DevOps

Your answer is incorrect.

Answer – C

When you want to automate deployment, the automatic choice is Cloudformation. Below is the excerpt from AWS on cloudformation.

AWS CloudFormation gives developers and systems administrators an easy way to create and manage a collection of related AWS resources, provisioning and updating them in an orderly and predictable fashion.

You can use AWS CloudFormation's sample templates or create your own templates to describe the AWS resources, and any associated dependencies or runtime parameters, required to run your application. You don't need to figure out the order for provisioning AWS services or the subtleties of making those dependencies work. CloudFormation takes care of this for you. After the AWS resources are deployed, you can modify and update them in a controlled and predictable way, in effect applying version control to your AWS infrastructure the same way you do with your software.

- **Option A** is incorrect because Elastic Beanstalk helps you to manage application in the cloud, but doesn't automate the different set of AWS resources in orderly fashion.
- **Option B** is incorrect because CloudFront is Content Delivery Network (CDN) service from AWS.
- **Option D** also incorrect

For more information on Cloud Formation, please visit the link:

- <https://aws.amazon.com/cloudformation/>
- <http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/deploying.applications.html#deployment-walkthrough-config>
- <http://www.tothenew.com/blog/install-lamp-stack-using-cloud-formation/>

The correct answer is: AWS Cloudformation

Question 49

Not answered



In which of the following ways can you manage lambda functions. Choose all that apply.

Please select :

- ☐ A. Console
- ☐ B. CLI
- ☐ C. SDK
- ☐ D. EC2 Instances

Your answer is incorrect.

Answer – A,B and C

This is given in the aws documentation

For more information on AWS Lambda, please visit the link

<https://aws.amazon.com/lambda/faqs/>

The correct answer is: Console, CLI, SDK

Question 50

Not answered



What is the maximum execution time for a Lambda function?

Please select :

- ☐ A. 3 seconds
- ☐ B. 300 seconds
- ☐ C. 24 hours
- ☐ D. No limit

Your answer is incorrect.

Answer – B

This is given in the aws documentation

For more information on AWS Lambda, please visit the link

<https://aws.amazon.com/lambda/faqs/>

The correct answer is: 300 seconds

Question 51

Not answered



If you want to point a domain name to an AWS elastic load balancer in Route 53, how would you need to configure the record set? Choose the correct answer from the options below

Please select :

- ☐ A. Non-Alias with a type "A" record set
- ☐ B. Alias with a type "AAAA" record set
- ☐ C. Alias with a type "CNAME" record set
- ☐ D. Alias with a type "A" record set

Your answer is incorrect.

Answer – D

This is given in the aws documentation

For more information on Route53, please visit the link

<http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-values-alias.html>

The correct answer is: Alias with a type "A" record set

Question 52

Not answered



Can you create a CNAME record at the zone apex level in Route53?

Please select :

- ☐ A. True
- ☐ B. False

Your answer is incorrect.

Answer – B

This is provided in the AWS documentation

For more information on Route53, please visit the link

<http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-choosing-alias-non-alias.html>

The correct answer is: False

Question **53**

Not answered



True or False: When you create an alias record set in Route 53 which points to an Amazon S3 bucket, you can also specify a TTL for the record.

Please select :

- ☐ A. True
- ☐ B. False

Your answer is incorrect.

Answer – B

This is provided in the AWS documentation

For more information on Route53, please visit the link:

<http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-choosing-alias-non-alias.html>

The correct answer is: False

Question **54**

Not answered



Which of the following statements are true when it comes to EBS volumes and snapshots. Choose all that apply.

Please select :

- ☐ A. You can change the size of an EBS volume.
- ☐ B. If you have an unencrypted volume, you can still create an encrypted snapshot from it.
- ☐ C. The volume change size can also happen when it is attached to an instance.
- ☐ D. The volume change size can only happen if the volume is detached from an instance.

Your answer is incorrect.

Answer – A and C

If your Amazon EBS volume is attached to a current generation EC2 instance type, you can increase its size, change its volume type, or (for an io1 volume) adjust its IOPS performance, all without detaching it.

For more information on changing the volume size, please visit the link

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-expand-volume.html>

If the snapshot needs to be encrypted , then the volume should have been encrypted during creation time.

For more information on changing the volume encryption, please visit the link

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html>

The correct answer is: You can change the size of an EBS volume., The volume change size can also happen when it is attached to an instance.

Question 55

Not answered



You have set up a CloudFront distribution but find that instead of each edge location serving up objects that should be cached, your application's origins are being hit for each request. What could be a possible cause of this behavior? Choose the correct answer from the options below

Please select :

- ☐ A. The requested content has never been requested before
- ☐ B. The objects file size are too large
- ☐ C. The cache expiration time is set to a low value
- ☐ D. You didn't configure the objects with a X.509 certificate

Your answer is incorrect.

Answer – C

You can control how long your objects stay in a CloudFront cache before CloudFront forwards another request to your origin. Reducing the duration allows you to serve dynamic content. Increasing the duration means your users get better performance because your objects are more likely to be served directly from the edge cache. A longer duration also reduces the load on your origin.

For more information on changing the volume encryption, please visit the link

<http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Expiration.html>

The correct answer is: The cache expiration time is set to a low value

Question 56

Not answered



Which of the following will occur when an EC2 instance in a VPC with an associated Elastic IP is stopped and started? Choose the 2 correct options.

Please select :

- ☐ A. The ENI (Elastic Network Interface) is detached from the EC2 instance.
- ☐ B. The underlying host for the instance can be changed
- ☐ C. The Elastic IP will be dissociated from the instance.
- ☐ D. All data on instance-store devices will be lost.

Your answer is incorrect.

Answer:- B and D

When an EC2 instance is stopped, the underlying host on which it resides gets changed. The EC2 instance may start on the same host or another host.

The ENI does not get detached when an instance is stopped and started, hence option A is the wrong option.

The only way to dissociate an Elastic IP, is to do via the console or CLI, hence option C is the wrong option.

If the data is on an instance store volume , by default all data gets deleted when the instance is stopped and started.

For full information on what happens when an instance is stopped or started, please visit the link - http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Stop_Start.html

The correct answer is: The underlying host for the instance can be changed, All data on instance-store devices will be lost.

Question 57

Not answered



You are setting up Route53 for your application. You have a set of EC2 instances to which the traffic needs to be distributed to. You want a certain percentage of traffic to go to each instance. Which routing policy would you use? Choose an answer from the options given below

Please select :

- ☐ A. Latency
- ☐ B. Failover
- ☐ C. Weighted
- ☐ D. Geolocation

Your answer is incorrect.

Answer – C

Use the weighted routing policy when you have multiple resources that perform the same function (for example, web servers that serve the same website) and you want Amazon Route 53 to route traffic to those resources in proportions that you specify (for example, one quarter to one server and three quarters to the other).

For more information on the routing policy, please visit the link

<http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html>

The correct answer is: Weighted

Question 58

Not answered



An application in AWS is currently running in the Singapore region. You have been asked to implement disaster recovery. So if the application goes down in the Singapore region, it has to be started in the Asia region. Your application relies on pre-built AMIs. As part of your disaster recovery strategy, which of the below points should you consider.

Please select :

- ☐ A. Nothing, because all AMI's de default are available in any region as long as it is created within the same account
- ☐ B. Copy the AMI from the Singapore region to the Asia region. Modify the Auto Scaling groups in the backup region to use the new AMI ID in the backup region
- ☐ C. Modify the image permissions and share the AMI to the Asia region.
- ☐ D. Modify the image permissions to share the AMI with another account, then set the default region to the backup region

Your answer is incorrect.

Answer:- B

If you need an AMI across multiple regions , then you have to copy the AMI across regions. Note that by default AMI's that you have created will not be available across all regions. So option A is automatically invalid.

Next you can share AMI's with other users, but they will not be available across regions. So option C and D is invalid. You have to copy the AMI across regions.

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.

For the entire details to copy AMI's , please visit the link -

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/CopyingAMIs.html>

The correct answer is: Copy the AMI from the Singapore region to the Asia region. Modify the Auto Scaling groups in the backup region to use the new AMI ID in the backup region

Question **59**

Not answered



In the basic monitoring package for RDS, Amazon CloudWatch provides the following metrics. Choose the correct option.

Please select :

- ☐ A. database visible metrics such as number of connections
- ☐ B. operating system visible metrics such as memory utilization
- ☐ C. database memory usage

- ☐ D. web service visible metrics such as number failed transaction requests

Your answer is incorrect.

Answer:- A

At the moment, memory utilization is not available in Cloudwatch metrics, so this is an invalid option.

Option A is correct, because monitoring does show the connections for an rds on aws. Currently memory optimization for databases is not available.

For the entire details on Cloudwatch , please visit the link -

<https://aws.amazon.com/cloudwatch/>

The correct answer is: database visible metrics such as number of connections

Question **60**

Not answered



What is the maximum size of an EBS Provisioned IOPS SSD volume? Choose the correct option.

Please select :

- ☐ A. 2TiB
- ☐ B. 16TiB
- ☐ C. 4Gib
- ☐ D. 16TB

Your answer is incorrect.

Answer:- B

The minimum size for an EBS Provisioned IOPS SSD volume is 4GiB and maximum size is 16TiB. This sort of volumes are normally used for hosting databases which require a lot of I/O operations. These types of volumes have better performance and are optimized for such scenarios.

For more information on EBS volume types, please visit the link:

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

The correct answer is: 16TiB

Save the state of the flags

Finish review

QUIZ NAVIGATION

1	2	3
4	5	6
7	8	9
10	11	12
13	14	15
16	17	18
19	20	21
22	23	24
25	26	27
28	29	30
31	32	33
34	35	36
37	38	39
40	41	42
43	44	45
46	47	48
49	50	51
52	53	54
55	56	57
58	59	60

Show one page at a
time

Finish review

