Question 5: Incorrect

You successfully configure VPC Peering between VPC-A and VPC-B. You then establish an IGW and a Direct-Connect connection in VPC-B. Can instances in VPC-A connect to your corporate office via the Direct-Connect service, and connect to the Internet via the IGW?

* NO

Explanation

VPC peering only routes traffic between source and destination VPCs. VPC peering does not support edge to edge routing

Question 6: Incorrect

You have created a Direct Connect Link from your on premise data center to your Amazon VPC. The link is now active and routes are being advertised from the on-premise data center. You can connect to EC2 instances from your data center; however, you cannot connect to your on premise servers from your EC2 instances. Which of the following solutions would remedy this issue? [Select 2]

Explanation

There is no route connecting your VPC back to the on premise data center. You need to add this route to the route table and then enable propagation on the Virtual Private Gateway.

DynamoDB - size limitation on the Attribute Name & Value

Auto Scaling cool-down timers

Auto Scaling – scaling in - <https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-instance-termination.html>

AWS reserves first four and last one IP address in a subnet

Which of the following RDS database engines have a limit to the number of databases that can run per instance? [Select 2]

Explanation

Both the Oracle and SQL Server database engines have limits to how many databases that can run per instance. Primarily, this is due to the underlying technology being proprietary and requiring specific licensing to operate. The database engines based on Open Source technology such as Aurora, MySQL, MariaDB or PostgreSQL have no such limits.

In addition to choosing the correct EBS volume type for your specific task, what else can be done to increase the performance of your volume? [Select 3]

* Schedule snapshots of HDD based volumes for periods of lower use
* Ensure that your EC2 instances are types that can be optimized for use with EBS
* Stripe volumes together in a RAID 0 configuration

Explanation

There are a number of ways you can optimise performance above that of choosing the correct EBS type. One of the easiest options is to drive more I/O throughput than you can provision for a single EBS volume, by striping using RAID 0. You can join multiple gp2, io1, st1, or sc1 volumes together in a RAID 0 configuration to use the available bandwidth for these instances. You can also choose an EC2 instance type that supports EBS optimisation. This ensures that network traffic cannot contend with traffic between your instance and your EBS volumes. The final option is to manage your snapshot times, and this only applies to HDD based EBS volumes. When you create a snapshot of a Throughput Optimized HDD (st1) or Cold HDD (sc1) volume, performance may drop as far as the volume's baseline value while the snapshot is in progress. This behaviour is specific to these volume types. Therefore you should ensure that scheduled snapshots are carried at times of low usage. The one option on the list which is entirely incorrect is the option that states "Never use HDD volumes, always ensure that SSDs are used" as the question first states "In addition to choosing the correct EBS volume type for your specific task". HDDs may well be suitable to certain tasks and therefore they shouldn't be discounted because they may not have the highest specification on paper.

When editing permissions (policies and ACLs), to whom does the concept of the "Owner" refer?

* The Owner refers to the identity and email address used to create the AWS account.

Which of the following strategies does AWS use to deliver the promised levels of DynamoDB performance? [Select 2]

* Data is on SSD’s
* The Database is partitioned across a number of nodes

Explanation

DynamoDB makes use of parallel processing to achieve predictable performance. You visualise each partition as an independent DB server of fixed size. Each responsible for a defined block of data. In SQL terminology it is called sharding. The documentation is specific about the SSDs, but makes no mention of read-replicas or EBS-Optimised. Caching in-front of DDB is an option (DAX), but it is not inherent to DDB.

Question 42: Incorrect

You work for a large media organization who has traditionally stored all their media on large SAN arrays. After evaluating AWS, they have decided to move their storage to the cloud. Staff will store their personal data on S3, and will have to use their Active Directory credentials in order to authenticate. These items will be stored in a single S3 bucket, and each staff member will have their own folder within that bucket named after their employee ID. Which of the following steps should you take in order to help set this up? [Select 3]

* Create either a federation proxy or identity provider
* Use AWS security token service to create temporary tokens
* Create an IAM role

Explanation

You cannot tag individual folders within an S3 bucket. If you create an individual user for each staff member, there will be no way to keep their active directory credentials synched when they change their password. You should either create a federation proxy or identity provider and then use AWS security token service to create temporary tokens. You will then need to create the appropriate IAM role for which the users will assume when writing to the S3 bucket.

The essence of a stateless installation is that the scalable components are disposable, and configuration is stored away from the disposable components

Which of the following are valid S3 data encryption options? [Select 4]

* The valid ways of encrypting data on S3 are Server Side Encryption (SSE)-S3, SSE-C, SSE-KMS or a client library such as Amazon S3 Encryption Client.

Question 47: Correct

You're building out a single-region application in us-west-2. However, disaster recovery is a strong consideration, and you need to build the application so that if us-west-2 becomes unavailable, you can fail-over to us-west-1. Your application relies exclusively on pre-built AMI's. In order to share those AMI's with the region you're using as a backup, which process would you follow?

* Copy the AMI from us-west-2, manually apply launch permissions, user-defined tags, and Amazon S3 bucket permissions of the default AMI to the new instance, and launch the instance

Explanation

AWS does not copy launch permissions, user-defined tags, or Amazon S3 bucket permissions from the source AMI to the new AMI.

Question 48: Incorrect

How is the Public IP address managed in an instance session via the instance GUI/RDP or Terminal/SSH session?

* The public IP address is not managed on the instance: it is, instead, an alias applied as a network address translation of the Private IP address

For all new accounts, there is a soft limit of 20 EC2 instances per region

Question 54: Incorrect

Your server logs are full of what appear to be application-layer attacks, so you deploy AWS Web Application Firewall. Which of the following conditions may you set when configuring AWS WAF? [Select 3]

* String Match Conditions
* IP Match Conditions
* Size Constraint Conditions

Question 55: Correct

By definition, a public subnet within a VPC is one that \_\_\_\_\_\_\_\_.

* Has at least one route in its routing table that uses an Internet Gateway (IGW).

Question 61 – check later

Question 64: Incorrect

You are a consultant planning to deploy DynamoDB across three AZs. Your lead DBA is concerned about data consistency. Which of the following do you advise the lead DBA to do?

* To ask the development team to code for strongly consistent reads. Will lead to increased cost

Explanation

The term consistency has specific meaning in relationship to DynamoDB. (due to its distributed nature?)

Question 65: Correct

Which of the following options allows users to have secure access to private files located in S3? [Select 3]

Explanation

There are three options in the question which can be used to secure access to files stored in S3 and therefore can be considered correct. Signed URLs and Signed Cookies are different ways to ensure that users attempting access to files in an S3 bucket can be authorised. One method generates URLs and the other generates special cookies but they both require the creation of an application and policy to generate and control these items. An Origin Access Identity on the other hand, is a virtual user identity that is used to give the CloudFront distribution permission to fetch a private object from an S3 bucket. Public S3 buckets should never be used unless you are using the bucket to host a public website and therefore this is an incorrect option.

Question 67: Incorrect

A client is concerned that someone other than approved administrators is trying to gain access to the Linux web app instances in their VPC. She asks what sort of network access logging can be added. Which of the following might you recommend? [Select 3]

* Set up a Flow Log for the group of instances and forward them to CloudWatch
* Set up a Flow Log for the group of instances and forward them to S3
* Make use of an OS level logging tools such as iptables and log events to CloudWatch or S3

Question 68 – Revisit later

Question 71: Incorrect

You are a systems administrator and you need to monitor the health of your production environment. You decide to do this using CloudWatch. However, you notice that you cannot see the health of every important metric in the default dashboard. When monitoring the health of your EC2 instances, for which of the following metrics do you need to design a custom CloudWatch metric?

* Memory Usage

Explanation

Remember under the shared security model that AWS can see the instance, but not inside the instance to what it is doing. AWS can see that you have Memory, but how much of the memory is being used cannot be seen by AWS. In the case of CPU AWS can see how much of CPU you are using, but cannot see what you are using if for.

Reduced Redundancy Storage is the only S3 Class that does not offer 99.999999999% durability

Question 74: Incorrect

Your company has asked you to investigate the use of KMS for storing and managing keys in AWS. From the options listed below, what key management features are available in KMS?

* Import your own keys, disable and re-enable keys and define key management roles in IAM

Explanation

There are many features which are native to the KMS service. However, of the above, only import your own keys, disable and re-enable keys and define key management roles in IAM are valid. Importing keys into a custom key store and migrating keys from the default key store to a custom key store are not possible. Lastly operating as a private, native HSM is a function of CloudHSM and is not possible directly within KMS.