AWS CSAA Practice Tests

Started on	Friday, 9 February 2018, 6:37 AM
State	Finished
Completed on	Friday, 9 February 2018, 6:37 AM
Time taken	9 secs
Grade	**0.00** out of 60.00 (**0**%)
Result	FAIL

QUESTION 1 **NOT ANSWERED** Submit Feedback

A VPC has been setup with public subnet and an internet gateway. You setup and EC2 instance with a public IP. But you are still not able to connect to it via the Internet. You can see that the right Security groups are in place. What should you do to ensure you can connect to the EC2 instance from the internet

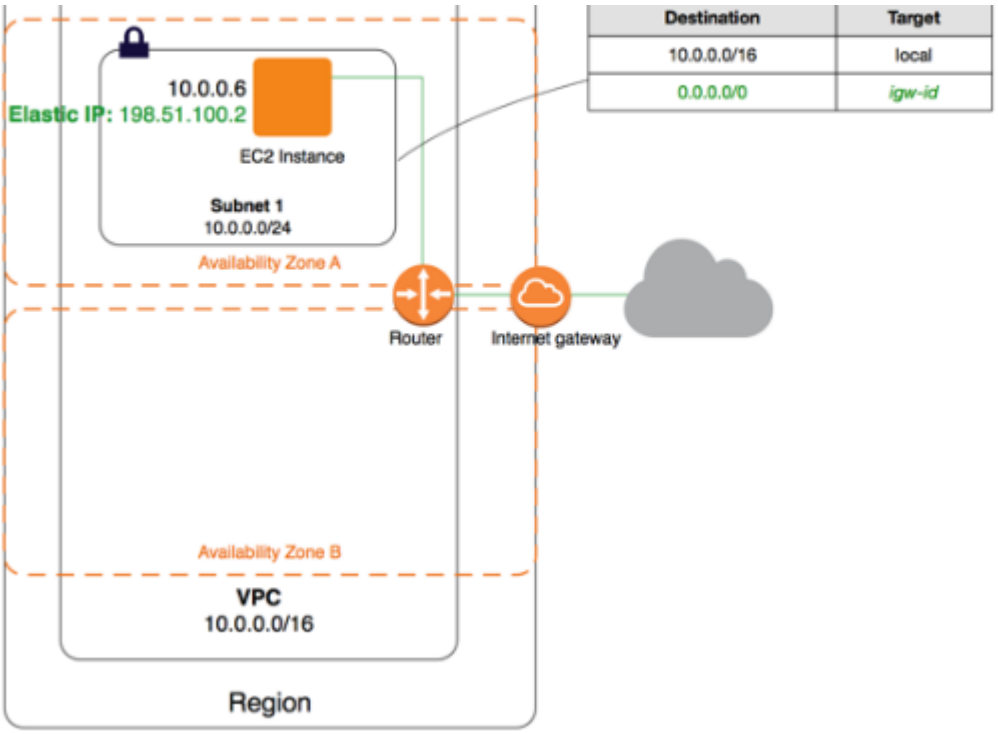
Please select :

- A. Set an Elastic IP Address to the EC2 instance
- B. Set a Secondary Private IP Address to the EC2 instance
- C. Ensure the right route entry is there in the Route table
- D. There must be some issue in the EC2 instance. Check the system logs.

Your answer is incorrect.

Answer – C

You have to ensure that the Route table has an entry to the Internet gateway because this is required for instances to communicate over the internet. The diagram shows the configuration of the public subnet in a VPC.



Option A is wrong because you already have a public IP Assigned to the instance, so this should be enough to connect to the Internet.
Option B is wrong because private IP's cannot be access from the internet
Option D is wrong because the Route table is what is causing the issue and not the system

For more information on aws public subnet, please visit the link

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

The correct answer is: Ensure the right route entry is there in the Route table

Feedback about this question and answer

QUESTION 2	NOT ANSWERED	Submit Feedback

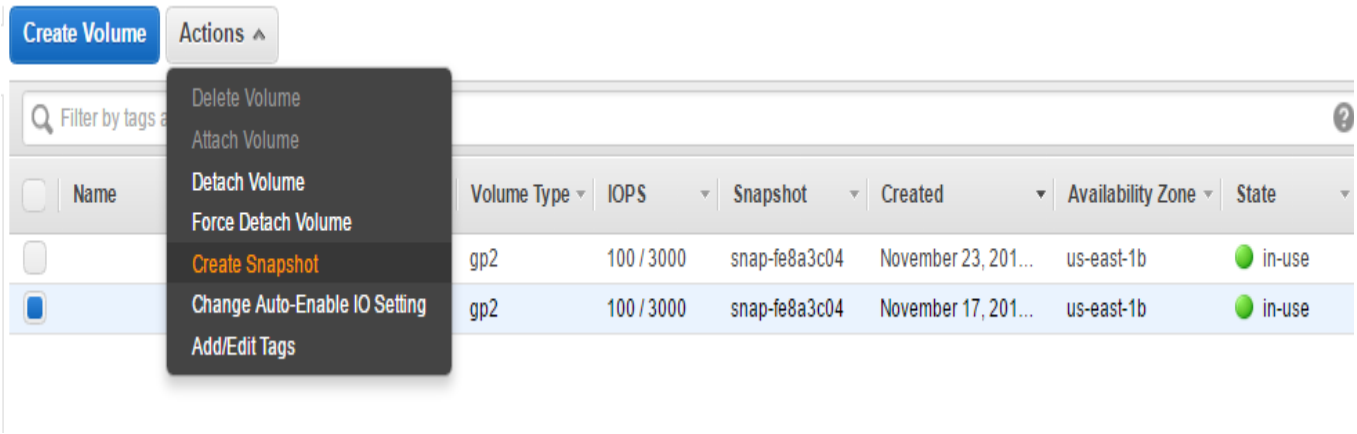
Which of the following approaches provides the lowest cost for Amazon Elastic Block Store snapshots while giving you the ability to fully restore data?

Please select :

- A. Maintain two snapshots: the original snapshot and the latest incremental snapshot.
- B. Maintain a volume snapshot; subsequent snapshots will overwrite one another
- C. Maintain a single snapshot the latest snapshot is both Incremental and complete.
- D. Maintain the most current snapshot, archive the original and incremental to Amazon Glacier.

EBS snapshots are incremental and complete, so you don't need to maintain multiple snapshots if you are looking on reducing costs.

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

The correct answer is: Maintain a single snapshot the latest snapshot is both Incremental and complete.

Feedback about this question and answer

QUESTION 3 **NOT ANSWERED** **Submit Feedback**

An existing application stores sensitive information on a non-boot Amazon EBS data volume attached to an Amazon Elastic Compute Cloud instance. Which of the following approaches would protect the sensitive data on an Amazon EBS volume?

Please select :

A. Upload your customer keys to AWS CloudHSM. Associate the Amazon EBS volume with AWS CloudHSM. Remount the Amazon EBS volume.

B. Create and mount a new, encrypted Amazon EBS volume. Move the data to the new volume. Delete
the old Amazon EBS volume.

C. Unmount the EBS volume. Toggle the encryption attribute to True. Re-mount the Amazon EBS volume.

D. Snapshot the current Amazon EBS volume. Restore the snapshot to a new, encrypted Amazon EBS volume. Mount the Amazon EBS volume

Here the only option available is to create a new mount volume

Option A is wrong because you cannot encrypt a volume once it is created. You would need to use some local encrypting algorithm if you want to encrypt the data on the volume.
Option C is wrong because even if you unmounts the volume, you cannot encrypt the volume. Encryption has to be done during volume creation.
Option D is wrong because even if the volume is not encrypted, the snapshot will also not be encrypted.

You can not create an encrypted snapshot of an unencrypted volume or change existing volume from unencrypted to encrypted. You have to create new encrypted volume and transfer data to the new volume. The other option is to

encrypt a volume's data by means of snapshot copying

1. Create a snapshot of your unencrypted EBS volume. This snapshot is also unencrypted.
2. Copy the snapshot while applying encryption parameters. The resulting target snapshot is encrypted.
3. Restore the encrypted snapshot to a new volume, which is also encrypted.

but that option is not listed.

Find more details here :
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html

1. Choose AMI | 2. Choose Instance Type | 3. Configure Instance | 4. Add Storage | 5. Add Tags | 6. Configure Security Group | 7. Review

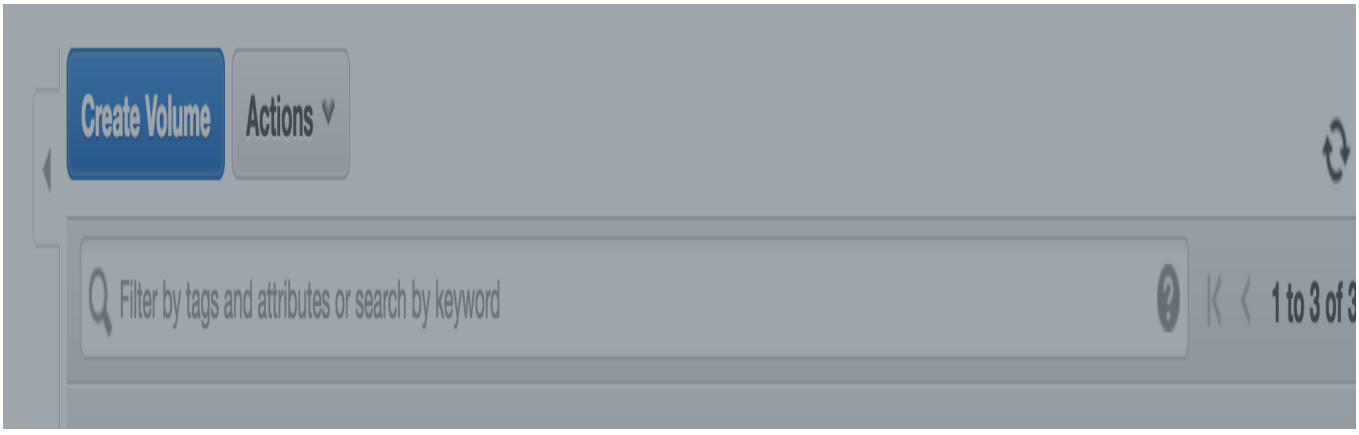
Step 4: Add Storage

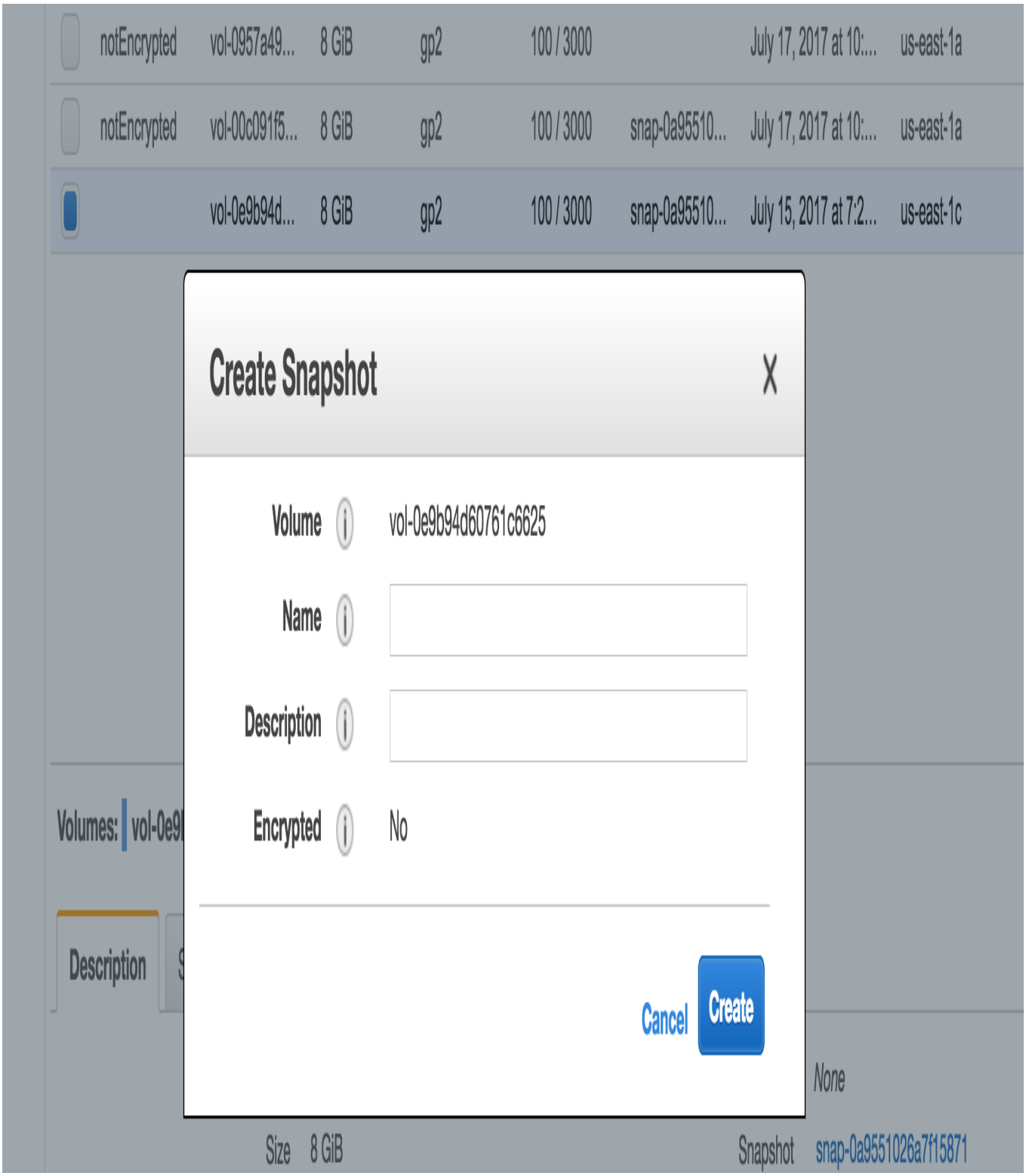
Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store
edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store
storage options in Amazon EC2.

Volumes that are created from encrypted snapshots are automatically encrypted, and volumes that are created from unencrypted snapshots are automatically unencrypted. If no snapshot is selected, you can choose to encrypt the volume.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Termination	Encrypted
Root	/dev/xvda	snap-0a9551026a7f15871	8	General Purpose SSD (GP2)	100 / 3000	N/A	✓	Not Encrypted

Add New Volume





The correct answer is: Create and mount a new, encrypted Amazon EBS volume. Move the data to the new volume. Delete
the old Amazon EBS volume.

Feedback about this question and answer

Which of the following are use cases for Amazon DynamoDB?
Choose 3 answers

Please select :

- [ ] A. Storing BLOB data.
- [ ] B. Managing web sessions.
- [ ] C. Storing JSON documents.
- [ ] D. Storing metadata for Amazon S3 objects.
- [ ] E. Running relational joins and complex updates.
- [ ] F. Storing large amounts of infrequently accessed data

Your answer is incorrect.

Answer - B, C and D

Amazon DynamoDB stores structured data, indexed by primary key, and allows low latency read and write access to items ranging from 1 byte up to 400KB. Amazon S3 stores unstructured blobs and suited for storing large objects up to 5 TB.

DynamoDB IS a good choice to store the metadata for a BLOB, such as name, date created, owner, etc... The Binary Large OBject itself would be stored in S3.

Q: When should I use Amazon DynamoDB vs Amazon S3?

Amazon DynamoDB stores structured data, indexed by primary key, and allows low latency read and write access to items ranging from 1 byte up to 400KB. Amazon S3 stores unstructured blobs and suited for storing large objects up to 5 TB. In order to optimize your costs across AWS services, large objects or infrequently accessed data sets should be stored in Amazon S3, while smaller data elements or file pointers (possibly to Amazon S3 objects) are best saved in Amazon DynamoDB.

For more information on Amazon Dynamo DB, please visit

- https://aws.amazon.com/dynamodb/faqs/

The correct answers are: Managing web sessions., Storing JSON documents., Storing metadata for Amazon S3 objects.

Feedback about this question and answer

In Amazon CloudWatch what is the retention period for a one minute datapoint. Choose the right answer from the options given below

Please select :

- a. 10 days
- b. 15 days
- c. 1 month
- d. 1 year

Your answer is incorrect.

Answer - B

Amazon CloudWatch is a monitoring service for AWS cloud resources and the applications you run on AWS. You can use Amazon CloudWatch to collect and track metrics, collect and monitor log files, set alarms, and automatically react to changes in your AWS resources. Amazon CloudWatch can monitor AWS resources such as Amazon EC2 instances, Amazon DynamoDB tables, and Amazon RDS DB instances, as well as custom metrics generated by your applications and services, and any log files your applications generate. You can use Amazon CloudWatch to gain system-wide visibility into resource utilization, application performance, and operational health.

Below is the retention period for the various data points

CloudWatch Metrics now supports the following three retention schedules:

- 1 minute datapoints are available for 15 days
- 5 minute datapoints are available for 63 days
- 1 hour datapoints are available for 455 days

For more information on Amazon Cloudwatch, please visit

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

The correct answer is: 15 days

Feedback about this question and answer

QUESTION 6	NOT ANSWERED	Submit Feedback

What is the minimum time Interval for the data that Amazon CloudWatch receives and aggregates for EC2 in basic monitoring?

Please select :

- C. One minute
- D. Three minutes
- E. Five minutes

Your answer is incorrect.

Answer – E

Enable or Disable Detailed Monitoring for Your Instances

By default, your instance is enabled for basic monitoring. You can optionally enable detailed monitoring. After you enable detailed monitoring, the Amazon EC2 console displays monitoring graphs with a 1-minute period for the instance. The following table describes basic and detailed monitoring for instances.

Type	Description
Basic	Data is available automatically in 5-minute periods at no charge.
Detailed	Data is available in 1-minute periods for an additional cost. To get this level of data, you must specifically enable it for the instance. For the instances where you've enabled detailed monitoring, you can also get aggregated data across groups of similar instances. For information about pricing, see the Amazon CloudWatch product page.

In Amazon CloudWatch for basic monitoring of EC2 instances, the following important metrics are collected at five minute intervals and stored for two weeks.

- CPU load
- disk I/O
- network I/O

For more information on Amazon Cloudwatch EC2 basic monitoring, please visit

- https://aws.amazon.com/blogs/aws/amazon-cloudwatch-basic-monitoring-for-ec2-at-no-charge/

The correct answer is: Five minutes

Feedback about this question and answer

QUESTION 7	NOT ANSWERED	Submit Feedback

production estate to AWS and you are in the process of setting up access to the AWS console using Identity Access Management (IAM). You have created 5 users for your system administrators. What further steps do you need to take to enable your system administrators to get access to the AWS console?

Please select :

- A. Generate an Access Key ID & Secret Access Key, and give these to your system administrators.
- B. Enable multi-factor authentication on their accounts and define a password policy.
- C. Generate a password for each user created and give these passwords to your system administrators.
- D. Give the system administrators the secret access key and access key id, and tell them to use these credentials to log in to the AWS console.

Your answer is incorrect.

Answer - C

In order to allow the users to log into the console, you need to provide a password for the users.

For more information on how to allow users to sign into an account, please refer to the below URL:

- http://docs.aws.amazon.com/IAM/latest/UserGuide/getting-started_how-users-sign-in.html

The correct answer is: Generate a password for each user created and give these passwords to your system administrators.

Feedback about this question and answer

QUESTION 8 **NOT ANSWERED** **Submit Feedback**

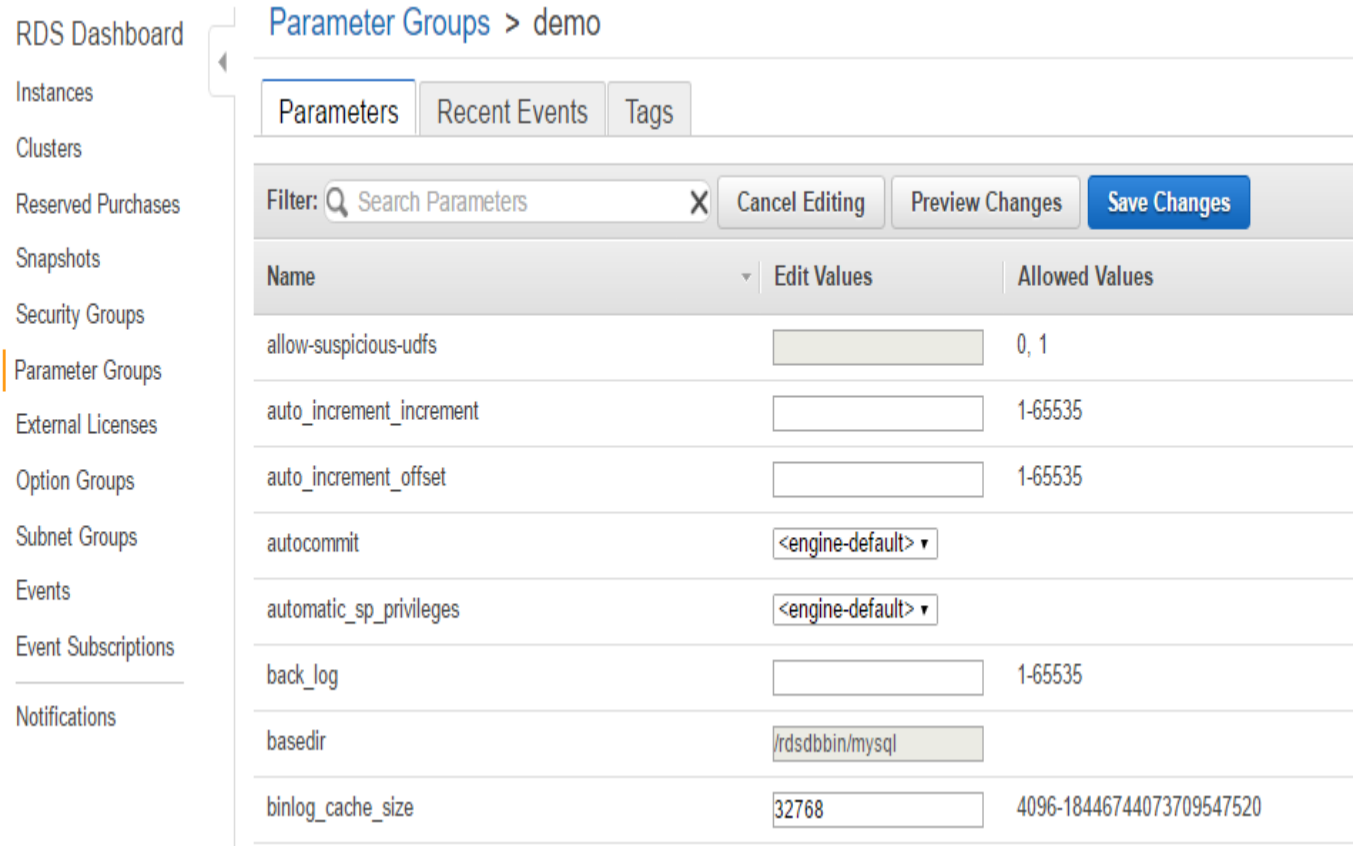
A customer wants to apply a group of database specific settings to their Relational Database Instances in their AWS acccount. Which of the following options can be used to apply the settings in one go for all of the Relational database instances

Please select :

- A. Security Groups
- B. NACL Groups
- C. Parameter Groups
- D. IAM Roles.

DB Parameter Groups are used to assign specific settings which can be applied to a set of RDS instances in aws.

In your RDS, when you go to Parameter Groups, you can create a new parameter group. In the parameter group itself, you have a lot of database related settings that can be assigned to the database.



Option A, B and D are wrong because this is specific to what resources have access to the database.

For more information on EB parameter groups, please visit

http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_WorkingWithParamGroups.html

The correct answer is: Parameter Groups

Feedback about this question and answer

QUESTION 9	NOT ANSWERED	Submit Feedback

A company is storing data on Amazon Simple Storage Service (S3). The company's security policy mandates
that data is encrypted at rest. Which of the following methods can achieve this? (Choose three.)

- [ ] B. Use Amazon S3 server-side encryption with customer-provided keys.
- [ ] C. Use Amazon S3 server-side encryption with EC2 key pair.
- [ ] D. Use Amazon S3 bucket policies to restrict access to the data at rest.
- [ ] E. Encrypt the data on the client-side before ingesting to Amazon S3 using their own master key.
- [ ] F. Use SSL to encrypt the data while in transit to Amazon S3.

Your answer is incorrect.

Answer – A,B and E

One can encrypt data in an S3 bucket using both server side encryption and client side encryption. The following techniques are available

- Use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)
- Use Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)
- Use Server-Side Encryption with Customer-Provided Keys (SSE-C)
- Use Client-Side Encryption with AWS KMS–Managed Customer Master Key (CMK)
- Use Client-Side Encryption Using a Client-Side Master Key

For more information on using encryption, please refer to the below URL:

- http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html

The correct answers are: Use Amazon S3 server-side encryption with AWS Key Management Service managed keys., Use Amazon S3 server-side encryption with customer-provided keys., Encrypt the data on the client-side before ingesting to Amazon S3 using their own master key.

Feedback about this question and answer

QUESTION 10 **NOT ANSWERED** **Submit Feedback**

Before I delete an EBS volume, what can I do if I want to recreate the volume later?

Please select :

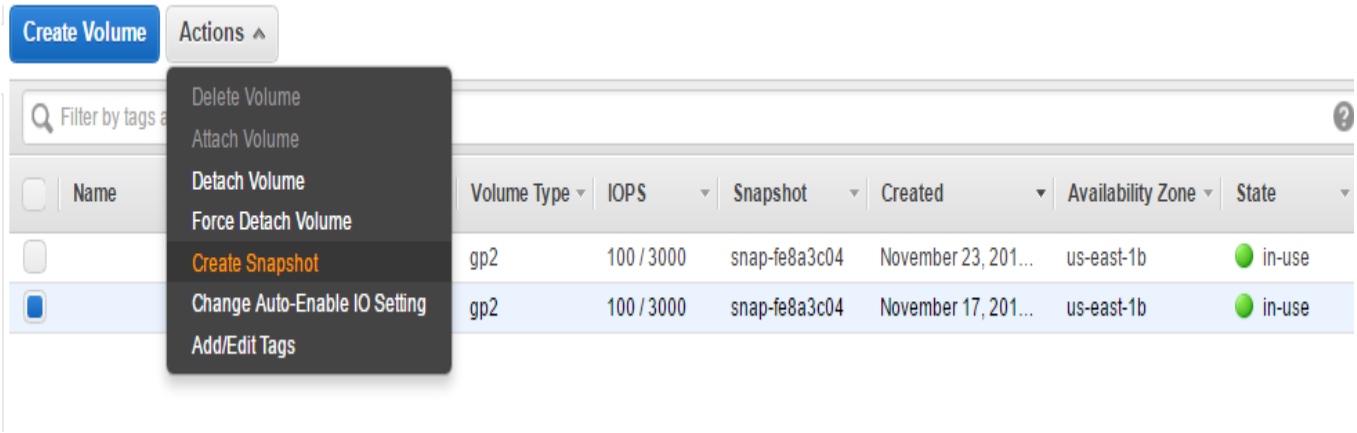
- ( ) A. Create a copy of the EBS volume (not a snapshot)
- ( ) B. Store a snapshot of the volume
- ( ) C. Download the content to an EC2 instance
- ( ) D. Back up the data in to a physical disk

Your answer is incorrect.

the volume, which you can use to re-create the volume later.
See more details here :
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-deleting-volume.html

Snapshots occur asynchronously; the point-in-time snapshot is created immediately, but the status of the snapshot is pending until the snapshot is complete (when all of the modified blocks have been transferred to Amazon S3), which can take several hours for large initial snapshots or subsequent snapshots where many blocks have changed. While it is completing, an in-progress snapshot is not affected by ongoing reads and writes to the 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 link -
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html

The correct answer is: Store a snapshot of the volume

Feedback about this question and answer

QUESTION 11 **NOT ANSWERED** **Submit Feedback**

All Amazon EC2 instances are assigned two IP addresses at launch, out of which one can only be reached from within the Amazon EC2 network?

Please select :

- A. Multiple IP address
- B. Public IP address
- C. Private IP address
- D. Elastic IP Address

A private IP address is an IP address that's not reachable over the Internet. You can use private IP addresses for communication between instances in the same network (EC2-Classic or a VPC).

When an instance is launched a private IP address is allocated for the instance using DHCP. Each instance is also given an internal DNS hostname that resolves to the private IP address of the instance; for example, ip-10-251-50-12.ec2.internal. You can use the internal DNS hostname for communication between instances in the same network, but we can't resolve the DNS hostname outside the network that the instance is in.

For more information on IP Addressing, please visit the link –

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-instance-addressing.html

The correct answer is: Private IP address

Feedback about this question and answer

QUESTION 12 **NOT ANSWERED** **Submit Feedback**

The below snapshot shows 2 instances in the Ec2 dashboard. What is the column name for the instances as highlighted in red below?

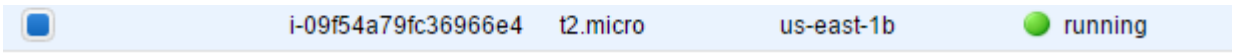
Please select :

- A. Instance ID
- B. VPC ID
- C. Subnet ID
- D. Public IP

Your answer is incorrect.

Answer - A

When resources are created, an assignment of each resource with a unique resource ID is done. You can use resource IDs to find your resources in the Amazon EC2 console. A resource ID takes the form of a resource identifier (such as snap for a snapshot) followed by a hyphen and a unique combination of letters and numbers



For more information on Instance ID, please visit the link

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/resource-ids.html

The correct answer is: Instance ID

Feedback about this question and answer

QUESTION 13 | **NOT ANSWERED** | **Submit Feedback**

Which technique can be used to integrate AWS IAM (Identity and Access Management) with an on-premise LDAP (Lightweight Directory Access Protocol) directory service?

Please select :

- A. Use an IAM policy that references the LDAP account identifiers and the AWS credentials.
- B. Use SAML (Security Assertion Markup Language) to enable single sign-on between AWS and LDAP.
- C. Use AWS Security Token Service from an identity broker to issue short-lived AWS credentials.
- D. Use IAM roles to automatically rotate the IAM credentials when LDAP credentials are updated.
- E. Use the LDAP credentials to restrict a group of users from launching specific EC2 instance types.

Your answer is incorrect.

Answer – C

For more information on AWS and SAML, please refer to the below URL:

- https://aws.amazon.com/blogs/aws/aws-identity-and-access-management-now-with-identity-federation/

The correct answer is: Use AWS Security Token Service from an identity broker to issue short-lived AWS credentials.

Feedback about this question and answer

QUESTION 14 | **NOT ANSWERED** | **Submit Feedback**

determined that write throughput to the database needs to be increased. Which of the following approaches can help achieve this? Choose 2 answers

Please select :

- A. Use an array of EBS volumes.
- B. Enable Multi-AZ mode.
- C. Place the instance in an Auto Scaling Groups
- D. Add an EBS volume and place into RAID 5.
- E. Increase the size of the EC2 Instance.
- F. Put the database behind an Elastic Load Balancer.

Your answer is incorrect.

Answer – A and E

The AWS Documentation mentions the following

With Amazon EBS, you can use any of the standard RAID configurations that you can use with a traditional bare metal server, as long as that particular RAID configuration is supported by the operating system for your instance. This is because all RAID is accomplished at the software level. For greater I/O performance than you can achieve with a single volume, RAID 0 can stripe multiple volumes together; for on-instance redundancy, RAID 1 can mirror two volumes together.

For more information on RAID configuration, please refer to the below URL:

- http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/raid-config.html

And then to offset the use of higher compute capacity, it is better to use a better instance type

For more information on Instance types, please refer to the below URL:

- https://aws.amazon.com/ec2/instance-types/

The correct answers are: Use an array of EBS volumes., Increase the size of the EC2 Instance.

Feedback about this question and answer

QUESTION 15	NOT ANSWERED	Submit Feedback

Where does AWS beanstalk store the application files and server log files? Choose one answer from the options given below

Please select :

- A. On the local server within Elastic beanstalk

- D. AWS DynamoDB

Your answer is incorrect.

Answer - B

AWS Elastic Beanstalk stores your application files and, optionally, server log files in Amazon S3. If you are using the AWS Management Console, the AWS Toolkit for Visual Studio, or AWS Toolkit for Eclipse, an Amazon S3 bucket will be created in your account for you and the files you upload will be automatically copied from your local client to Amazon S3. Optionally, you may configure Elastic Beanstalk to copy your server log files every hour to Amazon S3. You do this by editing the environment configuration settings

For more information on Elastic Beanstalk visit the below link

https://aws.amazon.com/elasticbeanstalk/faqs/

The correct answer is: AWS S3

Feedback about this question and answer

QUESTION 16 | **NOT ANSWERED** | **Submit Feedback**

A customer is looking for a hybrid cloud solution and learns about AWS Storage Gateway. What is the main use case of AWS Storage Gateway?

Please select :

- A. It allows to integrate on-premises IT environments with Cloud Storage.
- B. A direct encrypted connection to Amazon S3.
- C. It's a backup solution that provides an on-premises Cloud storage.
- D. It provides an encrypted SSL endpoint for backups in the Cloud.

Your answer is incorrect.

Answer – A

Option B is wrong because it is not an encrypted solution to S3
Option C is wrong because you can use S3 as a backup solution
Option D is wrong because the SSL endpoint can be achieved via S3

The AWS Storage Gateway's software appliance is available for download as a virtual machine (VM) image that you install on a host in your datacenter. Once you've installed your gateway and associated it with your AWS Account through our activation process, you can use the AWS Management Console to create either gateway-cached volumes, gateway-stored volumes, or a gateway-virtual tape library (VTL), which can be mounted as iSCSI devices by your on-premises applications.

2) Gateway-stored volumes store your primary data locally, while asynchronously backing up that data to AWS

For more information on AWS Storage gateways visit the below link

https://aws.amazon.com/storagegateway/details/

The correct answer is: It allows to integrate on-premises IT environments with Cloud Storage.

Feedback about this question and answer

QUESTION 17	NOT ANSWERED	Submit Feedback

What is the base URI for all requests for instance metadata? Choose one answer from the options given below

Please select :

- A. http://254.169.169.254/latest/
- B. http://169.169.254.254/latest/
- C. http://127.0.0.1/latest/
- D. http://169.254.169.254/latest/

Your answer is incorrect.

Answer – D

Instance metadata is data about your instance that you can use to configure or manage the running instance

Because your instance metadata is available from your running instance, you do not need to use the Amazon EC2 console or the AWS CLI. This can be helpful when you're writing scripts to run from your instance. For example, you can access the local IP address of your instance from instance metadata to manage a connection to an external application.

http://169.254.169.254/latest/meta-data/

For more information on Instance Metadata visit the below link

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

The correct answer is: http://169.254.169.254/latest/

Feedback about this question and answer

QUESTION 18	NOT ANSWERED	Submit Feedback

Please select :

- A. Nothing, you are actually saving resources on aws
- B. You are disabling the point-in-time recovery.
- C. Nothing really, you can still take manual backups.
- D. You cannot disable automated backups in RDS.

Your answer is incorrect.

Answer – B

Amazon RDS creates a storage volume snapshot of your DB instance, backing up the entire DB instance and not just individual databases. You can set the backup retention period when you create a DB instance. If you don't set the backup retention period, Amazon RDS uses a default period retention period of one day. You can modify the backup retention period; valid values are 0 (for no backup retention) to a maximum of 35 days

You will also specifically see AWS mentioning the risk of not allowing automated backups.

> **Important**
>
> We highly discourage disabling automated backups because it disables point-in-time recovery. If you disable and then re-enable automated backups, you are only able to restore starting from the time you re-enabled automated backups.

For more information on Automated backups, please visit

http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_WorkingWithAutomatedBackups.html

The correct answer is: You are disabling the point-in-time recovery.

Feedback about this question and answer

QUESTION 19 **NOT ANSWERED** **Submit Feedback**

Your customer is willing to consolidate their log streams (access logs application logs security logs etc.) in one single system. Once consolidated, the customer wants to analyze these logs in real time based on heuristics. From time to time, the customer needs to validate heuristics, which requires going back to data samples extracted from the last 12 hours? What is the best approach to meet your customer's requirements?

Please select :

- A. Send all the log events to Amazon SQS. Setup an Auto Scaling group of EC2 servers to consume the logs and apply the heuristics.

C. Configure Amazon Cloud Trail to receive custom logs, use EMR to apply heuristics the logs

D. Setup an Auto Scaling group of EC2 syslogd servers, store the logs on S3 use EMR to apply heuristics on the logs

Your answer is incorrect.

Answer – B

Amazon Kinesis is the best option for analyzing logs in real time

The AWS documentation mentions the following for AWS Kinesis

Amazon Kinesis makes it easy to collect, process, and analyze real-time, streaming data so you can get timely insights and react quickly to new information. Amazon Kinesis offers key capabilities to cost effectively process streaming data at any scale, along with the flexibility to choose the tools that best suit the requirements of your application. With Amazon Kinesis, you can ingest real-time data such as application logs, website clickstreams, IoT telemetry data, and more into your databases, data lakes and data warehouses, or build your own real-time applications using this data.

For more information on AWS Kinesis, please refer to the below URL:

- https://aws.amazon.com/kinesis/

The correct answer is: Send all the log events to Amazon Kinesis develop a client process to apply heuristics on the logs

Feedback about this question and answer

QUESTION 20 | **NOT ANSWERED** | **Submit Feedback**

In what events would cause Amazon RDS to initiate a failover to the standby replica?
Select 3 options.

Please select :

- A. Loss of availability in primary Availability Zone
- B. Loss of network connectivity to primary
- C. Storage failure on secondary
- D. Storage failure on primary

Your answer is incorrect.

Answer - A, B and D

- Loss of availability in primary Availability Zone
- Loss of network connectivity to primary
- Compute unit failure on primary
- Storage failure on primary

Note: When operations such as DB Instance scaling or system upgrades like OS patching are initiated for Multi-AZ deployments, for enhanced availability, they are applied first on the standby prior to an automatic failover. As a result, your availability impact is limited only to the time required for automatic failover to complete. Note that Amazon RDS Multi-AZ deployments do not failover automatically in response to database operations such as long running queries, deadlocks or database corruption errors.

For more information on read replicas, please visit

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

The correct answers are: Loss of availability in primary Availability Zone, Loss of network connectivity to primary, Storage failure on primary

Feedback about this question and answer

QUESTION 21 **NOT ANSWERED** **Submit Feedback**

What does the following command do with respect to the Amazon EC2 security groups?
revoke-security-group-ingress

Please select :

- A. Removes one or more security groups from a rule.
- B. Removes one or more security groups from an Amazon EC2 instance.
- C. Removes one or more rules from a security group.

Your answer is incorrect.

Answer – C

Removes one or more ingress rules from a security group. The values that you specify in the revoke request (for example, ports) must match the existing rule's values for the rule to be removed.

Each rule consists of the protocol and the CIDR range or source security group. For the TCP and UDP protocols, you must also specify the destination port or range of ports. For the ICMP protocol, you must also specify the ICMP type and code.

For more information on revoke-security-group-ingress CLI command, please visit

Feedback about this question and answer

QUESTION 22	NOT ANSWERED	Submit Feedback

What is the durability of S3 RRS?

Please select :

- A. 99.99%
- B. 99.95%
- C. 99.995%
- D. 99.999999999%

Your answer is incorrect.

Answer – A

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.

For more information on RRS, visit the link

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

The correct answer is: 99.99%

Feedback about this question and answer

QUESTION 23	NOT ANSWERED	Submit Feedback

Which aws service is used as a global content delivery network (CDN) service in aws?

Please select :

- A. Amazon SES

- D. Amazon S3

Your answer is incorrect.

Answer – C

Amazon CloudFront is a web service that gives businesses and web application developers an easy and cost effective way to distribute content with low latency and high data transfer speeds. Like other AWS services, Amazon CloudFront is a self-service, pay-per-use offering, requiring no long term commitments or minimum fees. With CloudFront, your files are delivered to end-users using a global network of edge locations.

For more information on CloudFront, please visit the link

https://aws.amazon.com/cloudfront/

The correct answer is: Amazon CloudFront

Feedback about this question and answer

QUESTION 24 | **NOT ANSWERED** | **Submit Feedback**

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

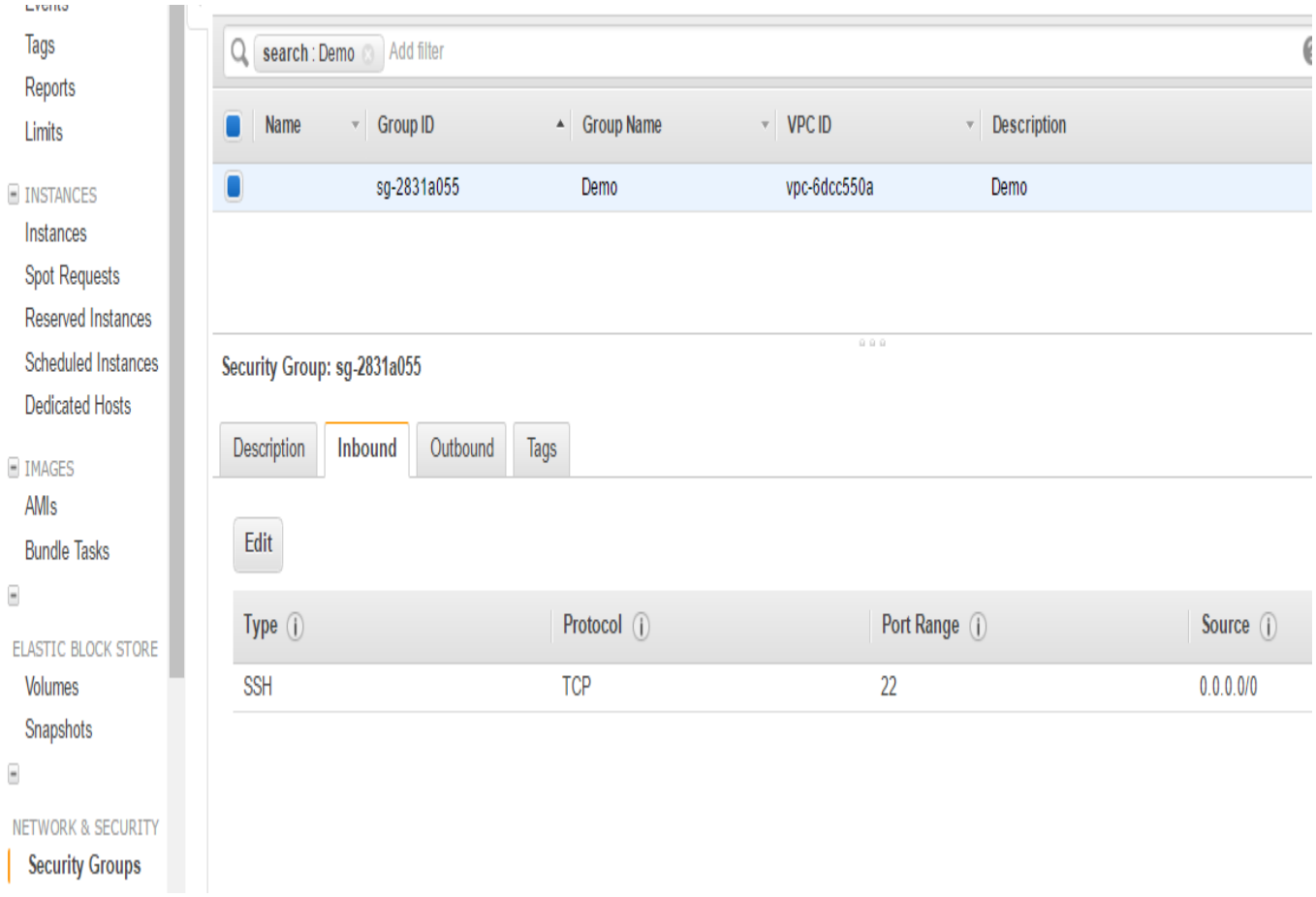
Please select :

- 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 that controls the traffic for one or more instances. When you launch an instance, you associate one or more security groups with the instance. You add rules to each security group that allow traffic to or from its associated instances. Below is an example of a security group for EC2 instances that allows inbound rules and ensure there is a rule for TCP on port 22.



For more information on EC2 Security groups, please visit the url - http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html

The correct answer is: Security group

Feedback about this question and answer

QUESTION 25	NOT ANSWERED	Submit Feedback

How many types of block devices does Amazon EC2 support? Choose one answer from the options below

Please select :

- A. 2
- B. 3
- C. 4
- D. 1

A block device is a storage device that moves data in sequences of bytes or bits (blocks). These devices support random access and generally use buffered I/O. Examples include hard disks, CD-ROM drives, and flash drives. A block device can be physically attached to a computer or accessed remotely as if it were physically attached to the computer. Amazon EC2 supports two types of block devices:

- Instance store volumes (virtual devices whose underlying hardware is physically attached to the host computer for the instance)

EBS volumes (remote storage devices)

Block Device Mapping Concepts

A *block device* is a storage device that moves data in sequences of bytes or bits (blocks). These devices support random access and generally use buffered I/O. Examples include hard disks, CD-ROM drives, and flash drives. A block device can be physically attached to a computer or accessed remotely as if it were physically attached to the computer. Amazon EC2 supports two types of block devices:

- Instance store volumes (virtual devices whose underlying hardware is physically attached to the host computer for the instance)
- EBS volumes (remote storage devices)

The correct answer is: 2

Feedback about this question and answer

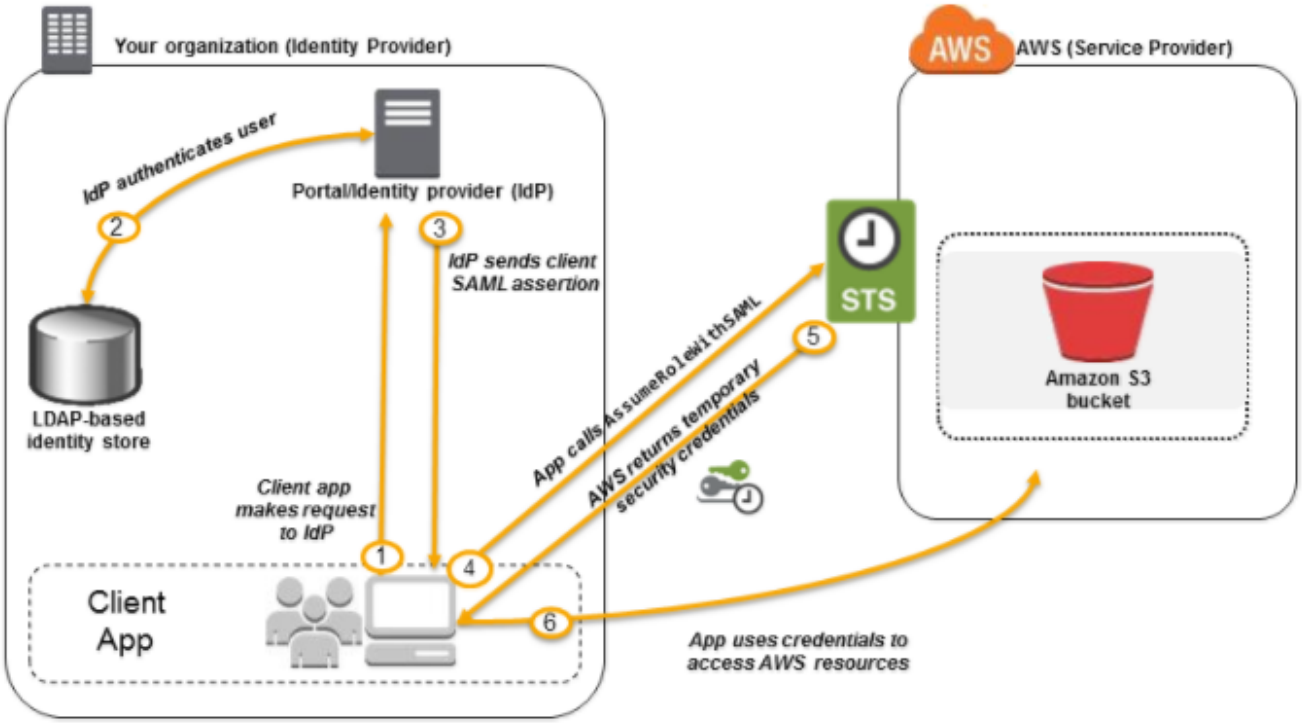
QUESTION 26 | **NOT ANSWERED** | **Submit Feedback**

Your fortune 500 company has under taken a TCO analysis evaluating the use of Amazon S3 versus acquiring more hardware The outcome was that ail employees would be granted access to use Amazon S3 for storage of their personal documents. Which of the following will you need to consider so you can set up a solution that incorporates single sign-on from your corporate AD or LDAP directory and restricts access for each user to a designated user folder in a bucket? Choose three answers from the options given below

Please select :

- [ ] A. Setting up a federation proxy or identity provider
- [ ] B. Using AWS Security Token Service to generate temporary tokens
- [ ] C. Tagging each folder in the bucket
- [ ] D. Configuring IAM role
- [ ] E. Setting up a matching IAM user for every user in your corporate directory that needs access to a folder in the bucket

The below diagram shows how the setup is done using the Secure token service to achieve integration between AWS and an on premise Active Directory infrastructure. You need to have an identity provider such as Active Directory Federation services. The Secure Token service is used to generate temporary credentials. These credentials are then mapped to corresponding IAM roles.



For more information please refer to the below link:

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

The correct answers are: Setting up a federation proxy or identity provider, Using AWS Security Token Service to generate temporary tokens, Configuring IAM role

Feedback about this question and answer

QUESTION 27	NOT ANSWERED	Submit Feedback

When running my DB Instance as a Multi-AZ deployment, can I use the standby for read and write operations?

Please select :

- A. Yes
- B. Only with MSSQL based RDS
- C. Only for Oracle RDS instances

Your answer is incorrect.

Answer – D

This is clearly mentioned in the aws documentation that you cannot use the secondary DB instances for writing purposes.

Q: When running my DB Instance as a Multi-AZ deployment, can I use the standby for read or write operations?

No, the standby replica cannot serve read requests. Multi-AZ deployments are designed to provide enhanced database availability and durability, rather than read scaling benefits. As such, the feature uses synchronous replication between primary and standby. Our implementation makes sure the primary and the standby are constantly in sync, but precludes using the standby for read or write operations. If you are interested in a read scaling solution, please see the FAQs on Read Replicas.

Here is the overview of Multi-AZ RDS Deployments:

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, Amazon RDS performs an automatic failover to the standby (or to a read replica in the case of Amazon Aurora), so that you can resume database operations as soon as the failover is complete. Since the endpoint for your DB Instance remains the same after a failover, your application can resume database operation without the need for manual administrative intervention.

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

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

The correct answer is: No

Feedback about this question and answer

QUESTION 28	NOT ANSWERED	Submit Feedback

Which Amazon service can I use to define a virtual network that closely resembles a traditional data center?

Please select :

- A. Amazon VPC
- B. Amazon ServiceBus
- C. Amazon EMR
- D. Amazon RDS

Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the Amazon Web Services (AWS) cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways.

You can easily customize the network configuration for your Amazon Virtual Private Cloud. For example, you can create a public-facing subnet for your webservers that has access to the Internet, and place your backend systems such as databases or application servers in a private-facing subnet with no Internet access. You can leverage multiple layers of security, including security groups and network access control lists, to help control access to Amazon EC2 instances in each subnet

For more information on Amazon VPC, please visit the link

https://aws.amazon.com/vpc/

The correct answer is: Amazon VPC

Feedback about this question and answer

QUESTION 29 | **NOT ANSWERED** | **Submit Feedback**

The common use for IAM is to manage what?
Select 3 options.

Please select :

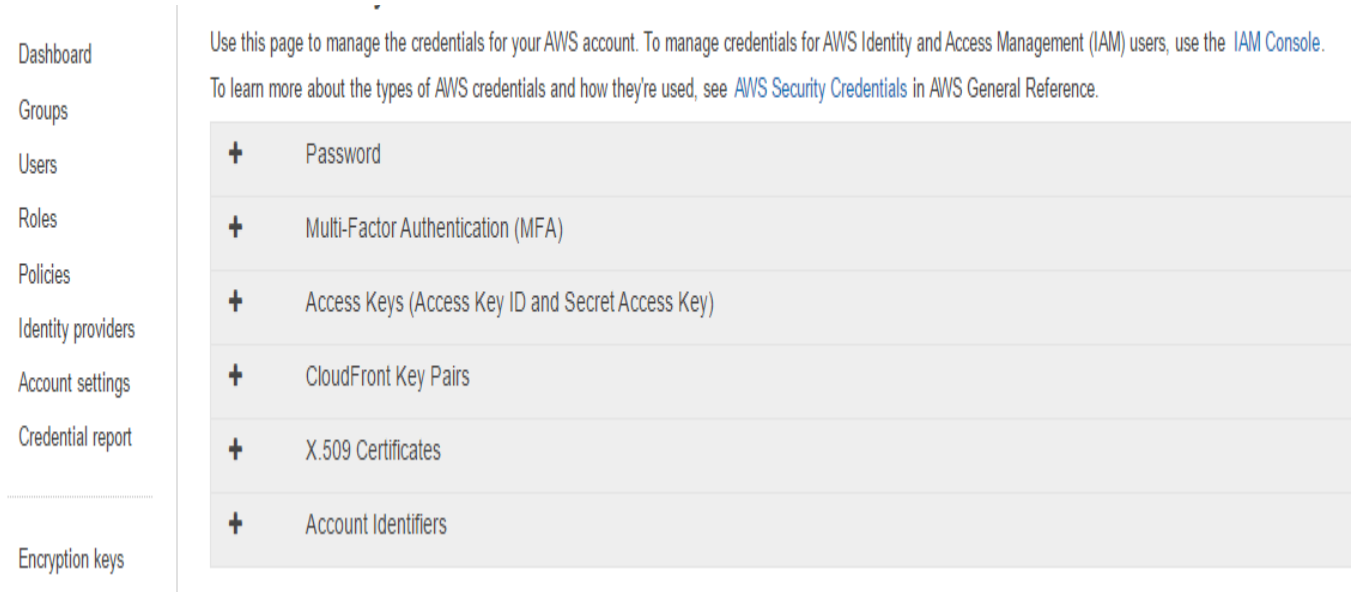
- [ ] A. Security Groups
- [ ] B. API Keys
- [ ] C. Multi-Factor Authentication
- [ ] D. Roles

Your answer is incorrect.

Answer – B,C and D

You can use IAM to manage API key and MFA along with roles.
Please find specific details below:
http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html
http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_enable.html

If you go on the IAM console, you will see the options on the left hand side. The Security groups are managed as part of the EC2 dashboard and not the IAM console.



For more information on IAM, please refer to the below link

https://aws.amazon.com/iam/

The correct answers are: API Keys, Multi-Factor Authentication, Roles

Feedback about this question and answer

QUESTION 30 **NOT ANSWERED** **Submit Feedback**

You have instances running on your VPC. You have both production and development based instances running in the VPC. You want to ensure that people who are responsible for the development instances don't have the access to work on the production instances to ensure better security. Using policies, which of the following would be the best way to accomplish this? Choose the correct answer from the options given below

Please select :

- A. Launch the test and production instances in separate VPC's and use VPC peering
- B. Create an IAM policy with a condition which allows access to only instances that are used for production or development
- C. Launch the test and production instances in different Availability Zones and use Multi Factor Authentication
- D. Define the tags on the test and production servers and add a condition to the IAM policy which allows access to specific tags

Your answer is incorrect.

instances and then ensure these tags are used when controlling access via an IAM policy.

For more information on tagging your resources, please refer to the below link

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html

The correct answer is: Define the tags on the test and production servers and add a condition to the IAM policy which allows access to specific tags

Feedback about this question and answer

QUESTION 31	NOT ANSWERED	Submit Feedback

Your company is concerned with EBS volume backup on Amazon EC2 and wants to ensure they have proper backups and that the data is durable. What solution would you implement and why? Choose the correct answer from the options below

Please select :

- A. Configure Amazon Storage Gateway with EBS volumes as the data source and store the backups on premise through the storage gateway
- B. Write a cronjob on the server that compresses the data that needs to be backed up using gzip compression, then use AWS CLI to copy the data into an S3 bucket for durability
- C. Use a lifecycle policy to back up EBS volumes stored on Amazon S3 for durability
- D. Write a cronjob that uses the AWS CLI to take a snapshot of production EBS volumes. The data is durable because EBS snapshots are stored on the Amazon S3 standard storage class

Your answer is incorrect.

Answer – D

You can take snapshots of EBS volumes and to automate the process you can use the CLI. The snapshots are automatically stored on S3 for durability.

For more information on EBS snapshots, please refer to the below link

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

The correct answer is: Write a cronjob that uses the AWS CLI to take a snapshot of production EBS volumes. The data is durable because EBS snapshots are stored on the Amazon S3 standard storage class

Feedback about this question and answer

QUESTION 32	NOT ANSWERED	Submit Feedback

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 correct answer from the options given below

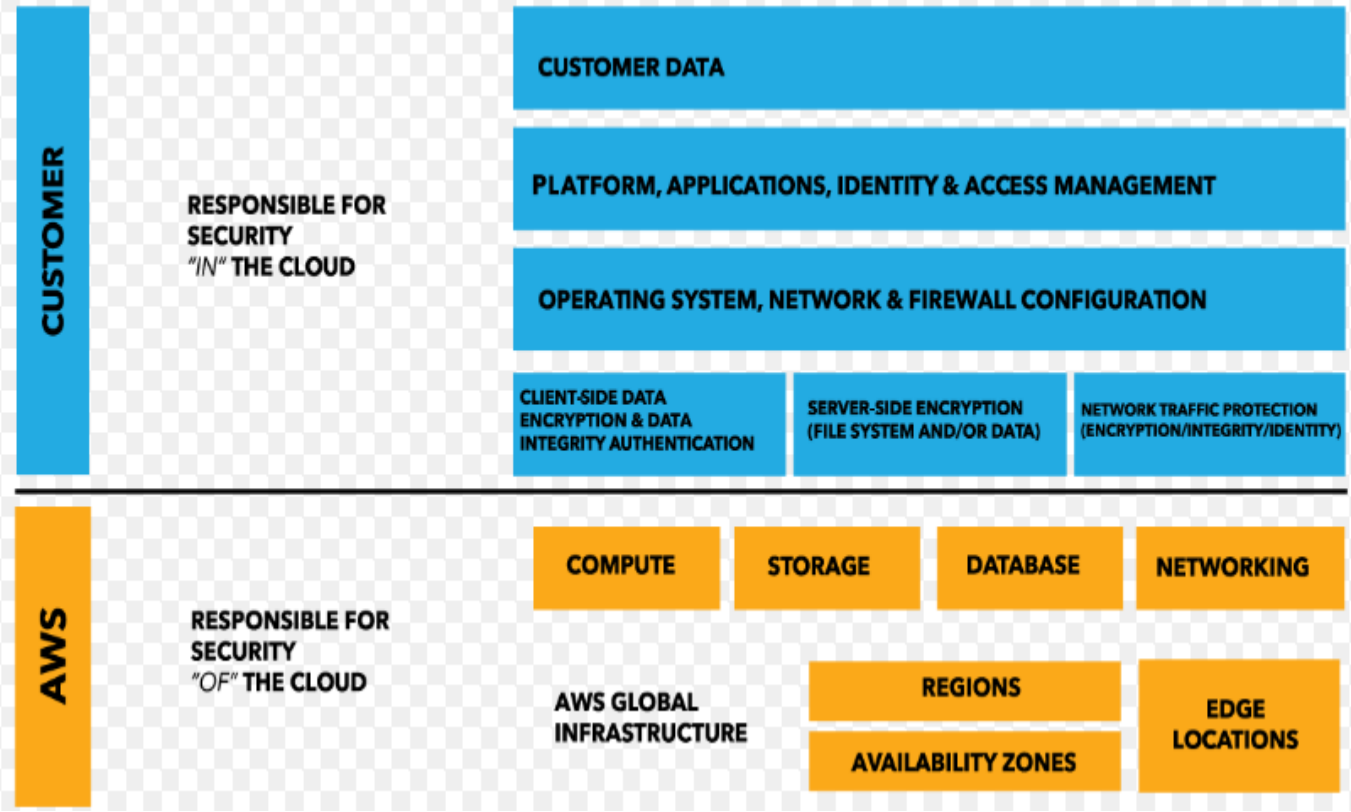
Please select :

- A. Customer Data
- B. Physical network infrastructure
- C. Instance security
- D. User access to the AWS environment

Your answer is incorrect.

Answer – B

As per the Shared responsibility model, the Physical network infrastructure is taken care by AWS. The below diagram clearly shows what has to be managed by customer and what is managed by AWS.



For more information on the Shared Responsibility model, please refer to the below link

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

The correct answer is: Physical network infrastructure

QUESTION 33 | NOT ANSWERED | Submit Feedback

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

Please select :

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

Your answer is incorrect.

Answer – A and C

EC2 instances are available in EBS backed storage and instance store backed storage. In fact, now more EC2 instances are EBS backed only so we need to consider both options while answering the question.

Find more details here :

- https://aws.amazon.com/ec2/instance-types/

If you have an EBS backed instance store , then the underling host is changed when the instance is stopped and started.

And if you have instance store volumes, the data on the instance store devices will be lost.

For more information on the AMI types, please refer to the below link:

- http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ComponentsAMIs.html

	General purpose	m4.xlarge	4	16	EBS only

- http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-lifecycle.html

QUESTION 34 | NOT ANSWERED | Submit Feedback

A customer is hosting their company website on a cluster of web servers that are behind a public-facing load balancer. The customer also uses Amazon Route 53 to manage their public DNS. How should the customer configure the DNS zone apex record to point to the load balancer?

Please select :

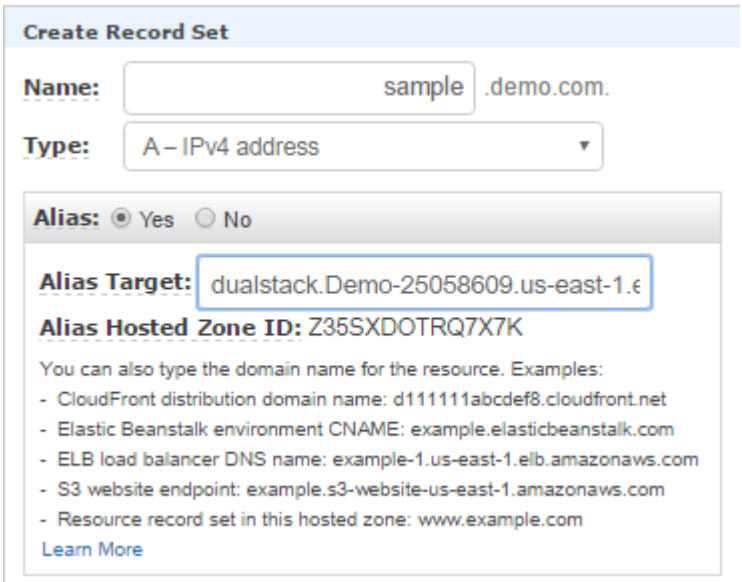
- A. Create an A record pointing to the IP address of the load balancer
- B. Create a CNAME record pointing to the load balancer DNS name.
- C. Create an alias for CNAME record to the load balancer DNS name.
- D. Create an A record aliased to the load balancer DNS name

Your answer is incorrect.

Answer – D

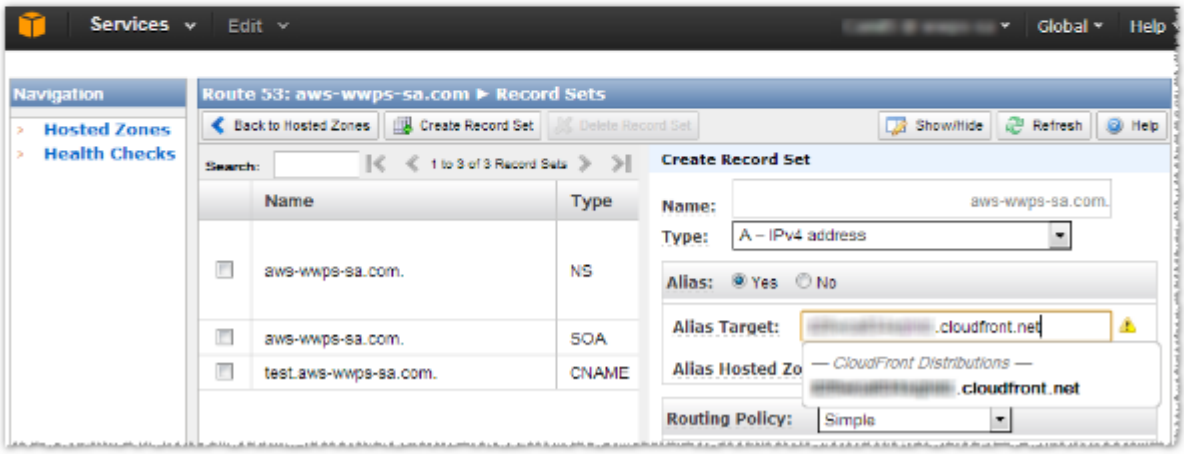
Alias resource record sets are virtual records that work like CNAME records. But they differ from CNAME records in that they are not visible to resolvers. Resolvers only see the A record and the resulting IP address of the target record. As such, unlike CNAME records, alias resource record sets are available to configure a zone apex (also known as a root domain or naked domain) in a dynamic environment.

So when you create a hosted zone and having a pointer to the load balancer , you need to mark 'yes' for the Alias option as shown below. Then you can choose the Elastic Load balancer which you have defined in aws.



Route 53 console.

2. Create a new alias resource record set for your root domain name. For **Alias**, choose **Yes**. From the **Alias Target** drop-down list, select the CloudFront distribution name you created earlier.



For more information on the zone apex, please visit the link

- http://docs.aws.amazon.com/govcloud-us/latest/UserGuide/setting-up-route53-zoneapex-elb.html

The correct answer is: Create an A record aliased to the load balancer DNS name

Feedback about this question and answer

QUESTION 35	NOT ANSWERED	Submit Feedback

To maintain compliance with HIPPA laws, 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, assuming S3 is being used for storing the healthcare-related data?
Choose the 2 correct answers from the options given below

Please select :

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

Data protection refers to protecting data while in-transit (as it travels to and from Amazon S3) and at rest (while it is stored on disks in Amazon S3 data centers). You can protect data in transit by using SSL or by using client-side encryption. You have the following options of protecting data at rest in Amazon S3.

- Use Server-Side Encryption – You request Amazon S3 to encrypt your object before saving it on disks in its data centers and decrypt it when you download the objects.
- Use Client-Side Encryption – You can encrypt data client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, the encryption keys, and related tools.

For more information on S3 encryption, please refer to the below link

http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html

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

Feedback about this question and answer

QUESTION 36	NOT ANSWERED	Submit Feedback

CloudHSM. Which of the following statements is right when it comes to CloudHSM and KMS. Choose the correct answer from the options given below

Please select :

- A. It probably doesn't matter as they both do the same thing
- B. AWS CloudHSM does not support the processing, storage, and transmission of credit card data by a merchant or service provider, as it has not been validated as being compliant with Payment Card Industry (PCI) Data Security Standard (DSS); hence, you will need to use KMS
- C. KMS is probably adequate unless additional protection is necessary for some applications and data that are subject to strict contractual or regulatory requirements for managing cryptographic keys, then HSM should be used
- D. AWS CloudHSM should be always be used for any payment transactions

Your answer is incorrect.

Answer – C

AWS Key Management Service (KMS) is a managed service that makes it easy for you to create and control the encryption keys used to encrypt your data, and uses Hardware Security Modules (HSMs) to protect the security of your keys. This is sufficient if you the basic needs of managing keys for security.

For more information on KMS, please refer to the below link

https://aws.amazon.com/kms/

For a higher requirement on security one can use CloudHSM. The AWS CloudHSM service helps you meet corporate, contractual and regulatory compliance requirements for data security by using dedicated Hardware Security Module (HSM) appliances within the AWS cloud. With CloudHSM, you control the encryption keys and cryptographic operations performed by the HSM

For more information on CloudHSM, please refer to the below link

https://aws.amazon.com/cloudhsm/

The correct answer is: KMS is probably adequate unless additional protection is necessary for some applications and data that are subject to strict contractual or regulatory requirements for managing cryptographic keys, then HSM should be used

Feedback about this question and answer

QUESTION 37	NOT ANSWERED	Submit Feedback

You are building a system to distribute confidential training videos to employees. Using CloudFront, what method would be used to serve content that is stored in S3, but not publicly accessible from S3 directly? Choose the correct answer from the options given below

bucket to that OAI

B. Create an Identity and Access Management (IAM) user for CloudFront and grant access to the objects in your S3 bucket to that IAM user.

C. Create a S3 bucket policy that lists the CloudFront distribution ID as the principal and the target bucket as the Amazon Resource Name (ARN)

D. Add the CloudFront account security group

Your answer is incorrect.

Answer – A

You can optionally secure the content in your Amazon S3 bucket so users can access it through CloudFront but cannot access it directly by using Amazon S3 URLs. This prevents anyone from bypassing CloudFront and using the Amazon S3 URL to get content that you want to restrict access to. This step isn't required to use signed URLs, but we recommend it.

To require that users access your content through CloudFront URLs, you perform the following tasks:

- Create a special CloudFront user called an origin access identity.
- Give the origin access identity permission to read the objects in your bucket.
- Remove permission for anyone else to use Amazon S3 URLs to read the objects.

For more information on Restricting access to AWS S3, please refer to the below link:

- http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html

The correct answer is: Create an Origin Access Identify (OAI) for CloudFront and grant access to the objects in your S3 bucket to that OAI

Feedback about this question and answer

QUESTION 38 **NOT ANSWERED** **Submit Feedback**

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 answer from the options given below

Please select :

A. Amazon S3 for storing the ELB log files and EC2 for processing the log files in analysis

B. Amazon DynamoDB to store the logs and EC2 for running custom log analysis scripts

C. Amazon S3 for storing ELB log files and Amazon EMR for processing the log files in analysis

Your answer is incorrect.

Answer – C

You can use Amazon EMR for processing the jobs

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 Amazon EMR please refer to the below 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

Feedback about this question and answer

QUESTION 39	NOT ANSWERED	Submit Feedback

You are designing a social media site and are considering how to mitigate distributed denial-of-service (DDoS) attacks. Which of the below are viable mitigation techniques? Choose 3 answers from the options below

Please select :

- A. Add multiple elastic network interfaces (ENIs) to each EC2 instance to increase the network bandwidth.
- B. Use dedicated instances to ensure that each instance has the maximum performance possible.
- C. Use an Amazon CloudFront distribution for both static and dynamic content.
- D. Use an Elastic Load Balancer with auto scaling groups at the web, App. Restricting direct internet traffic to Amazon Relational Database Service (RDS) tiers.
- E. Add alert Amazon CloudWatch to look for high Network in and CPU utilization.
- F. Create processes and capabilities to quickly add and remove rules to the instance OS firewall.

Your answer is incorrect.

	AWS Edge Locations			AWS Regions		
	Amazon CloudFront with AWS WAF (BP1, BP2)	Amazon API Gateway (BP4)	Amazon Route 53 (BP3)	Elastic Load Balancing (BP6)	Amazon VPC (BP5)	Amazon EC2 with Auto Scaling (BP7)
Layer 3 (e.g., UDP reflection) attack mitigation	✔	✔	✔	✔	✔	
Layer 4 (e.g., SYN flood) attack mitigation	✔	✔	✔	✔		
Layer 6 (e.g., SSL) attack mitigation	✔	✔	N/A	✔		
Reduce attack surface	✔	✔	✔	✔	✔	
Scale to absorb application layer traffic	✔	✔	✔	✔		✔
Layer 7 (application layer) attack mitigation	✔	✔	✔			
Geographic isolation and dispersion of excess traffic and larger DDoS attacks	✔	✔	✔			

For best practises against DDos attacks , please visit the below link

https://d0.awsstatic.com/whitepapers/DDoS_White_Paper_June2015.pdf

The correct answers are: Use an Amazon CloudFront distribution for both static and dynamic content., Use an Elastic Load Balancer with auto scaling groups at the web, App. Restricting direct internet traffic to Amazon Relational Database Service (RDS) tiers., Add alert Amazon CloudWatch to look for high Network in and CPU utilization.

Feedback about this question and answer

QUESTION 40 **NOT ANSWERED** **Submit Feedback**

Your company has moved a legacy application from an on-premise data center to the cloud. The legacy application requires a static IP address hard-coded into the backend, which prevents you from deploying the application with high availability and fault tolerance using the ELB. Which

Please select :

- [ ] A. Write a custom script that pings the health of the instance, and, if the instance stops responding, switches the elastic IP address to a standby instance
- [ ] B. Ensure that the instance it's using has an elastic IP address assigned to it
- [ ] C. Do not migrate the application to the cloud until it can be converted to work with the ELB and Auto Scaling
- [ ] D. Create an AMI of the instance and launch it using Auto Scaling which will deploy the instance again if it becomes unhealthy

Your answer is incorrect.

Answer – A and B

The best option is to configure an Elastic IP that can be switched between a primary and failover instance.

Here is a link on using Elastic IP for failover.

https://aws.amazon.com/articles/2127188135977316

The correct answers are: Write a custom script that pings the health of the instance, and, if the instance stops responding, switches the elastic IP address to a standby instance, Ensure that the instance it's using has an elastic IP address assigned to it

Feedback about this question and answer

QUESTION 41 | **NOT ANSWERED** | **Submit Feedback**

As an IT administrator you have been requested to ensure you create a highly decouple application in AWS. Which of the following help you accomplish this goal? Choose the correct answer from the options below

Please select :

- ( ) A. An SQS queue to allow a second EC2 instance to process a failed instance's job
- ( ) B. An Elastic Load Balancer to send web traffic to healthy EC2 instances
- ( ) C. IAM user credentials on EC2 instances to grant permissions to modify an SQS queue
- ( ) D. An Auto Scaling group to recover from EC2 instance failures

Your answer is incorrect.

Answer – A

reliability, and is best practice design for modern applications.

SQS is the best option for creating a decoupled application.

Amazon Simple Queue Service (SQS) is a fully-managed message queuing service for reliably communicating among distributed software components and microservices - at any scale. Building applications from individual components that each perform a discrete function improves scalability and reliability, and is best practice design for modern applications. SQS makes it simple and cost-effective to decouple and coordinate the components of a cloud application. Using SQS, you can send, store, and receive messages between software components at any volume, without losing messages or requiring other services to be always available. SQS *standard queues* offer maximum throughput, best-effort ordering, and at-least-once delivery. SQS *FIFO queues* are designed to guarantee that messages are processed exactly once, in the exact order that they are sent, with limited throughput. You can get started with SQS in a matter of minutes using the AWS console or SDK of your choice and just three simple commands. SQS lets you eliminate the complexity and overhead associated with managing and operating dedicated messaging software and infrastructure.

For more information on SQS, please refer to the below link

https://aws.amazon.com/sqs/

The correct answer is: An SQS queue to allow a second EC2 instance to process a failed instance's job

Feedback about this question and answer

QUESTION 42	NOT ANSWERED	Submit Feedback

A company has resources hosted in AWS and on on-premise servers. You have been requested to create a de-coupled architecture for applications which make use of both types of resources? Which of the below options are valid?
Select 2 options.

Please select :

- A. You can leverage SWF to utilize both on-premises servers and EC2 instances for your decoupled application
- B. SQS is not a valid option to help you use on-premises servers and EC2 instances in the same application, as it cannot be polled by on-premises servers

D. SWF is not a valid option to help you use on-premises servers and EC2 instances in the same application, as on-premises servers cannot be used as activity task workers

Your answer is incorrect.

Answer – A and C

You can use both SWF and SQS to coordinate with EC2 instances and on-premise servers.

Amazon Simple Queue Service (SQS) is a fully-managed message queuing service for reliably communicating among distributed software components and microservices - at any scale. Building applications from individual components that each perform a discrete function improves scalability and reliability, and is best practice design for modern applications.

For more information on SQS, please refer to the below link

https://aws.amazon.com/sqs/

The Amazon Simple Workflow Service (Amazon SWF) makes it easy to build applications that coordinate work across distributed components. In Amazon SWF, a task represents a logical unit of work that is performed by a component of your application. Coordinating tasks across the application involves managing intertask dependencies, scheduling, and concurrency in accordance with the logical flow of the application. Amazon SWF gives you full control over implementing tasks and coordinating them without worrying about underlying complexities such as tracking their progress and maintaining their state.

For more information on SWF, please refer to the below link

http://docs.aws.amazon.com/amazonswf/latest/developerguide/swf-welcome.html

The correct answers are: You can leverage SWF to utilize both on-premises servers and EC2 instances for your decoupled application, You can leverage SQS to utilize both on-premises servers and EC2 instances for your decoupled application

Feedback about this question and answer

QUESTION 43 | **NOT ANSWERED** | **Submit Feedback**

When reviewing the Auto Scaling events, it is noticed that an application is scaling up and down multiple times within the hour. What design change could you make to optimize cost while preserving elasticity? Choose the correct answer from the options below

Please select :

- A. Change the scale down CloudWatch metric to a higher threshold
- B. Increase the instance type in the launch configuration
- C. Increase the base number of Auto Scaling instances for the Auto Scaling group

Your answer is incorrect.

Answer – A

If the threshold for the scale down is too low then the instances will keep on scaling down rapidly. Hence it is best to keep on optimal threshold for your metrics defined for Cloudwatch.

For more information on scaling on demand, please refer to the below link

http://docs.aws.amazon.com/autoscaling/latest/userguide/as-scale-based-on-demand.html

The correct answer is: Change the scale down CloudWatch metric to a higher threshold

Feedback about this question and answer

QUESTION 44	NOT ANSWERED	Submit Feedback

You are working for a startup company that is building an application that receives large amounts of data. Unfortunately, current funding has left the start-up short on cash, cannot afford to purchase thousands of dollars of storage hardware, and has opted to use AWS. Which services would you implement in order to store a virtually unlimited amount of data without any effort to scale when demand unexpectedly increases? Choose the correct answer from the options below

Please select :

- A. Amazon S3, because it provides unlimited amounts of storage data, scales automatically, is highly available, and durable
- B. Amazon Glacier, to keep costs low for storage and scale infinitely
- C. Amazon Import/Export, because Amazon assists in migrating large amounts of data to Amazon S3
- D. Amazon EC2, because EBS volumes can scale to hold any amount of data and, when used with Auto Scaling, can be designed for fault tolerance and high availability

Your answer is incorrect.

Answer – A

The best option is to use S3 because you can host a large amount of data in S3 and is the best storage option provided by AWS.

The answer could be Glacier if question is just asking to choose the cheapest option to store a large amount of data , but here trick is in question where it mentioned to scale when "demand unexpectedly increase". As Galicer required 3 to 5 hrs duration to get data , so it will not able to handle unexpected demand increase thus S3 is the best choice here.

For more information on S3, please refer to the below link

automatically, is highly available, and durable

Feedback about this question and answer

QUESTION 45	NOT ANSWERED	Submit Feedback

A customer is running a multi-tier web application farm in a virtual private cloud (VPC) that is not connected to their corporate network. They are connecting to the VPC over the Internet to manage all of their Amazon EC2 instances running in both the public and private subnets. They have only authorized the bastion-security-group with Microsoft Remote Desktop Protocol (RDP) access to the application instance security groups, but the company wants to further limit administrative access to all of the instances in the VPC. Which of the following Bastion deployment scenarios will meet this requirement?

Please select :

- A. Deploy a Windows Bastion host on the corporate network that has RDP access to all instances in the VPC.
- B. Deploy a Windows Bastion host with an Elastic IP address in the public subnet and allow SSH access to the bastion from anywhere.
- C. Deploy a Windows Bastion host with an Elastic IP address in the private subnet, and restrict RDP access to the bastion from only the corporate public IP addresses.
- D. Deploy a Windows Bastion host with an Elastic IP address in the public subnet and allow RDP access to bastion only from corporate IP addresses.

Your answer is incorrect.

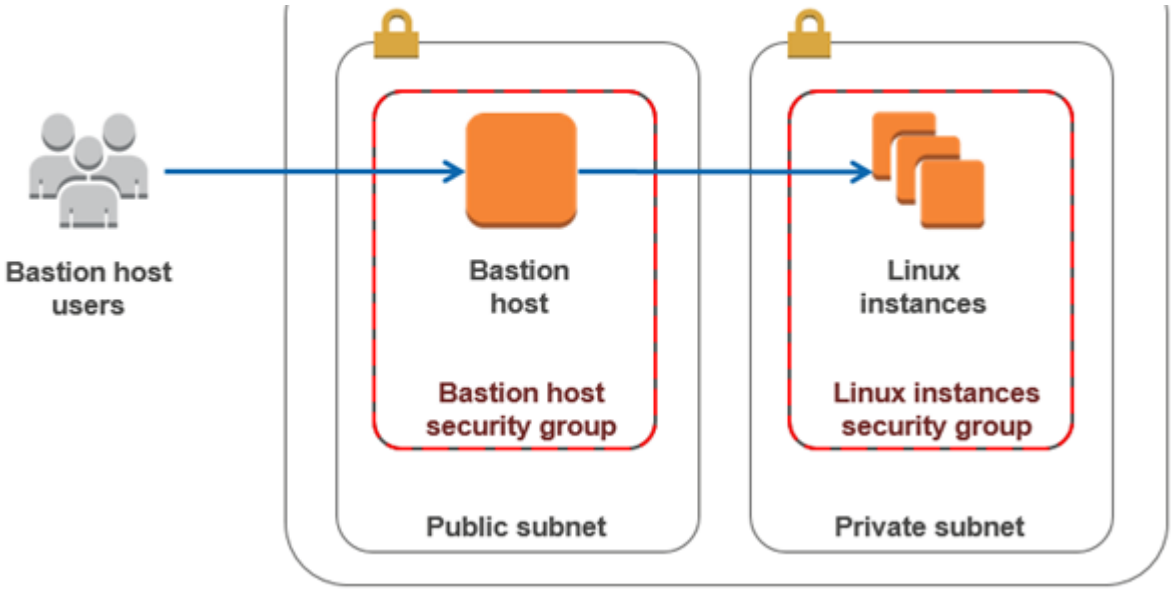
Answer – D

The bastion host should be in a public subnet with either a public or elastic IP and only allow RDP access from one IP from the corporate network.

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 practice adopted by many organization to secure the assets in their private subnets.



The correct answer is: Deploy a Windows Bastion host with an Elastic IP address in the public subnet and allow RDP access to bastion only from corporate IP addresses.

Feedback about this question and answer

QUESTION 46	NOT ANSWERED	Submit Feedback

You have started a new role as a solutions architect for an architectural firm that designs large sky scrapers in the Middle East. Your company hosts large volumes of data and has about 250 TB of data on internal servers. They have decided to store this data on S3 due to the redundancy offered by it. The company currently has a telecoms line of 2Mbps connecting their head office to the internet. What method should they use to import this data on to S3 in the fastest manner possible?

Please select :

- A. Upload it directly to S3
- B. Purchase and AWS Direct connect and transfer the data over that once it is installed.
- C. AWS Data pipeline
- D. AWS Snowball

Your answer is incorrect.

Answer – D

The AWS Documentation mentions the following

Transferring data with Snowball is simple, fast, secure, and can be as little as one-fifth the cost of high-speed Internet.

For more information on AWS Snowball , please visit the below link:

- https://aws.amazon.com/snowball/

The correct answer is: AWS Snowball

Feedback about this question and answer

QUESTION 47	NOT ANSWERED	Submit Feedback

How does using ElastiCache help to improve database performance? Choose the correct answer from the options below

Please select :

- A. It can store petabytes of data
- B. It provides faster internet speeds
- C. It can store high-taxing queries
- D. It uses read replicas

Your answer is incorrect.

Answer – C

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. 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.

For more information on AWS Elastic Cache, please refer to the below link

https://aws.amazon.com/elasticache/

The correct answer is: It can store high-taxing queries

Feedback about this question and answer

QUESTION 48	NOT ANSWERED	Submit Feedback

The Availability Zone that your RDS database instance is located in is suffering from outages, and you have lost access to the database. What could you have done to prevent losing access to your database (in the event of this type of failure) without any downtime? Choose the correct

- A. Made a snapshot of the database
- B. Enabled multi-AZ failover
- C. Increased the database instance size
- D. Created a read replica

Your answer is incorrect.

Answer – B

The best option is to enable Multi-AZ for the database.

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, Amazon RDS performs an automatic failover to the standby (or to a read replica in the case of Amazon Aurora), so that you can resume database operations as soon as the failover is complete. Since the endpoint for your DB Instance remains the same after a failover, your application can resume database operation without the need for manual administrative intervention

For more information on AWS Multi-AZ, please refer to the below link

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

The correct answer is: Enabled multi-AZ failover

Feedback about this question and answer

QUESTION 49 | **NOT ANSWERED** | **Submit Feedback**

As an AWS administrator you are trying to convince a team to use RDS Read Replica's. What are two benefits of using read replicas?
Choose the 2 correct answers from the options below

Please select :

- A. Creates elasticity in RDS
- B. Allows both reads and writes
- C. Improves performance of the primary database by taking workload from it
- D. Automatic failover in the case of Availability Zone service failures

Your answer is incorrect.

database.

Read Replica's don't provide write operations , hence option B is wrong. And Multi-AZ is used for failover so Option D is wrong.

For more information on Read Replica, please refer to the below link

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

The correct answers are: Creates elasticity in RDS, Improves performance of the primary database by taking workload from it

Feedback about this question and answer

QUESTION 50	NOT ANSWERED	Submit Feedback

What is the purpose of an SWF decision task? Choose the correct answer from the options below

Please select :

- A. It tells the worker to perform a function.
- B. It tells the decider the state of the work flow execution.
- C. It defines all the activities in the workflow.
- D. It represents a single task in the workflow.

Your answer is incorrect.

Answer – B

A decider is an implementation of the coordination logic of your workflow type that runs during the execution of your workflow. You can run multiple deciders for a single workflow type.

Because the execution state for a workflow execution is stored in its workflow history, deciders can be stateless. Amazon SWF maintains the workflow execution history and provides it to a decider with each decision task

For more information on Decider tasks, please refer to the below link

http://docs.aws.amazon.com/amazonswf/latest/developerguide/swf-dg-dev-deciders.html

The correct answer is: It tells the decider the state of the work flow execution.

Feedback about this question and answer

QUESTION 51	NOT ANSWERED	Submit Feedback

What is the best definition of an SQS message? Choose an answer from the options below

- B. A set of instructions stored in an SQS queue that can be up to 512KB in size
- C. A notification sent via SNS
- D. A set of instructions stored in an SQS queue that can be up to 256KB in size

Your answer is incorrect.

Answer – D

The maximum size of an SQS message as given in the AWS documentation is given below

Q: How do I configure the maximum message size for Amazon SQS?

To configure the maximum message size, use the console or the SetQueueAttributes method to set the MaximumMessageSize attribute. This attribute specifies the limit on bytes that an Amazon SQS message can contain. Set this limit to a value between 1,024 bytes (1 KB), and 262,144 bytes (256 KB). For more information, see Using Amazon SQS Message Attributes in the *Amazon SQS Developer Guide*.

For more information on SQS, please refer to the below link

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

The correct answer is: A set of instructions stored in an SQS queue that can be up to 256KB in size

Feedback about this question and answer

QUESTION 52 | **NOT ANSWERED** | **Submit Feedback**

CloudTrail can log API calls from? Choose the correct answer from the options below

Please select :

- A. The command line
- B. The SDK
- C. The Console
- D. All of the above

Your answer is incorrect.

Answer – D

Cloudtrail can log all API calls which enter AWS.

including API calls made through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This history simplifies security analysis, resource change tracking, and troubleshooting.

For more information on AWS Cloudtrail, please refer to the below link

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

The correct answer is: All of the above

Feedback about this question and answer

QUESTION 53	NOT ANSWERED	Submit Feedback

What best describes Recovery Time Objective (RTO)? Choose the correct answer from the options below

Please select :

- A. The time it takes after a disruption to restore operations back to its regular service level.
- B. Minimal version of your production environment running on AWS.
- C. A full clone of your production environment.
- D. Acceptable amount of data loss measured in time.

Your answer is incorrect.

Answer – A

The recovery time objective (RTO) is the targeted duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity

Please refer to the below link for more details

https://en.wikipedia.org/wiki/Recovery_time_objective

The correct answer is: The time it takes after a disruption to restore operations back to its regular service level.

Feedback about this question and answer

QUESTION 54	NOT ANSWERED	Submit Feedback

answer from the options below

Please select :

- A. CloudWatch
- B. CloudFront
- C. CloudTrail
- D. Kinesis

Your answer is incorrect.

Answer – B

The below snapshot from the aws documentation shows the best architecture practises for avoiding DDos attacks.

	AWS Edge Locations			AWS Regions		
	Amazon CloudFront with AWS WAF (BP1, BP2)	Amazon API Gateway (BP4)	Amazon Route 53 (BP3)	Elastic Load Balancing (BP6)	Amazon VPC (BP5)	Amazon EC2 with Auto Scaling (BP7)
Layer 3 (e.g., UDP reflection) attack mitigation	✔	✔	✔	✔	✔	
Layer 4 (e.g., SYN flood) attack mitigation	✔	✔	✔	✔		
Layer 6 (e.g., SSL) attack mitigation	✔	✔	N/A	✔		
Reduce attack surface	✔	✔	✔	✔	✔	
Scale to absorb application layer traffic	✔	✔	✔	✔		✔
Layer 7 (application layer) attack mitigation	✔	✔	✔			
Geographic isolation and dispersion of excess traffic and larger DDoS attacks	✔	✔	✔			

For best practises against DDos attacks , please visit the below link

https://d0.awsstatic.com/whitepapers/DDoS_White_Paper_June2015.pdf

QUESTION 55 | NOT ANSWERED | Submit Feedback

Perfect Forward Secrecy is used to offer SSL/TLS cipher suites for which two AWS services? Choose the correct answer from the options below

Please select :

- A. EC2 and S3
- B. CloudTrail and CloudWatch
- C. Cloudfront and Elastic Load Balancing
- D. Trusted advisor and GovCloud

Your answer is incorrect.

Answer – C

Its currently available for Cloudfront and ELB. Please find the below link for more details

https://aws.amazon.com/about-aws/whats-new/2014/02/19/elastic-load-balancing-perfect-forward-secrecy-and-more-new-security-features/

https://aws.amazon.com/blogs/aws/cloudfront-ssl-ciphers-session-ocsp-pfs/

The correct answer is: Cloudfront and Elastic Load Balancing

Feedback about this question and answer

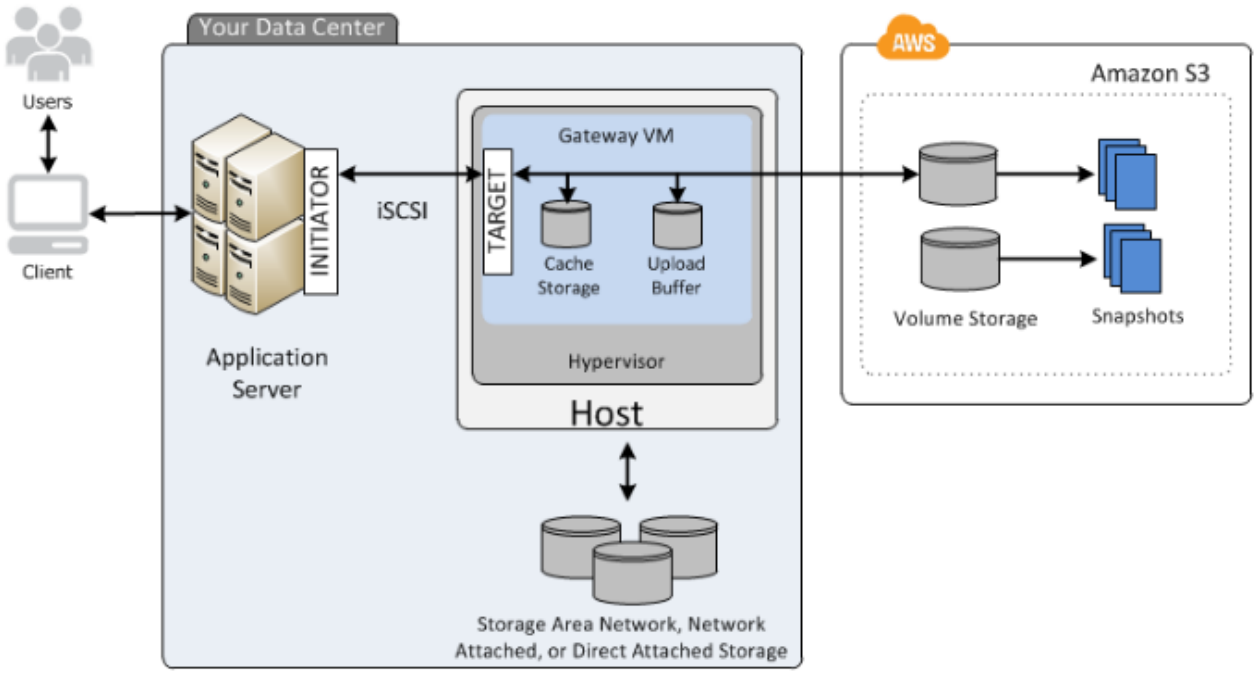
QUESTION 56 | NOT ANSWERED | Submit Feedback

A customer has a single 3-TB volume on-premises that is used to hold a large repository of images and print layout files. This repository is growing at 500 GB a year and must be presented as a single logical volume. The customer is becoming increasingly constrained with their local storage capacity and wants an off-site backup of this data, while maintaining low-latency access to their frequently accessed data. Which AWS Storage Gateway configuration meets the customer requirements?

Please select :

- A. Gateway-Cached volumes with snapshots scheduled to Amazon S3
- B. Gateway-Stored volumes with snapshots scheduled to Amazon S3
- C. Gateway-Virtual Tape Library with snapshots to Amazon S3
- D. Gateway-Virtual Tape Library with snapshots to Amazon Glacier

Gateway-cached volumes let you use Amazon Simple Storage Service (Amazon S3) as your primary data storage while retaining frequently accessed data locally in your storage gateway. Gateway-cached volumes minimize the need to scale your on-premises storage infrastructure, while still providing your applications with low-latency access to their frequently accessed data. You can create storage volumes up to 32 TiB in size and attach to them as iSCSI devices from your on-premises application servers. Your gateway stores data that you write to these volumes in Amazon S3 and retains recently read data in your on-premises storage gateway's cache and upload buffer storage.



For more information on Storage gateways, please visit the link

http://docs.aws.amazon.com/storagegateway/latest/userguide/storage-gateway-cached-concepts.html

The correct answer is: Gateway-Cached volumes with snapshots scheduled to Amazon S3

Feedback about this question and answer

QUESTION 57	NOT ANSWERED	Submit Feedback

Which of the following best describes what the CloudHSM has to offer? Choose the correct answer from the options given below

Please select :

- A. An AWS service for generating API keys
- B. EBS Encryption method

Your answer is incorrect.

Answer – D

The AWS CloudHSM service helps you meet corporate, contractual and regulatory compliance requirements for data security by using dedicated Hardware Security Module (HSM) appliances within the AWS cloud. With CloudHSM, you control the encryption keys and cryptographic operations performed by the HSM.

For more information on CloudHSM, please refer to the below link

https://aws.amazon.com/cloudhsm/

The correct answer is: A dedicated appliance that is used to store security keys

Feedback about this question and answer

QUESTION 58	NOT ANSWERED	Submit Feedback

A company wants to launch EC2 instances on aws. For the linux instance, they want to ensure that the Perl language are installed automatically when the instance is launched. In which of the below configurations can you achieve what is required by the customer.

Please select :

- A. User data
- B. EC2Config service
- C. IAM roles
- D. AWS Config

Your answer is incorrect.

Answer – A

When you configure an instance during creation, you can add custom scripts to the User data section.

So in Step 3 of creating an instance, in the Advanced Details section, we can enter custom scripts in the User Data section. The below script installs Perl during the instance creation of the EC2 instance.

The correct answer is: User data

Feedback about this question and answer

QUESTION 59	NOT ANSWERED	Submit Feedback

Which of the following are true regarding encrypted Amazon Elastic Block Store (EBS) volumes? Choose 2 answers

Please select :

- [ ] A. Supported on all Amazon EBS volume types
- [ ] B. Snapshots are automatically encrypted
- [ ] C. Available to all instance types
- [ ] D. Existing volumes can be encrypted
- [ ] E. shared volumes can be encrypted

Your answer is incorrect.

Answer - A and B

- Option E is wrong because Shared volumes cannot be encrypted.

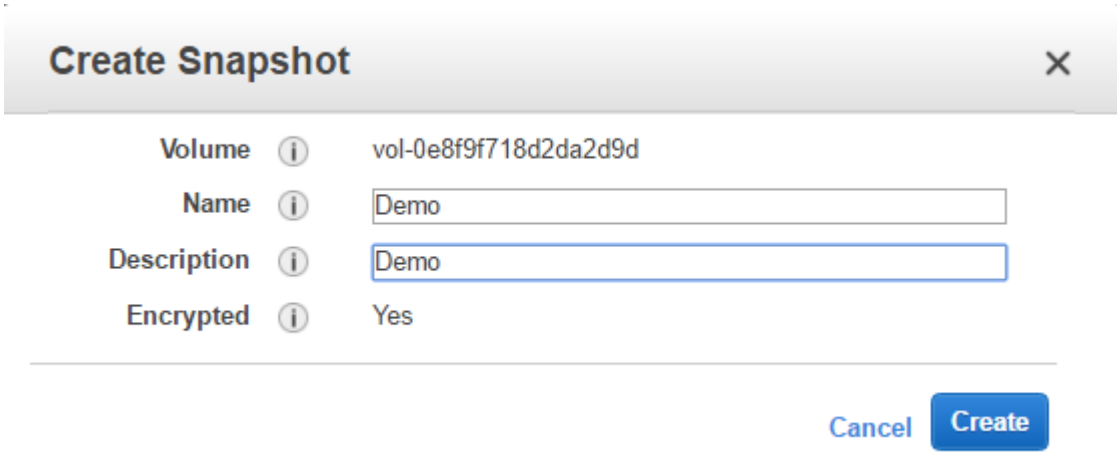
EBS volumes can be applied to all of the below Volume types:

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

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

So if we create a snapshot from a Volume that is encrypted:

The Encrypted option will automatically become true for the snapshot.



The correct answers are: Supported on all Amazon EBS volume types, Snapshots are automatically encrypted

Feedback about this question and answer

QUESTION 60	NOT ANSWERED	Submit Feedback

A company is deploying a new two-tier web application in AWS. The company wants to store their most frequently used data so that the response time for the application is improved. Which AWS service provides the solution for the company's requirements?

Please select :

- A. MySQL Installed on two Amazon EC2 Instances in a single Availability Zone
- B. Amazon RDS for MySQL with Multi-AZ
- C. Amazon ElastiCache
- D. Amazon DynamoDB

Your answer is incorrect.

data store or cache in the cloud. 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

- **Option A** is wrong because even if MySQL is installed on multiple systems, it will not help to serve the most recently used data.
- **Option B** is wrong because even a Multi-AZ option with an RDS will not suffice the requirement of the customer.
- **Option D** is wrong because this is a pure database option.

For more information on Elastic cache, please visit the link

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

The correct answer is: Amazon ElastiCache

Feedback about this question and answer

There is no Incorrect answer(s)