PRACTICE TEST IV

Attempt	1	**Completed on**	Tuesday , 29 January 2019 , 02:20 PM
Marks Obtained	2 / 60	**Time Taken**	00 H 00 M 27 S
Your score is	3.33%	**Result**	Fail

Domains / Topics wise Quiz Performance Report

S.No.	Topic	Total Questions	Correct	Incorrect	Unattempted
1	Other	60	2	0	58

60 Questions	2 Correct	0 Incorrect	58 Unattempted

Show Answers: All

QUESTION 1 CORRECT

What would we need to attach to a Bastion host or NAT host for high availability in the event that the primary host went down and that we needed to send traffic to a secondary host? Choose the correct answer from the options below

- **A.** Elastic IP Address ✔
- **B.** Secondary route table
- **C.** Direct Connect connection
- **D.** Secondary Network Interface

Explanation :

Answer – A

An Elastic IP address is a static IPv4 address designed for dynamic cloud computing. An Elastic IP address is associated with your AWS account. With an Elastic IP address, you can mask the failure of an instance or software by rapidly remapping the address to another instance in your account
For more information on Elastic IP Address, please refer to the link:

- http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html (http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html)

Note:
When you create an ENI, You have to select the specific subnet. So, You can only attach that particular ENI to the instances which are available in that particular subnet only. You can't attach that ENI to the instances launched in the different Availability Zone. You have to create different ENI in the different subnets(availability zones) separately. ENI includes Elastic IP also.

A network interface can include the following attributes:

- A primary private IPv4 address from the IPv4 address range of your VPC
- One or more secondary private IPv4 addresses from the IPv4 address range of your VPC
- One Elastic IP address (IPv4) per private IPv4 address
- One public IPv4 address
- One or more IPv6 addresses
- One or more security groups
- A MAC address
- A source/destination check flag
- A description

You can attach Elastic IP to any instance that available in your region. But elastic IP is a single attribute.

For more info:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html)

Ask our Experts

QUESTION 2 CORRECT

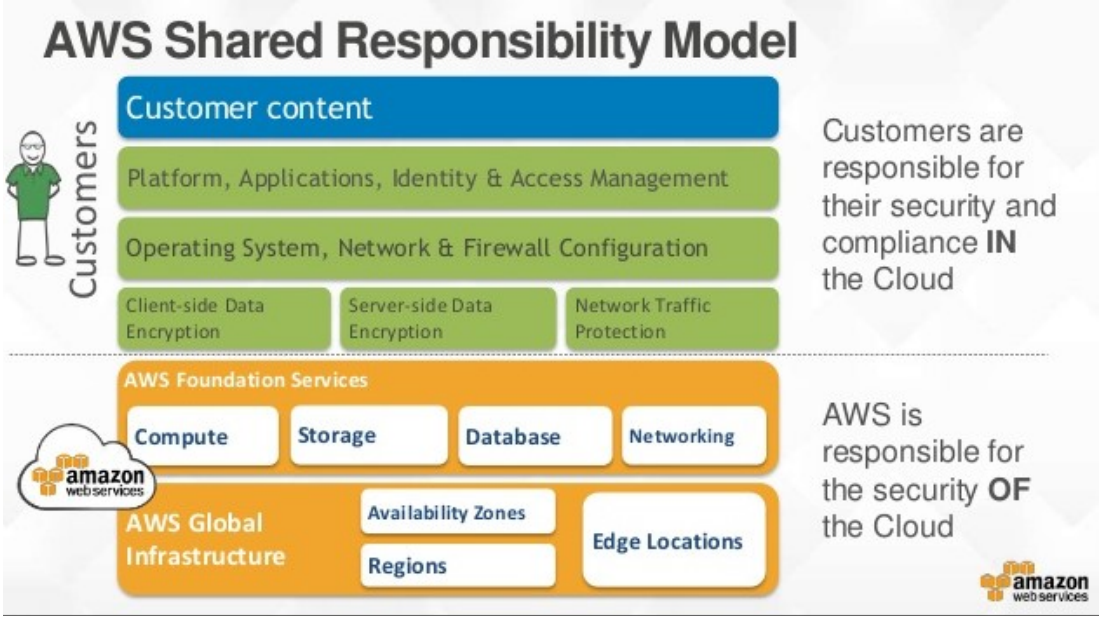
AWS is solely responsible for the security on the guest operating system. Choose the correct answer from the options below

- A. True
- B. False ✔

Explanation :

Answer – B

Please find the shared responsibility model as shared by AWS. Hence the OS responsibility is for the customer.478558+



Ask our Experts

QUESTION 3 UNATTEMPTED

Your company is setting up an application that is used to share files. Because these files are important to the sales team, the application must be highly available. Which AWS-specific storage option would you set up for low cost, reliability, and security? Choose the correct answer from the options below.

- A. Use Amazon S3, which can be accessed by end users with signed URLs. ✔

- **B.** Spin up EC2 with ephemeral type storage to keep the cost down.
- **C.** Create a Dropbox account to share your files.
- **D.** Attach an EBS volume to each of the EC2 servers where the files could be uploaded.

Explanation :

Answer – A
Amazon S3 provides a simple web service interface that you can use to store and retrieve any amount of data, at any time, from anywhere on the web. Using this web service, developers can easily build applications that make use of Internet storage. Since Amazon S3 is highly scalable and you only pay for what you use, developers can start small and grow their application as they wish, with no compromise on performance or reliability.
For more information on S3, please visit the link:

- https://aws.amazon.com/s3/faqs/ (https://aws.amazon.com/s3/faqs/)

Ask our Experts

QUESTION 4 UNATTEMPTED

Your website is hosted on 10 EC2 instances in five regions around the globe, with two instances per region. How could you configure your site to maintain availability with minimum downtime if one of the five regions was to lose network connectivity for an extended period?

Choose the correct answer from the options given below.

- **A.** Establish VPN connections between the instances in each region. Rely on BGP to failover in the case of region-wide connectivity failure for an extended period.
- **B.** Create a Route 53 Latency Based Routing Record Set that resolves to an Elastic Load Balancer in each region and has the Evaluate Target Health flag set to true. ✔
- **C.** Create a Route 53 Latency Based Routing Record Set that resolves to an Elastic Load Balancer in each region. Set an appropriate health check on each ELB.
- **D.** Create a Elastic Load Balancer to place in front of the EC2 instances. Set an appropriate health check on each ELB.

Explanation :

Answer – B
If your application is hosted on Amazon EC2 instances in multiple Amazon EC2 regions, you can reduce latency for your users by serving their requests from the Amazon EC2 region for which network latency is lowest. Amazon Route 53 latency-based routing lets you use DNS to route user requests to the Amazon EC2 region that will give your users the fastest response.
The Evaluate Target health check will ensure availability. If any one of the regions fails, since the evaluate target is set to true , the requests will be sent to another region.
For more information on latency based routing, please visit the link:

- http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html#routing-policy-latency (http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html#routing-policy-latency)

Ask our Experts

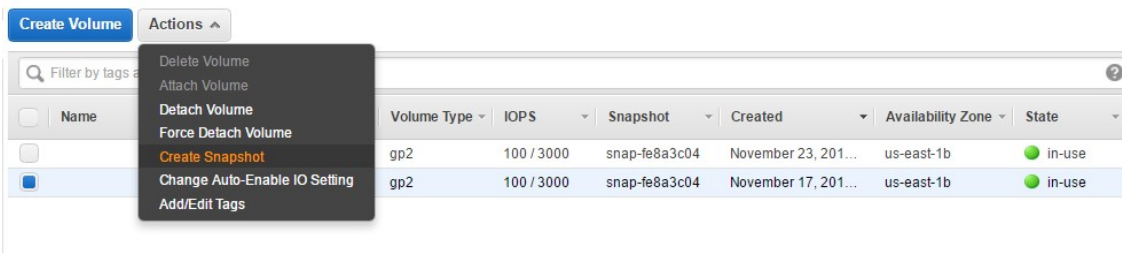
QUESTION 5 UNATTEMPTED

Assuming you have kept the default settings and have taken manual snapshots, which of the following manual snapshots will be retained? Choose the 2 correct answers from the options given below.

- ☐ **A.** A snapshot of an instance store root volume when the EC2 instance is terminated
- ☐ **B.** A snapshot of instance store root volume when the EC2 instance is stopped
- ☐ **C.** A snapshot of an EBS root volume when the EC2 instance is terminated ✔
- ☐ **D.** A snapshot of an RDS database when the RDS instance is terminated ✔

Explanation :

Answer – C and D
You can create EBS and RDS snapshots manually and they will be retained when the instance is termindated.
You can easily create a snapshot from a volume while the instance is running and the volume is in use.
You can do this from the EC2 dashboard.



For more information on EBS snapshots, please visit the link:

- http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html (http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html)

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

- http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_CreateSnapshot.html (http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_CreateSnapshot.html)

Ask our Experts

QUESTION 6 UNATTEMPTED

You run a stateless web application with the following components: an Elastic Load Balancer, three Web/Application servers on EC2, and a MySQL RDS database with 5000 Provisioned IOPS. Average response time for users is increasing. Looking at CloudWatch, you observe 95% CPU usage on the Web/Application servers and 20% CPU usage on the database. The average number of database disk operations varies between 2000 and 2500. How would you improve performance? Choose the 2 correct answers from the options given below

- ☐ **A.** Use Auto Scaling to add additional Web/Application servers based on a memory usage threshold
- ☐ **B.** Use Auto Scaling to add additional Web/Application servers based on CPU load threshold ✔
- ☐ **C.** Choose a different EC2 instance type for the Web/Application servers with a more appropriate CPU/Memory ratio ✔
- ☐ **D.** Increase the number of open TCP connections allowed per web/application EC2 instance

Explanation :

Answer – B and C
Since the CPU percentage is high on the Web/Application servers, it is ideal to either add more servers via Autoscaling or choose a high capacity EC2 instance.
For more information on Autoscaling, please visit the link:

- https://aws.amazon.com/autoscaling/ (https://aws.amazon.com/autoscaling/)

Ask our Experts

QUESTION 7 UNATTEMPTED

Which features can be used to restrict access to data in S3? Choose the 2 correct answers from the options below.

- [ ] **A.** Set an S3 bucket policy ✔
- [ ] **B.** Create a CloudFront distribution for the bucket
- [ ] **C.** Set an S3 ACL on the bucket or the object ✔
- [ ] **D.** Enable IAM Identity Federation

Explanation :

Answer – A and C
Bucket policy and user policy are two of the access policy options available for you to grant permission to your Amazon S3 resources. Both use JSON-based access policy language
For examples on bucket policy, please visit the URL:

- http://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies.html (http://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies.html)

Amazon S3 Access Control Lists (ACLs) enable you to manage access to buckets and objects. Each bucket and object has an ACL attached to it as a subresource. It defines which AWS accounts or groups are granted access and the type of access.
For examples on ACL, please visit the URL:

- 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 8 UNATTEMPTED

What is the result of the following bucket policy?

```
{
 "Statement":[
  {
   "Sid":"Sid2",
   "Action":"s3:*",
   "Effect":"Allow",
```

```
    "Resource":"arn:AWS:s3:::mybucket/*.",
    "Condition":{
      "ArnEquals":{
        "s3:prefix":"accounts_"
      }
    },
    "Principal":{
      "AWS":[
        "*"
      ]
    }
  }
 ]
}
```

Choose the correct answer from the options below.

- **A.** It allow all access objects in the accounts_ bucket name space
- **B.** It will allow all actions only against objects with the prefix accounts_ ✔
- **C.** It will deny all actions if the object prefix is accounts_
- **D.** It will allow all actions if the object is in the accounts subdirectory of mybucket

Explanation :

Answer – B
Since the prefix tag is used, hence all actions will only be marked against objects with the prefix accounts_
For examples on S3, please visit the URL:

- http://docs.aws.amazon.com/AmazonS3/latest/dev/amazon-s3-policy-keys.html (http://docs.aws.amazon.com/AmazonS3/latest/dev/amazon-s3-policy-keys.html)

Ask our Experts

QUESTION 9 UNATTEMPTED

An organization has created a Queue named “modularqueue” with SQS. The organization is not performing any operations such as SendMessage, ReceiveMessage, DeleteMessage, GetQueueAttributes, SetQueueAttributes, AddPermission, and RemovePermission on the queue. What can happen in this scenario?

- **A.** AWS SQS sends notification after 15 days for inactivity on queue
- **B.** AWS SQS can delete queue after 30 days without notification ✔
- **C.** AWS SQS marks queue inactive after 30 days
- **D.** AWS SQS notifies the user after 2 weeks and deletes the queue after 3 weeks.

Explanation :

Answer – B
AWS reserve the right to delete a queue without notification if one of the following actions hasn't been performed on it for 30 consecutive
days: SendMessage, ReceiveMessage, DeleteMessage, GetQueueAttributes, SetQueueAttributes, AddPermissior and RemovePermission.
For more information , please visit the URL:

- https://forums.aws.amazon.com/ann.jspa?annID=2532 (https://forums.aws.amazon.com/ann.jspa?annID=2532)

Ask our Experts

QUESTION 10 UNATTEMPTED

An organization has setup Auto Scaling with ELB. Due to some manual error, one of the instances got rebooted. Thus, it failed the Auto Scaling health check. Auto Scaling has marked it for replacement. How can the system admin ensure that the instance does not get terminated?

- **A.** Update the Auto Scaling group to ignore the instance reboot event
- **B.** It is not possible to change the status once it is marked for replacement
- **C.** Manually add that instance to the Auto Scaling group after reboot to avoid replacement

D. Change the health of the instance to healthy using the Auto Scaling commands ✔

Explanation :

Answer – D
One can change the status of an instance using Autoscaling commands. The command used here would be set-instance-health
For more information on the command, please visit the URL:

- http://docs.aws.amazon.com/cli/latest/reference/autoscaling/set-instance-health.html (http://docs.aws.amazon.com/cli/latest/reference/autoscaling/set-instance-health.html)

Ask our Experts

QUESTION 11 UNATTEMPTED

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

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

Explanation :

Answer – A
An example of the command is given below
AWS elb enable-availability-zones-for-load-balancer --load-balancer-name my-loadbalancer --availability-zones us-west-2b
For more information on adding zones to ELB , please visit the link:

- http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/enable-disable-az.html (http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/enable-disable-az.html)

Ask our Experts

QUESTION 12 UNATTEMPTED

What is the best practice when it comes to pre-warming (also called initialization for EC2)?

Choose the correct answer from the options below.

- **A.** Elastic load balancers that recently experienced a large increase in traffic.
- **B.** EBS volumes that were created from scratch. Pre-warm using the read and then write back method.
- **C.** EBS volumes newly created from snapshots. Pre-warm by accessing each block once. ✔
- **D.** Elastic load balancers that you are expecting to experience a large increase in traffic. Pre-warm using the read and write back method.

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.
For more information on pre-warming EBS, please refer to the link:

- http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-initialize.html (http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-initialize.html)

For ELB, you perform the pre warming when you are expecting a heavy traffic for e.g. load testing or flash sale.
This is done by raising a request to AWS Support. So Option A & Dare wrong for ELB.

Ask our Experts

QUESTION 13 UNATTEMPTED

An organization is planning to create a user with IAM. They are trying to understand the limitations of IAM so that they can plan accordingly. Which of the below mentioned statements is not true with respect to the limitations of IAM?

- **A.** One IAM user can be a part of a maximum of 5 groups ✔

- **B.** The organization can create 100 groups per AWS account
- **C.** One AWS account can have a maximum of 5000 IAM users
- **D.** One AWS account can have 250 roles

Explanation :

Answer – A
Option A : Its false. One IAM user can be a part of maximum 10 groups hence option A is wrong.
Option B : Its true. 100 groups can be created per account. It doesn't say maximum of 100 groups. Maximum default allowed is 300. 100 is within that limit.
Option C: Its true. 5000 is maximum default users in an AWS account.
Option D : Its true. 250 roles can be created in one AWS account. It doesn't say maximum of 1000 roles can be created per account. Maximum default is 1000. 250 is within that limit.

For more information in IAM limits please visit the link:

- http://docs.aws.amazon.com/IAM/latest/UserGuide/reference_iam-limits.html (http://docs.aws.amazon.com/IAM/latest/UserGuide/reference_iam-limits.html)

Ask our Experts

QUESTION 14 UNATTEMPTED

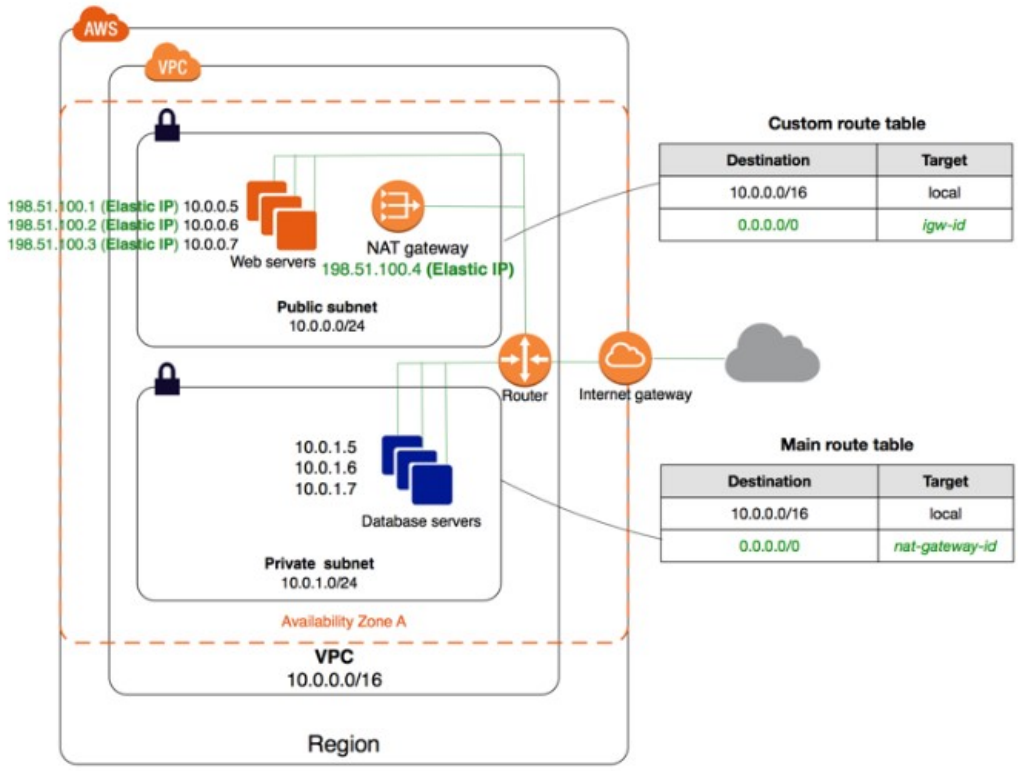
A user has created a VPC with two subnets: one public and one private. The user is planning to run the patch update for the instances in the private subnet. How can the instances in the private subnet connect to the internet?

- **A.** Use the internet gateway with a private IP
- **B.** Allow outbound traffic in the security group for port 80 to allow internet updates
- **C.** The private subnet can never connect to the internet
- **D.** Use NAT with an elastic IP ✔

Explanation :

Answer – D
You can use a network address translation (NAT) gateway to enable instances in a private subnet to connect to the Internet or other AWS services, but prevent the Internet from initiating a connection with those instances.

The below diagram from AWS showcases how the NAT instance is used



For more information on NAT Gateways, please visit the URL:

- http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-nat-gateway.html (http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-nat-gateway.html)

Ask our Experts

QUESTION 15 UNATTEMPTED

A user has configured an EC2 instance in the US-East-1a zone. The user has enabled detailed monitoring of the instance. The user is trying to get the data from CloudWatch using a CLI. Which of the below mentioned CloudWatch endpoint URLs should the user use?

- A. monitoring.us-east-1.amazonaws.com ✔
- B. monitoring.us-east-1-a.amazonaws.com
- C. monitoring.us-east-1a.amazonaws.com
- D. cloudwatch.us-east-1a.amazonaws.com

Explanation :

Answer – A
If you look at the table in AWS documentation and the end point url for cloudwatch you will see that A is the right option.

Region Name	Region	Endpoint	Protocol
US East (N. Virginia)	us-east-1	monitoring.us-east-1.amazonaws.com	HTTP and HTTPS
US East (Ohio)	us-east-2	monitoring.us-east-2.amazonaws.com	HTTP and HTTPS
US West (N. California)	us-west-1	monitoring.us-west-1.amazonaws.com	HTTP and HTTPS
US West (Oregon)	us-west-2	monitoring.us-west-2.amazonaws.com	HTTP and HTTPS

For more information on Cloudwatch monitoring, please visit the URL:

- http://docs.aws.amazon.com/general/latest/gr/rande.html#cw_region (http://docs.aws.amazon.com/general/latest/gr/rande.html#cw_region)

Ask our Experts

QUESTION 16 UNATTEMPTED

A user has configured ELB with Auto Scaling. The user suspended the Auto Scaling AddToLoadBalancer (which adds instances to the load balancer). process for a while. What will happen to the instances launched during the suspension period?

- A. The instances will not be registered with ELB and the user has to manually register when the process is resumed ✔
- B. The instances will be registered with ELB only once the process has resumed
- C. Auto Scaling will not launch the instance during this period due to process suspension
- D. It is not possible to suspend only the AddToLoadBalancer process

Explanation :

Answer – A
If you suspend AddToLoadBalancer, Auto Scaling launches the instances but does not add them to the load balancer or target group. If you resume the AddToLoadBalancer process, Auto Scaling resumes adding instances to the load balancer or target group when they are launched. However, Auto Scaling does not add the instances that were launched while this process was suspended. You must register those instances manually.
For more information on suspending and resuming Autoscaling processes, please visit the URL:

- 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 17 UNATTEMPTED

A user has moved an object to Glacier using the life cycle rules. The user requests to restore the archive after 6 months. When the restore request is completed the user accesses that archive. Which of the below mentioned statements is not true in this condition?

- **A.** The archive will be available as an object for the duration specified by the user during the restoration request
- **B.** The restored object's storage class will be RRS ✔
- **C.** The user can modify the restoration period only by issuing a new restore request with the updated period
- **D.** The user needs to pay storage for both RRS (restored. and Glacier (Archive. Rates

Explanation :

Answer – B
As per the AWS documentation , After you receive a temporary copy of the restored object, the object's storage class remains GLACIER (a GET or HEAD request will return GLACIER as the storage class)
For more information on restoring objects please visit the URL:

- http://docs.aws.amazon.com/AmazonS3/latest/dev/restoring-objects.html (http://docs.aws.amazon.com/AmazonS3/latest/dev/restoring-objects.html)

Note:
the question is about "Which of the below-mentioned statements is **not true** in this condition?"

Option B is the only incorrect statement. Rest all correct statements.

Ask our Experts

QUESTION 18 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), what is recommended to the user for the purpose of security?

- **A.** The user should not use his own security key as it is not secure
- **B.** Configure S3 to rotate the user's encryption key at regular intervals
- **C.** Configure S3 to store the user's keys securely with SSL
- **D.** Keep rotating the encryption key manually at the client side ✔

Explanation :

Answer – D
As per the AWS documentation one of the important elements is to rotate the keys at the client side.

- 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.

For more information on Server side encryption with client side keys please visit the URL:

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

Ask our Experts

QUESTION 19 UNATTEMPTED

A user has launched an EC2 instance and deployed a production application in it. The user wants to prohibit any mistakes from the production team to avoid accidental termination. How can the user achieve this?

- **A.** The user can the set DisableApiTermination attribute to avoid accidental termination ✔
- **B.** It is not possible to avoid accidental termination

- **C.** The user can set the Deletion termination flag to avoid accidental termination
- **D.** The user can set the InstanceInitiatedShutdownBehavior flag to avoid accidental termination

Explanation :

Answer – A
You can prevent an instance from being terminated accidentally by someone using the AWS Management Console, the CLI, and the API. This feature is available for both Amazon EC2 instance store-backed and Amazon EBS-backed instances. Each instance has a DisableApiTermination attribute with the default value of false (the instance can be terminated through Amazon EC2). You can modify this instance attribute while the instance is running or stopped (in the case of Amazon EBS-backed instances)
For more information on Terminating instances please visit the URL:

- http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/terminating-instances.html (http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/terminating-instances.html)

Ask our Experts

QUESTION 20 UNATTEMPTED

A user has created a launch configuration for Auto Scaling where CloudWatch detailed monitoring is disabled. The user wants to now enable detailed monitoring. How can the user achieve this?

- **A.** Update the Launch config with CLI to set InstanceMonitoringDisabled = false
- **B.** The user should change the Auto Scaling group from the AWS console to enable detailed monitoring
- **C.** Update the Launch config with CLI to set InstanceMonitoring.Enabled = true
- **D.** Create a new Launch Config with detail monitoring enabled and update the Auto Scaling group ✔

Explanation :

Answer – D
As per the AWS documentation this is clearly mentioned that you need to create a new launch configuration with detailed monitoring.

Enable Auto Scaling Instance Metrics

You can enable basic or detailed monitoring for the instances in your Auto Scaling group when you create a launch configuration. By default, basic monitoring is enabled when you create the launch configuration using the AWS Management Console and detailed monitoring is enabled when you create the launch configuration using the AWS CLI or an API.

If you have an Auto Scaling group and need to change which type of monitoring is enabled for your Auto Scaling instances, you must create a new launch configuration and update the Auto Scaling group to use this launch configuration.

For more information on Instance monitoring please visit the URL:

- http://docs.aws.amazon.com/autoscaling/latest/userguide/as-instance-monitoring.html (http://docs.aws.amazon.com/autoscaling/latest/userguide/as-instance-monitoring.html)

Ask our Experts

QUESTION 21 UNATTEMPTED

A user has launched an EC2 instance from an instance store backed AMI. The user has attached an additional instance store volume to the instance. The user wants to create an AMI from the running instance. Will the AMI have the additional instance store volume?

- **A.** Yes, the block device mapping will have information about the additional instance store volume ✔
- **B.** No, since the instance store backed AMI can have only the root volume bundled
- **C.** It is not possible to attach an additional instance store volume to the existing instance store backed AMI instance
- **D.** No, since this is ephermal storage it will not be a part of the AMI

Explanation :

Answer – A
Each instance that you launch has an associated root device volume, either an Amazon EBS volume or an instance store volume. You can use block device mapping to specify additional EBS volumes or instance store volumes to attach to an instance when it's launched
For more information on block device mapping please visit the URL:

- http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/block-device-mapping-concepts.html (http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/block-device-mapping-concepts.html)

Ask our Experts

QUESTION 22 UNATTEMPTED

A user has enabled termination protection on an EC2 instance. The user has also set Instance initiated shutdown behaviour to terminate. When the user shuts down the instance from the OS, what will happen?

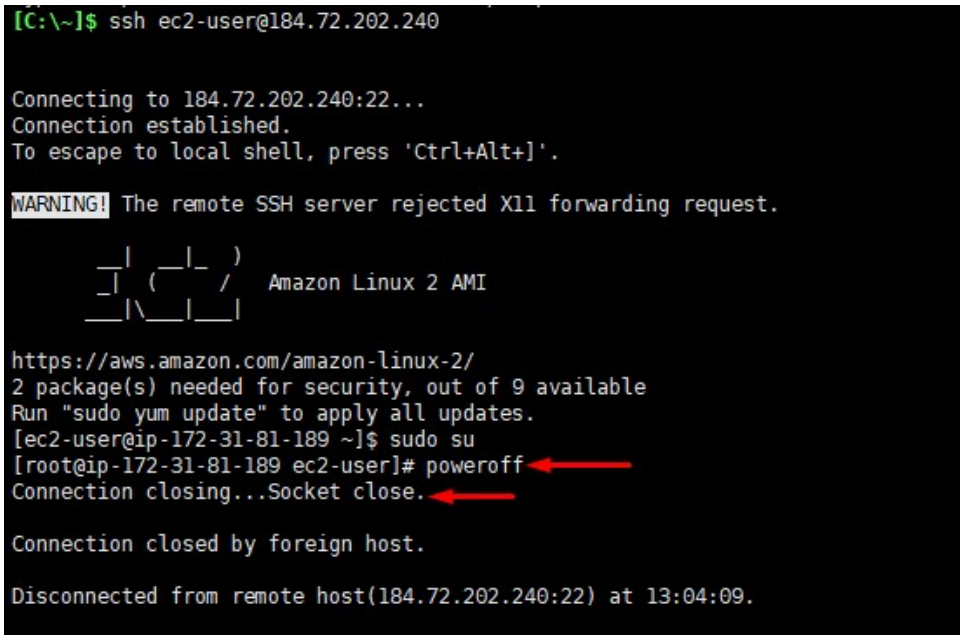
- A. The OS will shutdown but the instance will not be terminated due to protection
- B. It will terminate the instance ✔
- C. It will not allow the user to shutdown the instance from the OS
- D. It is not possible to set the termination protection when an Instance initiated shutdown is set to Terminate

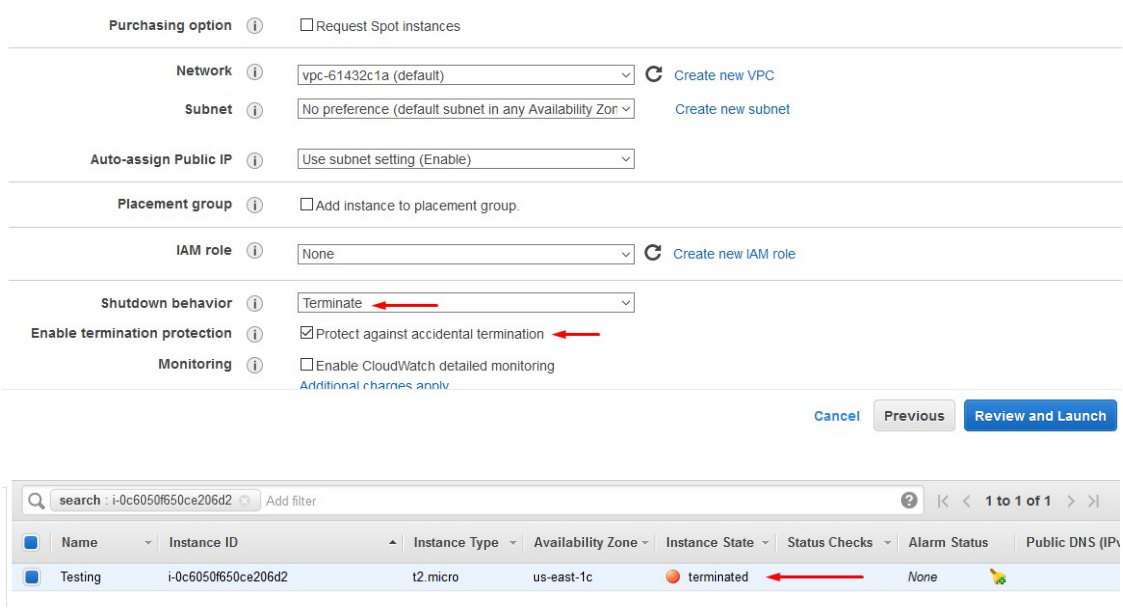
Explanation :

Answer – B

Since the shutdown behavior is Terminate the instance will still terminate.

Screenshots:





For more information on Terminating instances please visit the URL:

- http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/terminating-instances.html (http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/terminating-instances.html)

Ask our Experts

QUESTION 23 UNATTEMPTED

We need to run a business intelligence application against our production database. This application requires near real time data from the database. How might we configure our RDS setup so that our application does not increase I/O load against our production database?

Choose the correct answer from the options below.

- **A.** Copy the production instance and create a cron that dumps the RDS data into the secondary instance
- **B.** Point the application to the Multi-AZ failover instance
- **C.** Create a read replica from the production instance and point the application to the read replica ✔
- **D.** In order to receive real time information the application must query the primary database

Explanation :

Answer – C
You can reduce the load on your source DB Instance by routing read queries from your applications to the read replica. Read replicas allow you to elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads.
For more information on read replica's, please refer to the link:

- https://aws.amazon.com/rds/details/read-replicas/ (https://aws.amazon.com/rds/details/read-replicas/)

Ask our Experts

QUESTION 24 UNATTEMPTED

A user has launched a Windows based EC2 instance. However, the instance has some issues and the user wants to check the log. When the user checks the Instance console output from the AWS console, what will it display?

- A. All the event logs since instance boot
- B. The last 10 system event log error
- C. The Windows instance does not support the console output
- D. The last three system events' log errors ✔

Explanation :

Answer – D
For Linux/Unix instances, the instance console output displays the exact console output that would normally be displayed on a physical monitor attached to a computer. This output is buffered because the instance produces it and then posts it to a store where the instance's owner can retrieve it.
For Windows instances, the instance console output displays the last three system event log errors.
For more information on Windows EC2 logs please visit the URL:

- https://docs.aws.amazon.com/cli/latest/reference/ec2/get-console-output.html (https://docs.aws.amazon.com/cli/latest/reference/ec2/get-console-output.html)
- http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instance-console.html (http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instance-console.html)

Ask our Experts

QUESTION 25 UNATTEMPTED

A company is very insistent on the fact they want to retain administrative privileges or the underlying EC2 instances? Choose 2 answers from the below options which allow this.

- [ ] **A.** AWS Elastic Beanstalk ✔
- [ ] **B.** Amazon Elastic Map Reduce ✔
- [ ] **C.** Amazon Relational Database Service
- [ ] **D.** Amazon Elastic Cache

Explanation :

Answer - A and B
Remember that RDS, Elasticache and DynamoDB are hosted services by AWS, and they do not allow you to work with the underlying EC2 instances.
For more information on Elastic beanstalk and EMR please visit the URL:

- https://aws.amazon.com/elasticbeanstalk/faqs/ (https://aws.amazon.com/elasticbeanstalk/faqs/)
- https://aws.amazon.com/emr/ (https://aws.amazon.com/emr/)

Ask our Experts

QUESTION 26 UNATTEMPTED

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

- ○ **A.** Data is automatically deleted ✔
- ○ **B.** Data is automatically saved as an EBS snapshot.
- ○ **C.** Data is unavailable until the instance is restarted
- ○ **D.** Data is automatically saved as an EBS volume.

Explanation :

Answer – A
The root volume will always be deleted. Always remember to create additional EBS volumes , store

your data and created snapshots regularly for backup.
For more information on EBS volumes please visit the URL:

- http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumes.html (http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumes.html)
- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/RootDeviceStorage.html (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/RootDeviceStorage.html)

Note:
S3-based AMIs are actually instance store based AMIs.
For more information, please check below AWS Docs:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ComponentsAMIs.html
(https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ComponentsAMIs.html)

Ask our Experts

QUESTION 27 UNATTEMPTED

How can you secure data at rest on an EBS volume?

- **A.** Encrypt the volume using the S3 server-side encryption service.
- **B.** Attach the volume to an instance using EC2's SSL interface.
- **C.** Create an IAM policy that restricts read and write access to the volume.
- **D.** Write the data randomly instead of sequentially.
- **E.** Use EBS encryption to encrypt the volume. ✔

Explanation :

Answer – E
Amazon EBS encryption offers you a simple encryption solution for your EBS volumes without the need for you to build, maintain, and secure your own key management infrastructure. When you create an encrypted EBS volume and attach it to a supported instance type, the following types of data are encrypted:

- Data at rest inside the volume
- All data moving between the volume and the instance
- All snapshots created from the volume

For more information on EBS encryption please visit the URL:

- http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html (http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html)

Ask our Experts

QUESTION 28 UNATTEMPTED

In order to optimize performance for a compute cluster that requires low inter-node latency, which feature in the following list should you use?

- A. AWS Direct Connect
- B. Placement Groups ✔
- C. VPC private subnets
- D. EC2 Dedicated Instances
- E. Multiple Availability Zones

Explanation :

Answer – B
A placement group is a logical grouping of instances within a single Availability Zone. Placement groups are recommended for applications that benefit from low network latency, high network throughput, or both. To provide the lowest latency, and the highest packet-per-second network performance for your placement group, choose an instance type that supports enhanced networking
For more information on placement groups please visit the URL:

- http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html (http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html)

Ask our Experts

QUESTION 29 UNATTEMPTED

Amazon EBS snapshots have which of the following two characteristics? Choose 2 answers

- A. EBS snapshots only save incremental changes from snapshot to snapshot ✔
- B. EBS snapshots can be created in real-time without stopping an EC2 instance ✔
- C. EBS snapshots can only be restored to an EBS volume of the same size or smaller

☐ **D.** EBS snapshots can only be restored and mounted to an instance in the same Availability Zone as the original EBS volume

Explanation :

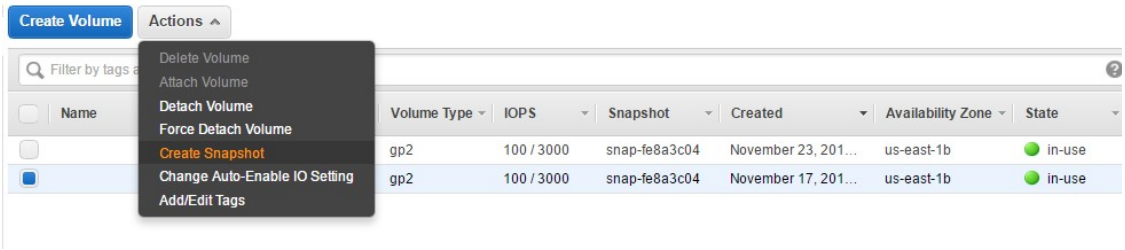
Answer - A and B

Snapshots are incremental, this is clear from the AWS documentation

Amazon EBS Snapshots

You can back up the data on your EBS volumes to Amazon S3 by taking point-in-time snapshots. Snapshots are incremental backups, which means that only the blocks on the device that have changed after your most recent snapshot are saved. This minimizes the time required to create the snapshot and saves on storage costs. When you delete a snapshot, only the data unique to that snapshot is removed. Active snapshots contain all of the information needed to restore your data (from the time the snapshot was taken) to a new EBS volume.

You can easily create a snapshot from a volume while the instance is running and the volume is in use. You can do this from the EC2 dashboard.



For more information on EBS snapshots please visit the URL:

- http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html (http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html)

Ask our Experts

QUESTION 30 UNATTEMPTED

You run a web application with the following components Elastic Load Balancer (ELB), 3 Web/Application servers, 1 MySQL RDS database with read replicas, and Amazon Simple Storage Service (Amazon S3) for static content. Average response time for users is increasing slowly. Which CloudWatch RDS metrics will not allow you to identify if the database is the bottleneck?

○ **A.** The number of outstanding IOs waiting to access the disk.

○ **B.** The amount of write latency.

- **C.** The amount of disk space occupied by binary logs on the master.
- **D.** The amount of time a Read Replica DB Instance lags behind the source DB Instance ✔
- **E.** The average number of disk I/O operations per second.

Explanation :

Answer - D
Please note the key word "**not allow**" in the question.
The following database metrics are available in cloudwatch for monitoring.

- DiskQueueDepth- The number of outstanding IOs (read/write requests) waiting to access the disk.
- WriteLatency- The average amount of time taken per disk I/O operation.
- ReplicaLag- The amount of time a Read Replica DB instance lags behind the source DB instance. Applies to MySQL, MariaDB, and PostgreSQL Read Replicas.

For more information on database metrics please visit the URL:

- http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/rds-metricscollected.html (http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/rds-metricscollected.html)

Generally speaking, acceptable values for performance metrics depend on what your baseline looks like and what your application is doing. Investigate consistent or trending variances from your baseline. Advice about specific types of metrics follows:

- **High CPU or RAM consumption –** High values for CPU or RAM consumption might be appropriate, provided that they are in keeping with your goals for your application (like throughput or concurrency) and are expected.
- **Disk space consumption –** Investigate disk space consumption if space used is consistently at or above 85 percent of the total disk space. See if it is possible to delete data from the instance or archive data to a different system to free up space.
- **Network traffic –** For network traffic, talk with your system administrator to understand what expected throughput is for your domain network and Internet connection. Investigate network traffic if throughput is consistently lower than expected.
- **Database connections –** Consider constraining database connections if you see high numbers of user connections in conjunction with decreases in instance performance and response time. The best number of user connections for your DB instance will vary based on your instance class and the complexity of the operations being performed. You can determine the number of database connections by associating your DB instance with a parameter group where the *User Connections* parameter is set to other than 0 (unlimited). You can either use an existing parameter group or create a new one. For more information, see Working with DB Parameter Groups (https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_WorkingWithParamGroups.html).

- **IOPS metrics –** The expected values for IOPS metrics depend on disk specification and server configuration, so use your baseline to know what is typical. Investigate if values are consistently different than your baseline. For best IOPS performance, make sure your typical working set will fit into memory to minimize read and write operations.

You may refer to the link below for more information:
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_BestPractices.html (https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_BestPractices.html)
"Readreplica lag can be a solution since it will not be a good metrics to identify whether there is a db bottleneck. In AWS docs it is noted that, You can expect to see a higher level of lag time for any Read Replica that is in a different AWS Region than the source instance, **due to the longer network channels between regional data centers.** So mainly replication lag is due to either long network channels or due to network contention."

Ask our Experts

QUESTION 31 UNATTEMPTED

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

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

Explanation :

Answer – A
A bucket policy as shown below can be used to prevent an IP address block from accessing public objects in an S3 bucket

```
{
 "Version": "2012-10-17",
 "Id": "S3PolicyId1",
 "Statement": [
  {
   "Sid": "IPAllow",
   "Effect": "Allow",
   "Principal": "*",
   "Action": "s3:*",
   "Resource": "arn:aws:s3:::examplebucket/*",
```

```
    "Condition": {
      "IpAddress": {"aws:SourceIp": "54.240.143.0/24"},
      "NotIpAddress": {"aws:SourceIp": "54.240.143.188/32"}
    }
   }
 ]
}
```

For more examples on bucket policies please visit the URL:

- http://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies.html (http://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies.html)

Ask our Experts

QUESTION 32 UNATTEMPTED

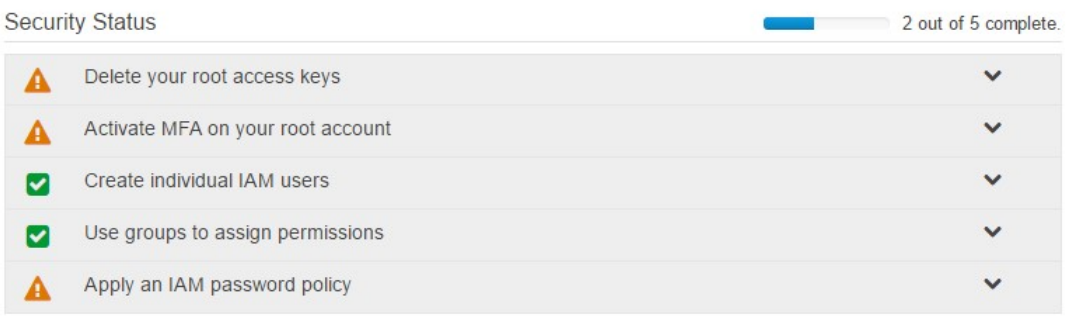
Your organization is preparing for a security assessment of your use of AWS. In preparation for this assessment, which two IAM best practices should you consider implementing? Choose 2 answers

- ☐ **A.** Create individual IAM users for everyone in your organization
- ☐ **B.** Configure MFA on the root account and for privileged IAM users ✔
- ☐ **C.** Assign IAM users and groups configured with policies granting least privilege access ✔
- ☐ **D.** Ensure all users have been assigned and are frequently rotating a password, access ID/secret key, and X.509 certificate

Explanation :

Answer – B and C

When you go to the security dashboard, the security status will show the best practices for initiating the first level of security.



For more information on best security practises please visit the URL:

- https://aws.amazon.com/whitepapers/aws-security-best-practices/ (https://aws.amazon.com/whitepapers/aws-security-best-practices/)

Ask our Experts

QUESTION 33 UNATTEMPTED

Your business is building a new application that will store its entire customer database on a RDS MySQL database, and will have various applications and users that will query that data for different purposes. Large analytics jobs on the database are likely to cause other applications to not be able to get the query results they need to, before time out. Also, as your data grows, these analytics jobs will start to take more time, increasing the negative effect on the other applications. How do you solve the contention issues between these different workloads on the same data?

- A. Enable Multi-AZ mode on the RDS instance
- B. Use ElastiCache to offload the analytics job data
- C. Create RDS Read-Replicas for the analytics work ✔
- D. Run the RDS instance on the largest size possible

Explanation :

Answer – C
Amazon RDS Read Replicas provide enhanced performance and durability for database (DB) instances. This replication feature makes it easy to elastically scale out beyond the capacity constraints of a single DB Instance for read-heavy database workloads. You can create one or more replicas of a given source DB Instance and serve high-volume application read traffic from multiple copies of your data, thereby increasing aggregate read throughput. Read replicas can also be promoted when needed to become standalone DB instances.

For more information on read replica's, please refer to the link:

- https://aws.amazon.com/rds/details/read-replicas/ (https://aws.amazon.com/rds/details/read-replicas/)

Ask our Experts

QUESTION 34 UNATTEMPTED

You are uploading 3 gigabytes of data every night to S3 from your on-premises data center. It takes 3 hours to upload and you are uploading it to Amazon S3. You are only using half of your available bandwidth through your internet provider. How might you decrease the amount of time to back up that 3GB of data from your on-premises data center to S3? Choose the 2 correct answers from the options below

- [ ] **A.** You could establish a Direct Connect connection between your on-premises data center and AWS VPC ✔
- [ ] **B.** Increase your provisioned IOPS
- [ ] **C.** Increase your instance size
- [ ] **D.** You can use multipart upload to speed up the upload process ✔

Explanation :

Answer – A and D
So if you are using the Multi Upload option for S3, then you can resume on failure. Below are the advantage of Multi Part upload

- Improved throughput—you can upload parts in parallel to improve throughput.
- Quick recovery from any network issues—smaller part size minimizes the impact of restarting a failed upload due to a network error.
- Pause and resume object uploads—you can upload object parts over time. Once you initiate a multipart upload there is no expiry; you must explicitly complete or abort the multipart upload.
- Begin an upload before you know the final object size—you can upload an object as you are creating it.

For more information on Multi-part file upload for S3, please visit the URL:

- http://docs.aws.amazon.com/AmazonS3/latest/dev/qfacts.html (http://docs.aws.amazon.com/AmazonS3/latest/dev/qfacts.html)

AWS Direct Connect makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect, you can establish private connectivity between AWS and your datacenter, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.
For more information on direct connect, please visit the URL:

- https://aws.amazon.com/directconnect/ (https://aws.amazon.com/directconnect/)

Ask our Experts

QUESTION 35 UNATTEMPTED

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

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

Explanation :

Answer - B and C
Option A is wrong cause Web server is behind the ELB and customer IPs will never reach web servers
Option B can be done by getting the customer IPs and creating a custom filter to restrict access
Option C ELB will see the customer IPs so can restrict access, deny all is basically have no rules in outbound traffic, implicit, and its stateful so would work
Option D NACL is stateless, deny all will not work
For more information on X-Forwarded-For request , please refer to the link:

- https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/x-forwarded-headers.html (https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/x-forwarded-headers.html)

Note:

A security group is stateful, which means that the traffic that we permit using the inbound rule will be allowed to flow out even if we haven't configured any outbound rules on the Security Group.
If you send a request from your instance, the response traffic for that request is allowed to flow in regardless of inbound security group rules. Responses to allowed inbound traffic are allowed to flow out, regardless of outbound rules.

We can **only allow** traffic using Security group. **There is no deny rule for Security Groups.**

By default Security Groups in a VPC allows all outbound traffic. But we can change this behavior by editing the outbound rule and removing this rule from it.
For more information please click the link given below.
https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html (https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html)

Connection tracking gives us a clear picture on the Stateful behaviour of SecurityGroups.
Your security groups use connection tracking to track information about traffic to and from the instance. Rules are applied based on the connection state of the traffic to determine if the traffic is allowed or denied. This allows security groups to be stateful — responses to inbound traffic are allowed to flow out of the instance regardless of outbound security group rules, and vice versa. For example, if you initiate an ICMP **ping** command to your instance from your home computer, and your inbound security group rules allow ICMP traffic, information about the connection (including the port information) is tracked. Response traffic from the instance for the **ping** command is not tracked as a new request, but rather as an established connection and is allowed to flow out of the instance, even if your outbound security group rules restrict outbound ICMP traffic.

For more information please click the link given below:

- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html#security-group-connection-tracking (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html#security-group-connection-tracking)

We can specify to allow traffic from a single IP address in Security Groups but we need to specify it in the CIDR notation. for eg: 203.0.113.25/32

For more information please click the link given below.

- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/authorizing-access-to-an-instance.html (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/authorizing-access-to-an-instance.html)

Ask our Experts

QUESTION 36 UNATTEMPTED

How can software determine the public and private IP addresses of the Amazon EC2 instance that it is running on?

- **A.** Query the local instance metadata. ✔
- **B.** Query the appropriate Amazon CloudWatch metric.
- **C.** Query the local instance userdata.
- **D.** Use ipconfig or ifconfig command.

Explanation :

Answer – A
Instance metadata is data about your instance that you can use to configure or manage the running instance.
To view all categories of instance metadata from within a running instance, use the following URI:
http://169.254.169.254/latest/meta-data/
For more information on instance metadata , please refer to the link:

- http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html (http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html)

Ask our Experts

QUESTION 37 UNATTEMPTED

The compliance department within your multi-national organization requires that all data for your customers that reside in the European Union (EU) must not leave the EU and also data for customers that reside in the US must not leave the US without explicit authorization. What must you do to comply with this requirement for a web based profile management application running on EC2?

- **A.** Run EC2 instances in multiple AWS Availability Zones in single Region and leverage an Elastic Load Balancer with session stickiness to route traffic to the appropriate zone to create their profile
- **B.** Run EC2 instances in multiple Regions and leverage Route 53's Latency Based Routing capabilities to route traffic to the appropriate region to create their profile

- **C.** Run EC2 instances in multiple Regions and leverage a third party data provider to determine if a user needs to be redirect to the appropriate region to create their profile ✔
- **D.** Run EC2 instances in multiple AWS Availability Zones in a single Region and leverage a third party data provider to determine if a user needs to be redirect to the appropriate zone to create their profile

Explanation :

Answer – C
Option A is incorrect because EC2 instances must be in 2 different regions(US and Europe).
Option B is incorrect because Latency based routing policy will not guarantee the compliance requirement.
Option D is incorrect because EC2 instances must be in 2 different regions(US and Europe).

Ask our Experts

QUESTION 38 UNATTEMPTED

You have private video content in S3 that you want to serve to subscribed users on the Internet. User IDs, credentials, and subscriptions are stored in an Amazon RDS database. Which configuration will allow you to securely serve private content to your users?

- **A.** Generate pre-signed URLs for each user as they request access to protected S3 content ✔
- **B.** Create an IAM user for each subscribed user and assign the GetObject permission to each IAM user
- **C.** Create an S3 bucket policy that limits access to your private content to only your subscribed users'credentials
- **D.** Create a CloudFront Origin Identity user for your subscribed users and assign the GetObject permission to this user

Explanation :

Answer – A
All objects and buckets by default are private. The pre-signed URLs are useful if you want your user/customer to be able upload a specific object to your bucket, but you don't require them to have AWS security credentials or permissions. When you create a pre-signed URL, you must provide your

security credentials, specify a bucket name, an object key, an HTTP method (PUT for uploading objects), and an expiration date and time. The pre-signed URLs are valid only for the specified duration.
For more information on pre-signed urls , please refer to the link:

- https://docs.aws.amazon.com/AmazonS3/latest/dev/ShareObjectPreSignedURL.html (https://docs.aws.amazon.com/AmazonS3/latest/dev/ShareObjectPreSignedURL.html)

Ask our Experts

QUESTION 39 UNATTEMPTED

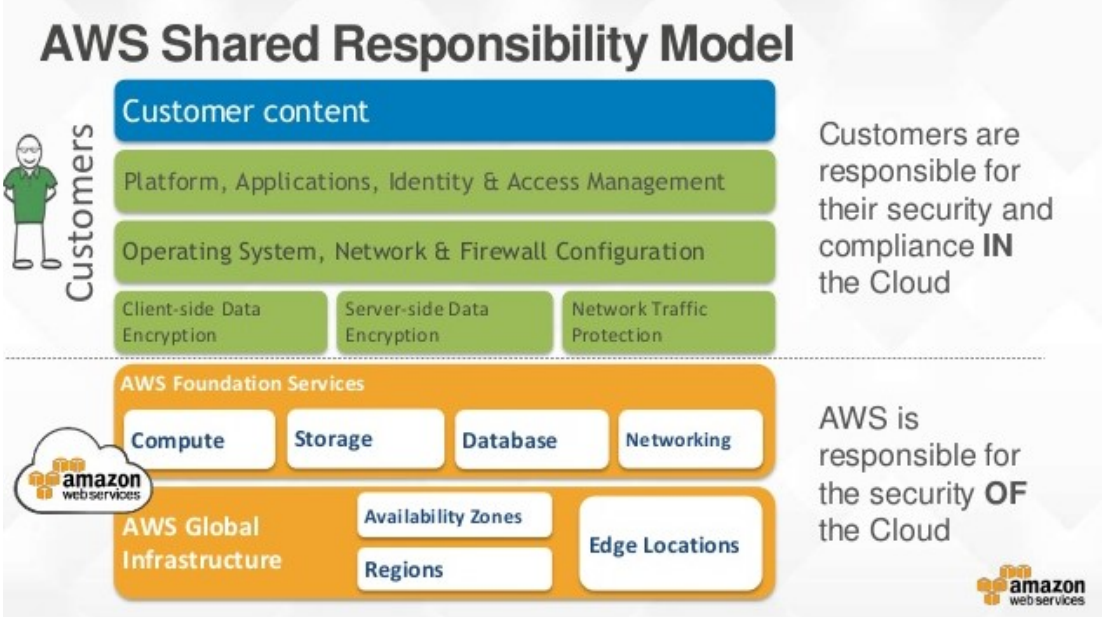
In AWS, which security aspects are the customer's responsibility? Choose 4 answers

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

Explanation :

Answer - B,C,D and F
As per the shared responsibility shown below, the users are required to

- Patch management on the EC2 instances operating system
- Encryption of EBS (Elastic Block Storage) volumes
- Life-cycle management of IAM credentials
- Security Group and ACL (Access Control List) settings



For more information on AWS shared responsibility model, please visit the link:

- https://aws.amazon.com/blogs/security/tag/shared-responsibility-model/ (https://aws.amazon.com/blogs/security/tag/shared-responsibility-model/)

Ask our Experts

QUESTION 40 UNATTEMPTED

An application you maintain consists of multiple EC2 instances in a default tenancy VPC. This application has undergone an internal audit and has been determined to require dedicated hardware for one instance. Your compliance team has given you a week to move this instance to single-tenant hardware. Which process will have minimal impact on your application while complying with this requirement?

- **A.** Create a new VPC with tenancy=dedicated and migrate to the new VPC
- **B.** Use ec2-reboot-instances command line and set the parameter "dedicated=true"
- **C.** Right click on the instance, select properties and check the box for dedicated tenancy
- **D.** Stop the instance, create an AMI, launch a new instance with tenancy=dedicated, and terminate the old instance ✔

Explanation :

Answer – D

As per the AWS documentation , you cannot change the tenancy once the instance is created. Hence D is the only right option.

Each instance that you launch into a VPC has a tenancy attribute. This attribute has the following values.

Value	Description
`default`	Your instance runs on shared hardware.
`dedicated`	Your instance runs on single-tenant hardware.
`host`	Your instance runs on a Dedicated Host, which is an isolated server with configurations that you can control.

You cannot change the tenancy of a default instance after you've launched it. You can change the tenancy of an instance from `dedicated` to `host` after you've launched it, and vice versa. For more information, see Changing the Tenancy of an Instance.

For more information on tenancy, please visit the link:

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

Ask our Experts

QUESTION 41 UNATTEMPTED

A .NET application that you manage is running in Elastic Beanstalk. Your developers tell you they will need access to application log files to debug issues that arise. The infrastructure will scale up and down. How can you ensure the developers will be able to access only the log files?

- **A.** Access the log files directly from Elastic Beanstalk
- **B.** Enable log file rotation to S3 within the Elastic Beanstalk configuration ✔
- **C.** Ask your developers to enable log file rotation in the applications web.config file
- **D.** Connect to each Instance launched by Elastic Beanstalk and create a Windows Scheduled task to rotate the log files to S3.

Explanation :

Answer – B

The EC2 instances in your Elastic Beanstalk environment generate logs that you can view to troubleshoot issues with your application or configuration files. Logs created by the web server, application server, Elastic Beanstalk platform scripts, and AWS CloudFormation are stored locally on individual instances, and can be easily retrieved with the environment management console or the EB CLI. You can also enable log rotation to Amazon S3.
For more information on Elastic Beanstalk logs please visit the link:

- http://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.logging.html (http://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.logging.html)

Ask our Experts

QUESTION 42 UNATTEMPTED

A user has deployed an application on his Amazon Private Cloud. The user is using his own monitoring tool. He wants to configure that whenever there is an error, the monitoring tool should notify him via SMS. Which of the below mentioned AWS services will help in this scenario?

- A. None because the user infrastructure is in the private cloud
- B. AWS SNS ✔
- C. AWS SES
- D. AWS SMS

Explanation :

Answer – B
Amazon Simple Notification Service (Amazon SNS) is a fast, flexible, fully managed push notification service that lets you send individual messages or to fan-out messages to large numbers of recipients. Amazon SNS makes it simple and cost effective to send push notifications to mobile device users, email recipients or even send messages to other distributed services.
With Amazon SNS, you can send notifications to Apple, Google, Fire OS, and Windows devices, as well as to Android devices in China with Baidu Cloud Push. You can use SNS to send SMS messages to mobile device users worldwide.For more information on SNS please visit the link:

- https://aws.amazon.com/sns/ (https://aws.amazon.com/sns/)

Ask our Experts

QUESTION 43 UNATTEMPTED

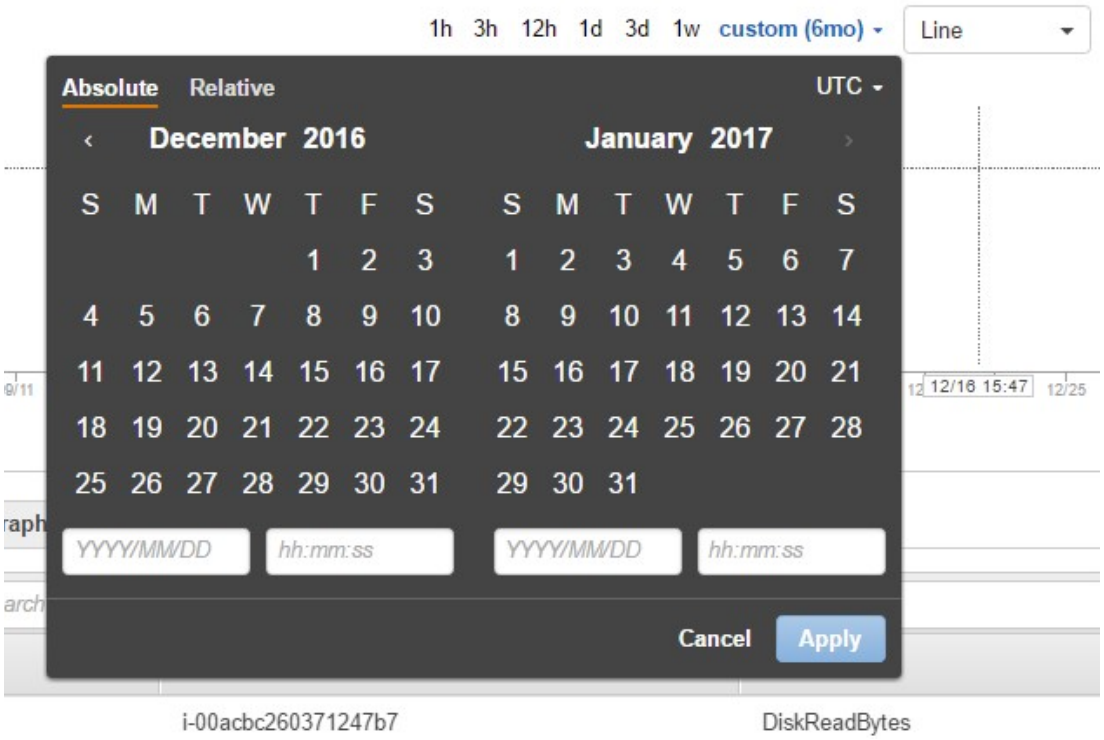
A user has received a message from the support team that an issue occurred 1 week back between 3 AM to 4 AM and the EC2 server was not reachable. The user is checking the CloudWatch metrics of that instance. How can the user find the data easily using the CloudWatch console?

- **A.** The user can find the data by giving the exact values in the time Tab under CloudWatch metrics
- **B.** The user can find the data by filtering values of the last 1 week for a 1 hour period in the Relative tab under CloudWatch metrics
- **C.** It is not possible to find the exact time from the console. The user has to use CLI to provide the specific time
- **D.** The user can find the data by giving the exact values in the Absolute tab under CloudWatch metrics ✔

Explanation :

Answer – D

The below snapshot from cloudwatch shows how to use the Absolute tab under cloudwatch.



For more information on AWS cloudwatch please visit the link:

- https://aws.amazon.com/cloudwatch/ (https://aws.amazon.com/cloudwatch/)

Ask our Experts

QUESTION 44 UNATTEMPTED

Your application currently leverages AWS Auto Scaling to grow and shrink as load Increases/ decreases and has been performing well Your marketing team expects a steady ramp up in traffic to follow an upcoming campaign that will result in a 20x growth in traffic over 4 weeks Your forecast for the approximate number of Amazon EC2 instances necessary to meet the peak demand is 175. What should you do to avoid potential service disruptions during the ramp up in traffic?

- **A.** Ensure that you have pre-allocated 175 Elastic IP addresses so that each server will be able to obtain one as it launches
- **B.** Check the service limits in Trusted Advisor and adjust as necessary so the forecasted count remains within limits. ✔
- **C.** Change your Auto Scaling configuration to set a desired capacity of 175 prior to the launch of the marketing campaign
- **D.** Pre-warm your Elastic Load Balancer to match the requests per second anticipated during peak demand prior to the marketing campaign

Explanation :

Answer – B
Option A. is Incorrect because max limit 5 EIP and a service request needs to be submitted.
Option C. is incorrect because it will cause 175 instances to be launched and running but not gradually scale.
Option D. is incorrect because it does not need pre-warming as the load is increasing steadily.

For more information on ELB specifics, please visit the link:

- https://aws.amazon.com/ec2/faqs/#How_many_instances_can_I_run_in_Amazon_EC2 (https://aws.amazon.com/ec2/faqs/#How_many_instances_can_I_run_in_Amazon_EC2)
- https://aws.amazon.com/articles/1636185810492479 (https://aws.amazon.com/articles/1636185810492479)

Note:
Amazon EC2 Auto Scaling helps you ensure that you have the correct number of Amazon EC2 instances available to handle the load for your application. You create collections of EC2 instances, called Auto Scaling groups.

You can specify the minimum number of instances in each Auto Scaling group, and Auto Scaling

ensures that your group never goes below this size.

You can specify the maximum number of instances in each Auto Scaling group, and Auto Scaling ensures that your group never goes above this size.

If you specify the desired capacity, either when you create the group or at any time thereafter, Auto Scaling ensures that your group has this many instances. If you specify scaling policies, then Auto Scaling can launch or terminate instances as demand on your application increases or decreases

Hence, we don't want our application to start with 175 instances. We just want to increase it only if required.

Please check the below link to know more about it.

- https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-dg.pdf (https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-dg.pdf)

Ask our Experts

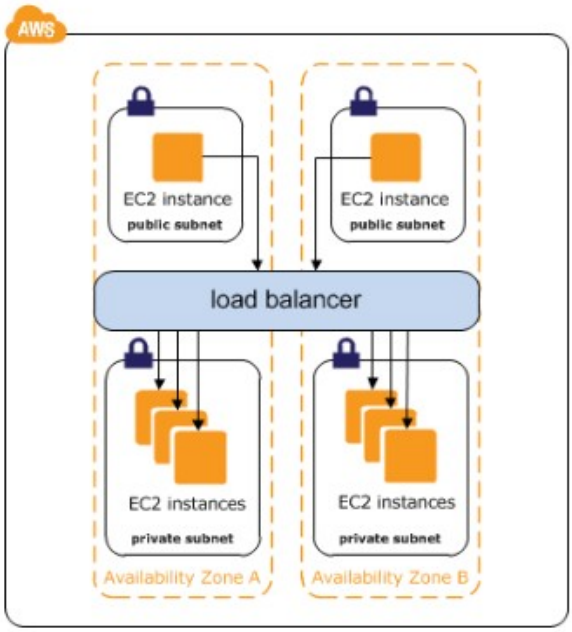
QUESTION 45 UNATTEMPTED

You can configure an internal elastic load balancer to load balance internal traffic.

- A. True ✔
- B. False

Explanation :

Answer – A
Below is a snapshot of how an internal load balancer works. So you have 2 EC2 instances in a subnet which have an internal load balancer connecting to 2 EC2 instances in a private subnet.



For more information on internal ELB, please visit the URL:

- http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-internal-load-balancers.html (http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-internal-load-balancers.html)

Ask our Experts

QUESTION 46 UNATTEMPTED

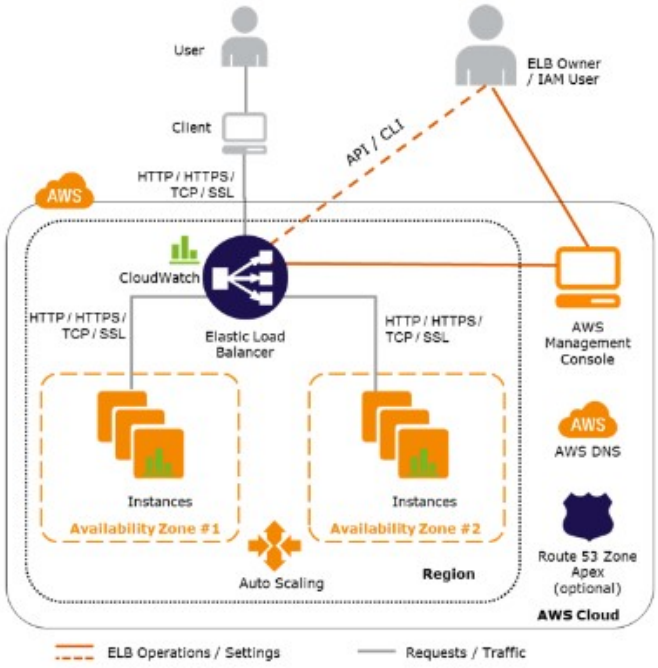
An organization has configured a VPC with an Internet Gateway (IGW) with pairs of public and private subnets each with one subnet per Availability Zone, and an Elastic Load Balancer (ELB) configured to use the public subnets. The application's web tier leverages the ELB, Auto Scaling and a multi AZ RDS database instance. The organization would like to eliminate any potential single point of failure in this design. What step should you take to achieve this objective of the Organization?

- **A.** Nothing, there are no single points of failure in this architecture. ✔
- **B.** Create and attach a second IGW to provide redundant internet connectivity.
- **C.** Create and configure a second Elastic Load Balancer to provide a redundant load balancer.
- **D.** Create a second multi-AZ RDS instance in another Availability Zone and configure replication to provide a redundant database.

Explanation :

Answer – A

The below diagram shows an example of a highly available system in AWS. The question already states all the aspects of a proper highly available system.



Ask our Experts

QUESTION 47 UNATTEMPTED

You have a web application leveraging an Elastic Load Balancer (ELB). The ELB is in front of web servers deployed using an Auto Scaling Group. Your database is running on Relational Database Service (RDS). The web application serves technical articles and responses to them. In general, there are more views of an article than there are responses to the article.

On occasion, an article on the site becomes extremely popular resulting in a significant traffic increase that causes the site to go down. What could you do to alleviate the load on the infrastructure and maintain availability during these events?

Choose 3 answers

- [ ] **A.** Leverage CloudFront for the delivery of the articles. ✔

- [ ] **B.** Add RDS read-replicas for the read traffic going to your relational database ✔
- [ ] **C.** Leverage ElastiCache for caching the most frequently used data. ✔
- [ ] **D.** Use SQS to queue up the requests for the technical posts and deliver them out of the queue.
- [ ] **E.** Use Route53 health checks to fail over to an S3 bucket for an error page.

Explanation :

Answer - A, B and C
Amazon CloudFront can be used to deliver your entire website, including dynamic, static, streaming, and interactive content using a global network of edge locations. Requests for your content are automatically routed to the nearest edge location, so content is delivered with the best possible performance URL:

- https://aws.amazon.com/cloudfront/ (https://aws.amazon.com/cloudfront/)

Amazon RDS Read Replicas provide enhanced performance and durability for database (DB) instances. This replication feature makes it easy to elastically scale out beyond the capacity constraints of a single DB Instance for read-heavy database workloads. You can create one or more replicas of a given source DB Instance and serve high-volume application read traffic from multiple copies of your data, thereby increasing aggregate read throughput. Read replicas can also be promoted when needed to become standalone DB instances.
For more information on read replica's, please refer to the link:

- https://aws.amazon.com/rds/details/read-replicas/ (https://aws.amazon.com/rds/details/read-replicas/)

Amazon ElastiCache is a web service that makes it easy to deploy, operate, and scale an in-memory data store or cache in the cloud (https://aws.amazon.com/what-is-cloud-computing/). The service improves the performance of web applications by allowing you to retrieve information from fast, managed, in-memory data stores, instead of relying entirely on slower disk-based databases URL:

- https://aws.amazon.com/elasticache/ (https://aws.amazon.com/elasticache/)

Ask our Experts

QUESTION 48 UNATTEMPTED

An application that you are managing has EC2 instances & Dynamo DB tables deployed to several AWS Regions In order to monitor the performance of the application globally, you would like to see two graphs 1) Avg CPU Utilization across all EC2 instances and 2) Number of Throttled Requests for all DynamoDB tables. How can you accomplish this?

- **A.** Tag your resources with the application name, and select the tag name as the dimension in the Cloudwatch Management console to view the respective graphs
- **B.** Use the Cloud Watch CLI tools to pull the respective metrics from each regional endpoint Aggregate the data offline & store it for graphing in CloudWatch. ✔
- **C.** Add SNMP traps to each instance and DynamoDB table Leverage a central monitoring server to capture data from each instance and table Put the aggregate data into Cloud Watch for graphing.
- **D.** Add a CloudWatch agent to each instance and attach one to each DynamoDB table. When configuring the agent set the appropriate application name & view the graphs in CloudWatch.

Explanation :

Answer – B
Option A is incorrect because CloudWatch metrics are regional.
Option C is incorrect because we can't add SNMP traps to DynamoDB since it is a managed service.
Option D incorrect because we can't add agents to DynamoDB since it is a managed service.

CloudWatch allows publishing custom metrics with put-metric-data CLI command

- Data can also be aggregated before being published to CloudWatch
- Aggregating data minimizes the number of calls reducing it to a single call per minute with the statistic set of data
- Statistics include Sum, Average, Minimum, Maximum, Data Sample

For more information on Cloudwatch please visit the link:

- https://aws.amazon.com/cloudwatch/ (https://aws.amazon.com/cloudwatch/)

Ask our Experts

QUESTION 49 UNATTEMPTED

Your entire AWS infrastructure lives inside of one Amazon VPC. You have an Infrastructure monitoring application running on an Amazon instance in Availability Zone (AZ) A of the region, and another application instance running on AZ B. The monitoring application needs to make use of ICMP ping to confirm network reachability of the instance hosting the application. Can you configure the security groups for these instances to only allow the ICMP ping to pass from the monitoring instance to the application instance and nothing else? If so, how?

- **A.** No Two instances in two different AZ's can't talk directly to each other via ICMP ping as that protocol is not allowed across subnet (i.e broadcast) boundaries
- **B.** Yes Both the monitoring instance and the application instance have to be a part of the same security group, and that security group needs to allow inbound ICMP
- **C.** Yes, the security group for the monitoring instance needs to allow outbound ICMP and the application instance's security group needs to allow Inbound ICMP ✔
- **D.** Yes, Both the monitoring instance's security group and the application instance's security group need to allow both inbound and outbound ICMP ping packets since ICMP is not a connection-oriented protocol

Explanation :

Answer – C
Security groups are stateful — if you send a request from your instance, the response traffic for that request is allowed to flow in regardless of inbound security group rules. Responses to allowed inbound traffic are allowed to flow out, regardless of outbound rules.
For more information on security groups please visit the link:

- http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html (http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html)

Ask our Experts

QUESTION 50 UNATTEMPTED

You are managing a legacy application Inside VPC with hard coded IP addresses in its configuration. Which two mechanisms will allow the application to failover to new instances without the need for reconfiguration? Choose 2 answers

- **A.** Create an ELB to reroute traffic to a failover instance
- **B.** Create a secondary ENI that can be moved to a failover instance ✔
- **C.** Use Route53 health checks to fail traffic over to a failover instance
- **D.** Assign a secondary private IP address to the primary ENI that can be moved to a failover instance ✔

Explanation :

Answer - B and D

You can create a network interface, attach it to an instance, detach it from an instance, and attach it to another instance. The attributes of a network interface follow it as it's attached or detached from an instance and reattached to another instance. When you move a network interface from one instance to another, network traffic is redirected to the new instance.
For more information on ENI 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

QUESTION 51 UNATTEMPTED

You run a web application where web servers on EC2 instances are in an Auto scaling group. After monitoring the system for the last 6 months , it is noticed that 6 web servers are necessary to handle the minimum load. During the day, it seems that 12 servers are needed. During 5 to 6 days in the year, the number of web servers need might go to 15. What would you recommend to minimize costs while being able to provide high availability.

- **A.** 6 Reserved instances (heavy workload), 6 Reserved instances (medium workload), rest covered by On-Demand instances ✔
- **B.** 6 Reserved instances (heavy workload), 6 On-Demand instances, rest covered by Spot Instances
- **C.** 6 Reserved instances (heavy workload), 6 Spot instances, rest covered by On-Demand instances
- **D.** 6 Reserved instances (heavy workload), 6 Reserved instances (medium workload), rest covered by Spot instances

Explanation :

Answer – A
Although as per AWS we are aware that the Spot instance prices are definitely lower than on demand price the question focus on high availability along with the cost factor. Considering the fact that we are discussing on a website which might (although the scenario does not say; "it requires") need an extra 3 more instances for 5-6 days an year ; indicates that it could be due to heavy traffic on the website due to certain online sale happening on the website; in that case we cannot rely on spot instances as it cannot guarantee its availability.

In-order to manage spot instance interruptions AWS is recommending to use the default maximum

price for these spot instances which is the On-Demand price of the instance.

Please refer to the following link for more info:

- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/spot-interruptions.html#using-spot-instances-managing-interruptions (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/spot-interruptions.html#using-spot-instances-managing-interruptions)

Considering these factors, in this scenario we need Reserved instances and On-Demand instances to ensure both cost and availability factors are taken into consideration.

Ask our Experts

QUESTION 52 UNATTEMPTED

You have set up Individual AWS accounts for each project. You have been asked to make sure your AWS Infrastructure costs do not exceed the budget set per project for each month. Which of the following approaches can help ensure that you do not exceed the budget each month?

- **A.** Consolidate your accounts so you have a single bill for all accounts and projects
- **B.** Set up auto scaling with CloudWatch alarms using SNS to notify you when you are running too many Instances in a given account
- **C.** Set up CloudWatch billing alerts for all AWS resources used by each project, with a notification occurring when the amount for each resource tagged to a particular project matches the budget allocated to the project.
- **D.** Set up CloudWatch billing alerts for all AWS resources used by each account, with email notifications when it hits 50%, 80% and 90% of its budgeted monthly spend ✔

Explanation :

Answer – D
You can monitor your estimated AWS charges using Amazon CloudWatch. When you enable the monitoring of estimated charges for your AWS account, the estimated charges are calculated and sent several times daily to CloudWatch as metric data.
Option A is incorrect because consolidation will not help limit per account.
Option B is incorrect because many instances do not directly map to cost and it would not give exact cost.
Option C is incorrect since each project already has a account, So there is no need for resource tagging.

For creation of billing alarms, please visit the URL:

- http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/free-tier-alarms.html (http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/free-tier-alarms.html)

Ask our Experts

QUESTION 53 UNATTEMPTED

Your team is excited about the use of AWS because now they have access to programmable infrastructure. You have been asked to manage your AWS infrastructure in a manner similar to the way you might manage application code. You want to be able to deploy exact copies of different versions of your infrastructure, stage changes into different environments, revert back to previous versions, and identify what versions are running at any particular time (development, test QA and production). Which approach addresses this requirement?

- **A.** Use cost allocation reports and AWS Opsworks to deploy and manage your infrastructure.
- **B.** Use AWS CloudWatch metrics and alerts along with resource tagging to deploy and manage your infrastructure.
- **C.** Use AWS Beanstalk and a version control system like GIT to deploy and manage your infrastructure.
- **D.** Use AWS CloudFormation and a version control system like GIT to deploy and manage your infrastructure. ✔

Explanation :

Answer – D
AWS CloudFormation is a service that gives developers and businesses an easy way to create a collection of related AWS resources and provision them in an orderly and predictable fashion.
For more information on Cloudformation, please visit the link:

- https://aws.amazon.com/cloudformation/ (https://aws.amazon.com/cloudformation/)

Ask our Experts

QUESTION 54 UNATTEMPTED

A user has launched 10 instances from the same AMI ID using Auto Scaling. The user is trying to see the average CPU utilization across all instances of the last 2 weeks under the CloudWatch console. How can the user achieve this?

- **A.** View the Auto Scaling CPU metrics ✔
- **B.** Aggregate the data over the instance AMI ID
- **C.** The user has to use the CloudWatch analyser to find the average data across instances
- **D.** It is not possible to see the average CPU utilization of the same AMI ID since the instance ID is different

Explanation :

Answer – A
For more information refer to the AWS Documentation @ URL:

- https://docs.aws.amazon.com/autoscaling/latest/userguide/as-instance-monitoring.html (https://docs.aws.amazon.com/autoscaling/latest/userguide/as-instance-monitoring.html)

Option B works but needs detailed monitoring enabled, hence is not a right answer.

Ask our Experts

QUESTION 55 UNATTEMPTED

A user has created an ELB with three instances. How many security groups will ELB create by default?

- **A.** 3
- **B.** 5
- **C.** 2
- **D.** 1 ✔

Explanation :

Answer – D
A security group acts as a firewall that controls the traffic allowed to and from one or more instances. When you launch an EC2 instance, you can associate one or more security groups with the instance. For each security group, you add one or more rules to allow traffic.

Only If you use EC2 classic other than VPC, will u have 2 security groups.
For more information on ELB security groups, please visit the link:

- http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-security-groups.html (http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-security-groups.html)

Ask our Experts

QUESTION 56 UNATTEMPTED

In which of the following circumstances a deny action is taken precedence over an allow action.
Select 2 options.

- [ ] **A.** S3 bucket access is implicitly denied for all users and an explicit allow is set on an S3 bucket via an S3 bucket policy.
- [ ] **B.** A NACL associated with subnet A defines two rules. Rule #100 explicitly denies TCP traffic on port 21 from 0.0.0.0/0 and rule #105 explicitly allows TCP traffic on port 21 from 0.0.0.0/0. ✔
- [ ] **C.** An explicit allow is set in an IAM policy governing S3 access and an explicit deny is set on an S3 bucket via an S3 bucket policy. ✔
- [ ] **D.** A NACL associated with subnet B defines two rules. Rule #105 explicitly denies TCP traffic on port 21 from 0.0.0.0/0 and rule #100 explicitly allows TCP traffic on port 21 from 0.0.0.0/0.

Explanation :

Answer – B and C
An explicit deny overrides any allows.
For more information on policy logic, please visit the URL:

- https://docs.AWS.amazon.com/IAM/latest/UserGuide/reference_policies_evaluation-logic.html#policy-eval-denyallow (https://docs.AWS.amazon.com/IAM/latest/UserGuide/reference_policies_evaluation-logic.html#policy-eval-denyallow)

Rule number. Rules are evaluated starting with the lowest numbered rule. As soon as a rule matches traffic, it's applied regardless of any higher-numbered rule that may contradict it.
For more information on ACL rules, please visit the URL:

- https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html#ACLRules (https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html#ACLRules)

Option C is correct. An explicit deny action takes precedence over the allow action on S3 policies

Ask our Experts

QUESTION 57 UNATTEMPTED

An application is generating a log file every 5 minutes. The log file is not critical but may be required only for verification in case of some major issue. The file should be accessible over the internet whenever required. Which of the below mentioned storage options satisfy our requirements and provide high durability, high throughput, and low latency with low cost?

- A. AWS S3 - Standard
- B. AWS S3 - IA ✔
- C. AWS RRS
- D. AWS Glacier

Explanation :

Answer – B
Original question was "Which of the below mentioned options is a best possible storage solution for it?" - This seemed little confusing and non-sensical so we have updated the question. This gives clear answer to be AWS S3 - IA.
Option A is incorrect. It fits all requirements except it is expensive compared to S3-IA. Amazon S3 Standard offers high durability, availability, and performance object storage for frequently accessed data.
Option B is correct. Amazon S3 Standard-Infrequent Access (S3 Standard-IA) is an Amazon S3 storage class for data that is accessed less frequently, but requires rapid access when needed. S3 Standard-IA offers the high durability, high throughput, and low latency of S3 Standard, with a low per GB storage price and per GB retrieval fee.
Option C is incorrect. RRS is an Amazon S3 storage option that enables customers to store noncritical, reproducible data at lower levels of redundancy than Amazon S3's standard storage. Since the data cannot be easily reproducible in this case this option is invalid.
Option D is incorrect. Glacier fits all requirements except that it doesn't have low latency when files are being retrieved. Amazon Glacier is a secure, durable, and extremely low-cost storage service for data archiving.

Ask our Experts

QUESTION 58 UNATTEMPTED

A company has decided to deploy a "Pilot Light" AWS environment to keep minimal resources in AWS with the intention of rapidly expanding the environment in the event of a disaster in your on-premises Datacenter. Which of the following services will you likely not make use of? Choose the correct answer from the options below.

- **A.** A Gateway-Cached implementation of Storage Gateway for storing snapshot copies of on-premises data ✔
- **B.** EC2 for storing updated AMI copies of on-premises VMs
- **C.** A Gateway-Stored implementation of Storage Gateway for storing snapshot copies of on-premises data
- **D.** RDS for replicating mission-critical databases to AWS

Explanation :

Answer – A
Please note that the question has negation. "Which of the following services will you likely **not** make use of?"
So, Option D. RDS for replicating mission-critical databases to AWS - is a required service and will be incorrect answer.
In a pilot light deployment , you can just keep the main and key artefacts required for a failover. Hence keeping track of AMI's and mission critical data is required. You also need to store and ensure all backup is in place and the best implementation for this is Gateway-Stored implementation.
Option B- incorrect
Amazon Machine Images (AMIs) are preconfigured with operating systems, and some preconfigured AMIs might also include application stacks. You can also configure your own AMIs. In the context of DR, we strongly recommend that you configure and identify your own AMIs so that they can launch as part of your recovery procedure. Such AMIs should be preconfigured with your operating system of choice plus appropriate pieces of the application stack.

Option C is incorrect : Gateway-stored volumes— In the event that you need low-latency access to your entire data set, you can configure your gateway to store your primary data locally, and asynchronously back up point-in-time snapshots of this data to Amazon S3. Gateway-stored volumes provide durable and inexpensive off-site backups that you can recover locally or from Amazon EC2 if, for example, you need replacement capacity for disaster recovery.

Option D is incorrect : Amazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and scale a relational database in the cloud. You can use Amazon RDS either in the preparation phase for DR to hold your critical data in a database that is already running, or in the recovery phase to run your production database.
More information is available at:

- https://media.amazonwebservices.com/AWS_Disaster_Recovery.pdf (https://media.amazonwebservices.com/AWS_Disaster_Recovery.pdf)

For more information on disaster recovery, please visit the URL:

- https://aws.amazon.com/blogs/aws/new-whitepaper-use-aws-for-disaster-recovery/ (https://aws.amazon.com/blogs/aws/new-whitepaper-use-aws-for-disaster-recovery/)

Ask our Experts

QUESTION 59 UNATTEMPTED

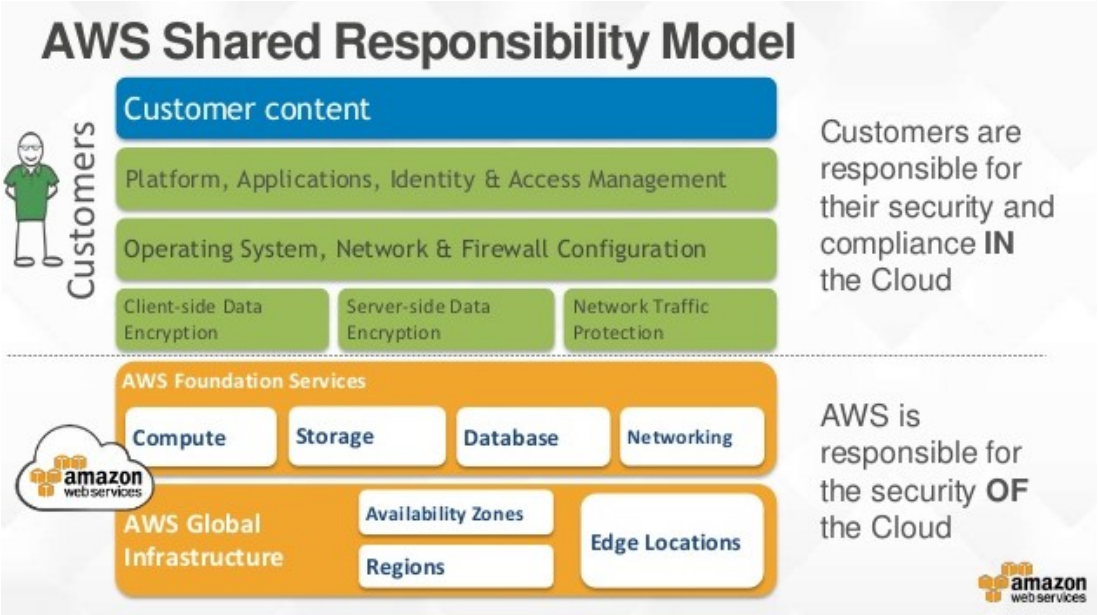
In the shared responsibility model at AWS, what two options are you responsible for in the case of an audit? Choose the 2 correct answers from the options below.

- [ ] **A.** The global infrastructure that hosts the virtualization hypervisors
- [ ] **B.** Physical security to AWS data centers
- [ ] **C.** The operating systems' administrators group ✔
- [ ] **D.** An application that you have running within AWS EC2 ✔

Explanation :

Answer – C and D

Please find the shared responsibility model as shared by AWS



Ask our Experts

QUESTION 60 UNATTEMPTED

We have terminated an instance which had a root EBS volume attached to it. What do we do now if we need to access the important data that was on this volume if we created this instance with the default storage options? Choose the correct answer from the options below.

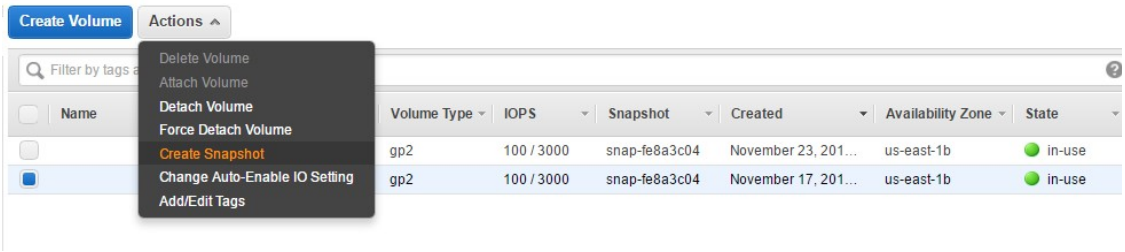
- A. We can restore the data from a snapshot which is automatically created on instance termination by default
- B. If we did not first take a snapshot of the EBS volume we will not be able to access the data after an instance termination because the volume was deleted ✔
- C. AWS has high availability so our data is still available
- D. Create multiple EBS volumes and replicate the data between them

Explanation :

Answer – B

You need to ensure you create EBS snapshots, because these are not automatically created. Hence if the snapshot has not been taken, you will not be able to access the data.

You can easily create a snapshot from a volume while the instance is running and the volume is in use. You can do this from the EC2 dashboard.



For more information on EBS snapshots, please visit the linkl:

- http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html (http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html)

Ask our Experts

Finish Review (https://www.whizlabs.com/learn/course/aws-csyopaa-practice-tests/quiz/12749)

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

Mobile App

- Android Coming Soon

Company

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

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)