Return to Review

Attempt 1

All Questions

Question 1: Skipped

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?

- 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. **(Correct)**
- 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

Explanation

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

Question 2: Skipped

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

- A. 10 days
- B. 15 days **(Correct)**

C. 1 month

D. 1 year

Explanation

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/

Question 3: Skipped

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

A. Security Groups

B. NACL Groups

C. Parameter Groups **(Correct)**

D. IAM Roles.

Explanation

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

Question 4: Skipped

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

A. Create a copy of the EBS volume (not a snapshot)

B. Store a snapshot of the volume **(Correct)**

C. Download the content to an EC2 instance

D. Back up the data in to a physical disk

Explanation

After you no longer need an Amazon EBS volume, you can delete it. After deletion, its data is gone and the volume can't be attached to any instance. However, before deletion, you can store a snapshot of 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

Question 5: Skipped

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?

A. Multiple IP address

B. Public IP address

C. Private IP address **(Correct)**

D. Elastic IP Address

Explanation

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

Question 6: Correct

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

A. On the local server within Elastic beanstalk

B. AWS S3 (Correct)

C. AWS Cloudtrail

D. AWS DynamoDB

Explanation

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/

Question 7: Skipped

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?

A. It allows to integrate on-premises IT environments with Cloud Storage. (Correct)

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.

Explanation

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. You have primarily 2 types of volumes 1) Gateway-cached volumes allow you to utilize Amazon S3 for your primary data, while retaining some portion of it locally in a cache for frequently accessed data. 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/

Question 8: Skipped

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

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/ **(Correct)**

Explanation

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

Question 9: Skipped

When you disable automated backups for aws rds, what are you compromising on? Choose on answer from the options given below

A. Nothing, you are actually saving resources on aws

B. You are disabling the point-in-time recovery. **(Correct)**

C. Nothing really, you can still take manual backups.

D. You cannot disable automated backups in RDS.

Explanation

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. For more information on Automated backups, please visit http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_WorkingWithAutomatedBackups.html

Question 10: Skipped

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?

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.

- B. Send all the log events to Amazon Kinesis develop a client process to apply heuristics on the logs **(Correct)**
- 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

Explanation

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/

Question 11: Skipped

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

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

Explanation

Amazon RDS detects and automatically recovers from the most common failure scenarios for Multi-AZ deployments so that you can resume database operations as quickly as possible without administrative intervention. Amazon RDS automatically performs a failover in the event of any of the following: 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/

Question 12: Skipped

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

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. **(Correct)**

Explanation

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 http://docs.aws.amazon.com/cli/latest/reference/ec2/revoke-security-group-ingress.html

Question 13: Skipped

What is the durability of S3 RRS?

A. 99.99% **(Correct)**

B. 99.95%

C. 99.995%

D. 99.999999999%

Explanation

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/

Question 14: Skipped

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

A. Amazon SES

B. Amazon Cloudtrail

C. Amazon CloudFront **(Correct)**

D. Amazon S3

Explanation

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/

Question 15: Skipped

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

A. Security group **(Correct)**

B. ACL

C. IAM

D. Private IP Addresses

Explanation

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

Question 16: Skipped

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

A. 2 **(Correct)**

B. 3

C. 4

D. 1

Explanation

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)

Question 17: Skipped

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

- A. Yes
- B. Only with MSSQL based RDS
- C. Only for Oracle RDS instances
- D. No **(Correct)**

Explanation

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

Question 18: Skipped

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

- A. Amazon VPC **(Correct)**
- B. Amazon ServiceBus
- C. Amazon EMR
- D. Amazon RDS

Explanation

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/

Question 19: Skipped

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

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

Explanation

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/

Question 20: Skipped

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

- ( ) 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 **(Correct)**

Explanation

You can easily add tags which define which instances are production and which are development 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

Question 21: Skipped

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

- 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 **(Correct)**

Explanation

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

Question 22: Skipped

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

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

Explanation

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/

Question 23: Skipped

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.

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

Explanation

Find more details here : https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Stop_Start.html 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

Question 24: Skipped

Your company currently has an on-premise infrastructure. They are currently running low on storage and want to have the ability to extend their storage on to the cloud. Which of the following AWS services can help achieve this purpose.

- ( ) A. Amazon EC2
- (•) B. Amazon Storage gateways **(Correct)**
- ( ) C. Amazon Storage devices
- ( ) D. Amazon SQS

Explanation

The AWS Documentation mentions the following on storage gateways AWS Storage Gateway connects an on-premises software appliance with cloud-based storage to provide seamless integration with data security features between your on-premises IT

environment and the Amazon Web Services (AWS) storage infrastructure. You can use the service to store data in the AWS Cloud for scalable and cost-effective storage that helps maintain data security. For more information on Storage gateways , please refer to the below URL: http://docs.aws.amazon.com/storagegateway/latest/userguide/WhatIsStorageGateway.html

Question 25: Skipped

If you want to process data in real-time, what AWS service should you use? Choose the correct answer from the options below.

- A. Kinesis **(Correct)**
- B. DynamoDB
- C. Elastic MapReduce
- D. Redshift

Explanation

Amazon Kinesis is a platform for streaming data on AWS, offering powerful services to make it easy to load and analyze streaming data, and also providing the ability for you to build custom streaming data applications for specialized needs. Web applications, mobile devices, wearables, industrial sensors, and many software applications and services can generate staggering amounts of streaming data – sometimes TBs per hour – that need to be collected, stored, and processed continuously. Amazon Kinesis services enable you to do that simply and at a low cost. For more information on Kinesis, please refer to the below link https://aws.amazon.com/kinesis/

Question 26: Skipped

After a Amazon Kinesis consumer consumes the records of a stream , which are the preferred data stores to where all can the consumer store the resulting records. Choose 3 answers from the options given below:

- A. Amazon S3 **(Correct)**
- B. DynamoDB **(Correct)**
- C. Amazon Redshift **(Correct)**
- D. SQS

Explanation

In Amazon Kinesis , the producers continually push data to Streams and the consumers process the data in real time. Consumers can store their results using an AWS service such as Amazon DynamoDB, Amazon Redshift, or Amazon S3. Its better to put the records to a persistent data store for any further processing at a later point in time. For more information on the key concepts of Amazon Kinesis, please refer to the below link: http://docs.aws.amazon.com/streams/latest/dev/key-concepts.html

Question 27: Skipped

Your company is currently running EC2 instances in the Europe region. These instances are based on pre-built AMI's. They now want to implement disaster recovery. What are one of the steps they would need to implement for disaster recovery? Choose the correct answer from the options given below

- A. Copy the AMI from the current region to another region, modify any Auto Scaling groups if required in the backup region to use the new AMI ID in the backup region **(Correct)**
- B. Modify the image permissions to share the AMI with another account, then set the default region to the backup region
- C. Nothing, because all AMI's are available in any region as long as it is created within the same account
- D. Modify the image permissions to share to the designated backup region

Explanation

In order to implement disaster recovery you need to copy the AMI to the desired region, since AMI's are different region wise. For more information on AMI's, please visit the below url http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html

Question 28: Skipped

You are using IOT sensors to monitor all data by using Kinesis with the default settings. You then send the data to an S3 bucket after 2 days. When you go to interpret the data in S3 there is only data for the last day and nothing for the first day. Which of the following is the most probable cause of this? Choose the correct answer from the options below

- A. Temporary loss of IoT device
- B. You cannot send Kinesis data to the same bucket on consecutive days.
- C. Data records are only accessible for a default of 24 hours from the time they are added to a stream. **(Correct)**
- D. The access to the S3 bucket is not given to the Kinesis stream

Explanation

By default, Records of a stream are accessible for up to 24 hours from the time they are added to the stream. You can raise this limit to up to 7 days by enabling extended data retention. So since the Kinesis stream is created with the default settings, the streams are not being added to S3 for one day. For more information on Kinesis streams , please visit the below url https://aws.amazon.com/kinesis/streams/faqs/

Question 29: Skipped

You are configuring EC2 instances in a subnet which currently is in a VPC with an Internet gateway attached. All of these instances are able to be accessed from the internet. You then launch another subnet and launch an EC2 instance in it, but you are not able to access the EC2 instance from the internet. What could be the possible two reasons for this? Select 2 options.

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

Explanation

The subnet could have created as a private subnet and not either not have the Route table updated with the internet gateway and the public IP is not attached to the EC2 instance. For more information on VPC and subnets, please visit the below url http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2.html

Question 30: Skipped

You are the system administrator for your company's AWS account of approximately 100 IAM users. A new company policy has just been introduced that will change the access of 20 of the IAM users to have a particular sort of access to S3 buckets. How can you implement this effectively so that there is no need to apply the policy at the individual user level? Choose the correct answer from the options below

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

Explanation

The best option is to group the set of users in a group and then apply a policy with the required access to the group. For more information on IAM Groups, please visit the below url http://docs.aws.amazon.com/IAM/latest/UserGuide/id_groups.html

Question 31: Skipped

As a system administrator, you have been requested to implement the best practices for using Autoscaling, SQS and EC2. Which of the following items is not a best practice?

- A. Use the same AMI across all regions **(Correct)**
- B. Utilize AutoScaling to deploy new EC2 instances if the SQS queue grows too large
- C. Utilize CloudWatch alarms to alert when the number of messages in the SQS queue grows too large
- D. Utilize an IAM role to grant EC2 instances permission to modify the SQS queue

Explanation

The AMI's differ from the region to region, hence this is a not a required practice. You need to copy the AMI from region to region if you want to implement disaster recovery as a best practise. For more information on AMI's, please visit the below url http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html

Question 32: Skipped

A company is currently using Autoscaling for their application. A new AMI now needs to be used for launching the Ec2 instances. Which of the following changes needs to be carried out. Choose an answer from the options below

- A. Nothing, you can start directly launching instances in the Autoscaling group
- B. Create a new launch configuration **(Correct)**
- C. Create a new target group
- D. Create a new target group and launch configuration

Explanation

Since the AMI is changed, you need to create a new launch configuration that can be used by the Autoscaling group. For more information on Launch configuration, please visit the below url http://docs.aws.amazon.com/autoscaling/latest/userguide/LaunchConfiguration.html

Question 33: Skipped

In order to add current EC2 instances to an Autoscaling group, which of the following criteria must be met. Choose 3 options from the answers given below

- A. The instance is in the stopped state.

B. The AMI used to launch the instance must still exist. **(Correct)**

C. The instance is not a member of another Auto Scaling group. **(Correct)**

D. The instance is in the same Availability Zone as the Auto Scaling group. **(Correct)**

Explanation

This is given in the aws documentation For more information on adding instances to Autoscaling groups, please visit the below url http://docs.aws.amazon.com/autoscaling/latest/userguide/attach-instance-asg.html

Question 34: Skipped

When designing an application architecture utilizing EC2 instances and the ELB, to determine the instance size required for your application what questions might be important? Choose the 2 correct answers from the options below

A. Determine the required I/O operations **(Correct)**

B. Determining the minimum memory requirements for an application **(Correct)**

C. Determining where the client intends to serve most of the traffic

D. Determining the peak expected usage for a clients application

Explanation

When designing which EC2 instances to use, you need to know the I/O and memory requirements. These are some of the core components of an Ec2 instance type. For more information on EC2 instance types, please visit the below url https://aws.amazon.com/ec2/instance-types/

Question 35: Skipped

You have an order processing system which is currently using SQS. It was noticed that an order was processed twice which had led to great customer dissatisfaction. Your management has requested that this should not happen in the future. What can you do to avoid this happening in the future? Choose an answer from the options given below

A. Change the retention period of SQS

B. Change the visibility timeout of SQS

C. Change the system to use SWF **(Correct)**

D. Change the message size in SQS

Explanation

Amazon SWF promotes a separation between the control flow of your background job's stepwise logic and the actual units of work that contain your unique business logic. This allows you to separately manage, maintain, and scale "state machinery" of your application from the core business logic that differentiates it. As your business requirements change, you can easily change application logic without having to worry about the underlying state machinery, task dispatch, and flow control. When you use SWF you are guaranteed that a message will be processed only once. For more information on SWF, please visit the below url https://aws.amazon.com/swf/

Question 36: Skipped

You have a couple of EC2 instances that have just been added to an ELB. You have verified that the right security groups are open for port 80 for HTTP. But the EC2 instances are still showing out of service. What could be one of the possible reasons for this? Choose an answer from the options given below

A. The EC2 instances are using the wrong AMI

B. The page used for the health check does not exist on the EC2 instance **(Correct)**

C. The wrong instance type was used for the EC2 instance

D. The wrong subnet was used

Explanation

When defining a health check, in addition to the port number and protocol , you have to also define the page which will be used for the health check. If you don't have the page defined on the web server then the health check will always fail. For more information on Health checks, please visit the below url http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-healthchecks.html

Question 37: Skipped

Your web application front end consists of multiple EC2 instances behind an Elastic Load Balancer. You configured ELB to perform health checks on these EC2 instances, if an instance fails to pass health checks, which statement will be true?

A. The instance gets terminated automatically by the ELB.

B. The instance gets quarantined by the ELB for root cause analysis.

C. The instance is replaced automatically by the ELB.

D. The ELB stops sending traffic to the instance that failed its health check **(Correct)**

Explanation

To discover the availability of your EC2 instances, a load balancer periodically sends pings, attempts connections, or sends requests to test the EC2 instances. These tests are called health checks. The status of the instances that are healthy at the time of the health check is InService. The status of any instances that are unhealthy at the time of the health check is OutOfService. The load balancer performs health checks on all registered instances, whether the instance is in a healthy state or an unhealthy state. The load balancer routes requests only to the healthy instances. When the load balancer determines that an instance is unhealthy, it stops routing requests to that instance. The load balancer resumes routing requests to the instance when it has been restored to a healthy state. You can see the status of the instance in the Registered Instances section of the load balancer.

Question 38: Skipped

A company is currently SWF for their order processing. Some of the orders seem to be stuck for 3 weeks. What could be the possible reason for this? Choose the correct answer from the options below

- A. SWF is awaiting human input from an activity task. **(Correct)**
- B. The last task has exceeded SWF's 14-day maximum task execution time
- C. The workflow has exceeded SWF's 14-day maximum workflow execution time
- D. SWF is not the right service to be used

Explanation

The issue is probably due to the fact they maybe a human interaction such as an approval is required for the orders to be further processed. For more information on SWF, please visit the below url https://aws.amazon.com/swf/

Question 39: Skipped

You have a web application running on six Amazon EC2 instances, consuming about 45% of resources on each instance. You are using auto-scaling to make sure that six instances are running at all times. The number of requests this application processes is consistent and does not experience spikes. The application is critical to your business and you want high availability at all times. You want the load to be distributed evenly between all instances. You also want to use the same Amazon Machine Image (AMI) for all instances. Which of the following architectural choices should you make?

- A. Deploy 6 EC2 instances in one availability zone and use Amazon Elastic Load Balancer.
- B. Deploy 3 EC2 instances in one region and 3 in another region and use Amazon Elastic Load Balancer.
- C. Deploy 3 EC2 instances in one availability zone and 3 in another availability zone and use Amazon Elastic Load Balancer. **(Correct)**
- D. Deploy 2 EC2 instances in three regions and use Amazon Elastic Load Balancer.

Explanation

Option A is automatically incorrect because remember that the question asks for high availability. For option A, if the AZ goes down then the entire application fails. For Option B and D, the ELB is designed to only run in one region in aws and not across multiple regions. So these options are wrong. The right option is C. The below example shows an Elastic Loadbalancer connected to 2 EC2 instances connected via Auto Scaling. This is an example of an elastic and scalable web tier. By scalable we mean that the Auto scaling process will increase or decrease the number of EC2 instances as required.

Question 40: Skipped

When you put objects in Amazon S3, what is the indication that an object was successfully stored?

- A. HTTP 200 result code and MD5 checksum, taken together, indicate that the operation was successful. **(Correct)**
- B. Amazon S3 is engineered for 99.999999999% durability. Therefore there is no need to confirm that data was inserted.
- C. A success code is inserted into the S3 object metadata.
- D. Each S3 account has a special bucket named _s3_logs. Success codes are written to this bucket with a timestamp and checksum.

Explanation

When an object is placed in S3, it is done via HTTP via a POST or PUT object request. When a success occurs, you will get a 200 HTTP response. But since a 200 Response can also contain error information, a check of the MD5 checksum confirms on whether the request was a success or not. For more information on the POST request for an object in S3, please visit the link: http://docs.aws.amazon.com/AmazonS3/latest/API/RESTObjectPOST.html For more information on the PUT request for an object in S3, please visit the link: http://docs.aws.amazon.com/AmazonS3/latest/API/RESTObjectCOPY.html

Question 41: Skipped

An instance is launched into a VPC subnet with the network ACL configured to allow all inbound traffic and deny all outbound traffic. The instance's security group is configured to allow SSH from any IP address and deny all outbound traffic. What changes need to be made to allow SSH access to the instance?

- A. The outbound security group needs to be modified to allow outbound traffic.
- B. The outbound network ACL needs to be modified to allow outbound traffic. **(Correct)**
- C. Nothing, it can be accessed from any IP address using SSH.
- D. Both the outbound security group and outbound network ACL need to be modified to allow outbound traffic.

Explanation

For an EC2 instance to allow SSH, you can have 'Allow' configuration for both Security and Network ACL for Inbound Traffic. For Outbound Traffic 'Allow' for Network ACL and 'Deny' for Security The reason why Network ACL has to have both an Allow for Inbound and Outbound is because network ACL's are stateless. Responses to allowed inbound traffic are subject to the rules for outbound traffic (and vice versa). Whereas for Security groups, responses are stateful. So if an incoming request is granted, by default and outgoing request will also be granted.

Question 42: Skipped

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

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

Explanation

An IAM group is used to collectively manage users who need the same set of permissions. By having groups, it becomes easier to manage permissions. So if you change the permissions on the group scale, it will affect all the users in that group. Please find the steps below for the group creation. Step 1) Go to IAM and click on the Groups section. Click on Create New Group. Step 2) Provide a name for the Group Step 3) Next you need to attach a policy. Since the question asks that this group needs full access to S3 , choose the AmazonS3FullAccess role. Step 4) Once the group is created, you can then add the 50 users to the group For more information on users and groups, please visit the url - http://docs.aws.amazon.com/IAM/latest/UserGuide/id.html

Question 43: Skipped

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

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

Explanation

As per the shared responsibility shown below, the users are required to control the EC2 security via security groups and network access control layers. Also it is the user's responsibility model, aws takes care of the physical components and the infrastructure to provide Virtualization. For more information on aws shared responsibility model, please visit the link
- https://aws.amazon.com/blogs/security/tag/shared-responsibility-model/

Question 44: Skipped

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

- A. DynamoDB **(Correct)**
- B. ElasticMap Reduce
- C. Amazon RDS
- D. SimpleDB

Explanation

DynamoDB is an aws service that provides a NoSQL database option to users. DynamoDB is a hosted solution by aws , there is no requirement to manage the environment for DynamoDB. And the question clearly states there are no resources in place to manage the DynamoDB environment. DynamoDB lets you offload the administrative burdens of operating and scaling a distributed database, so that you don't have to worry about hardware provisioning, setup and configuration, replication, software patching, or cluster scaling. ElasticMapReduce is not a NoSQL solution. SimpleDB is a simplified DB solution given by aws and hence is not a solution. For more information on DynamoDB, please visit the link
- http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Introduction.html

Question 45: Skipped

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

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

Explanation

Encryption in aws needs to be done by the users and can be done on different levels. For EBS , we can enable encryption at the volume level. This can be done when the volume Is created, this is shown in the screenshot below. On S3, For any object you can enable server side encryption by going to the Permissions section of the object in S3 and enable the server side encryption option. And finally , one can use Linux based tools to Encrypt a volume if it is not encrypted.

Question 46: Skipped

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

- [ ] A. Cached session data
- [x] B. Infrequently accessed data **(Correct)**
- [x] C. Data archives **(Correct)**
- [ ] D. Active database storage

Explanation

Amazon Glacier is an extremely low-cost storage service that provides secure, durable, and flexible storage for data backup and archival. So Amazon glacier is used for Infrequently accessed data and Data archives. For Cached Data Session , the service provided by aws is known as elastic cache. So Amazon glacier is the wrong option. For Active database storage , this is done via EBS volumes , so this option is also incorrect. For more information on Amazon Glacier , please visit the link - https://aws.amazon.com/glacier/faqs/

Question 47: Skipped

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

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

Explanation

The best practise for IAM is to create roles which has specific access to an AWS service and then give the user permission to the AWS service via the role. To get the role in place , follow the below steps Step 1) Create a role which has the required ELB access Step 2) You need to provide permissions to the underlying EC2 instances in the Elastic Load Balancer For the best practises on IAM policies, please visit the link: http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-user.html

Question 48: Skipped

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

- A. CloudTrail for security logs **(Correct)**
- B. S3 logging
- C. Encrypted data storage
- D. Multi Factor Authentication

Explanation

AWS Cloudtrail is the defacto service provided by aws for monitoring all API calls to AWS and is used for logging and monitoring purposes for compliance purposes. Amazon cloudtrail detects every call made to aws and creates a log which can then be further used for analysis. For more information on Amazon Cloudtrail , please visit the link – https://aws.amazon.com/cloudtrail/

Question 49: Skipped

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

- A. Elastic Beanstalk **(Correct)**
- B. EC2 **(Correct)**
- C. DynamoDB
- D. RDS

Explanation

EC2 and Elastic Beanstalk are aws services that allow the developer access to the underlying infrastructure. When you create an Elastic beanstalk environment as shown below , you will have access to the underlying EC2 instance. So in the below example

for the Elastic beanstalk environment , you will have access to the Windows Server 2012 environment. DynamoDB and RDS are services provided and the infrastructure is managed by aws.

Question 50: Skipped

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

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

Explanation

To protect objects in S3 from both accidental deletion and accidental overwriting, the methodology adopted by aws is to Enable versioning on the bucket. Versioning allows to store every version of an object , so that if by mistake there is a version deleted , you can recover other versions, because the entire object is not deleted. Enable Multi-Factor Authentication (MFA) protected access on S3 is only used to add an additional security layer to S3. So that users who are authenticated properly before having access to the bucket. But this is not what the question is asking. To enable versioning on S3 , you need to go to the bucket , and in the properties , you can enable versioning.

Question 51: Skipped

By default is data in S3 encrypted?

- A. Yes, S3 always encrypts data for security purposes.
- B. Yes, but only in government cloud data centers
- C. No, but it can be when the right APIs are called for SSE **(Correct)**
- D. No, it must be encrypted before upload of any data to S3.

Explanation

Please note that, no , by default , Encryption is not enabled. So option A and B are incorrect. Also note that it is not necessary to encrypt before every upload. For any object you can enable server side encryption by going to the Permissions section of the object in S3 and enable the server side encryption option. For more information on Encryption for S3 , please refer to the link - http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html

Question 52: Skipped

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

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

Explanation

Reserved Instances provide a significant discount (up to 75%) compared to On-Demand instance pricing. There is a fixed quote of reserved power that it is given to the account. You have the Flexibility to change families, OS types, and tenancies while benefitting from Reserved Instance pricing. Now reserved instances are bought upfront for a specified duration. Unlike On-demand instances, there is no cost difference if you stop the instances, so option A is incorrect. Since you have already bought the reserved instances, you cannot ask aws to recover the costs. The only 2 options available are to terminate the instances immediately and sell them on AWS Reserved Instance Marketplace for a specified price. Note that all Reserved Instances are grouped according to the duration of the term remaining and the hourly price in the market place. Hence, terminating the instance immediately would help to save remaining term. You can purchase reserved instances from the reserved instances section in the EC2 dashboard. In the next screen, you can choose the reserved instance to buy. But you are making an upfront commitment to buy the instances. For more information on reserved instances please follow the link - https://aws.amazon.com/ec2/pricing/reserved-instances/

Question 53: Skipped

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

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

Explanation

The question asks for Encryption at rest for S3, so any answer related to EBS encryption does not correspond to the right answer. For any object you can enable server side encryption by going to the Permissions section of the object in S3 and enable the server side encryption option. And then for client side encryption, you can encrypt the object and send it to S3 when you

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

Question 54: Skipped

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

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

Explanation

If you look at the SQS FAQ, it is clearly mentioned that SQS messages are guaranteed to be delivered at least once. The message size for SQS can be 256KB in size. The message formats can be in XML, JSON and unformatted text. The messages can live in the queue for a maximum of 14 days. For more information on SQS messages, please follow the link
https://aws.amazon.com/sqs/faqs/

Question 55: Skipped

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

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

Explanation

Anything that is stored on an instance store volume is destroyed when the instance is shutdown. Instance store volumes are ephemeral, which means that they only survive when the instance is active. EBS backed Volumes are not ephemeral and exists even if the instance is stopped and started, so Option B is wrong. Even if EBS volume is not big enough, it does not mean that it will not be present when the instance is stopped and started, so Option C is wrong. If the instance is compromised, then the instance would not even start , so Option C is wrong. For more information on instance store volumes, please visit http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/InstanceStorage.html

Question 56: Skipped

What database services are provided by aws from the list mentioned below. Choose the 3 correct answers.

- [x] A. Aurora **(Correct)**
- [x] B. MariaDB **(Correct)**
- [x] C. MySQL **(Correct)**
- [ ] D. DB2

Explanation

DB2 is the only database service not provided by AWS. For the list of DB services , please visit the link - https://aws.amazon.com/rds/ For more information on Aurora , please visit the link - https://aws.amazon.com/rds/aurora/ For more information on mySQL , please visit the link - https://aws.amazon.com/rds/mysql/ For more information on MariaDB , please visit the link - https://aws.amazon.com/rds/mariadb/

Question 57: Skipped

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

- (x) A. Amazon Import/Export **(Correct)**
- ( ) B. Amazon Direct Connect
- ( ) C. Amazon S3 MultiPart Upload
- ( ) D. Amazon S3 Connector

Explanation

AWS Import/Export is a service that accelerates transferring large amounts of data into and out of AWS using physical storage appliances, bypassing the Internet. For Amazon S3 Multipart Upload, there are the following restrictions, so then it's better to use the Amazon Import/Export. For more information on aws import/export, please visit the link - https://aws.amazon.com/snowball/ Amazon Direct Connect is used as a connection between AWS and On-premise so this is the wrong option.

Question 58: Skipped

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

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

Explanation

In aws , there are regions with each region separated in a seperate geographic area. Each region has multiple, isolated locations known as Availability Zones. An availability zone is used to host resources in a specific region. For more information on Regions and availability zone, please visit the url - http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html An edge location is used to deliver content depending on the location of the user. So if the user is located in Australia, the Australia region can be used to deliver content. If a user was in Australia and you delivered content in Asia , there would a delay in the relay of information to the user. Each edge location synchronizes data so that integrity of data is maintained across all edge locations. For more information on Edge locations, please visit the url – https://aws.amazon.com/about-aws/global-infrastructure/

Question 59: Skipped

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

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

Explanation

This is a tricky question and note that Options A,B and D can be used to decrease the likelihood of duplicate messages , but cannot remove the change entirely. For option A , even if the code is inserted , which should be the case already , if the EC2 instance goes down , the same issue can occur again. The message will not be deleted and when it comes in the SQS queue , it will be processed again. For option B , even if you increase the visibility timeout , if the process has taken the message but not deleted the message , after the visibility timeout expires , the EC2 instance will again process the message and the same issue will happen again. If you use long polling instead of short polling , you still have the same problem with Option A and B. For more information on SQS , please visit the link – https://aws.amazon.com/sqs/faqs/

Question 60: Skipped

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

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

Explanation

Below is a sample VPC from the aws VPC guides. For an instance to be available from the internet , you need to ensure 1) The Internet gateway is in place – This is has been confirmed in the question. 2) There is a route entry for the internet gateway – This should be in place , because out of the 2 instances , one is working. 3) The EC2 instance should have a public or Elastic IP – From the question , there is no mention of one being allocated to the problem instance. Hence option D is the right answer. For more information on VPC public subnets , please visit the url
- http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario1.html

Question 61: Skipped

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

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

Explanation

A bastion host is a special purpose computer on a network specifically designed and configured to withstand attacks. The computer generally hosts a single application, for example a proxy server, and all other services are removed or limited to reduce the threat to the computer. In AWS , A bastion host is kept on a public subnet. Users log on to the bastion host via SSH or RDP and then use that session to manage other hosts in the private subnets. This is a security practise adopted by many organization to secure the assets in their private subnets.

Question 62: Skipped

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

- A. An apology for the delay in processing requests and telling them that unfortunately they have to resubmit all the requests.
- B. An apology for the delay in processing requests, assurance that the application will be operational shortly, and a note that requests greater than five days old will need to be resubmitted.
- C. An apology for the delay in processing requests, assurance that the application will be operational shortly, and a note that all received requests will be processed at that time. **(Correct)**
- D. An apology for the delay in processing requests and telling them that unfortunately they have to resubmit all the requests since the queue would not be able to process the 2000 messages together.

Explanation

Since the question states that the SQS is configured with the maximum retention period , it means that messages can last for 14 days. So option A is invalid , since the messages will still be in the queue even after 10 days Option B is invalid for the same reason noted in Option B Option D is invalid because a queue can have up to 120,000 messages. For more information on SQS , please visit the link: https://aws.amazon.com/sqs/

Question 63: Skipped

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

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

D. Enable short polling on the SQS message by setting the ReceiveMessageWaitTimeSeconds to a number = 0

Explanation

By default an SQS queue is configured with Shortpolling , which means that the queue is polled every so often for new messages. There is an option of long polling which allows for a shorter poll time but taking in more messages during the long polling cycle. In order to reduce the number of polling cycles , it better to have bigger gaps by enabling long polling. And this can be done by setting the ReceiveMessageWaitTimeSeconds attribute of the queue to a value greater than 0. You can do this by changing the queue attributes as shown below Answer - B For more information on polling, please visit the link
- http://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-long-polling.html

Question 64: Skipped

Your company has resources set up on the AWS Cloud. Your company is now going through a set of scheduled audits by an external auditing firm. Which of the following services can be utilized to help ensure the right information is present for auditing purposes.

A. AWS CloudTrail **(Correct)**

B. AWS VPC

C. AWS EC2

D. AWS Cloudwatch

Explanation

The AWS Documentation mentions the following on Cloudtrail AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting. For more information on Cloudtrail, please refer to the below URL: https://aws.amazon.com/cloudtrail/

Question 65: Skipped

Which of the following will incur a cost when working with AWS resources. Choose 2 answers from the options given below

A. A running EC2 Instance **(Correct)**

B. A stopped EC2 Instance

C. EBS Volumes attached to stopped EC2 Instances **(Correct)**

D. Using an Amazon VPC

Explanation

The AWS Documentation clearly mentions the cost to EC2 Instances Billing commences when Amazon EC2 initiates the boot sequence of an AMI instance. Billing ends when the instance terminates, which could occur through a web services command, by running "shutdown -h", or through instance failure. When you stop an instance, we shut it down but don't charge hourly usage for a stopped instance, or data transfer fees, but we do charge for the storage for any Amazon EBS volumes. For more information, please visit the below URL: https://aws.amazon.com/ec2/faqs/ The AWS Documentation clearly mentions the cost with regards to the VPC There are no additional charges for creating and using the VPC itself. For more information, please visit the below URL: https://aws.amazon.com/vpc/faqs

Question 66: Skipped

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

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

Explanation

This question is not that complicated, even though if you don't understand the options. By default when you see "collection of logs and processing of logs", directly think of AWS EMR. Amazon EMR provides a managed Hadoop framework that makes it easy, fast, and cost-effective to process vast amounts of data across dynamically scalable Amazon EC2 instances. You can also run other popular distributed frameworks such as Apache Spark, HBase, Presto, and Flink in Amazon EMR, and interact with data in other AWS data stores such as Amazon S3 and Amazon DynamoDB. Amazon EMR securely and reliably handles a broad set of big data use cases, including log analysis, web indexing, data transformations (ETL), machine learning, financial analysis, scientific simulation, and bioinformatics. For more information on EMR, please visit the link – https://aws.amazon.com/emr/

Question 67: Skipped

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

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

D. A small EC2 instance and a security group which only allows access on port 22 via your IP address **(Correct)**

Explanation

A bastion host should always be a small EC2 instance, because there is no requirement of applications to run on it. Also you should only open port 22 from your IP address and no other IP Address. In AWS , A bastion host is kept on a public subnet. Users log on to the bastion host via SSH or RDP and then use that session to manage other hosts in the private subnets. This is a security practise adopted by many organization to secure the assets in their private subnets.

Question 68: Skipped

You have a web application hosted in AWS on EC2 Instances. The application provides newspaper content to users around the world. Off late , the load on the web application has increased and is subsequently increasing the response time for the application for end users. Which of the below services can be used to alleviate this problem. Choose 2 answers from the options given below

A. Use Cloudfront and use the web application as the origin **(Correct)**

B. Use AWS Storage gateways to distribute the content across multiple storage devices for better read throughput.

C. Use Elastic cache behind of the web application. **(Correct)**

D. Consider using SQS to process some of the user requests

Explanation

The AWS Documentation provides the following information on Cloudfront and Elastic Cache Amazon CloudFront is a web service that speeds up distribution of your static and dynamic web content, such as .html, .css, .php, and image files, to your users. CloudFront delivers your content through a worldwide network of data centers called edge locations. When a user requests content that you're serving with CloudFront, the user is routed to the edge location that provides the lowest latency (time delay), so that content is delivered with the best possible performance. For more information on AWS Cloudfront, please visit the below URL: http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html 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 visit the below URL: https://aws.amazon.com/elasticache/

Question 69: Skipped

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

A. Multiple Availability Zones

B. Multiple subnets

C. An SQS queue (Correct)

D. An auto scaling group to recover from EC2 instance failures

Explanation

For highly available websites, yes Multiple Availability Zones and Multiple subnets are required. Below is a simple architecture of a highly available website consisting of an ELB and 2 AZ's. BY default each AZ should be located in a different subnet. Also auto-scaling is used to add additional EC2 instances for fault tolerance. SQS is not an option, because SQS is only used to decouple components in an architecture, it is not necessary for a high available web site.

Question 70: Skipped

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

A. 10 TB

B. 5 TB (Correct)

C. 1 TB

D. 5 GB

Explanation

Please refer to the table in the KB Article which gives the restrictions for the Multi-part file upload for S3. From here it clearly shows that the right answer is 5TB. For more information on Multi-part file upload for S3 , please visit the url
- http://docs.aws.amazon.com/AmazonS3/latest/dev/qfacts.html

Question 71: Skipped

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

A. The total volume of data and number of objects you can store are unlimited (Correct)

B. Individual Amazon S3 objects can range in size from a minimum of 0 bytes to a maximum of 1 terabytes

C. You can use Multi-Object Delete to delete large numbers of objects from Amazon S3 (Correct)

D. You can store only objects of a particular format in S3

Explanation

The screenshots are from the S3 FAQ's of AWS. Visit KB Article. Option B is incorrect, because as per the S3 definition, the maximum size of objects can be 5 TB Option D is incorrect because you can virtually store objects of any type For more information on S3 , please visit the URL – https://aws.amazon.com/s3/faqs/

Question 72: Skipped

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

- A. Policy **(Correct)**
- B. Permission
- C. Role
- D. Resource

Explanation

A policy is a JSON document that specifies what a user can do on AWS. This document consists of Actions: what actions you will allow. Each AWS service has its own set of actions. Resources: which resources you allow the action on. Effect: what the effect will be when the user requests access—either allow or deny. Below is a sample snippet of a policy document that allows access to all users to Describe EC2 Instances. You can clearly see the Actions, Resources and Effect which define the policy document. For more information on policies, please visit the url - http://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html

Question 73: Skipped

Which of the following is not required to ensure that you can SSH into a Linux instance hosted in a VPC from the internet.

- A. Private IP Address **(Correct)**
- B. Public IP Address
- C. Internet gateway attached to the VPC
- D. Elastic IP

Explanation

The AWS Documentation provides the following information A private IPv4 address is an IP address that's not reachable over the Internet. You can use private IPv4 addresses for communication between instances in the same network (EC2-Classic or a VPC). For more information on AWS IP Addressing, please visit the below URL: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-instance-addressing.html

Question 74: Skipped

What are the two permission types used by AWS?

- A. Resource-based and Product-based
- B. Product-based and Service-based
- C. Service-based
- D. User-based and Resource-based **(Correct)**

Explanation

Permissions are defined via policies which consist of the following elements Actions: what actions you will allow. Each AWS service has its own set of actions. Resources: which resources you allow the action on. Effect: what the effect will be when the user requests access—either allow or deny. Below is a sample snippet of a policy document that allows access to all users to Describe EC2 Instances. You can clearly see the Actions, Resources and Effect which define the policy document. For more information on policies, please visit the url: http://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html

Question 75: Skipped

A company has resources hosted both on their on-premise network and in AWS. They want their IT administrators to access resources in both environments using their on-premise credentials which is stored in Active Directory. Which of the following can be used to fulfil this requirement?

- A. Use Web Identity Federation
- B. Use SAML Federation **(Correct)**
- C. Use IAM users
- D. Use AWS VPC

Explanation

The AWS Documentation provides the following information on SAML Federation AWS supports identity federation with SAML 2.0 (Security Assertion Markup Language 2.0), an open standard that many identity providers (IdPs) use. This feature enables federated single sign-on (SSO), so users can log into the AWS Management Console or call the AWS APIs without you having to create an IAM user for everyone in your organization. By using SAML, you can simplify the process of configuring federation with AWS, because you can use the IdP's service instead of writing custom identity proxy code. For more information on SAML Federation, please visit the below URL: http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_saml.html

Question 76: Skipped

Amazon RDS DB snapshots and automated backups are stored in

- A. Amazon S3 **(Correct)**
- B. Amazon ECS Volume
- C. Amazon RDS
- D. Amazon EMR

Explanation

Automated backups automatically back up your DB instance during a specific, user-definable backup window. Amazon RDS keeps these backups for a limited period that you can specify. You can later recover your database to any point in time during this backup retention period. And all of these backups get stored to S3 by default. Option B is not correct, because that is used to store data for EC2 instances Option C is not correct because an RDS cannot be used to store snapshots Option D because EMR is used for storing and processing logs. For more information on DB instance backup's , go to the url
- http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.BackingUpAndRestoringAmazonRDSInstances.html

Question 77: Skipped

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

- A. 5 minutes **(Correct)**
- B. 500 milliseconds.
- C. 30 seconds
- D. 1 minute

Explanation

AWS free tier gives you access to the basic metrics for Cloudwatch and by default the basic package gives 5 minutes of aggregation of Cloudwatch metrics. If you need a further shorter interval, the you need to pay extra. For more information on the free tier , please feel free to visit the url - https://aws.amazon.com/free/

Question 78: Skipped

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

A. wildcards

B. pointers

C. Tags (Correct)

D. special filters

Explanation

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

Question 79: Skipped

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

A. Security group (Correct)

B. ACL

C. IAM

D. Private IP Addresses

Explanation

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. When you launch an instance in a VPC, you can assign the instance to up to five security groups. Security groups act at the instance level. Below is an example of a security group which has inbound rules. The below rule states that users can only SSH into EC2 instances that are attached to this security group. For more information on Security Groups , please visit the url
- http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html

Question 80: Skipped

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

A. This is expected behavior when using short polling because SQS does not guarantee that there will not be duplicate messages processed

B. You can only have one EC2 instance polling the SQS queue at a time

C. This is expected behavior when using long polling because SQS does not guarantee that there will not be duplicate messages processed

D. Your application does not issue a delete command to the SQS queue after processing the message **(Correct)**

Explanation

You need to ensure that after a message is processed in SQS, the message is deleted. For more information on SQS, please visit the below url https://aws.amazon.com/sqs/faqs/

Question 81: Skipped

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

A. Deploy 2 instances in each of 3 Availability Zones, add a load balancer and an Auto Scaling group to launch more instances if required. **(Correct)**

B. Deploy 2 instances in each of 2 Availability Zones, add a load balancer and an Auto Scaling group to launch more instances if required.

C. Deploy 4 instances in one Availability Zone, add a load balancer and an Auto Scaling group to launch more instances if required.

D. Deploy 1 instance in each of 3 Availability Zones, add a load balancer and an Auto Scaling group to launch more instances if required.

Explanation

Since there is a minimum of 4 instances required to run, if you deploy them in 3 AZ's and even if one AZ goes down , you will have at least 4 instances running. Requirement is to look for Best Option. Since in question's context ensuring it will be fault tolerant and high availability system, 2 extra instances shall be created in another AZ. This will ensure the requirement is fulfilled properly. For more information on fault tolerance and high availability, please visit the below URL: https://media.amazonwebservices.com/architecturecenter/AWS_ac_ra_ftha_04.pdf

Question 82: Skipped

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

A. The VPC must have at least one subnet

B. The VPC must have at least one subnet in one Availability Zone

C. Your VPC must have at least one subnet in at least two of the Availability Zones **(Correct)**

D. None of the above

Explanation

One of the important aspects of hosting databases in VPC's is the following: Your VPC must have at least one subnet in at least two of the Availability Zones in the region where you want to deploy your DB instance. A subnet is a segment of a VPC's IP address range that you can specify and that lets you group instances based on your security and operational needs. Few important points about VPC: When you create a VPC, it spans all the Availability Zones in the region. After creating a VPC, you can add one or more subnets in each Availability Zone. For more information on working with RDS instances , please refer to the below link: http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_VPC.WorkingWithRDSInstanceinaVPC.html

Question 83: Skipped

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

A. Create an AD policy to modify the Windows Firewall settings on all hosts in the VPC to deny access from the IP Address block.

B. Modify the Network ACLs associated with all public subnets in the VPC to deny access from the IP Address block. **(Correct)**

C. Add a rule to all of the VPC Security Groups to deny access from the IP Address block.

D. Modify the Windows Firewall settings on all AMI's that your organization uses in that VPC to deny access from the IP address block.

Explanation

A network access control list (ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. Option A and D are wrong because this is a tedious task and it only works for Windows systems. You need something that will work for Linux systems as well. Option C is only adequate for EC2 instances, but you need rules that will apply to the whole subnet. Otherwise the task of having this done for all servers becomes a tedious task. For more information on Network ACL's, please visit the URL http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html

Question 84: Skipped

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

A. AWS SQS

B. AWS STS (Correct)

C. AWS SES

D. None of the above. You need to use a third party software to achieve this.

Explanation

You can use the AWS Security Token Service (AWS STS) to create and provide trusted users with temporary security credentials that can control access to your AWS resources. Temporary security credentials work almost identically to the long-term access key credentials that your IAM users can use. Option A is wrong because this is the queuing service provided by AWS. Option C is wrong because this is the emailing service provided by AWS. Option D is wrong because there is a service which exists from AWS. For more information on STS, please visit the below URL
http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp.html

Question 85: Skipped

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

A. A network ACL that allows communication between the two subnets. (Correct)

B. Both instances are the same instance class and using the same Key-pair.

C. That the default route is set to a NAT instance or internet Gateway (IGW) for them to communicate.

D. Security groups are set to allow the application host to talk to the database on the right port/protocol. (Correct)

Explanation

When you design a web server and database server, the security groups must be defined so that the web server can talk to the database server. An example image from the AWS documentation is given below Also when communicating between subnets you need to have the NACL's defined Option B is wrong since the EC2 instances need not be of the same class or same key pair to communicate to each other. Option C is wrong since there the NAT and Internet gateway is used for the subnet to communicate to the internet. For more information on VPC and Subnets, please visit the below URL
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html

Question 86: Skipped

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

A. With RRS you have to copy data and extract data which can take up to 3 hours.

B. RRS only has 99.99% availability

C. With RRS, you don't need to worry since AWS will take care of the durability of RRS.

D. RRS only has 99.99% durability and you have to design automation around replacing lost objects **(Correct)**

Explanation

RRS only has 99.99% durability and there is a chance that data can be lost. So you need to ensure you have the right steps in place to replace lost objects. Even though RRS has 99.99% availability, all storage types have the same availability, so it does not answer the question on the specific trade-offs for RRS. For more information on RRS , visit the link https://aws.amazon.com/s3/reduced-redundancy/

Question 87: Skipped

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

A. Protect the EC2 instances against unsolicited access by enforcing the principle of least-privilege access

B. Protect against IP spoofing or packet sniffing **(Correct)**

C. Assure all communication between EC2 instances and ELB is encrypted

D. Install latest security patches on ELB, RDS and EC2 instances

Explanation

As per the shared responsibility shown below, the users are required to control the EC2 security via security groups and network access control layers. For more information on the Shared Responsibility model, please refer the below URL: https://aws.amazon.com/compliance/shared-responsibility-model/

Question 88: Skipped

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?

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 **(Correct)**

Explanation

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. 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

Question 89: Skipped

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?

A. Enable SSE on an S3 bucket to make use of AES-256 encryption **(Correct)**

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 **(Correct)**

D. Store the data on EBS volumes with encryption enabled instead of using Amazon S3

Explanation

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

Question 90: Skipped

There is a requirement by a company that does online credit card processing to have a secure application environment on AWS. They are trying to decide on whether to use KMS or CloudHSM. Which of the following statements is right when it comes to CloudHSM and KMS. Choose the correct answer from the options given below

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 **(Correct)**

D. AWS CloudHSM should be always be used for any payment transactions

Explanation

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/

Question 91: Skipped

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

A. Create an Origin Access Identify (OAI) for CloudFront and grant access to the objects in your S3 bucket to that OAI **(Correct)**

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

Explanation

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

Question 92: Skipped

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

- 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 **(Correct)**
- D. Amazon EC2 for storing and processing the log files

Explanation

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/

Question 93: Skipped

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 steps would you take to apply high availability and fault tolerance to this application? Select 2 options.

- 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 **(Correct)**
- B. Ensure that the instance it's using has an elastic IP address assigned to it **(Correct)**
- 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

Explanation

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

Question 94: Skipped

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

- A. An SQS queue to allow a second EC2 instance to process a failed instance's job **(Correct)**
- 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

Explanation

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 is the best option for creating a decoupled application. For more information on SQS, please refer to the below link https://aws.amazon.com/sqs/

Question 95: Skipped

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.

- A. You can leverage SWF to utilize both on-premises servers and EC2 instances for your decoupled application **(Correct)**
- 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
- C. You can leverage SQS to utilize both on-premises servers and EC2 instances for your decoupled application **(Correct)**
- 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

Explanation

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

Question 96: Skipped

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

- A. Change the scale down CloudWatch metric to a higher threshold **(Correct)**
- B. Increase the instance type in the launch configuration
- C. Increase the base number of Auto Scaling instances for the Auto Scaling group
- D. Add provisioned IOPS to the instances

Explanation

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

Question 97: Skipped

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

- A. Amazon S3, because it provides unlimited amounts of storage data, scales automatically, is highly available, and durable **(Correct)**
- 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

Explanation

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

Question 98: Skipped

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?

- 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. **(Correct)**

Explanation

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.

Question 99: Skipped

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?

- 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 (Correct)

Explanation

The AWS Documentation mentions the following Snowball is a petabyte-scale data transport solution that uses secure appliances to transfer large amounts of data into and out of the AWS cloud. Using Snowball addresses common challenges with large-scale data transfers including high network costs, long transfer times, and security concerns. 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/

Question 100: Skipped

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

A. It can store petabytes of data

B. It provides faster internet speeds

C. It can store high-taxing queries (Correct)

D. It uses read replicas

Explanation

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/

Question 101: Skipped

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 answer from the options below

A. Made a snapshot of the database

B. Enabled multi-AZ failover (Correct)

C. Increased the database instance size

D. Created a read replica

Explanation

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/

Question 102: Skipped

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

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

Explanation

By creating a read replica RDS, you have the facility to scale out the reads for your application, hence increasing the elasticity for your application. Also it can be used to reduce the load on the main 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/

Question 103: Skipped

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

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

Explanation

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

Question 104: Skipped

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

- A. A mobile push notification
- 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 **(Correct)**

Explanation

The maximum size of an SQS message as given in the AWS documentation is given below For more information on SQS, please refer to the below link https://aws.amazon.com/sqs/faqs/

Question 105: Skipped

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

- A. The command line
- B. The SDK
- C. The Console
- D. All of the above **(Correct)**

Explanation

Cloudtrail can log all API calls which enter AWS. AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain events related to API calls across your AWS infrastructure. CloudTrail provides a history of AWS API calls for your account, 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/

Question 106: Skipped

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

- A. The time it takes after a disruption to restore operations back to its regular service level. **(Correct)**
- 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.

Explanation

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

Question 107: Skipped

What AWS service, if used as part of your application's architecture, has an added benefit of helping to mitigate DDoS attacks from hitting your back-end instances? Choose the correct answer from the options below

- A. CloudWatch
- B. CloudFront **(Correct)**
- C. CloudTrail
- D. Kinesis

Explanation

The below snapshot from the aws documentation shows the best architecture practises for avoiding DDos attacks. For best practises against DDos attacks , please visit the below link
https://d0.awsstatic.com/whitepapers/DDoS_White_Paper_June2015.pdf

Question 108: Skipped

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

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

Explanation

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/

Question 109: Skipped

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?

- A. Gateway-Cached volumes with snapshots scheduled to Amazon S3 **(Correct)**
- 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

Explanation

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

Question 110: Skipped

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

- A. An AWS service for generating API keys
- B. EBS Encryption method
- C. S3 encryption method
- D. A dedicated appliance that is used to store security keys **(Correct)**

Explanation

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/

Question 111: Skipped

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.

- A. User data **(Correct)**
- B. EC2Config service
- C. IAM roles
- D. AWS Config

Explanation

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.

Question 112: Skipped

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?

A. MySQL Installed on two Amazon EC2 Instances in a single Availability Zone

B. Amazon RDS for MySQL with Multi-AZ

C. Amazon ElastiCache (Correct)

D. Amazon DynamoDB

Explanation

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 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/

Question 113: Skipped

Regarding the attaching of ENI to an instance, what does 'warm attach' refer to?

A. Attaching an ENI to an instance when it is stopped. (Correct)

B. Attaching an ENI to an instance during the launch process

C. Attaching an ENI to an instance when it is running

Explanation

You can attach an elastic network interface to an instance when it's running (hot attach), when it's stopped (warm attach), or when the instance is being launched (cold attach). An elastic network interface (ENI) is a virtual network interface that you can attach to an instance in a VPC. An Elastic network interface can have the following A primary private IP address. One or more secondary private IP addresses. One Elastic IP address per private IP address. One public IP address, which can be auto-assigned to the elastic network interface for eth0 when you launch an instance. For more information, see Public IP Addresses for Network Interfaces. One or more security groups. A MAC address. A source/destination check flag. A description. The below article shows where the ENI is present for an instance. When you click on eth0, you will get more details on the network interface For more information on Elastic Network interfaces, please visit the url
- http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html#attach_eni_launch

Question 114: Skipped

What can be used to monitor your EC2 instances and warn the Operational Department in case there are any issues?

A. AWS Cloudtrail

B. AWS Cloudwatch (Correct)

C. Configure scheduled jobs on the EC2 instance to notify the Ops department in case of any CPU utilization hikes.

D. AWS SQS

Explanation

A Cloudwatch alarm is used to monitor any Amazon Cloudwatch metric in your account. For example, you can create alarms on an Amazon EC2 instance CPU utilization, Amazon ELB request latency, Amazon Dynamo DB table throughput, Amazon SQS queue length, or even the charges on your AWS bill. Option A is wrong because Cloudtrail is used for logging purposes and not monitoring purposes Option C is partially correct and you can implement this policy, but since you have the option to use an AWS service, you need to opt for this Option B instead. Option D is wrong because SQS is used as a Queuing service. For more information on Cloudwatch, please visit the link - https://aws.amazon.com/cloudwatch/faqs/

Question 115: Skipped

A company wants to store their primary data in S3 but at the same time they want to store frequently access data locally. This is because they are not having the option to extend their on-premise storage, hence they are looking at aws for an option. What is the best solution that can be provided?

A. an EC2 instance with EBS volumes to store the commonly used data.

B. A Redis cache for frequently accessed data and S3 for frequently accessed data

C. Use the Gateway Cached Volumes (Correct)

D. There is no option available

Explanation

Gateway-Cached Volumes provides a durable and inexpensively way to store your primary data in Amazon S3, and retain your frequently accessed data locally. Gateway-Cached Volumes provide substantial cost savings on primary storage, minimize the need to scale your storage on-premises, and provide low-latency access to your frequently accessed data. In addition to storing your primary data in Amazon S3 using Gateway-Cached Volumes, you can also take point-in-time snapshots of your Gateway-Cached volume data in Amazon S3, enabling you to make space-efficient versioned copies of your volumes for data protection and various data reuse needs. Option A and B are invalid because the burden of trying to sync the most recently used data on either EBS volumes or S3 would be a burden for the IT Department. For more information on Gateway-Cached Volumes, please visit the link https://aws.amazon.com/storagegateway/faqs/

Question 116: Skipped

A customer wants to have the ability to transfer stale data from their S3 location to a low cost storage system. If there is a possibility to automate this, they would be more than happy. As an AWS Solution Architect, what is the best solution you can provide to them?

A. Use an EC2 instance and a scheduled job to transfer the stale data from their S3 location to Amazon Glacier.

B. Use Life-Cycle Policies **(Correct)**

C. Use AWS SQS

D. There is no option, the users will have to download the data and then transfer the data to aws manually.

Explanation

With Amazon lifecycle policies you can create transition actions in which you define when objects transition to another Amazon S3 storage class. For example, you may choose to transition objects to the STANDARD_IA (IA, for infrequent access) storage class 30 days after creation, or archive objects to the GLACIER storage class one year after creation. Follow the below steps to get this in place Step 1) Go the Lifecycle section of the S3 bucket and click on Add Rule Step 2) Choose what you want to export Step 3) Choose the Action to perform and then confirm on the Rule creation in the next screen. For more information on Lifecycle management, click on the link - http://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html

Question 117: Skipped

A company has a workflow that sends video files from their on-premise system to AWS for transcoding. They use EC2 worker instances that pull transcoding jobs from SQS. Why is SQS an appropriate service for this scenario?

A. SQS guarantees the order of the messages.

B. SQS synchronously provides transcoding output.

C. SQS checks the health of the worker instances.

D. SQS helps to facilitate horizontal scaling of encoding tasks. **(Correct)**

Explanation

Now even though SQS does guarantees the order of the messages for FIFO queues, this is still not the reason as to why this is the appropriate reason. The normal reason for using SQS, is for decoupling of systems and helps in horizontal scaling of aws resources. SQS does not either do transcoding output or checks the health of the worker instances. The health of the worker instances can be done via ELB or Cloudwatch. For more information on SQS, please visit the link
- https://aws.amazon.com/sqs/faqs/

Question 118: Skipped

When creation of an EBS snapshot is initiated, but not completed, the EBS volume:

A. Can be used while the snapshot is in progress. **(Correct)**

B. Cannot be detached or attached to an EC2 instance until the snapshot completes

C. Can be used in read-only mode while the snapshot is in progress.

D. Cannot be used until the snapshot completes.

Explanation

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

Question 119: Skipped

A customer needs to capture all client connection information from their ELB every five minutes. The company wants to use this data for analyzing traffic patterns and troubleshooting their applications. Which of the following options meets the customer requirements?

A. Enable AWS CloudTrail for the load balancer.

B. Enable access logs on the load balancer. **(Correct)**

C. Install the Amazon CloudWatch Logs agent on the load balancer.

D. Enable Amazon CloudWatch metrics on the load balancer.

Explanation

Elastic Load Balancing provides access logs that capture detailed information about requests or connections sent to your load balancer. Each log contains information such as the time it was received, the client's IP address, latencies, request paths, and server responses. You can use these access logs to analyze traffic patterns and to troubleshoot issues. Perform the following steps to enable load balancing Step 1) Go to the Description tab for your load balancer Step 2) Go to the Attributes section and click on Edit Attributes Step 3) In the next screen, enable Access logging and choose the S3 bucket where the logs need to be added to. For more information on ELB logging, please visit the link – http://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-access-logs.html

Question 120: Skipped

Which Amazon Elastic Compute Cloud feature can you query from within the instance to access instance properties?

A. Instance user data

B. Resource tags

C. Instance metadata (Correct)

D. Amazon Machine Image

Explanation

Instance metadata is data about your instance that you can use to configure or manage the running instance. Option A is incorrect because, user data is what you enter when you launch an instance. This can be accessed by the instance later on. Option B is incorrect, because you use this feature to tag your resources to help you manage your instances, images, and other Amazon EC2 resources, you can optionally assign your own metadata to each resource in the form of tags. For more information on metadata, please visit the link - http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html

Question 121: Skipped

You are tasked with setting up a Linux bastion host for access to Amazon EC2 instances running in your VPC. Only clients connecting from the corporate external public IP address 72.34.51.100 should have SSH access to the host. Which option will meet the customer requirement?

A. Security Group Inbound Rule: Protocol – TCP. Port Range – 22, Source 72.34.51.100/32 (Correct)

B. Security Group Inbound Rule: Protocol – UDP, Port Range – 22, Source 72.34.51.100/32

C. Network ACL Inbound Rule: Protocol – UDP, Port Range – 22, Source 72.34.51.100/32

D. Network ACL Inbound Rule: Protocol – TCP, Port Range-22, Source 72.34.51.100/0

Explanation

For SSH access, the protocol has to be TCP, so Option B and C are wrong. For Bastion host, only the IP of the client should be put and not the entire network of 72.34.51.100/0 as given in option D. So this option is also wrong. 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.

Question 122: Skipped

You run an ad-supported photo sharing website using S3 to serve photos to visitors of your site. At some point you find out that other sites have been linking to the photos on your site, causing loss to your business. What is an effective method to mitigate this?

A. Remove public read access and use signed URLs with expiry dates. **(Correct)**

B. Use Cloud Front distributions for static content.

C. Block the IPs of the offending websites in Security Groups.

D. Store photos on an EBS volume of the web server.

Explanation

Cloud front is only used for distribution of content across edge or region locations. It is not used for restricting access to content, so Option B is wrong. Blocking IP's is challenging because they are dynamic in nature and you will not know which sites are accessing your main site, so Option C is also not feasible. Storing photos on EBS volume is not a good practice or architecture approach for an AWS Solution Architect.

Question 123: Skipped

What are the use case scenarios when you need Enhanced Networking? Choose 2 answers from the options given below

A. high packet-per-second performance **(Correct)**

B. low packet-per-second performance

C. high latency networking

D. low latency networking **(Correct)**

Explanation

Enhanced networking uses single root I/O virtualization (SR-IOV) to provide high-performance networking capabilities on supported instance types. SR-IOV is a method of device virtualization that provides higher I/O performance and lower CPU utilization when compared to traditional virtualized network interfaces. Enhanced networking provides higher bandwidth, higher packet per second (PPS) performance, and consistently lower inter-instance latencies For more information on EBS volumes, please visit the link - http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enhanced-networking.html

Question 124: Skipped

You are working with a customer who is using Chef Configuration management in their data center. Which service is designed to let the customer leverage existing Chef recipes in AWS?

A. Amazon Simple Workflow Service

B. AWS Elastic Beanstalk

C. AWS CloudFormation

D. AWS OpsWorks (Correct)

Explanation

AWS OpsWorks is a configuration management service that helps you configure and operate applications of all shapes and sizes using Chef. You can define the application's architecture and the specification of each component including package installation, software configuration and resources such as storage. Start from templates for common technologies like application servers and databases or build your own to perform any task that can be scripted. AWS OpsWorks includes automation to scale your application based on time or load and dynamic configuration to orchestrate changes as your environment scales. For more information on Opswork, please visit the link – https://aws.amazon.com/opsworks/

Question 125: Skipped

A company wants to create standard templates for deployment of their Infrastructure. Which AWS service can be used in this regard? Please choose one option.

A. Amazon Simple Workflow Service

B. AWS Elastic Beanstalk

C. AWS CloudFormation (Correct)

D. AWS OpsWorks

Explanation

AWS CloudFormation gives developers and systems administrators an easy way to create and manage a collection of related AWS resources, provisioning and updating them in an orderly and predictable fashion. You can use AWS Cloud Formation's sample templates or create your own templates to describe the AWS resources, and any associated dependencies or runtime parameters, required to run your application. You don't need to figure out the order for provisioning AWS services or the subtleties of making those dependencies work. CloudFormation takes care of this for you. After the AWS resources are deployed, you can modify and update them in a controlled and predictable way, in effect applying version control to your AWS infrastructure the same way you do with your software. You can also visualize your templates as diagrams and edit them using a drag-and-drop interface with the AWS CloudFormation Designer. For more information on Cloudformation, please visit the link – https://aws.amazon.com/cloudformation/

Question 126: Skipped

A company wants to create standard templates for deployment of their Infrastructure. They have heard that aws provides a service call CloudFormation which can meet their needs? But they are worried about the cost. As an AWS Architect what advise can you give them with regards to the cost. Please choose one option.

A. You can tell them the cost is minimal and that they should not worry on that aspect.

B. Tell them that 'yes' , they have to bear the cost if they want Automation

C. Cloudformation is a free service and you only charged for the underlying aws resources (Correct)

D. Tell them to buy a product and implement on their on-premise location.

Explanation

There is no additional charge for AWS CloudFormation. You only pay for the AWS resources that are created (e.g., Amazon EC2 instances, Elastic Load Balancing load balancers etc.) For more information on Cloudformation, please visit the link – https://aws.amazon.com/cloudformation/

Question 127: Skipped

You have an environment that consists of a public subnet using Amazon VPC and 3 instances that are running in this subnet. These three instances can successfully communicate with other hosts on the Internet. You launch a fourth instance in the same subnet, using the same AMI and security group configuration you used for the others, but find that this instance cannot be accessed from the internet. What should you do to enable Internet access?

A. Deploy a NAT instance into the public subnet.

B. Assign an Elastic IP address to the fourth instance. (Correct)

C. Configure a publically routable IP Address in the host OS of the fourth instance.

D. Modify the routing table for the public subnet.

Explanation

Option A is wrong because it already mentioned that your instances are in a public subnet. Only when your instances are in a private Subnet, then only you have to configure a NAT instance. Option C is wrong because the public IP address has to be configured in AWS and not on the EC2 instance. Option D is wrong because if the routing table was wrong then you would have an issue with the other 3 instances as well. And the question says that there is no issue with the other instances. For more information on Elastic IP's, please visit the link: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html

Question 128: Skipped

You have a video transcoding application running on Amazon EC2. Each instance polls a queue to find out which video should be transcoded, and then runs a transcoding process. If this process is interrupted, the video will be transcoded by another instance based on the queuing system. You have a large backlog of videos which need to be transcoded and would like to reduce this backlog by adding more instances. You will need these instances only until the backlog is reduced. Which type of Amazon EC2 instances should you use to reduce the backlog in the most cost efficient way?

A. Reserved instances

B. Spot instances (Correct)

C. Dedicated instances

D. On-demand instances

Explanation

Since this is like a batch processing job, the best type of instance to use is a Spot instances. Spot instances are normally used in batch processing jobs. Since these jobs don't last for the entire duration of the year, they can bid upon and allocated and de-allocated as requested. Reserved Instances/Dedicated instances cannot be used because this is not a 100% used application. There is no mentioned on a continuous demand of work from the question so there is no need to use On-demand instances. What is Spot Instance? - These are spare unused Amazon EC2 instances that you can bid for. Once your bid exceeds the current spot price (which fluctuates in real time based on demand-and-supply) the instance is launched. The instance can go away anytime the spot price becomes greater than your bid price. Note that spot instance also a category of on-demand instance, but it is demanded based on the low cost bidding. What is On-demand instance? - They let you pay for your computing capacity needs by the hour. There is not much planning required from the user's end and no one time cost that you need to pay upfront like in case of reserved instances. Suitable for use cases where you do not want any long term commitment like testing and POCs, spiky, not to be interrupted workloads. For more information on Spot Instances, please visit the URL – https://aws.amazon.com/ec2/spot/ http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/how-spot-instances-work.html

Question 129: Skipped

You have a distributed application that periodically processes large volumes of data across multiple Amazon EC2 Instances. The application is designed to recover gracefully from Amazon EC2 instance failures. You are required to accomplish this task in the most cost-effective way. Which of the following will meet your requirements?

A. Spot Instances (Correct)

B. Reserved instances

C. Dedicated instances

D. On-Demand instances

Explanation

When you think of cost effectiveness, you can either have to choose Spot or Reserved instances. Now when you have a regular processing job, the best is to use spot instances and since your application is designed recover gracefully from Amazon EC2 instance failures, then even if you lose the Spot instance , there is no issue because your application can recover. For more information on spot instances, please visit the link https://aws.amazon.com/ec2/spot/

Question 130: Skipped

What are the possible Event Notifications available for S3 buckets? Please choose 3 answers from the options given below.

A. SNS (Correct)

B. SES

C. SQS (Correct)

D. Lambda function (Correct)

Explanation

Amazon S3 event notifications enable you to run workflows, send alerts, or perform other actions in response to changes in your objects stored in Amazon S3. You can use Amazon S3 event notifications to set up triggers to perform actions including transcoding media files when they are uploaded, processing data files when they become available, and synchronizing Amazon S3 objects with other data stores. When you go to the Events section in S3, you can see the options present there for SNS, SQS and Lambda function.

Question 131: Skipped

A company needs to deploy services to an AWS region which they have not previously used. The company currently has an AWS identity and Access Management (IAM) role for the Amazon EC2 instances, which permits the instance to have access to Amazon DynamoDB. The company wants their EC2 instances in the new region to have the same privileges. How should the company achieve this?

A. Create a new IAM role and associated policies within the new region

B. Assign the existing IAM role to the Amazon EC2 instances in the new region (Correct)

C. Copy the IAM role and associated policies to the new region and attach it to the instances

D. Create an Amazon Machine Image (AMI) of the instance and copy it to the desired region using the AMI Copy feature

Explanation

Since you already have an existing role, you don't need to create a new one, so Option A is wrong. Remember that roles are a global service that is available across all regions. So Option C is also wrong. Option D is wrong because this has to do with roles and no need of creating an AMI image. So when you create a role choose the Amazon EC2 option in the Select Role type. In the next screen, you can select the Amazon DynamoDB type of access required. Once the role is created, choose the role in the Configure Instance Details screen when creating the EC2 instance.

Question 132: Skipped

You are deploying an application to collect votes for a very popular television show. Millions of users will submit votes using mobile devices. The votes must be collected into a durable, scalable, and highly available data store for real-time public tabulation. Which service should you use?

A. Amazon DynamoDB (Correct)

B. Amazon Redshift

C. Amazon Kinesis

D. Amazon Simple Queue Service

Explanation

Amazon DynamoDB is a fully managed NoSQL database service that provides fast and predictable performance with seamless scalability. Amazon DynamoDB enables customers to offload the administrative burdens of operating and scaling distributed databases to AWS, so they don't have to worry about hardware provisioning, setup and configuration, replication, software patching, or cluster scaling. DynamoDB is durable, scalable, and highly available data store in aws and can be used for real time tabulation. Option B is wrong because it is a petabyte storage engine and is used in cases where there is a requirement for an OLAP solution. Option C is wrong because it is used for processing streams and not for storage. Option D is wrong because it is a de-coupling solution. For more information on Amazon DynamoDB, please visit https://aws.amazon.com/dynamodb/faqs/

Question 133: Skipped

Which of the below aws services allows you to run code without the need to host an EC2 instances

A. AWS Lambda (Correct)

B. AWS IoT

C. AWS SQS

D. AWS SES

Explanation

AWS Lambda lets you run code without provisioning or managing servers. You pay only for the compute time you consume - there is no charge when your code is not running. With Lambda, you can run code for virtually any type of application or backend service - all with zero administration. Just upload your code and Lambda takes care of everything required to run and scale your code with high availability. You can set up your code to automatically trigger from other AWS services or call it directly from any web or mobile app For more information on Amazon Lambda, please visit https://aws.amazon.com/lambda/?nc2=h_m1

Question 134: Skipped

You are deploying an application to track GPS coordinates of delivery trucks in the United States. Coordinates are transmitted from each delivery truck once every three seconds. You need to design an architecture that will enable real-time processing of these coordinates from multiple consumers. Which service should you use to implement data ingestion?

A. Amazon Kinesis (Correct)

B. AWS Data Pipeline

C. Amazon AppStream

D. Amazon Simple Queue Service

Explanation

Use Amazon Kinesis Streams to collect and process large streams of data records in real time. You'll create data-processing applications, known as Amazon Kinesis Streams applications. A typical Amazon Kinesis Streams application reads data from an Amazon Kinesis stream as data records. These applications can use the Amazon Kinesis Client Library, and they can run on Amazon EC2 instances. The processed records can be sent to dashboards, used to generate alerts, dynamically change pricing and advertising strategies, or send data to a variety of other AWS services For more information on Amazon Kinesis, please visit http://docs.aws.amazon.com/streams/latest/dev/introduction.html

Question 135: Skipped

You have an application running on an Amazon Elastic Compute Cloud instance that uploads 5 GB video objects to Amazon Simple Storage Service (S3). Video uploads are taking longer than expected, resulting in poor application performance. Which method will help improve performance of your application?

A. Enable enhanced networking

B. Use Amazon S3 multipart upload (Correct)

C. Leveraging Amazon CloudFront, use the HTTP POST method to reduce latency.

D. Use Amazon Elastic Block Store Provisioned IOPs and use an Amazon EBS-optimized instance

Explanation

When uploading large videos it's always better to make use of aws multi part file upload. So if you are using the Multi Upload option for S3, then you can resume on failure. Below are the advantage of Multi Part upload Improved throughput—you can upload parts in parallel to improve throughput. Quick recovery from any network issues—smaller part size minimizes the impact of restarting a failed upload due to a network error. Pause and resume object uploads—you can upload object parts over time. Once you initiate a multipart upload there is no expiry; you must explicitly complete or abort the multipart upload. Begin an upload before you know the final object size—you can upload an object as you are creating it. For more information on Multi-part file upload for S3, please visit the URL - http://docs.aws.amazon.com/AmazonS3/latest/dev/qfacts.html

Question 136: Skipped

A customer wants to track access to their Amazon Simple Storage Service (S3) buckets and also use this information for their internal security and access audits. Which of the following will meet the Customer requirement?

internal security and access audits. Which of the following will meet the customer requirement?

- A. Enable AWS CloudTrail to audit all Amazon S3 bucket access.
- B. Enable server access logging for all required Amazon S3 buckets. **(Correct)**
- C. Enable the Requester Pays option to track access via AWS Billing
- D. Enable Amazon S3 event notifications for Put and Post.

Explanation

Logging provides a way to get detailed access logs delivered to a bucket you choose. An access log record contains details about the request, such as the request type, the resources specified in the request worked, and the time and date the request was processed. Since you don't want logging of every aws service, there is no need to Cloudtrail, hence you can neglect Option A. Option C is not valid because that refers to billing. Option D is invalid because event notifications is different from logging. To enable logging just go to the Logging section in your S3 bucket For more information on S3 Logging, please visit the URL - http://docs.aws.amazon.com/AmazonS3/latest/UG/ManagingBucketLogging.html

Question 137: Skipped

A company is deploying a two-tier, highly available web application to AWS. Which service provides durable storage for static content while utilizing lower Overall CPU resources for the web tier?

- A. Amazon EBS volume
- B. Amazon S3 **(Correct)**
- C. Amazon EC2 instance store
- D. Amazon RDS instance

Explanation

When you think of storage, the automatic choice should aws S3. Amazon S3 is storage for the Internet. It's a simple storage service that offers software developers a highly-scalable, reliable, and low-latency data storage infrastructure at very low costs. For more information on S3 Logging, please visit the URL - https://aws.amazon.com/s3/faqs/

Question 138: Skipped

A company is building a two-tier web application to serve dynamic transaction-based content. The data tier is leveraging an Online Transactional Processing (OLTP) database. What services should you leverage to enable an elastic and scalable web tier?

A. Elastic Load Balancing, Amazon EC2, and Auto Scaling (Correct)

B. Elastic Load Balancing, Amazon RDS with Multi-AZ, and Amazon S3

C. Amazon RDS with Multi-AZ and Auto Scaling

D. Amazon EC2, Amazon Dynamo DB, and Amazon S3

Explanation

The question mentioned a scalable web tier and not a database tier. So Option C, D and B are already automated eliminated, since we do not need a database option. The below example shows an Elastic Load balancer connected to 2 EC2 instances connected via Auto Scaling. This is an example of an elastic and scalable web tier. By scalable we mean that the Auto scaling process will increase or decrease the number of EC2 instances as required.

Question 139: Skipped

You are designing a web application that stores static assets in an Amazon Simple Storage Service (S3) bucket. You expect this bucket to immediately receive over 150 PUT requests per second. What should you do to ensure optimal performance?

A. Use multi-part upload.

B. Add a random prefix to the key names. (Correct)

C. Amazon S3 will automatically manage performance at this scale.

D. Use a predictable naming scheme, such as sequential numbers or date time sequences, in the key names

Explanation

If your workload in an Amazon S3 bucket routinely exceeds 100 PUT/LIST/DELETE requests per second or more than 300 GET requests per second then you need to perform some guidelines for your S3 bucket. One way to add a hash prefix key to the key name - One way to introduce randomness to key names is to add a hash string as prefix to the key name. For example, you can compute an MD5 hash of the character sequence that you plan to assign as the key name. For performance considerations, please visit the URL http://docs.aws.amazon.com/AmazonS3/latest/dev/request-rate-perf-considerations.html

Question 140: Skipped

A company has an AWS account that contains three VPCs (Dev, Test, and Prod) in the same region. Test is peered to both Prod and Dev. All VPCs have non-overlapping CIDR blocks. The company wants to push minor code releases from Dev to Prod to speed up time to market. Which of the following options helps the company accomplish this?

A. Create a new peering connection Between Prod and Dev along with appropriate routes. (Correct)

B. Create a new entry to Prod in the Dev route table using the peering connection as the target.

C. Attach a second gateway to Dev. Add a new entry in the Prod route table identifying the gateway as the target.

D. The VPCs have non-overlapping CIDR blocks in the same account. The route tables contain local routes for all VPCs.

Explanation

Transitive VPC peering is not allowed in AWS. Here Test VPC has peered with Dev VPC and Test VPC also peered with Prod VPC but in order to establish private communication between Dev and Prod resources, new VPC peering has to create between Dev VPC and Prod VPC. A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IP addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account within a single region The below diagram shows an example of VPC peering. Now please note that VPC B cannot communicate to VPC C because there is no peering between them. Hence in the same way the above question there is no peering between Prod and Dev. , hence the only way for them to communicate is to have a VPC peering setup between them. For more information on VPC peering, please visit the url http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-peering.html

Question 141: Skipped

What is the service provided by aws that allows developers to easily deploy and manage applications on the cloud?

A. CloudFormation

B. Elastic Beanstalk **(Correct)**

C. Opswork

D. Container service

Explanation

AWS Elastic Beanstalk makes it even easier for developers to quickly deploy and manage applications in the AWS Cloud. Developers simply upload their application, and Elastic Beanstalk automatically handles the deployment details of capacity provisioning, load balancing, auto-scaling, and application health monitoring. For more information on Elastic Beanstalk, please visit the URL https://aws.amazon.com/elasticbeanstalk/faqs/

Question 142: Skipped

What is the service provided by aws that allows developers to let connected devices interact with cloud based applications? Please choose on answer from the options below.

A. CloudFormation

B. Elastic Beanstalk

C. AWS IoT (Correct)

D. Container service

Explanation

AWS IoT is a managed cloud platform that lets connected devices easily and securely interact with cloud applications and other devices. AWS IoT can support billions of devices and trillions of messages, and can process and route those messages to AWS endpoints and to other devices reliably and securely. With AWS IoT, your applications can keep track of and communicate with all your devices, all the time, even when they aren't connected. For more information on aws IoT, please visit the URL https://aws.amazon.com/iot/

Question 143: Skipped

An Account has an ID of 085566624145. Which of the below mentioned URL's would you provide to the IAM user to log in to aws?

A. https://085566624145.signin.aws.amazon.com/console (Correct)

B. https://signin.085566624145.aws.amazon.com/console

C. https://signin.aws.amazon.com/console

D. https://aws.amazon.com/console

Explanation

After you create IAM users and passwords for each, users can sign in to the AWS Management Console for your AWS account with a special URL. By default, the sign-in URL for your account includes your account ID. You can create a unique sign-in URL for your account so that the URL includes a name instead of an account ID By default the URL will be of the format shown below https://AWS-account-ID-or-alias.signin.aws.amazon.com/console

Question 144: Skipped

What are the different types of identities available AWS. Please choose 3 answers form the options given below.

A. Roles (Correct)

B. Users (Correct)

C. EC2 Instances

D. Groups (Correct)

Explanation

An IAM user is an entity that you create in AWS. The IAM user represents the person or service who uses the IAM user to interact with AWS. An IAM group is a collection of IAM users. You can use groups to specify permissions for a collection of users, which can make those permissions easier to manage for those users An IAM role is very similar to a user, in that it is an identity with permission policies that determine what the identity can and cannot do in AWS For more information on Identities, please visit the URL http://docs.aws.amazon.com/IAM/latest/UserGuide/id.html

Question 145: Skipped

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

A. The IP of the primary DB instance is switched to the standby DB instance

B. The RDS (Relational Database Service) DB instance reboots

C. A new DB instance is created in the standby availability zone

D. The canonical name record (CNAME) is changed from primary to standby (Correct)

Explanation

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

Question 146: Skipped

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

A. AWS Elastic Beanstalk (Correct)

B. AWS Cloudfront

C. AWS Cloudformation

C. AWS CloudFormation

D. AWS DevOps

Explanation

The Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services We can simply upload code and Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitering. Meanwhile we can retain full control over the AWS resources used in the application and can access the underlying resources at any time. Launch LAMP stack with Elastic Beanstalk: https://aws.amazon.com/getting-started/projects/launch-lamp-web-app/ We can do it on AWS CloudFormation as well in a harder way and it will be less Native: https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/deploying.applications.html

Question 147: Skipped

In which of the following ways can you manage lambda functions. Choose all 3 correct answers.

A. Console **(Correct)**

B. CLI **(Correct)**

C. SDK **(Correct)**

D. EC2 Instances

Explanation

This is given in the AWS documentation: For more information on AWS Lambda, please visit the link: https://aws.amazon.com/lambda/faqs/

Question 148: Skipped

What is the maximum execution time for a Lambda function?

A. 3 seconds

B. 300 seconds **(Correct)**

C. 24 hours

D. No limit

Explanation

This is given in the aws documentation For more information on AWS Lambda, please visit the link https://aws.amazon.com/lambda/faqs/

Question 149: Skipped

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

- A. Non-Alias with a type "A" record set
- B. Alias with a type "AAAA" record set
- C. Alias with a type "CNAME" record set
- D. Alias with a type "A" record set **(Correct)**

Explanation

Yes, You need to configure ALIAS record for ELB but it should point to A record. You can find details in below AWS document http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-to-elb-load-balancer.html This is given in the aws documentation For more information on Route53, please visit the link http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-values-alias.html

Question 150: Skipped

Which of the following statement is false with regards to the AWS Simple Queue Service?

- A. Standard queues provide at-least-once delivery, which means that each message is delivered at least once
- B. Both FIFO queues and Standard queues preserve the order of messages **(Correct)**
- C. Amazon SQS can help you build a distributed application with decoupled components
- D. FIFO queues provide exactly-once processing

Explanation

Only FIFO queues can preserve the order of messages and not standard queues. For more information on standard queues, please visit the below URL https://aws.amazon.com/sqs/faqs/

Question 151: Skipped

A company want to implement a hybrid architecture where it wants to connect VPC's in its account to its on-premise architecture. Which of the following can be used to create a secure private connection between the Company's on-premise architecture and the VPC's hosted in AWS.

- A. AWS Direct Connect + VPN **(Correct)**
- B. Route53
- C. ClassicLink
- D. AWS Direct Link

Explanation

AWS Direct Connect provides private connectivity between AWS and your data center, office, or co-location environment. It makes it easy to establish a dedicated connection from an on- premise network to Amazon VPC. However if you want to have a secure private connection between your on-premise architecture and VPC's hosted in AWS we can combine AWS Direct Connect dedicated network connection along with the Amazon VPC hardware VPN. AWS Direct Connect along with VPN can provide an IP-Sec encrypted private connection that also reduces network costs. Option A is correct answer for a secured private connection. Option B, Route 53 is AWS Domain Name service. Incorrect answer for this question Option C ClassicLink allows you to link your EC2-Classic instance to a VPC in your account, within the same region. Incorrect answer Option D is Incorrect. Further information is available on the following white-paper.
https://media.amazonwebservices.com/AWS_Amazon_VPC_Connectivity_Options.pdf

Question 152: Skipped

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

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

Explanation

If your Amazon EBS volume is attached to a current generation EC2 instance type, you can increase its size, change its volume type, or (for an io1 volume) adjust its IOPS performance, all without detaching it. For more information on changing the volume size, please visit the link: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-expand-volume.html For more information on changing the EBS encryption, please visit the link
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html

Question 153: Skipped

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

- A. The requested contest has never been requested before
- B. The objects file size are 10GB in size.
- C. The cache expiration time is set to a low value **(Correct)**
- D. You didn't configure the objects with a X.509 certificate

Explanation

You can control how long your objects stay in a CloudFront cache before CloudFront forwards another request to your origin. Reducing the duration allows you to serve dynamic content. Increasing the duration means your users get better performance because your objects are more likely to be served directly from the edge cache. A longer duration also reduces the load on your origin. For more information on changing the volume encryption, please visit the link http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Expiration.html

Question 154: Skipped

You are using an EC2 instance that is backed by an S3-based AMI. You are planning on terminating that instance. When the instance is terminated, what happens to the data on the root volume?

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

Explanation

The AWS documentation mentions the following The data in an instance store persists only during the lifetime of its associated instance. If an instance reboots (intentionally or unintentionally), data in the instance store persists. However, data in the instance store is lost under the following circumstances: · The underlying disk drive fails · The instance stops · The instance terminates For more information on Instance store AMI's, please visit the below URL: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/InstanceStorage.html AWS docs provides following details: it's an instance store. Storage for the Root Device All AMIs are categorized as either backed by Amazon EBS or backed by instance store. The former means that the root device for an instance launched from the AMI is an Amazon EBS volume created from an Amazon EBS snapshot. The latter means that the root device for an instance launched from the AMI is an instance store volume created from a template stored in Amazon S3. For more information, see Amazon EC2 Root Device Volume. https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ComponentsAMIs.html#storage-for-the-root-device

Question 155: Skipped

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

- A. Latency
- B. Failover
- C. Weighted **(Correct)**
- D. Geolocation

Explanation

Use the weighted routing policy when you have multiple resources that perform the same function (for example, web servers that serve the same website) and you want Amazon Route 53 to route traffic to those resources in proportions that you specify (for example, one quarter to one server and three quarters to the other). For more information on the routing policy, please visit the link http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html

Question 156: Skipped

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

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

Explanation

If you need an AMI across multiple regions , then you have to copy the AMI across regions. Note that by default AMI's that you have created will not be available across all regions. So option A is automatically invalid. Next you can share AMI's with other users, but they will not be available across regions. So option C and D is invalid. You have to copy the AMI across regions. To copy AMI's , follow the below steps Step 1) The first step is to create an AMI from your running instance by choosing on Image->Create Image. Step 2) Once the Image has been created, go to the AMI section in the EC2 dashboard and click on the Copy AMI option. Step 3) In the next screen , you can specify where to copy the AMI to. For the entire details to copy AMI's , please visit the link

Step 3) In the next screen , you can specify where to copy the AMI to. For the entire details to copy AMI's , please visit the link - http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/CopyingAMIs.html

Question 157: Skipped

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

- [ ] A. Database visible metrics such as number of connections **(Correct)**
- [ ] B. Disk OPS metrics **(Correct)**
- [ ] C. Database memory usage **(Correct)**
- [ ] D. Web service visible metrics such as number failed transaction requests

Explanation

As RDS Instance is completely managed by AWS and user doesn't have access Operating System metrics, So it is logical for AWS to provide us those metrics. Please refer to AWS documentation http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Monitoring.html Refer to the screenshot attached which shows metrics like Freeable Memory, Freeable Space, Swap Usage etc which are Operating System visible metrics.

Question 158: Skipped

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

- ( ) A. 2TiB
- ( ) B. 16TiB **(Correct)**
- ( ) C. 4Gib
- ( ) D. 500 GiB

Explanation

The maximum size for EBS provisioned IOPS volume allowed is 16384 GiB which 16 TiB. See error while trying to create volume more than available size : The minimum size for an EBS Provisioned IOPS SSD volume is 4GiB and maximum size is 16TiB. This sort of volumes are normally used for hosting databases which require a lot of I/O operations. These types of volumes have better performance and are optimized for such scenarios. For more information on EBS volume types, please visit the link: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html

Question 159: Skipped

A company wants to store data that is not frequently accessed. What is the best and cost efficient solution that should be considered?

- A. Amazon Storage Gateway
- B. Amazon Glacier **(Correct)**
- C. Amazon EBS
- D. Amazon S3

Explanation

Since the data is not required to be accessed frequently, the data can be stored on Amazon glacier for cheaper storage. Remember that the recovery time for getting data from Glacier is from 3-5 hours. You can look at the FAQ section of aws glacier - https://aws.amazon.com/glacier/faqs/

Question 160: Skipped

You have an EC2 instance that is transferring data from S3 in the same region. The project sponsor is worried about the cost of the infrastructure. What can you do to convince him that you have a cost effective solution.

- A. You are going to be hosting only 4 instances, so you are minimizing on cost.
- B. There is no cost for transferring data from EC2 to S3 if they are in the same region. **(Correct)**
- C. AWS provides a discount if you transfer data from EC2 to S3 if they are in the same region.
- D. Both EC2 and S3 are in the same availability zone, so you can save via consolidated billing.

Explanation

Please note that there is no cost when data is transferred from EC2 to S3 if they are in the same region. This is very important for an AWS Solution Architect to know.