CSAA Practice Test 2

Completed on 17-October-2020

Attempt	Marks Obtained	Your score	Time Taken	Result
03	0 / 65	0.0%	N/A	Failed

Domains wise Quiz Performance Report

No	Domain	Total Question	Correct	Incorrect	Unattempted	Marked as Review
1	Design High-Performing Architectures	22	0	0	22	0
2	Design Secure Applications and Architectures	23	0	0	23	0
3	Design Resilient Architectures	16	0	0	16	0
4	Design Cost-Optimized Architectures	4	0	0	4	0
Total	All Domain	65	0	0	65	0

Review the Answers

Sorting by All

Question 1 **Unattempted**

Domain :Design High-Performing Architectures

You need to deploy a machine learning application in AWS EC2. The performance of inter-instance communication is very critical for the application and you want to attach a network

device to the instance so that the performance can be greatly improved. Which option is the most appropriate to improve the performance?

A. **Enable enhanced networking feature in the EC2 instance.**

B. **Configure Elastic Fabric Adapter (EFA) in the instance.**

C. **Attach high speed Elastic Network Interface (ENI) in the instance.**

D. **Create Elastic File System (EFS) and mount the file system in the instance.**

Explanation:

Correct Answer – B

With Elastic Fabric Adapter (EFA), users can get a better performance if compared with enhanced networking (Elastic Network Adapter) or Elastic Network Interface. Check the differences between EFAs and ENAs in https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/efa.html.

Option A is incorrect: Because with Elastic Fabric Adapter (EFA), users can achieve a better network performance than enhanced networking.

Option B is CORRECT: Because EFA is the most suitable method for accelerating High Performance Computing (HPC) and machine learning application.

Option C is incorrect: Because Elastic Network Interface (ENI) cannot improve the performance as required.

Option D is incorrect: The Elastic File System (EFS) cannot accelerate the inter-instance communication.

Ask our Experts Rate this Question?

View Queries open

Question 2 **Unattempted**

Domain :Design Secure Applications and Architectures

You have an application that has been dockerized. You plan to deploy the application in an AWS ECS cluster. As the application gets configuration files from an S3 bucket, the ECS containers should have the AmazonS3ReadOnlyAccess permission. What is the correct method to configure

the IAM permission?

A. **Add an environment to the ECS cluster configuration to allow the S3 read only access.**

B. **Add the AmazonS3ReadOnlyAccess permission to the IAM entity that creates the ECS cluster.**

C. **Modify the user data of ECS instances to assume an IAM role that has the AmazonS3ReadOnlyAccess permission.**

D. **Attach the AmazonS3ReadOnlyAccess policy to the ECS container instance IAM role. Attach this role when creating the ECS cluster.**

Explanation:

Correct Answer – D

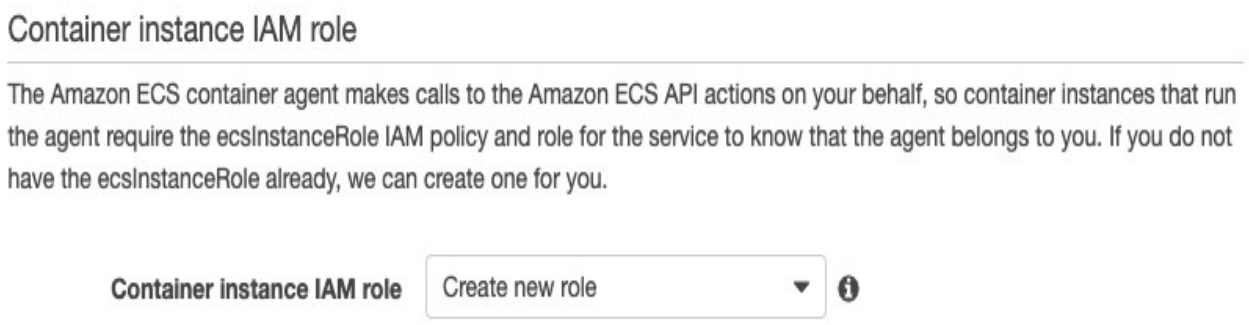
ECS containers have access to permissions that are supplied to the container instance role. Details please check the ECS documentation in https://docs.aws.amazon.com/AmazonECS/latest/developerguide/instance_IAM_role.html.

Option A is incorrect: Because ECS cluster uses the container instance IAM role instead of environment variables to control its permissions.

Option B is incorrect: Because the IAM entity that creates the ECS cluster does not pass its permissions to the ECS cluster. You need to configure an IAM role and attach it to the ECS cluster.

Option C is incorrect: This is not the correct method to configure IAM permissions for an ECS cluster.

Option D is CORRECT: After the AmazonS3ReadOnlyAccess policy is attached to the IAM role, the ECS instances can use the role to get objects from S3. When launching an ECS cluster, you can associate the container instance role as follows:



Ask our Experts Rate this Question?

View Queries open

Question 3 **Unattempted**

Domain :Design High-Performing Architectures

A company is planning on testing a large set of IoT enabled devices. These devices will be streaming data every second. A proper service needs to be chosen in AWS which could be used to collect and analyze these streams in real-time. Which AWS service would be the most appropriate for this purpose?

A. **Use AWS EMR to store and process the streams.**

B. **Use AWS Kinesis to process and analyze the data.**

C. **Use AWS SQS to store the data.**

D. **Use SNS to store the data.**

Explanation:

Correct Answer - B

AWS Documentation mentions the following on Amazon 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 video, audio, application logs, website clickstreams, and IoT telemetry data for machine learning, analytics, and other applications.

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

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

Option A is incorrect. Amazon EMR can be used to process applications with data-intensive

workloads.

Option B is correct. Amazon Kinesis can be used to store, process, and analyze real-time streaming data.

Option C is incorrect. SQS is a fully managed message queuing service that makes it easy to decouple and scale microservices, distributed systems, and serverless applications.

Option D is incorrect. SNS is a flexible, fully managed pub/sub messaging and mobile notifications service for coordinating the delivery of messages to subscribing to endpoints and clients.

Ask our Experts Rate this Question?

View Queries open

Question 4 **Unattempted**

Domain :Design Resilient Architectures

Your company currently has a set of EC2 Instances hosted in AWS. The states of these instances need to be monitored and each state needs to be changed when a metric breaches a threshold value. Which step could be helpful to fulfill this requirement? (**SELECT TWO**)

A. **Use CloudWatch logs to store the state change of the instances.**

B. **Create an Amazon CloudWatch alarm that monitors an Amazon EC2 instance**

C. **Use SQS to trigger a record to be added to a DynamoDB table.**

D. **Use AWS Lambda to store a change record in a DynamoDB table.**

Explanation:

Correct Answer: A and B

Create Alarms That Stop, Terminate, Reboot, or Recover an Instance

Using Amazon CloudWatch alarm actions, you can create alarms that automatically stop, terminate, reboot or recover your instances. You can use the stop or terminate actions to save money when you no longer need an instance. You can use the reboot and recover actions to

automatically reboot those instances or recover them onto new hardware if a system impairment occurs.

The AWSServiceRoleForCloudWatchEvents service-linked role enables AWS to perform alarm actions on your behalf. The first time you create an alarm in the AWS Management Console, the IAM CLI, or the IAM API, CloudWatch creates the service-linked role for you.

There are a number of scenarios in which you might want to automatically stop or terminate your instance. For example, you might have instances dedicated to batch payroll processing jobs or scientific computing tasks that run for a period of time and then complete their work. Rather than letting those instances sit idle (and accrue charges), you can stop or terminate them, which could help you to save money. The main difference between using the stop and the terminate alarm actions is that you can easily restart a stopped instance if you need to run it again later, and you can keep the same instance ID and root volume. However, you cannot restart a terminated instance instead, you must launch a new instance.

You can add the stop, terminate, reboot or recover actions to any alarm that is set on an Amazon EC2 per-instance metric, including basic and detailed monitoring metrics provided by Amazon CloudWatch (in the AWS/EC2 namespace), as well as any custom metrics that include the InstanceId dimension, as long as its value refers to a valid running Amazon EC2 instance.

For more information on Amazon EC2, please visit the following
URL: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-ug.pdf

Breakdown

Option A is correct. Using Cloudwatch logs collect, store, view, and search logs from AWS and non-AWS resources.

Option B is correct. CloudWatch alarms are used to trigger notifications for any metric. Alarms can go to auto-scaling, EC2 actions(stop, terminate, recover, or reboot) and SNS notifications.

Option C is incorrect as SQS cannot be used for monitoring.

Option D is incorrect as AWS Lambda cannot be used for monitoring.

Please refer the below link for more information on Cloudwatch:

https://docs.aws.amazon.com/AmazonCloudWatch/latest/events/CloudWatch-Events-Monitoring-CloudWatch-Metrics.html

https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/acw-ug.pdf

Try now labs related to this question

Using CloudWatch for Resource Monitoring, Create CloudWatch Alarms and Dashboards

This lab walks you through the various CloudWatch features available which are used for resource monitoring.

Credit Needed 10 Time 0 : 45 Try Now

Ask our Experts Rate this Question?

View Queries open

Question 5 **Unattempted**

Domain :Design Secure Applications and Architectures

You have instances hosted in a private subnet in a VPC. There is a need for instances to download updates from the Internet. As an architect, what change would you suggest to the IT Operations team that would also be the most efficient and secure?

A. **Create a new public subnet and move the instance to that subnet.**

B. **Create a new EC2 Instance to download the updates separately and then push them to the required instance.**

C. **Use a NAT Gateway to allow the instances in the private subnet to download the updates.**

D. **Create a VPC link to the Internet to allow the instances in the private subnet to download the updates.**

Explanation:

Correct Answer – C

The NAT Gateway is an ideal option to ensure that instances in the private subnet have the ability to download updates from the Internet.

For more information on the NAT Gateway, please refer to the below URL:

https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-nat-gateway.html

Option A is incorrect because there may be a security reason for keeping these instances in the private subnet. (for example DB instances)

Option B is incorrect. The instances in the private subnet may be running various applications and DB instances. Hence, it is not advisable or practical for an EC2 Instance to download the updates separately and then push them to the required instance.

Option D is incorrect because a VPC link is not used to connect to the Internet.

Try now labs related to this question

Build Amazon VPC with Public and Private Subnets from Scratch

1. Learn how to build Public and Private subnets from scratch.
2. VPC wizard will not be used. So every component required to build public and private subnets will be created and configured manually.
3. This will give an in-depth understanding of internal components of VPC and subnets.

Credit Needed 10 Time 0 : 30 Try Now

Ask our Experts Rate this Question?

View Queries open

Question 6 **Unattempted**

Domain :Design Resilient Architectures

You have an S3 bucket that receives photos uploaded by customers. When an object is uploaded, an event notification is sent to an SQS queue with the object details. You also have an ECS cluster that gets messages from the queue to do the batch processing. The queue size may change greatly depending on the number of incoming messages and backend processing speed. Which metric would you use to scale up/down the ECS cluster capacity?

A. The number of messages in the SQS queue.

B. Memory usage of the ECS cluster.

C. Number of objects in the S3 bucket.

D. Number of containers in the ECS cluster.

Explanation:

Correct Answer – A

In this scenario, SQS queue is used to store the object details which is a highly scalable and reliable service. ECS is ideal to perform batch processing and it should scale up or down based on the number of messages in the queue. Details please check https://github.com/aws-samples/ecs-refarch-batch-processing.

Option A is CORRECT: Users can configure a CloudWatch alarm based on the number of messages in the SQS queue and notify the ECS cluster to scale up or down using the alarm.

Option B is incorrect: Because the memory usage may not be able to reflect the workload.

Option C is incorrect: Because the number of objects in S3 cannot determine if the ECS cluster should change its capacity.

Option D is incorrect: Because the number of containers cannot be used as a metric to trigger an auto-scaling event.

Ask our Experts Rate this Question?

View Queries open

Question 7 **Unattempted**

Domain :Design High-Performing Architectures

You have an EC2 instance in the AWS us-east-1 region. The application in the instance needs to access a DynamoDB table that is located in the AWS us-east-2 region. The connection must be private without leaving the Amazon network and the instance should not use any public IP for communication. How would you configure this?

A. Configure an inter-region VPC endpoint for the DynamoDB service.

B. Configure inter-region VPC peering and create a VPC endpoint for DynamoDB in us-east-2.

C. Create an inter-region VPC peering connection between us-east-1 and us-east-2.

D. There is no way to setup the private inter-region connections.

Explanation:

Correct Answer – B

For the private connections between regions, VPC peering should be used. Then VPC endpoint allows users to privately access the DynamoDB service. Please check the reference in https://aws.amazon.com/about-aws/whats-new/2018/10/aws-privatelink-now-supports-access-over-inter-region-vpc-peering/.

Option A is incorrect: Because you cannot configure an inter-region VPC endpoint directly.

Option B is CORRECT: With inter-region VPC peering and VPC endpoint (PrivateLink), the EC2 instance can communicate with the DynamoDB table privately even if they belong to different regions.

Option C is incorrect: This option does not mention the usage of VPC endpoint.

Option D is incorrect: Because VPC peering supports the inter-region connections.

Ask our Experts Rate this Question?

View Queries open

Question 8 **Unattempted**

Domain :Design Secure Applications and Architectures

You have planned to host a web application on AWS. You create an EC2 Instance in a public subnet which needs to connect to an EC2 Instance that will host an Oracle database. Which steps would ensure a secure setup? (SELECT TWO)

A. Place the EC2 Instance with the Oracle database in the same public subnet as the Webserver for faster communication.

B. Place the ec2 instance in a public subnet and the oracle database in a private subnet

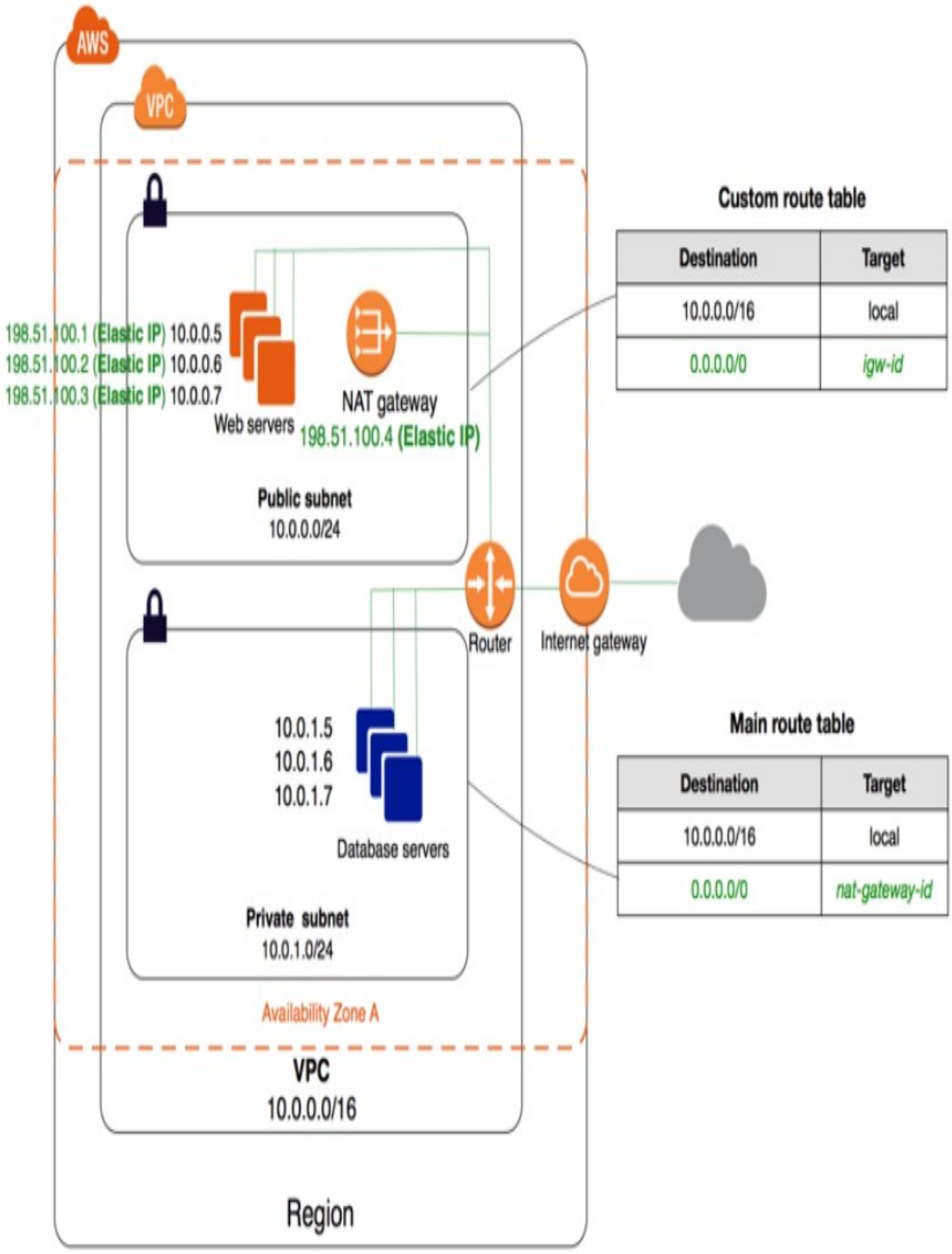
C. Create a database Security group which allows incoming traffic only from the Web server's security group.

D. Ensure that the database security group allows incoming traffic from 0.0.0.0/0

Explanation:

Correct Answer – B and C

The best and most secure option is to place the database in a private subnet. The below diagram from AWS Documentation shows this setup. Also, you ensure that access is not allowed from all sources but only from the web servers.



For more information on this type of setup, please refer to the below URL:

https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2.html

Option A is incorrect because as per the best practice guidelines, DB instances are placed in Private subnets and allowed to communicate with web servers in the public subnet.

Option D is incorrect because allowing all incoming traffic from the Internet to the DB instance is a security risk.

Try now labs related to this question

Build Amazon VPC with Public and Private Subnets from Scratch

1. Learn how to build Public and Private subnets from scratch.
2. VPC wizard will not be used. So every component required to build public and private subnets will be created and configured manually.
3. This will give an in-depth understanding of internal components of VPC and subnets.

Credit Needed 10 Time 0 : 30 Try Now

Ask our Experts Rate this Question?

View Queries open

Question 9 **Unattempted**

Domain :Design Secure Applications and Architectures

An EC2 Instance hosts a Java-based application that accesses a DynamoDB table. This EC2 Instance is currently serving production users. What would be a secure way for the EC2 Instance to access the DynamoDB table?

A. **Use IAM Roles with permissions to interact with DynamoDB and assign it to the EC2 Instance.**

B. Use KMS Keys with the right permissions to interact with DynamoDB and assign it to the EC2 Instance.

C. Use IAM Access Keys with the right permissions to interact with DynamoDB and assign it to the EC2 Instance.

D. Use IAM Access Groups with the right permissions to interact with DynamoDB and assign it to the EC2 Instance.

Explanation:

Correct Answer - A

Always assign a role to the EC2 Instance to ensure secure access to AWS resources from EC2 Instances.

For more information on IAM Roles, please refer to the below URL:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html

An IAM role is similar to a user; it is an AWS identity with permission policies that determine what the identity can and cannot do in AWS. However, instead of being uniquely associated with one person, a role is intended to be assumable by anyone who needs it. Also, an IAM role does not have standard long-term credentials (password or access keys) associated with it. Instead, if a user assumes a role, temporary security credentials are created dynamically and provided to the user.

You can use roles to delegate access to users, applications, or services that normally don't have access to your AWS resources.

Note:

You can attach IAM role to the existing EC2 instance. To know more, please visit the following URL:

https://aws.amazon.com/about-aws/whats-new/2017/02/new-attach-an-iam-role-to-your-existing-amazon-ec2-instance/

Ask our Experts Rate this Question?

View Queries open

Question 10 **Unattempted**

Domain :Design High-Performing Architectures

You have an RDS instance in a VPC. In the same AWS account, there is an EC2-Classic instance that does not belong to any VPC. The EC2 instance needs to communicate with the RDS instance using its private IPv4 address. Which method would you use?

A. **Modify the security group of the RDS instance to allow the incoming traffic from the EC2-Classic instance.**

B. **Attach a security group to the EC2 instance to allow all outgoing traffic.**

C. **Enable PrivateLink for the VPC and link the EC2-Classic instance.**

D. **Enable ClassicLink for the VPC and link the EC2 instance to the VPC.**

Explanation:

Correct Answer – D

For the communication between EC2-Classic instance and resources in VPC, ClassicLink should be used. Please check https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/vpc-classiclink.html#classiclink-basics.

Option A is incorrect: Even if the security group is modified, the EC2-Classic instance still cannot talk with the RDS instance in the VPC.

Option B is incorrect: Same as option A.

Option C is incorrect: Because PrivateLink is used for resources within the VPC. It is not suitable for EC2-Classic instances.

Option D is CORRECT: Because ClassicLink is the correct method to link EC2-Classic instances to VPC resources. Check the above link for how to work with ClassicLink.

Ask our Experts Rate this Question?

View Queries open

Question 11 **Unattempted**

Domain :Design High-Performing Architectures

A company has set up an application in AWS that interacts with DynamoDB. It is required that when an item is modified in a DynamoDB table, immediate entry is made to the associating application. How can this be accomplished? (SELECT TWO)

A. **Setup CloudWatch to monitor the DynamoDB table for changes. Then trigger a Lambda function to send the changes to the application.**

B. **Setup CloudWatch logs to monitor the DynamoDB table for changes. Then trigger AWS SQS to send the changes to the application.**

C. **Use DynamoDB streams to monitor the changes to the DynamoDB table.**

D. **Trigger a lambda function to make an associated entry in the application as soon as the DynamoDB streams are modified.**

Explanation:

Correct Answer – C and D

When you enable DynamoDB Streams on a table, you can associate the stream ARN with a Lambda function that you write. Immediately after an item in the table is modified, a new record appears in the table's stream. AWS Lambda polls the stream and invokes your Lambda function synchronously when it detects new stream records. Since our requirement is to have an immediate entry made to an application in case an item in the DynamoDB table is modified, a lambda function is also required.

Let us try to analyze this with an example:

Consider a mobile gaming app that writes to a GamesScores table. Whenever the top score of the Game Scores table is updated, a corresponding stream record is written to the table's stream. This event could then trigger a Lambda function that posts a Congratulatory message on a Social media network handle.

DynamoDB streams can be used to monitor the changes to a DynamoDB table.

AWS Documentation mentions the following:

A *DynamoDB stream* is an ordered flow of information about changes to items in an Amazon DynamoDB table. When you enable a stream on a table, DynamoDB captures information about every modification to data items in the table.

For more information on DynamoDB streams, please refer to the URL below.

https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Streams.html

Note:
DynamoDB is integrated with Lambda so that you can create *triggers* to events in DynamoDB Streams.

If you enable DynamoDB Streams on a table, you can associate the stream ARN with a Lambda function that you write. Immediately after an item in the table is modified, a new record appears in the table's stream.

AWS Lambda polls the stream and invokes your Lambda function synchronously when it detects new stream records. Since our requirement states that an item modified in a DynamoDB table causes an immediate entry to an associating application, a lambda function is also required.

For more information on DynamoDB streams Lambda, please refer to the URL below.

https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Streams.Lambda.html

Ask our Experts Rate this Question?

View Queries open

Question 12 **Unattempted**

Domain :Design Resilient Architectures

You are working as an AWS Consultant for an E-Commerce organization. The organization is planning to migrate to a managed database service using Amazon RDS. To avoid any business loss due to any deletion in the database, the management team is looking for a backup process which will restore Database at any specific time during the last month. Which action should be performed as a part of Amazon RDS Automated backup process?

A. **AWS performs storage volume snapshot of database instance during the backup window once a day, captures transactions logs every 5 minutes, and store in S3 buckets.**

B. AWS performs a full snapshot of the database every 12 hours during the backup window, captures transactions logs throughout the day, and store in S3 buckets.

C. AWS performs full daily snapshot during the backup window. Given this doesnt provide point in time restoration it does not meet the requirements.

D. AWS performs storage volume snapshot of the database instance every 12 hours during the backup window, captures transactions logs throughout the day, store in S3 buckets.

Explanation:

Correct Answer – A

During automated backup, Amazon RDS performs a storage volume snapshot of the entire Database Instance. Also, it captures transaction logs every 5 minutes. To restore a DB instance at a specific point of time, a new DB instance is created using this DB snapshot.

Option B is incorrect as Database Snapshots are the manual backups initiated by users, not by AWS. These Backups can be performed at any time.

Option C is incorrect as Database Snapshots are the manual backups initiated by users, not by AWS.

Option D is incorrect as AWS performs storage volume snapshot on a daily basis, not every 12 hours.

For more information on Amazon RDS Automated backup process and Restoring a DB instance to a specified time, refer to the following URL:

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

Ask our Experts Rate this Question?

View Queries open

Question 13 **Unattempted**

Domain :Design Secure Applications and Architectures

You configure an Amazon S3 bucket as the origin for a new CloudFront distribution. You need to restrict access so that users cannot view the files by directly using the S3 URLs. The files should

be only fetched through the CloudFront URL. Which method is the most appropriate?

A. **Configure Signed URLs to serve private content by using CloudFront.**

B. **Configure Signed Cookies to restrict access to S3 files.**

C. **Create the origin access identity (OAI) and associate it with the distribution.**

D. **Configure the CloudFront web distribution to ask viewers to use HTTPS to request S3 objects.**

Explanation:

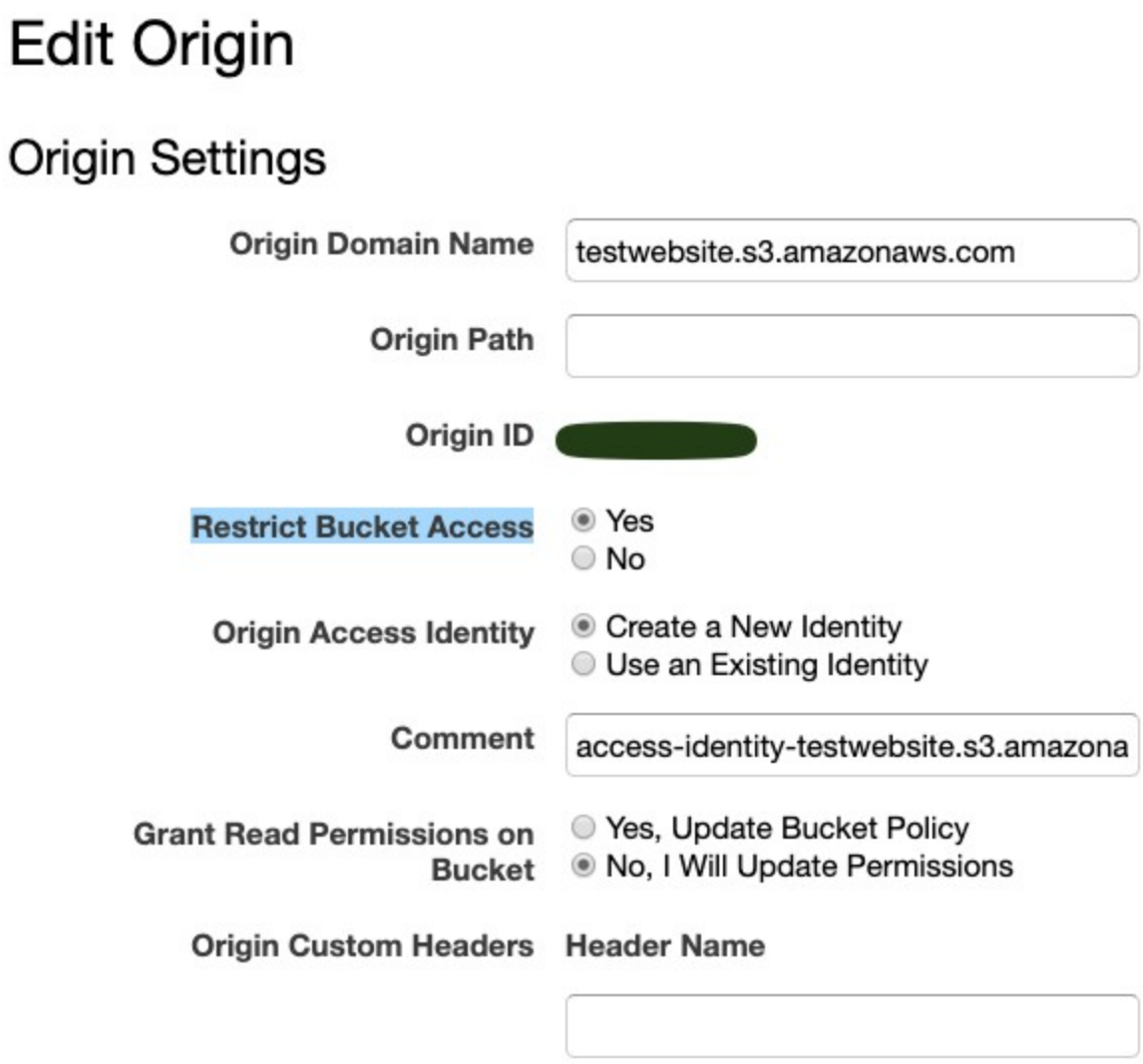
Correct Answer – C

In this scenario, users should only access S3 files through CloudFront instead of S3 URLs. Option C is the correct option. About how to work with origin access identities, please check https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html.

Option A is incorrect: Because Signed URLs are used to restrict access to files in CloudFront edge caches. It cannot prevent users from fetching files directly through S3 URLs. Check https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/PrivateContent.html.

Option B is incorrect: Same reason as option A.

Option C is CORRECT: Because you can configure the CloudFront origin to restrict bucket access through OAI:



Option D is incorrect: With HTTPS, connections are encrypted between CloudFront and viewers. However, it does not restrict access to the S3 content.

Ask our Experts

Rate this Question?

View Queries

open

Question 14

Unattempted

Domain :Design High-Performing Architectures

As a Solutions Architect for a multinational organization having more than 150000 employees, management has decided to implement a real-time analysis for their employees' time spent in offices across the globe. You are tasked to design an architecture that will receive the inputs from

10000+ sensors with swipe machine sending in and out data across the globe, each sending 20KB data every 5 Seconds in JSON format. The application will process and analyze the data and upload the results to dashboards in real-time.
Other application requirements will include the ability to apply real-time analytics on the captured data, processing of captured data will be parallel and durable, the application must be scalable as per the requirement as the load varies and new sensors are added or removed at various facilities. The analytic processing results are stored in a persistent data storage for data mining.
What combination of AWS services would be used for the above scenario?

A. **Use EMR to copy the data coming from Swipe machines into DynamoDB and make it available for analytics**

B. **Use Amazon Kinesis Streams to ingest the Swipe data coming from sensors, Custom Kinesis Streams Applications to analyze the data and then move analytics outcomes to RedShift using AWS EMR**

C. **Use SQS to receive the data coming from sensors, Kinesis Firehose to analyze the data from SQS, then save the results to a Multi-AZ RDS instance**

D. **Use Amazon Kinesis Streams to ingest the sensors' data, custom Kinesis Streams applications to analyze the data, and move analytics outcomes to RDS using AWS EMR**

Explanation:

Correct Answer - B

Option A is incorrect. EMR is not for receiving the real-time data from thousands of sources, EMR is mainly used for Hadoop ecosystem-based data used for Big data analysis.

Option B is correct as the Amazon Kinesis streams are used to read the data from thousands of sources like social media, survey-based data, etc. The Kinesis streams can be used to analyze the data and can feed it using AWS EMR to the analytics-based database like RedShift which works on OLAP.

Option C is incorrect, SQS cannot be used to read the real-time data from thousands of sources. Besides, the Kinesis Firehose is used to ship the data to other AWS service, not for the analysis. And finally, RDS is again an OLTP based database.

Option D is incorrect as the AWS EMR can read large amounts of data, however, RDS is a transactional database that works based on the OLTP. Thus, it cannot store the analytical data.

Ask our Experts

Rate this Question?

View Queries

open

Question 15

Unattempted

Domain :Design Cost-Optimized Architectures

You have a local data center on premise which stores archived files. The total amount of the files is about 70TB. The data needs to be transferred to Amazon Simple Storage Service (S3). After the data transfer is finished, the local data center will not be used. Which solution is the most appropriate?

A. **AWS Direct Connect.**

B. **AWS Snowball.**

C. **Amazon S3 Transfer Acceleration.**

D. **AWS Global Accelerator.**

Explanation:

Correct Answer – B

AWS Snowball has 80TB and 50TB models. The 80TB model is suitable to transfer 70TB of data to AWS. Please refer to https://docs.aws.amazon.com/snowball/latest/ug/whatissnowball.html.

Option A is incorrect: Because Direct Connect establishes a network connection from on premises to an AWS Region. It is not suitable to move 70TB of data.

Option B is CORRECT: Because AWS Snowball is a data transport solution that accelerates moving terabytes to petabytes of data to AWS.

Option C is incorrect: S3 Transfer Acceleration uses Amazon CloudFront's globally distributed edge locations. It does not help in this scenario.

Option D is incorrect: Because AWS Global Accelerator improves availability and performance for applications, which does not help on the data transfer.

Ask our Experts Rate this Question?

View Queries open

Question 16 **Unattempted**

Domain :Design Secure Applications and Architectures

You have designed an application that uses AWS resources, such as S3 to operate and store users' documents. You currently use Cognito identity pools and user pools. To increase usage and ease of signing up, you decide that adding social identity federation is the best path forward. How would you differentiate the Cognito identity pool and the federated identity providers (e.g. Google)?

A. **They are the same and just called different things**

B. **First, you sign-in via Cognito then through a federated site, like Google**

C. **Federated identity providers and identity pools are used to authenticate services**

D. **Sign-in via AWS Cognito User Pool and sign-in via AWS Cognito Identity Pool are independent of one another**

Explanation:

Correct Answer - D

Option D is correct. Sign-in through a third party (federation) is available in Amazon Cognito user pools. This feature is independent of the federation through Amazon Cognito identity pools (federated identities).

Option A is incorrect. Cognito identity pool and the federated identity providers are separate, independent authentication methods.

Option B is incorrect. Only one log-in event is needed, not two.

Option C is incorrect. Identity providers authenticate users, not authenticate services.

For more information, refer to the following URLs:

https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-user-pools-identity-federation.html

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_oidc.html

https://aws.amazon.com/articles/web-identity-federation-with-mobile-applications/

https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-getting-started.html

Ask our Experts

Rate this Question?

View Queries

open

Question 17

Unattempted

Domain :Design High-Performing Architectures

You have a web application hosted on an EC2 Instance in AWS which is being accessed by users across the globe. The Operations team has been receiving support requests about extreme slowness from users in some regions. What can be done to the architecture to improve the response time for these users?

A. **Add more EC2 Instances to support the load.**

B. **Change the Instance type to a higher instance type.**

C. **Add Route 53 health checks to improve the performance.**

D. **Place the EC2 Instance behind CloudFront.**

Explanation:

Correct Answer – D

AWS Documentation mentions the following:

Amazon CloudFront is a web service that speeds up distribution of your static and dynamic web content, such as .html, .css, .js, 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 Amazon CloudFront, please refer to the below URL:

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html

Option A is incorrect. The latency issue is experienced by people from certain parts of the world only. So, increasing the number of EC2 Instances or increasing the instance size will not make much difference.

Option B is incorrect. The latency issue is experienced by people from certain parts of the world only. So, changing the Instance type to a higher instance type will not make much difference.

Option C is incorrect. Route 53 health checks are meant to see whether the instance status is healthy or not.

Since this case deals with responding to requests from users, we do not have to worry about this. However, for improving latency issues, CloudFront is a good solution.

Ask our Experts

Rate this Question?

View Queries

open

Question 18

Unattempted

Domain :Design Resilient Architectures

You currently have your EC2 instances running in multiple availability zones. You have a NAT gateway defined for your private instances and you want to make this highly available. How could this be accomplished?

A. **Create another NAT Gateway and place it behind an ELB.**

B. **Create a NAT Gateway in another Availability Zone.**

C. **Create a NAT Gateway in another region.**

D. **Use Auto Scaling groups to scale the NAT Gateway.**

Explanation:

Correct Answer - B

AWS Documentation mentions the following:

If you have resources in multiple Availability Zones and they share one NAT Gateway, in the event that the NAT Gateway's Availability Zone is down, resources in the other Availability Zones lose internet access. To create an Availability Zone-independent architecture, create a NAT Gateway in each Availability Zone and configure your routing to ensure that resources use the NAT Gateway in the same Availability Zone.

For more information on the NAT Gateway, please refer to the below URL:

https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-nat-gateway.html

Try now labs related to this question

Creating NAT Gateways in AWS

This lab walks you through the steps to Create A NAT Gateway and allow internet access to Instance in Private Subnet.

Credit Needed 10 Time 0 : 45 Try Now

Ask our Experts Rate this Question?

View Queries open

Question 19 **Unattempted**

Domain :Design Resilient Architectures

A company wants to have a fully managed data store in AWS. It should be a compatible MySQL database, which is an application requirement. Which AWS database engine could be used for this purpose?

A. **AWS RDS**

B. **AWS Aurora**

C. **AWS DynamoDB**

D. **AWS Redshift**

Explanation:

Correct Answer - B

AWS Documentation mentions the following:

Amazon Aurora (Aurora) is a fully managed, MySQL and PostgreSQL compatible, relational database engine. It combines the speed and reliability of high-end commercial databases with the simplicity and cost-effectiveness of open-source databases. It delivers up to five times the throughput of MySQL and up to three times the throughput of PostgreSQL without requiring changes to most of your existing applications.

For more information on AWS Aurora, please refer to the URL below.

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Aurora.Overview.html

Note:

RDS is a generic service to provide Relational Database service which supports 6 database engines. They are Aurora, MySQL, MariaDB, PostgreSQL, Oracle, and Microsoft SQL Server. Our

question is to select MySQL compatible database from the options provided. Out of the given options, **Amazon Aurora** is a MySQL and PostgreSQL compatible enterprise-class database.

Hence Option B is the correct answer.

If you see the question "A company wants to have a fully managed data store in AWS. It should be a compatible MySQL database, which is an application requirement. Which **database engine could be used for this purpose?", We have to select the database engine. RDS is not the correct answer because RDS is not a database engine. MySQL is one of the offerings of the RDS service. This question is about understanding the terminology.**

Try now labs related to this question

Introduction to Amazon Aurora

This lab walks you through the creation and testing of an Amazon Aurora database. We will create an Aurora MySQL Database and and test the connection.

Credit Needed 10 Time 1 : 30 Try Now

Ask our Experts Rate this Question?

View Queries open

Question 20 **Unattempted**

Domain :Design High-Performing Architectures

A Solutions Architect is designing an online shopping application running in a VPC on EC2 Instances behind an Elastic Load Balancer. The instances run in an Auto Scaling group across multiple Availability Zones. The application tier must read and write data to a customer-managed database cluster. There should be no access to the database from the Internet but the cluster must be able to obtain software patches from the Internet. Which VPC design meets these requirements?

A. **Public subnets for both the application tier and the database cluster.**

B. **Public subnets for the application tier and private subnets for the database cluster.**

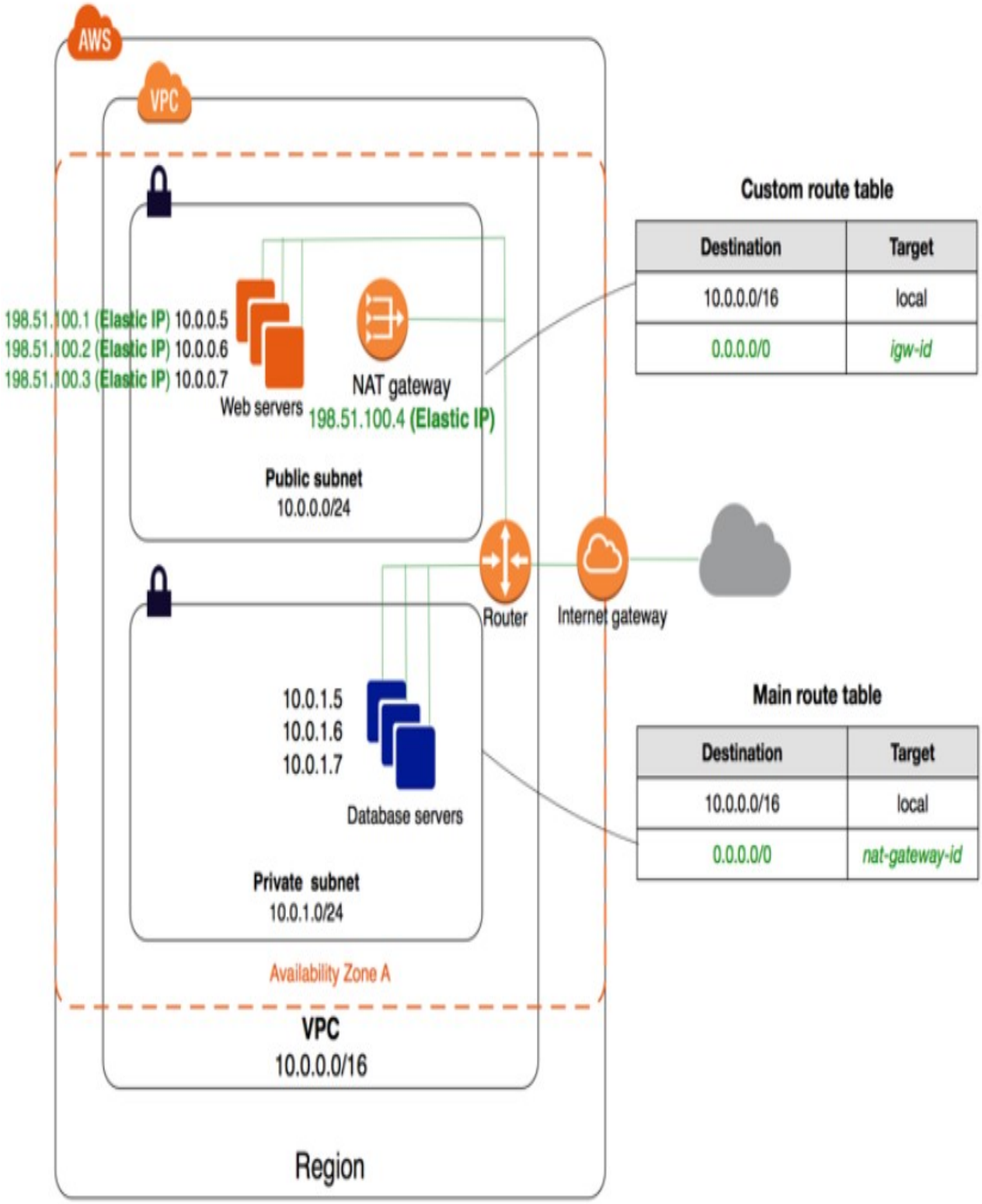
C. Public subnets for both application tier and NAT Gateway and private subnets for the database cluster.

D. Private subnets for the application tier and private subnets for both the database cluster and NAT Gateway

Explanation:

Correct Answer – C

The following diagram from AWS Documentation shows the right setup for this scenario:



We always need to keep NAT gateway on public Subnet only, because it needs to communicate the Internet.

AWS says that "To create a NAT gateway, you must specify the public subnet in which the NAT

gateway should reside. You must also specify an Elastic IP address to associate with the NAT gateway when you create it. After you've created a NAT gateway, you must update the route table associated with one or more of your private subnets to point Internet-bound traffic to the NAT gateway. This enables instances in your private subnets to communicate with the internet."

For more information on this setup, please refer to the below URL:

https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-nat-gateway.html

NOTE:

Here the requirement is that "**There should be no access to the database from the Internet, but the cluster must be able to obtain software patches from the Internet.**"

1) **There should be no access to the database from the Internet.**
To achieve this step, we have to launch the database inside the private subnet.

2) **But the cluster must be able to obtain software patches from the Internet.**
For this, we have to create NAT Gateway inside the **Public Subnet.** Because the subnet with internet gateway attached is known as Public Subnet. Through the NAT Gateway, a database inside the Private subnet can access the internet. **Option D is saying that "Use private subnet for NAT gateway".**

Option C includes these discussed Points and thus, it's a perfect answer.

Try now labs related to this question

Creating NAT Gateways in AWS

This lab walks you through the steps to Create A NAT Gateway and allow internet access to Instance in Private Subnet.

Credit Needed 10 Time 0 : 45 Try Now

Ask our Experts Rate this Question?

View Queries open

Question 21 **Unattempted**

Domain :Design High-Performing Architectures

It is expected that only certain specified customers can upload images to the S3 bucket for a certain period of time. What would you suggest as an architect to fulfill this requirement?

A. **Create a secondary S3 bucket. Then, use an AWS Lambda to sync the contents to the primary bucket.**

B. **Use pre-signed URLs for uploading the images.**

C. **Use ECS Containers to upload the images.**

D. **Upload the images to SQS and then push them to the S3 bucket.**

Explanation:

Correct Answer – B

The S3 bucket owner can create Pre-Signed URLs to upload the images to S3.

For more information on Pre-Signed URLs, please refer to the URL below.

https://docs.aws.amazon.com/AmazonS3/latest/dev/PresignedUrlUploadObject.html

Option A is incorrect. Since Amazon has provided us with an inbuilt function for this requirement, using this option is expensive and time-consuming. As a Solution Architect, you are supposed to pick the best and cost-effective solution.

Option C is incorrect. ECS is a highly scalable, fast, container management service that makes it easy to run, stop, and manage Docker containers on a cluster.

Option D is incorrect. SQS is a message queue service used by distributed applications to exchange messages through a polling model and not through a push mechanism.

Note:

This question is based on the scenario where we can use the pre-signed URL.

You need to understand about pre-signed URL - which contains the user login credentials

particular resources, such as S3 in this scenario. And user must have the permission enabled that other application can use the credential to upload the data (images) in S3 buckets.

AWS Definition:

"A pre-signed URL gives you access to the object identified in the URL, provided that the creator of the pre-signed URL has permissions to access that object. That is, if you receive a pre-signed URL to upload an object, you can upload the object only if the creator of the pre-signed URL has the necessary permissions to upload that object.

All objects and buckets by default are private. The pre-signed URLs are useful if you want your user/customer to be able to upload a specific object to your bucket, but you don't require them to have AWS security credentials or permissions. When you create a pre-signed URL, you must provide your security credentials and then specify a bucket name, an object key, an HTTP method (PUT for uploading objects), and expiration date and time. The pre-signed URLs are valid only for the specified duration."

For more information, please visit the following URL:

https://docs.aws.amazon.com/AmazonS3/latest/dev/PresignedUrlUploadObject.html

Ask our Experts Rate this Question?

View Queries open

Question 22 **Unattempted**

Domain :Design High-Performing Architectures

A company requires to use the AWS RDS service to host a MySQL database. This database is going to be used for production purposes and is expected to experience a high number of read/write activities. Which EBS volume type would be ideal for this database?

A. **General Purpose SSD**

B. **Provisioned IOPS SSD**

C. **Throughput Optimized HDD**

D. Cold HDD

Explanation:

Correct Answer - B

The below snapshot from AWS Documentation shows that the ideal storage option in this scenario is the Provisioned IOPS SSD since it provides a high number of IOPS for the underlying database.

	Solid-State Drives (SSD)		Hard disk Drives (HDD)	
Volume Type	General Purpose SSD (gp2)*	Provisioned IOPS SSD (io1)	Throughput Optimized HDD (st1)	Cold HDD (sc1)
Description	General purpose SSD volume that balances price and performance for a wide variety of workloads	Highest-performance SSD volume for mission-critical low-latency or high-throughput workloads	Low cost HDD volume designed for frequently accessed, throughput-intensive workloads	Lowest cost HDD volume designed for less frequently accessed workloads
Use Cases	• Recommended for most workloads • System boot volumes • Virtual desktops • Low-latency interactive apps • Development and test environments	• Critical business applications that require sustained IOPS performance, or more than 10,000 IOPS or 160 MiB/s of throughput per volume • Large database workloads, such as: ◦ MongoDB ◦ Cassandra ◦ Microsoft SQL Server ◦ MySQL ◦ PostgreSQL ◦ Oracle	• Streaming workloads requiring consistent, fast throughput at a low price • Big data • Data warehouses • Log processing • Cannot be a boot volume	• Throughput-oriented storage for large volumes of data that is infrequently accessed • Scenarios where the lowest storage cost is important • Cannot be a boot volume

For more information on EBS volume types, please refer to the URL below.

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html

Try now labs related to this question

Introduction to AWS Relational Database Service

This lab walks you through to the creation and testing of an Amazon Relational Database Service (Amazon RDS) database. We will create an RDS MySql Database and test the connection using MySQL Workbench.

Credit Needed 10 Time 0 : 50 Try Now

Ask our Experts Rate this Question?

View Queries open

Question 23 **Unattempted**

Domain :Design High-Performing Architectures

You own a MySQL RDS instance in AWS Region us-east-1. The instance has a Multi-AZ instance in another availability zone for high availability. As business grows, there are more and more clients coming from Europe (eu-west-2) and most of the database workload is read-only. What is the proper way to reduce the load on the source RDS instance?

A. **Create a snapshot of the instance and launch a new instance in eu-west-2.**

B. **Promote the Multi-AZ instance to be a Read Replica and move the instance to eu-west-2 region.**

C. **Configure a read-only Multi-AZ instance in eu-west-2 as Read Replicas cannot span across regions.**

D. **Create a Read Replica in the AWS Region eu-west-2.**

Explanation:

Correct Answer – D

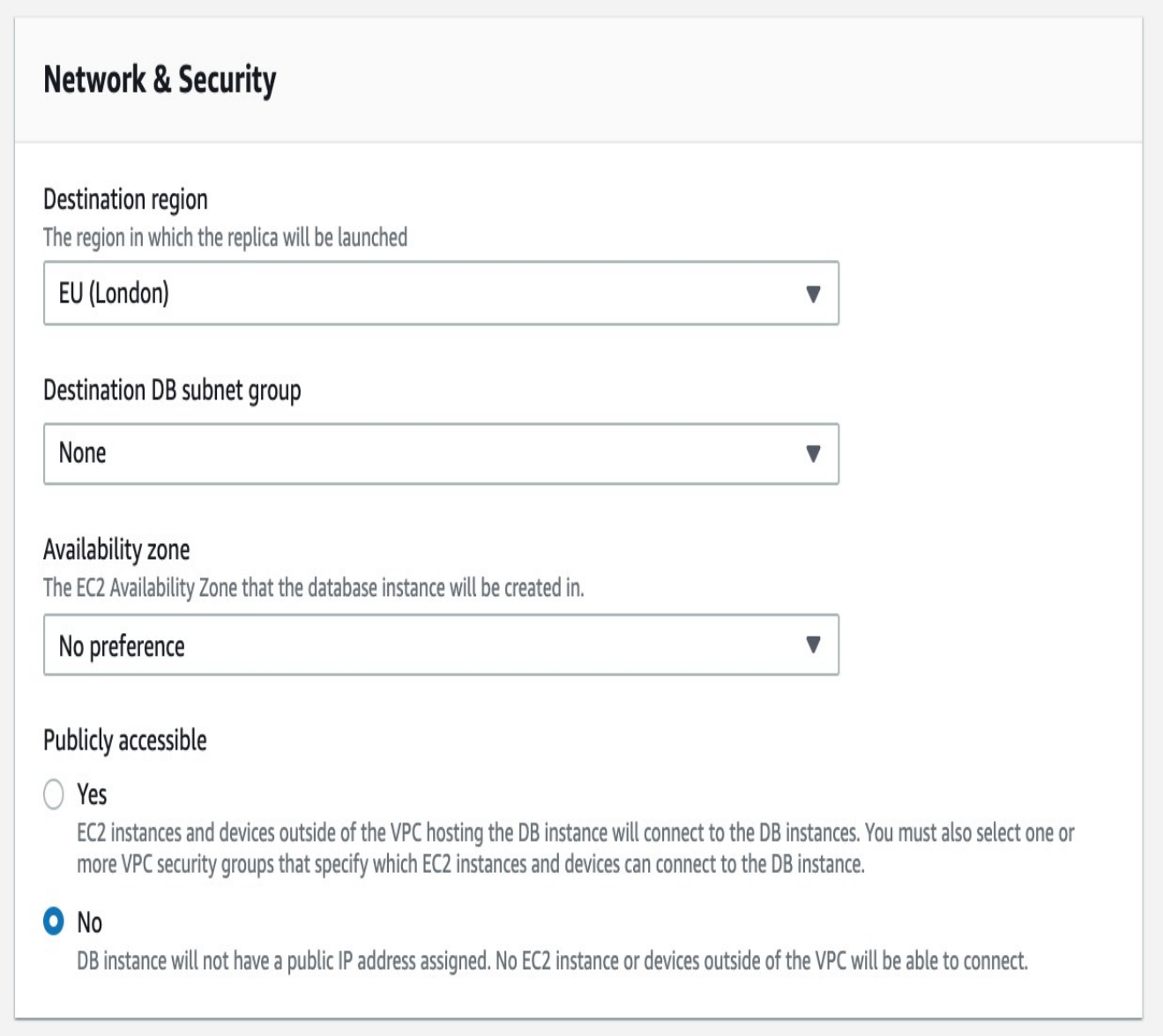
Read Replica should be used to share the read workload of the source DB instance. Read Replica can also be configured in a different AWS region. Refer to https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html.

Option A is incorrect: Because Read Replica should be configured to share the read traffic. You should not launch a totally new instance.

Option B is incorrect: Because a Multi-AZ instance cannot be promoted to be a Read Replica.

Option C is incorrect: Because a Read Replica can be launched in another region for RDS MySQL.

Option D is CORRECT: Users can quickly configure a Read Replica in another region:



Ask our Experts Rate this Question?

View Queries open

Question 24 **Unattempted**

Domain :Design Secure Applications and Architectures

A company has a set of web servers. It is required to ensure that all the logs from these web servers can be analyzed in real-time for any sort of threat detection. What could be the right choice in this regard?

A. **Upload all the logs to the SQS Service and then use EC2 Instances to scan the logs.**

B. **Upload the logs to Amazon Kinesis and then analyze the logs accordingly.**

C. **Upload the logs to CloudTrail and then analyze the logs accordingly.**

D. **Upload the logs to Glacier and then analyze the logs accordingly.**

Explanation:

Correct Answer – B

AWS Documentation provides the following information to support this requirement:

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 process streaming data cost-effectively 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 video, audio, application logs, website clickstreams, and IoT telemetry data for machine learning, analytics, and other applications.

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

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

Ask our Experts Rate this Question?

View Queries open

Question 25 **Unattempted**

Domain :Design High-Performing Architectures

You currently have the following architecture in AWS:
a. A couple of EC2 Instances located in us-west-2a
b. The EC2 Instances are launched via an Auto Scaling group.
c. The EC2 Instances sit behind a Classic ELB.
Which additional step would ensure that the above architecture conforms to a well-architected framework?

A. **Convert the Classic ELB to an Application ELB.**

B. **Add an additional Auto Scaling Group.**

C. **Add additional EC2 Instances to us-west-2a.**

D. **Add or spread existing instances across multiple Availability Zones.**

Explanation:

Correct Answer - D

AWS Documentation provides the following information to support this concept:

Balancing resources across Availability Zones is a best practice for well-architected applications, as this greatly increases aggregate system availability. Auto Scaling automatically balances EC2 instances across zones when you configure multiple zones in your Auto Scaling group settings. Auto Scaling always launches new instances such that they are balanced between zones as evenly as possible across the entire fleet.

For more information on managing resources with Auto Scaling, please refer to the URL below.

https://aws.amazon.com/blogs/compute/fleet-management-made-easy-with-auto-scaling/

Ask our Experts Rate this Question?

View Queries open

Question 26 **Unattempted**

Domain :Design Resilient Architectures

Your company manages an application that currently allows users to upload images to an S3 bucket. These images are picked up by EC2 Instances for processing and then placed in another S3 bucket. You need an area where the metadata for these images can be stored. What would be an ideal data store for this?

A. AWS Redshift

B. AWS Glacier

C. AWS DynamoDB

D. AWS SQS

Explanation:

Correct Answer - C

Option A is incorrect because this is normally used for petabyte based storage.

Option B is incorrect because this is used for archive storage.

Option C is correct. AWS DynamoDB is the best, light-weight and durable storage option for metadata.

Option D is incorrect because this used for messaging purposes.

For more information on DynamoDB, please refer to the URL below.

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

Ask our Experts Rate this Question?

View Queries open

Question 27 **Unattempted**

Domain :Design High-Performing Architectures

An application team needs to quickly provision a development environment consisting of a web and database layer. What would be the quickest and most ideal way to get this set up in place?

A. **Create Spot Instances and install the web and database components.**

B. **Create Reserved Instances and install the web and database components.**

C. **Use AWS Lambda to create the web components and AWS RDS for the database layer.**

D. **Use Elastic Beanstalk to quickly provision the environment.**

Explanation:

Correct Answer – D

AWS Documentation mentions the following:

With Elastic Beanstalk, you can quickly deploy and manage applications in the AWS Cloud without worrying about the infrastructure that runs those applications. AWS Elastic Beanstalk reduces management complexity without restricting choice or control. You simply upload your application, and Elastic Beanstalk automatically handles the details of capacity provisioning, load balancing, scaling, and application health monitoring.

For more information on AWS Elastic Beanstalk, please refer to the URL below.

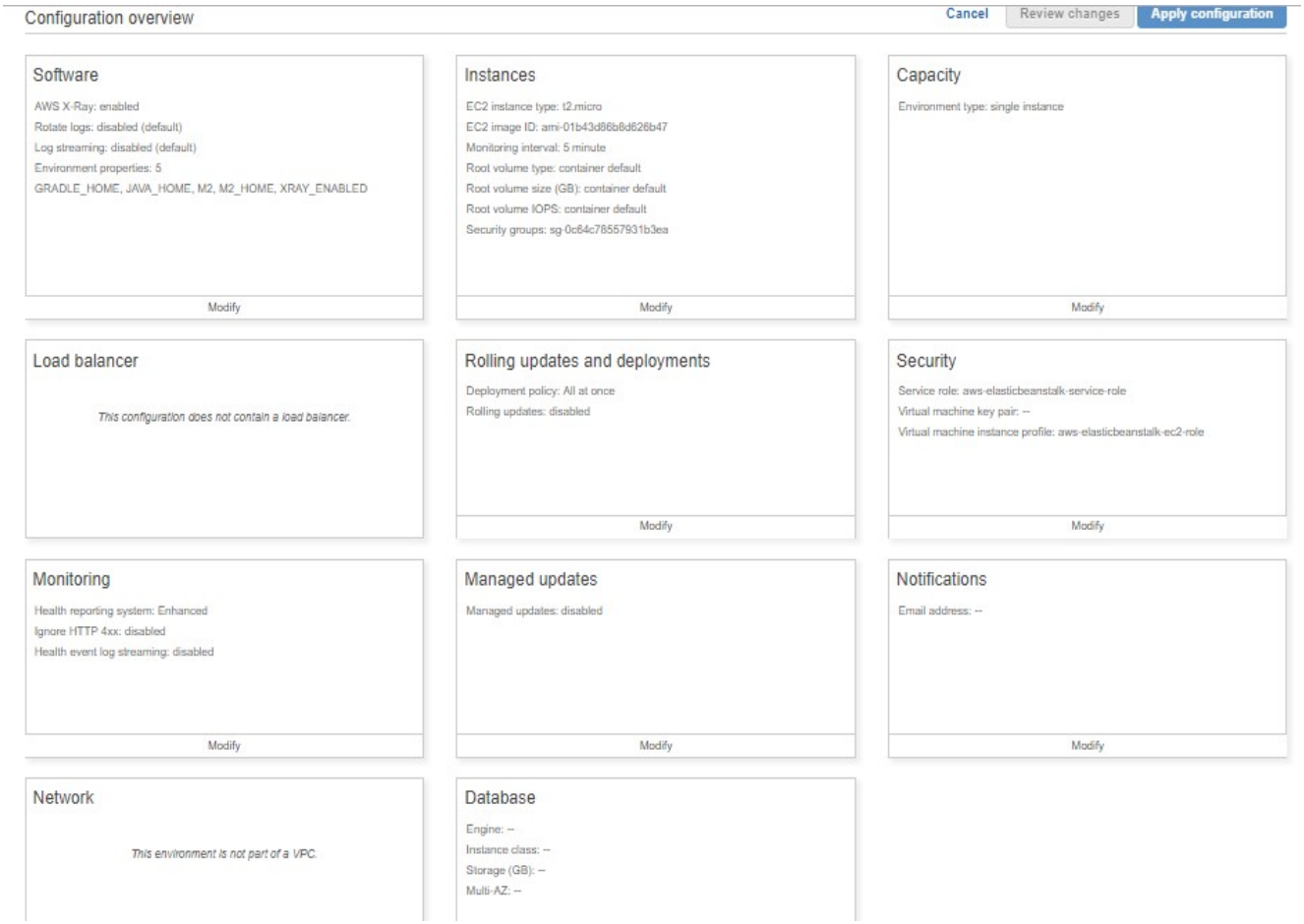
https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/Welcome.html

Option A is incorrect. Amazon EC2 Spot instances are spare compute capacity in the AWS cloud available to you at steep discounts compared to On-Demand prices.

Option B is incorrect. A Reserved Instance is a reservation of resources and capacity, for either one or three years for a particular Availability Zone within a region.

Option C is incorrect. AWS Lambda is a compute service that makes it easy for you to build applications that respond quickly to new information and not for provisioning a new environment.

Currently, the Elastic Beanstalk environment supports the following configurations:



It supports RDS.

Database Configuration Setting

AWS Elastic Beanstalk provides connection information to your instances by setting environment properties for the database hostname, username, password, table name, and port. When you add a database to your environment, its lifecycle is tied to your environments.

Ask our Experts Rate this Question?

View Queries open

Question 28 **Unattempted**

Domain :Design Secure Applications and Architectures

Third-party sign-in (Federation) has been implemented in your web application to allow users who need access to AWS resources. Users have been successfully logging in using Google, Facebook, and other third-party credentials. Suddenly, their access to some AWS resources has been restricted. What is the most likely cause of the restricted use of AWS resources?

A. IAM policies for resources were changed, thereby restricting access to AWS resources

B. Federation protocols are used to authorize services and need to be updated

C. AWS changed the services allowed to be accessed via federated login

D. The identity providers no longer allow access to AWS services

Explanation:

Correct Answer: A

Option A is correct. When IAM policies are changed, they can impact the user experience and services they can connect to.

Option B is incorrect. Federation is used to authenticate users, not to authorize services.

Option C is incorrect. Federation is used to authenticate users, not to authorize services.

Option D is incorrect. The identity providers don't have the capability to authorize services; they authenticate users.

References:

https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-user-pools-identity-federation.html

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_oidc.html

https://aws.amazon.com/articles/web-identity-federation-with-mobile-applications/

Ask our Experts

Rate this Question?

View Queries

open

Question 29

Unattempted

Domain :Design Cost-Optimized Architectures

A company has an application that stores images and thumbnails on S3. The thumbnail needs to be available for download immediately. Additionally, both the images and thumbnails are not accessed frequently. What would be the cost-efficient storage option that meets the above-mentioned requirements?

A. Amazon Glacier with Expedited Retrievals.

B. Amazon S3 Standard Infrequent Access

C. Amazon EFS

D. Amazon S3 Standard

Explanation:

Correct Answer – B

Amazon S3 Infrequent access is perfect if you want to store data that is not frequently accessed. It is more cost-effective than Option D (Amazon S3 Standard). If you choose Amazon Glacier with Expedited Retrievals, you defeat the whole purpose of the requirement, because of its increased cost.

For more information on AWS Storage Classes, please visit the following URL:

https://aws.amazon.com/s3/storage-classes/

Try now labs related to this question

Introduction to Amazon Simple Storage Service (S3)

This lab walks you through to Amazon Simple Storage Service. Amazon S3 has a simple web services interface that you can use to store and retrieve any amount of data, at any time, from anywhere on the web. In this lab we will demonstrate AWS S3 by creating a sample S3 bucket, uploading an object to S3 bucket and setting up bucket permission and policy.

Credit Needed 10 Time 0 : 30 Try Now

Ask our Experts Rate this Question?

View Queries open

Question 30 **Unattempted**

Domain :Design Secure Applications and Architectures

A security audit discovers that one of your RDS MySQL instances is not encrypted. The instance has a Read Replica in the same AWS region which is also not encrypted. You need to fix this issue as soon as possible. What is the proper way to add encryption to the instance and its replica?

A. **Copy a DB snapshot and encrypt the snapshot. Restore a new DB instance from the encrypted snapshot and add a Read Replica.**

B. **Encrypt the DB instance. Launch a new Read Replica and the replica is encrypted automatically.**

C. **Create a DB snapshot and encrypt the snapshot. Launch a new instance and its Read Replica from the snapshot.**

D. **Promote the Read Replica to be a standalone instance and encrypt it. Add a new Read Replica to the standalone instance.**

Explanation:

Correct Answer – A

Existing unencrypted RDS instances and their snapshots cannot be encrypted. Users can only enable encryption for an RDS DB instance when they create it. The limitations can be found in

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html.

Option A is CORRECT: Because you can encrypt a copy of an unencrypted DB snapshot. Then the new RDS instance launched from the snapshot and its Read Replica are encrypted.

Option B is incorrect: Because you cannot encrypt an unencrypted RDS instance directly.

Option C is incorrect: Because you cannot encrypt an unencrypted DB snapshot according to the above reference.

Option D is incorrect: Because an unencrypted DB Read Replica cannot be encrypted. The correct method is to launch a new instance from an encrypted DB snapshot.

Ask our Experts Rate this Question?

View Queries open

Question 31 **Unattempted**

Domain :Design High-Performing Architectures

You have an application hosted on AWS consisting of EC2 Instances launched via an Auto Scaling Group. You notice that the EC2 Instances are not scaling on demand. Which checks should be done to ensure that the scaling occurs as expected? **(Select 2)**

A. **Ensure that the right metrics are being used to trigger the scale-out.**

B. **Check your scaling policies to see whether more than one policy is triggered by an event.**

C. **Ensure that AutoScaling health checks are being used.**

D. **Ensure that you are using Load Balancers.**

Explanation:

Correct Answer – A and B

There could be a number of reasons as mentioned in AWS Documentation but only options A and B are applicable from the given choices.

Option A is correct because if your scaling events are not based on the right metrics and do not

have the right threshold defined, then the scaling will not occur as you want it to happen.

Option B is correct because f two policies are executed at the same time, Amazon EC2 Auto Scaling follows the policy with the greater impact. For example, if you have one policy to add two instances and another policy to add four instances, Amazon EC2 Auto Scaling adds four instances when both policies are triggered at the same time.

Option C is incorrect because health checks will help us know the health status of an Auto Scaling instance. It is not a Check if AutoScaling is not working as expected. It is a health check for **Instance.**

Option D is incorrect because AutoScaling can be used without Load Balancer also.

For more information on Auto Scaling Dynamic Scaling and troubleshooting, please visit the following URsL:

https://aws.amazon.com/premiumsupport/knowledge-center/auto-scaling-troubleshooting/

https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scale-based-on-demand.html

https://docs.aws.amazon.com/autoscaling/ec2/userguide/ts-as-instancelaunchfailure.html

Try now labs related to this question

Introduction to Amazon Auto Scaling

AWS Auto Scaling will automatically scale resources as needed to align to your selected scaling strategy, This lab walks you through to use Auto Scaling to automatically launch or terminate EC2's instances based on user defined policies, schedules and health checks.

Credit Needed 10 Time 0 : 55 Try Now

Ask our Experts Rate this Question?

View Queries open

Question 32 **Unattempted**

Domain :Design Resilient Architectures

A Media firm has a global presence for its sports programming & broadcasting network which

uses AWS Infrastructure. They have multiple AWS accounts created based upon verticals & to manage these accounts they have used AWS Organizations. Recently this firm was acquired by another media firm which is also using AWS Infrastructure for media streaming services. Both of these firms need to merge AWS accounts to have new policies created & enforce these policies on all the member AWS accounts of the merged entities.
As an AWS Consultant, which of the following steps would you suggest to the client to move the master account of the original media firm to the organization used by the merged entity? (Select Three.)

A. **Remove all member accounts from the old organization.**

B. **Make another member account the master account.**

C. **Delete the old organization.**

D. **Invite the old master account to join the new organization as a member account.**

E. **Invite the old master account to join the new organization as a master account.**

Explanation:

Correct Answer – A, C, D

To move the master account from one organization to other organization, the following steps needs to be implemented,

· Remove all member accounts from the old organization.

· Delete the old organization.

· Invite the master account of the old organization to be a member account of the new organization.

Option B is incorrect as the master account of an AWS organization cannot be replaced by another member account.

Option E is incorrect as a master account will be joining as a member account of the new organization, not as a master account.

For more information on migrating accounts between AWS organizations, refer to the following URL,

https://aws.amazon.com/premiumsupport/knowledge-center/organizations-move-

accounts/

Ask our Experts

Rate this Question?

View Queries

open

Question 33

Unattempted

Domain :Design Secure Applications and Architectures

Your company has designed an app and requires it to store data in DynamoDB. The company has registered the app with identity providers so users can sign-in using third-parties like Google and Facebook. What must be in place such that the app can obtain temporary credentials to access DynamoDB?

A. **Multi-factor authentication must be used to access DynamoDB**

B. **AWS CloudTrail needs to be enabled to audit usage**

C. **An IAM role allowing the app to have access to DynamoDB**

D. **The user must additionally log into the AWS console to gain database access**

Explanation:

Correct Answer: C

Option C is correct. The user will have to assume a role that has the permissions to interact with DynamoDB.

Option A is incorrect. Multi-factor authentication is available, but not required

Option B is incorrect. CloudTrail is recommended for auditing but is not required

Option D is incorrect. A second log-in event to the management console is not required

References:

https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-user-pools-identity-federation.html

ttps://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_oidc.html

https://aws.amazon.com/articles/web-identity-federation-with-mobile-applications/

Try now labs related to this question

Introduction to AWS Identity Access Management(IAM)

This lab walks you through the steps on how to create IAM Users, IAM Groups and adding IAM User to the IAM Group in AWS IAM service

Credit Needed 0 Time 0 : 20 Try Now

Ask our Experts Rate this Question?

View Queries open

Question 34 **Unattempted**

Domain :Design Resilient Architectures

A company has an entire infrastructure hosted on AWS. It requires to create code templates used to provide the same set of resources in another region in case of a disaster in the primary region. Which AWS service can be helpful in this regard?

A. AWS Beanstalk

B. AWS CloudFormation

C. AWS CodeBuild

D. AWS CodeDeploy

Explanation:

Correct Answer – B

AWS Documentation provides the following information to support this requirement:

AWS CloudFormation provisions your resources in a safe and repeatable manner, allowing you to build and rebuild your infrastructure and applications, without having to perform manual actions or write custom scripts. CloudFormation takes care of determining the right operations to perform while managing your stack and rolls back changes automatically if errors are detected.

For more information on AWS CloudFormation, please visit the following URL:

https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/Welcome.html

AWS Beanstalk - is an orchestration service for deploying applications that orchestrate various AWS Services, including EC2, S3, SNS, CloudWatch, AutoScaling, and ELB.

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

AWS CodeBuild - is a fully managed continuous integration(CI) service that compiles source code, run tests, and produces software packages that are ready to deploy. Using it, you don't need to provision, manage, and scale your own build servers.

https://aws.amazon.com/codebuild/

AWS CodeDeploy - is a service that automates application deployments to a variety of computing services including EC2, Fargate, Lambda, and on-premises instances. It protects your application from downtime during deployments through rolling updates and deployment health tracking.

https://aws.amazon.com/codedeploy/

Try now labs related to this question

Introduction to Amazon CloudFormation

This lab walks you through to AWS CloudFormation features. In this lab, we will demonstrate the use AWS CloudFormation Stack in creating a simple LAMP Server.

Credit Needed 10 Time 0 : 30 Try Now

Ask our Experts Rate this Question?

View Queries open

Question 35 **Unattempted**

Domain :Design High-Performing Architectures

You are working as an AWS Architect for a start-up company. The company has web-servers deployed in all AZ's in the eu-central-1 (Frankfurt) region. These web servers have German news & local web content for people accessing these websites within Germany. These web servers have multiple records created for a single domain. The company is looking for a random selection of web-servers that will increase its availability. What would be the most appropriate routing policy for this requirement?

A. **Latency routing policy**

B. **Weighted routing policy**

C. **Multivalue answer routing policy**

D. **Geolocation routing policy**

Explanation:

Correct Answer – C

When Route 53 is configured with Multi-value answer routing, it returns multiple values for web-servers. Route 53 responds to DNS queries with up to eight healthy records and traffic is approximately load-balanced between these multiple web-servers.

Option A is incorrect. Latency routing policy is used when multiple resources are mapped with single domain & resource with the best latency to the resource is provided. Since most of the times these servers will be accessing locally from the German region, latency to the web servers will be approximately the same.

Option B is incorrect. Weighted routing policy is used when multiple resources are mapped with a single domain & you need to route traffic in a weighted proportionate to each resource. As in this case, the requirement is to use all web servers randomly, the weighted routing policy will not be an ideal option.

Option D is incorrect as Geolocation routing policy is used to choose resources based upon the user's location. In this case, all users will be Germany-based & so there would not be random selection on the resource.

For more information on using Multi-value Answer Routing for Route 53, refer to the following URL:

https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html#routing-policy-multivalue

Ask our Experts Rate this Question?

View Queries open

Question 36 **Unattempted**

Domain :Design Secure Applications and Architectures

Your recent security review revealed a large spike in attempted logins to your AWS account. With respect to sensitive data stored in encryption enabled S3, the data has not been encrypted and is susceptible to fraud if it was to be stolen. You've recommended AWS Key Management Service as a solution. Which of the following is true regarding the operation of KMS?

A. **Only KMS generated keys can be used to encrypt or decrypt data**

B. **Data is encrypted at rest**

C. **KMS allows all users and roles to use the keys by default**

D. **Data is decrypted in transit**

Explanation:

Correct Answer: B

Option B is correct. Data is encrypted at rest; data is encrypted once uploaded to S3. Encryption while in transit is handled by SSL or by using client-side encryption.

Option A is incorrect. Data can be encrypted/decrypted using AWS keys or keys provided by your company

Option C is incorrect. Users are granted permissions explicitly, not by default by KMS

Option D is incorrect. Data is not decrypted in transit (while moving to and from S3). Data is encrypted or decrypted while in S3 and then while in transit can be encrypted using SSL.

References:

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

ttps://d1.awsstatic.com/whitepapers/AWS_Securing_Data_at_Rest_with_Encryption.pdf

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

https://docs.aws.amazon.com/general/latest/gr/rande.html#kms_region

https://www.slideshare.net/AmazonWebServices/encryption-and-key-management-in-aws

Ask our Experts Rate this Question?

View Queries open

Question 37 **Unattempted**

Domain :Design Resilient Architectures

Your company has a set of EC2 Instances hosted in AWS. It is mandatory to prepare for disasters and come up with the necessary disaster recovery procedures. What would be helpful in mitigating the effects of a disaster for the EC2 Instances?

A. **Place an ELB in front of the EC2 Instances.**

B. **Use Auto Scaling to ensure that the minimum number of instances are always running.**

C. **Use CloudFront in front of the EC2 Instances.**

D. **Use AMIs to recreate the EC2 Instances in another region.**

Explanation:

Correct Answer – D

You can create an AMI from the EC2 Instances and then copy them to another region. In case of a disaster, an EC2 Instance can be created from the AMI.

Options A and B are good for fault tolerance, but cannot help completely in disaster recovery for the EC2 Instances.

Option C is incorrect because we cannot determine if CloudFront would be helpful in this scenario or not without knowing what is hosted on the EC2 Instance.

For disaster recovery, we have to make sure that we can launch instances in another region when required. Hence, options A, B and C are not the feasible solutions.

For more information on AWS AMIs, please visit the following URL:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html

Try now labs related to this question

Creating AMI From EC2 Instance

This lab walks you through the steps to create AMI from Amazon EC2 Instance. You will practice using Amazon Machine Images to launch Amazon EC2 Instance and Create AMI of that EC2 Instance.

Credit Needed 10 Time 0 : 30 Try Now

Ask our Experts Rate this Question?

View Queries open

Question 38 **Unattempted**

Domain :Design Secure Applications and Architectures

A company currently hosts a Redshift cluster in AWS. For security reasons, it should ensure that all traffic from and to the Redshift cluster does not go through the Internet. Which features can be used to fulfill this requirement in an efficient manner?

A. **Enable Amazon Redshift Enhanced VPC Routing.**

B. **Create a NAT Gateway to route the traffic.**

C. **Create a NAT Instance to route the traffic.**

D. **Create a VPN Connection to ensure traffic does not flow through the Internet.**

Explanation:

Correct Answer - A

AWS Documentation mentions the following:

When you use Amazon Redshift Enhanced VPC Routing, Amazon Redshift forces all COPY and UNLOAD traffic between your cluster and your data repositories through your Amazon VPC.

If Enhanced VPC Routing is not enabled, Amazon Redshift routes traffic through the Internet, including traffic to other services within the AWS network.

For more information on Redshift Enhanced Routing, please visit the following URL:

https://docs.aws.amazon.com/redshift/latest/mgmt/enhanced-vpc-routing.html

Ask our Experts Rate this Question?

View Queries open

Question 39 **Unattempted**

Domain :Design Resilient Architectures

A company has a set of Hyper-V machines and VMware virtual machines. They are now planning to migrate these resources to the AWS Cloud. What should they use to move these resources to the AWS Cloud?

A. DB Migration utility

B. AWS Server Migration Service

C. Use AWS Migration Tools.

D. Use AWS Config Tools.

Explanation:

Correct Answer - B

AWS Server Migration Service (SMS) is an agentless service which makes it easier and faster for you to migrate thousands of on-premises workloads to AWS. AWS SMS allows you to automate, schedule, and track incremental replications of live server volumes, making it easier for you to coordinate large-scale server migrations.

For more information on AWS Server Migration Service, please visit the following URL:

https://aws.amazon.com/server-migration-service/

Ask our Experts

Rate this Question?

View Queries

open

Question 40

Unattempted

Domain :Design Secure Applications and Architectures

You've implemented AWS Key Management Service to protect your data in your applications and other AWS services. Your global headquarters is in Northern Virginia (US East (N. Virginia)) where you created your keys and have provided the appropriate permissions to designated users and specific roles within your organization. While the N. American users are not having issues, German and Japanese users are unable to get KMS to function. What is the most likely cause of it?

A. **KMS is only offered in North America**

B. **AWS CloudTrail has not been enabled to log events**

C. **KMS master keys are region-specific and the applications are hitting the wrong API endpoints**

D. **The master keys have been disabled**

Explanation:

Correct Answer: C

Option C is correct. This is the most likely cause as the application should be sure to hit correct region endpoint.

Option A is incorrect. KMS is offered in several regions but keys are not transferrable out of the region they were created in.

Option B is incorrect. CloudTrail is recommended for auditing but is not required

Option D is incorrect. The keys are working as expected where they were created; keys are region-specific

References:

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

ttps://docs.aws.amazon.com/general/latest/gr/rande.html#kms_region

https://www.slideshare.net/AmazonWebServices/encryption-and-key-management-in-aws

Ask our Experts

Rate this Question?

View Queries

open

Question 41

Unattempted

Domain :Design Cost-Optimized Architectures

A company with a set of Admin jobs (.NET core) currently set up in the C# programming language, is moving its infrastructure to AWS. What would be an efficient mean of hosting the Admin related jobs in AWS?

A. **Use AWS DynamoDB to store the jobs and then run them on demand.**

B. **Use AWS Lambda functions with C# for the Admin jobs.**

C. **Use AWS S3 to store the jobs and then run them on demand.**

D. **Use AWS Config functions with C# for the Admin jobs.**

Explanation:

Correct Answer - B

The best and most efficient option is to host the jobs using AWS Lambda. This service has the facility to have the code run in the C# programming language.

AWS Documentation mentions the following on AWS Lambda:

AWS Lambda is a compute service that lets you run code without provisioning or managing servers. AWS Lambda executes your code only when needed and scales automatically, from a few requests per day to thousands per second. You pay only for the compute time you consume - there is no charge when your code is not running. With AWS Lambda, you can run code virtually for any type of application or backend service - all with zero administration.

For more information on AWS Lambda, please visit the following URL:

https://docs.aws.amazon.com/lambda/latest/dg/welcome.html

Try now labs related to this question

Introduction to Amazon Lambda

This lab walks you through creation and usage of AWS Serverless service called AWS Lambda. In this lab, we will create a sample lambda function which is triggered on S3 Object upload event and makes a copy of that object on another S3 Bucket.

Credit Needed 10 Time 0 : 30 Try Now

Ask our Experts Rate this Question?

View Queries open

Question 42 **Unattempted**

Domain :Design Secure Applications and Architectures

A Singapore based large Architect firm is using Amazon S3 bucket to save all architecture drawings. This firm works globally & multiple accounts are created within the Singapore region as well in other regions to access AWS resources. Users in all these accounts access the Amazon S3 bucket for architectural drawings. AWS Organisation is created for accounts in the Singapore region. Central IT Teams are managing access to S3 buckets using Service Control Policies with AWS Organisations.
While applying SCP to an AWS Organisation which of the following needs to be considered to avoid blocking of legitimate user access?

A. SCP will block access to Amazon S3 bucket to all accounts within the Singapore region including root users of each account within AWS Organisation as well as access to users outside this region who have access to S3 bucket.

B. SCP will block access to Amazon S3 bucket to all accounts within the Singapore region including root users of each account within AWS Organisation & not to users outside this region who have access to S3 bucket.

C. SCP will block access to Amazon S3 bucket to all accounts within the Singapore region excluding root users of each account within AWS Organisation as well as access to users outside this region who have access to S3 bucket.

D. SCP will block access to Amazon S3 bucket to all accounts within the Singapore region excluding root users of each account within AWS Organisation & not to users outside this region who have access to S3 bucket.

Explanation:

Correct Answer – B

Service Control Policies will be applied to all users within member accounts including root accounts within each of accounts. These policies are not applied to users who are part of these accounts under Aws Organisations & have permission to access Aws resources.

Option A is incorrect as SCP doesn't impact users outside the accounts with AWS Organisations having access to AWS resources.

Option C is incorrect as SCP will apply to all accounts within AWS organizations including root accounts of individual accounts in an AWS Organisation.

Option D is incorrect as SCP will apply to all accounts within AWS organizations including root accounts of individual accounts in an AWS Organisation.

For more information on using Service Control Policies with AWS Organisations, refer to the following URL,

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scp.html

Ask our Experts

Rate this Question?

View Queries open

Question 43 **Unattempted**

Domain :Design Resilient Architectures

You are planning to use Docker containers on a cluster of EC2 instances. These EC2 instances will be launched in a VPC and will require access to ECR and S3 to download Docker images and other images respectively. Additionally, the EC2 instances require secure connectivity to the ECS control plane.
You have created public and private subnets to launch the EC2 instances. What would be helpful to enable secure connectivity and ensure all container orchestration traffic stays within the VPC? **(SELECT TWO)**

A. **Use AWS PrivateLink to connect to the Amazon S3 buckets for downloading images.**

B. **For the instances in the public subnets, use Internet Gateway to access Amazon ECS, ECR, and S3 buckets.**

C. **Use a Gateway VPC Endpoint to download images from the S3 bucket.**

D. **Use AWS PrivateLink to connect to Amazon ECS for control plane connectivity and ECR for downloading Docker images.**

E. **For the instances in the private subnets, use NAT to access Amazon ECS, ECR, and S3.**

F. **Use a Gateway VPC Endpoint to connect to Amazon ECS for control plane connectivity and ECR for downloading Docker images.**

Explanation:

Correct Answer – C and D

Gateway VPC Endpoint provides secure private access to Amazon S3 and DynamoDB without traffic routing via the Internet. When Gateway Endpoints are created, VPC Endpoint is created along with the addition of S3 prefixes in the routing table, pointing to VPCE.

AWS PrivateLink provides secure private access to various AWS services by adding an Elastic Network Interface within a VPC. AWS creates a local/ regional DNS entry that resolves to the local IP address assigned to ENI.

Option A is incorrect as AWS PrivateLink does not support access to Amazon S3. Amazon S3 can be accessed privately from a VPC via Gateway VPC Endpoint.

Options B and E are incorrect as with this, the Traffic from EC2 instance to ECS, ECR, and

Amazon S3 will be flowing over the Internet.

Option F is incorrect as Gateway VPC Endpoint does not support access to Amazon ECR; it supports private access only to Amazon S3 & Amazon DynamoDB.

For more information on VPC, Gateway VPC Endpoints, and AWS PrivateLink, refer to the following URLs:

https://docs.aws.amazon.com/vpc/latest/userguide/vpce-interface.html

https://docs.aws.amazon.com/vpc/latest/userguide/vpce-gateway.html

https://docs.aws.amazon.com/AmazonECR/latest/userguide/vpc-endpoints.html

Ask our Experts Rate this Question?

View Queries open

Question 44 **Unattempted**

Domain :Design Resilient Architectures

A start-up firm is using AWS Organizations for managing policies across its Development and Production accounts. The development account is looking for an EC2 dedicated host that would provide visibility on the number of sockets used. The Production account has subscribed to an EC2 dedicated host for its application but is currently not in use. Sharing has not been enabled with AWS Organizations using the AWS RAM. Which of the following can be done to share the Amazon EC2 dedicated host from the Production account to the Development account?

A. **Remove both Development & Production Accounts from Organisation & then share resources between them.**

B. **You can share resources without enabling sharing within an Organisation.**

C. **Share Resources as an individual account in an Organisation.**

D. **Remove the destination Development account from an Organisation & then share resources with it.**

Explanation:

Correct Answer – C

For accounts that are part of the AWS Organization, Resource sharing can be done on an individual account basis in case resource sharing is not enabled at the AWS Organisation level. With this, resources are shared within accounts as external accounts & an invitation needs to be shared between these accounts to start resource sharing.

Option A is incorrect as removing both accounts from AWS Organisation for Resource sharing is not a valid option.

Option B is incorrect because if sharing needs to be done within accounts in an AWS Organisation, then "sharing" needs to be enabled for the resources. Resource sharing can be done within accounts of AWS Organisation as an individual account.

Option D is incorrect as removing a destination account from AWS Organisation is not required for resource sharing.

For more information on using AWS Resource Access Manager, refer to the following URL,

https://docs.aws.amazon.com/ram/latest/userguide/getting-started-sharing.html

Ask our Experts Rate this Question?

View Queries open

Question 45 **Unattempted**

Domain :Design Secure Applications and Architectures

A global content management company is using Amazon Aurora as a database for scaling millions of documents with high throughput. The Development Team has created a new version of the database which needs to be shared with TEST and PRODUCTION accounts within the company which will run their own OLAP queries. The company is using AWS Organisations to manage policies & have consolidated billing across all AWS accounts. Which of the following can be done to share DB clusters with the TEST account?

A. **Enable sharing for Master account of AWS organizations & grant access to TEST account sharing DB cluster from its own account as well as DB shared by Production account.**

B. **Enable sharing for member accounts of AWS organizations & grant access to the TEST account sharing DB cluster from its own account.**

C. **Enable sharing for Master & member account of AWS organizations & grant access TEST account sharing DB cluster from its own account as well as DB shared by Production account.**

D. **Enable sharing for Master account of AWS organizations & grant access to TEST account sharing DB cluster from its own account.**

Explanation:

Correct Answer – D

For sharing AWS Resources with AWS Resource Access Manager, sharing needs to be enabled with the master account of AWS Organisation. Only resources that are owned by the account are shared with other accounts & resources are not re-shared from other accounts.

Option A is incorrect as Resources shared by other accounts cannot be reshared to other accounts. Only Own resources can be shared.

Option B is incorrect as Resource sharing needs to be enabled for the master account & not member account.

Option C is incorrect as Sharing needs to be enabled only for Master Account & not member account within an Organisation.

For more information on using AWS Resource Access Manager, refer to the following URL,

https://aws.amazon.com/blogs/aws/new-aws-resource-access-manager-cross-account-resource-sharing/

Ask our Experts Rate this Question?

View Queries open

Question 46 **Unattempted**

Domain :Design Resilient Architectures

An application consists of the following architecture:
a. EC2 Instances in a single AZ behind an ELB
b. A NAT Instance which is used to ensure that instances can download updates from the Internet
What could be done to ensure better fault tolerance in this set up? (SELECT TWO)

A. **Add more instances in the existing Availability Zone.**

B. **Add an Auto Scaling Group to the setup.**

C. **Add more instances in another Availability Zone.**

D. **Add another ELB for more fault tolerance.**

Explanation:

Correct Answer – B and C

AWS Documentation mentions the following:

Adding Auto Scaling to your application architecture is one way to maximize the benefits of the AWS Cloud. When you use Auto Scaling, your applications gain the following benefits:

Better fault tolerance. Auto Scaling can detect when an instance is unhealthy. Then it terminates that instance, and launches an instance to replace it. You can also configure Auto Scaling to use multiple Availability Zones. If one Availability Zone becomes unavailable, Auto Scaling can launch instances in another one to compensate.

Better availability. Auto Scaling can help you ensure that your application always has the right amount of capacity to handle the current traffic demands.

For more information on the benefits of Auto Scaling, please visit the following URL:

https://docs.aws.amazon.com/autoscaling/ec2/userguide/auto-scaling-benefits.html

Try now labs related to this question

Build Amazon VPC with Public and Private Subnets from Scratch

1. Learn how to build Public and Private subnets from scratch.

2. VPC wizard will not be used. So every component required to build public and private subnets will be created and configured manually.

3. This will give an in-depth understanding of internal components of VPC and subnets.

Credit Needed 10 Time 0 : 30 Try Now

Ask our Experts Rate this Question?

View Queries open

Question 47 **Unattempted**

Domain :Design High-Performing Architectures

A company has a lot of data hosted on their On-premises infrastructure. Running out of storage space, the company wants a quick win solution using AWS. Which of the following would allow easy extension of their data infrastructure to AWS?

A. **The company could start using Gateway Cached Volumes.**

B. **The company could start using Gateway Stored Volumes.**

C. **The company could start using the DEEP_ARCHIVE storage class.**

D. **The company could start using Amazon Glacier.**

Explanation:

Correct Answer - A

Volume Gateways and Cached Volumes can be used to start storing data in S3.

AWS Documentation mentions the following:

You store your data in Amazon Simple Storage Service (Amazon S3) and retain a copy of frequently accessed data subsets locally. Cached volumes offer substantial cost savings on primary storage and minimize the need to scale your storage on-premises. You also retain low-

latency access to your frequently accessed data.

For more information on Storage Gateways, please visit the following URL:

https://docs.aws.amazon.com/storagegateway/latest/userguide/WhatIsStorageGateway.html

Note:

The question states that they are running out of storage space and they need a solution to store data with AWS rather than a backup. So for this purpose, gateway-cached volumes are appropriate which will help them to avoid scaling their on-premises data center and allows them to store on AWS storage service while having the most recent files available for them at low latency.

This is the difference between Cached and stored volumes:

Cached volumes – You store your data in S3 and retain a copy of frequently accessed data subsets locally. Cached volumes offer substantial cost savings on primary storage and "minimize the need to scale your storage on-premises. You also retain low-latency access to your frequently accessed data."

Stored volumes – If you need low-latency access to your entire data set, first configure your on-premises gateway to store all your data locally. Then asynchronously back up point-in-time snapshots of this data to Amazon S3. "This configuration provides durable and inexpensive off-site backups that you can recover to your local data center or Amazon EC2." For example, if you need replacement capacity for disaster recovery, you can recover the backups to Amazon EC2.

As described in the answer: The company wants a quick win solution to store data with AWS, avoiding scaling the on-premise setup rather than backing up the data.

In the question, they mentioned that **"A company has a lot of data hosted on their On-premises infrastructure."** From On-premises to cloud infrastructure, you can use AWS storage gateways. Option C is talking about the storage class. But here the requirement is (How) to transfer or migrate your data from On-premises to Cloud infrastructure. So there is no clear process mentioned in Option C.

Ask our Experts Rate this Question?

View Queries open

Question 48 **Unattempted**

Domain :Design Resilient Architectures

A Large Medical Institute is using a legacy database for saving all its patient details. Due to compatibility issues with the latest software they are planning to migrate this database to AWS cloud infrastructure. This large size database will be using a NoSQL database Amazon DynamoDB in AWS. As an AWS consultant, you need to ensure that all tables of the current legacy database are migrated without a glitch to Amazon DynamoDB. Which of the following is the most cost-effective way of transferring legacy databases to Amazon DynamoDB?

A. **Use AWS DMS with AWS Schema Conversion Tool to save data to Amazon S3 bucket & then upload all data to Amazon DynamoDB.**

B. **Use AWS DMS with engine conversion tool to save data to Amazon S3 bucket & then upload all data to Amazon DynamoDB.**

C. **Use AWS DMS with engine conversion tool to save data to Amazon EC2 & then upload all data to Amazon DynamoDB.**

D. **Use AWS DMS with AWS Schema Conversion Tool to save data to Amazon EC2 instance & then upload all data to Amazon DynamoDB.**

Explanation:

Correct Answer – A

In this case Legacy Database will be converted to Amazon DynamoDB which will be a heterogenous conversion. Using AWS Schema Conversion Tool is best suited for such conversion along with AWS DMS to transfer data from on-premise to AWS. Using Amazon S3 bucket will help to save any amount of data in a most cost-effective way before its uploaded to Amazon DynamoDB.

Option B is incorrect as engine conversion tool is best suited for homogeneous database migration, in this case it's heterogeneous database, so using AWS SCT along with AWS DMS is a best option.

Option C & D are incorrect as using Amazon S3 bucket is a more cost-effective option than using Amazon EC2 instance.

For more information on using AWS Database Migration Service with AWS SCT, refer to the following URL,

https://docs.aws.amazon.com/dms/latest/userguide/CHAP_BestPractices.html#CHAP_BestPractices.SchemaConversion

Ask our Experts

Rate this Question?

View Queries

open

Question 49

Unattempted

Domain :Design High-Performing Architectures

A Financial firm is planning to build a highly resilient application with primary database servers at on-premise data centers while DB snapshots at Amazon S3 bucket. IT Team is looking for a cost-effective secure way of the initial transfer of large customer financial databases between on-premise servers to Amazon S3 bucket with no impact on client usage of these applications. Also, post this data transfer, the on-premise application will be fetching data from the database in Amazon S3 in case of a primary database fails.
So, your solution should ensure the Amazon S3 database is fully synced with the on-premise database. Which of the following can be used to meet this requirement?

A. Use Amazon S3 Transfer Acceleration for transferring data between the on-premise & Amazon S3 bucket while using AWS Data Sync for accessing these S3 bucket data from the on-premise application.

B. Use AWS Data Sync for transferring data between the on-premise & Amazon S3 bucket while using AWS Storage Gateway for accessing these S3 bucket data from the on-premise application.

C. Use AWS Snowball Edge for transferring data between the on-premise & Amazon S3 bucket while using AWS Storage Gateway for accessing these S3 bucket data from the on-premise application.

D. Use AWS Transfer for transferring data between the on-premise & Amazon S3 bucket while using AWS Data Sync for accessing these S3 bucket data from the on-premise application.

Explanation:

Correct Answer – B

AWS Data Sync can be used for huge amounts of data transfer between on-premise & AWS. AWS Data Sync is a secure way of online data transfer. Once Data is transferred to the AWS S3 bucket, AWS Storage Gateway can be used to have data synced between on-premise servers & AWS S3 buckets.

Option A is incorrect as Amazon S3 Transfer Acceleration can be used for applications that have already integrated with Amazon S3 API.

Option C is incorrect as AWS Snowball Edge can be used for offline data transfer between on-premise & AWS S3 bucket.

Option D is incorrect as AWS Transfer is a better choice for transferring SFTP data between on-premise & Amazon S3.

For more information on using AWS DataSync, refer to the following URLs,

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

https://aws.amazon.com/blogs/storage/migrating-hundreds-of-tb-of-data-to-amazon-s3-with-aws-datasync/

Ask our Experts Rate this Question?

View Queries open

Question 50 **Unattempted**

Domain :Design Cost-Optimized Architectures

A company has an application that delivers objects from S3 to users. Of late, some users spread across the globe, have been complaining of slow response times. Which additional step would help in building a cost-effective solution and ensure that the users get an optimal response to objects from S3?

A. **Use S3 Replication to replicate the objects to regions closest to the users.**

B. **Ensure S3 Transfer Acceleration is enabled to ensure that all users get the desired response times.**

C. **Place an ELB in front of S3 to distribute the load across S3.**

D. **Place the S3 bucket behind a CloudFront distribution.**

Explanation:

Correct Answer - D

AWS Documentation mentions the following:

If your workload is mainly sending GET requests, in addition to the preceding guidelines, you should consider using Amazon CloudFront for performance optimization.

Integrating Amazon CloudFront with Amazon S3, you can distribute content to your users with low latency and a high data transfer rate. You will also send fewer direct requests to Amazon S3, which will reduce your costs.

For example, suppose that you have a few objects that are very popular. Amazon CloudFront fetches those objects from Amazon S3 and caches them. Amazon CloudFront can then serve future requests for the objects from its cache, reducing the number of GET requests it sends to Amazon S3.

For more information on performance considerations in S3, please visit the following URL:

https://docs.aws.amazon.com/AmazonS3/latest/dev/request-rate-perf-considerations.html

Option A is incorrect. S3 Cross-Region Replication is not the correct answer for this business

scenario. You are asked on how to provide easier & faster access to data in S3 bucket, and this option is used to replicate S3 bucket data across regions.

Option B is incorrect. S3 TA is used for fast, easy, and secure file transfer over long distances between your client and your Amazon S3 bucket. S3 Transfer Acceleration does leverage Amazon CloudFront's globally distributed AWS Edge Locations, but would be too costly for this situation.

Option C is incorrect. ELB is used to distribute traffic on to EC2 Instances.

Try now labs related to this question

Introduction to Amazon CloudFront

This lab walks you through to Amazon CloudFront creation and working. In this lab you will create an Amazon CloudFront distribution. It will distribute a publicly accessible image file stored in an Amazon S3 bucket.

Credit Needed 10 Time 1 : 30 Try Now

Ask our Experts Rate this Question?

View Queries open

Question 51 **Unattempted**

Domain :Design Resilient Architectures

A popular blogging site is planning to save all its data to EFS as a redundancy plan. This database is constantly fetch & updated by client information. You need to ensure that all files saved at EFS using AWS DataSync are validated for data-integrity for each packet. Which of the following will ensure fast transfer for data between on-premise & EFS with data integrity done as per security guidelines?

A. **Enable Verification & perform all data transfer.**

B. **Enable verification during initial file transfers & disable it post last data transfer.**

C. **Disable verification during initial file transfers & enable it post last data transfer.**

D. **Disable Verification & perform all data transfer.**

Explanation:

Correct Answer – C

While transferring a constantly changing database between on-premise servers & EFS using AWS DataSync, data verification can be disabled during data transfer & can be enabled post data transfer for data integrity checks & ensure that all data is properly copied between on-premise servers & EFS.

Option A is incorrect as enabling data verification for a constantly changing database will lead to slow transfer of data.

Option B is incorrect as Verification needs to be performed post data transfer to ensure all data is properly copied to EFS.

Option D is incorrect as Disabling verification will not perform data integrity check on data transfer between on-premise servers & EFS.

For more information on using AWS DataSync, refer to the following URL,

https://aws.amazon.com/blogs/storage/migrating-storage-with-aws-datasync/

Ask our Experts Rate this Question?

View Queries open

Question 52 **Unattempted**

Domain :Design High-Performing Architectures

A company is planning to build an application using the services available on AWS. This application will be stateless in nature, and the service must have the ability to scale according to the demand. Which compute service should be used in this scenario?

A. **AWS DynamoDB**

B. **AWS Lambda**

C. AWS S3

D. AWS SQS

Explanation:

Correct Answer - B

The following content from an AWS Whitepaper supports the usage of AWS Lambda for this requirement:

A stateless application is an application that needs no knowledge of previous interactions and stores no session information. Such an example could be an application that, given the same input, provides the same response to any end-user. A stateless application can scale horizontally since any request can be serviced by any of the available compute resources (e.g., EC2 instances, AWS Lambda functions).

For more information on AWS Cloud best practices, please visit the following URL:

https://d1.awsstatic.com/whitepapers/AWS_Cloud_Best_Practices.pdf

Try now labs related to this question

Introduction to Amazon Lambda

This lab walks you through creation and usage of AWS Serverless service called AWS Lambda. In this lab, we will create a sample lambda function which is triggered on S3 Object upload event and makes a copy of that object on another S3 Bucket.

Credit Needed 10 Time 0 : 30 Try Now

Ask our Experts Rate this Question?

View Queries open

Question 53 **Unattempted**

Domain :Design Secure Applications and Architectures

A large IT company is using Amazon CloudFront for its web application. Static Content for this

application is saved in Amazon S3 bucket. Amazon CloudFront is configured for this application to provide faster access to these files for global users.
IT Team is concerned for some critical files which needs to be accessed only by users from certain white-list IP pools which you have defined in Amazon CloudFront & no users should be able to access these files directly using Amazon S3 URL. Which of the following is the most secure way controlling access to these files?

A. **Create an OAI user to associate with distribution & modify permission on Amazon S3 bucket using bucket policy.**

B. **Create Amazon CloudFront Signed URLs to limit access to these files & modify permission on Amazon S3 bucket using bucket policy.**

C. **Create an OAI user to associate with distribution & modify permission on Amazon S3 bucket using object ACL's.**

D. **Create Amazon CloudFront Signed URLs to limit access to these files & modify permission on Amazon S3 bucket using object ACL's.**

Explanation:

Correct Answer – C

Amazon CloudFront Origin Access Identity is a special user which can be used to control access to content in Amazon S3 bucket. Using Object ACL's provides a granular control on each file in Amazon S3 bucket. Associating Amazon CloudFront OAI to a distribution & modifying permission on S3 bucket to allow access only to OAI, ensures that no users can directly access content in S3 bucket & all access is pass through Amazon CloudFront using OAI.

Option A is incorrect as modifying permission in Amazon S3 bucket using bucket policy will not provide granular control on access to each file in a bucket.

Option B & D are incorrect as Amazon CloudFront Signed URLs will provide access only to authorised users for a specified time period, but it will not ensure that this access is through Amazon CloudFront.

For more information on using restricting access using Amazon CloudFront OAI, refer to the following URL,

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

Ask our Experts Rate this Question?

View Queries open

Question 54 **Unattempted**

Domain :Design Secure Applications and Architectures

Developer Team is working on a new RTMP based flash application. They want to test this application with a few users spread across multiple in-house locations before making this application live. For this they have created a RTMP distribution in Amazon CloudFront. IT Head has asked you to control access to application so that only specific users from these locations can access this application during a specific time. Which of the following can meet this requirement?

A. **Create Signed cookies specifying start date, time & IP address range from which users can access this content.**

B. **Create Signed cookies specifying end date, time & IP address range from which users can access this content.**

C. **Create Signed URLs specifying only start date, time & IP address range from which users can access this content.**

D. **Create Signed URLs specifying only end date, time & IP address range from which users can access this content.**

Explanation:

Correct Answer – D

For RTMP distribution, Signed URLs can be used to control access to private content. While specifying periods with Signed URLs, start time & date is optional while end time date / time is required. Also, we can specify the IP address range of users who need to have access to this RTMP application.

Options A & B are incorrect as Signed Cookies do not support RTMP distribution according to https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-choosing-signed-urls-cookies.html.

Option C is incorrect as Specifying start date is an optional feature, specifying end date time is required for each Signed URLs.

For more information on using restricting access using Amazon CloudFront, refer to the following

URL,

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-overview.html

Ask our Experts Rate this Question?

View Queries open

Question 55 **Unattempted**

Domain :Design Resilient Architectures

A company stores its log data in an S3 bucket. There is a current need to have search capabilities available for the data in S3. What could be helpful to achieve this in an efficient manner? (SELECT TWO)

A. **Use Amazon Athena to query the S3 bucket.**

B. **Create a Lifecycle Policy for the S3 bucket.**

C. **Load the data into Amazon Elasticsearch.**

D. **Load the data into Amazon S3 Glacier.**

Explanation:

Correct Answer – A and C

Amazon Athena is a service that enables a data analyst to perform interactive queries in the AWS public cloud on data stored in Amazon S3. Since it's a serverless query service, an analyst doesn't need to manage any underlying compute infrastructure to use it.

For more information on Amazon Athena, please refer to the following URLs:

https://aws.amazon.com/athena/

https://aws.amazon.com/blogs/aws/amazon-athena-interactive-sql-queries-for-data-in-amazon-s3/

Elasticsearch is a highly scalable open-source full-text search and analytics engine. It allows you

to store, search, and analyze big volumes of data quickly and in near real-time. It is generally used as the underlying engine/technology that powers applications that have complex search features and requirements.

https://aws.amazon.com/blogs/database/use-amazon-s3-to-store-a-single-amazon-elasticsearch-service-index/

https://aws.amazon.com/blogs/database/analyze-url-paths-to-search-individual-elements-in-amazon-elasticsearch-service/

Ask our Experts Rate this Question?

View Queries open

Question 56 **Unattempted**

Domain :Design High-Performing Architectures

A company plans to deploy a batch processing application in AWS. Which of the following would ideally help to host this application? (SELECT TWO)

A. **Copy the batch processing application to an ECS Container.**

B. **Create a docker image of your batch processing application.**

C. **Deploy the image as an Amazon ECS task.**

D. **Deploy the container behind the ELB.**

Explanation:

Correct Answer – B and C

AWS Documentation mentions the following:

Docker containers are particularly suited for batch job workloads. Batch jobs are often short-lived and embarrassingly parallel. You can package your batch processing application into a Docker image so that you can deploy it anywhere, such as in an Amazon ECS task.

For more information on the use cases for AWS ECS, please visit the following URL:

https://docs.aws.amazon.com/AmazonECS/latest/developerguide/common_use_cases.html

Ask our Experts Rate this Question?

View Queries open

Question 57 **Unattempted**

Domain :Design Secure Applications and Architectures

A start-up firm has a corporate office at New York & regional office in Washington & Chicago. These offices are interconnected over Internet links. Recently they have migrated a few application servers to EC2 instance launched in AWS US-east-1 region. The Developer Team located at the corporate office requires secure access to these servers for initial testing & performance checks before go-live of new application. Since the go-live date is approaching soon, the IT team is looking for quick connectivity to be established. As an AWS consultant which link option will you suggest for a cost effective & quick way to establish secure connectivity from on-premise to servers launched in AWS?

A. **Use AWS Direct Connect to establish IPSEC connectivity from On-premise to VGW.**

B. **Use Hardware VPN to establish IPSEC connectivity from On-premise to VGW.**

C. **Use Hardware VPN over AWS Direct Connect to establish IPSEC connectivity from On-premise to VGW.**

D. **Use Software VPN to establish IPSEC connectivity from On-premise to EC2 instance.**

Explanation:

Correct Answer – B

Using AWS VPN is the fastest & cost-effective way of establishing IPSEC connectivity from on-premise to AWS. Since Internet links are already available, IT teams can quickly setup a VPN connection with VGW in the US-east-1 region.

Option A is incorrect as AWS Direct Connect does not provide IPSEC connectivity & it is not a quick way to establish connectivity.

Option C is incorrect as Although this will provide a high performance secure IPSEC

connectivity from On-premise to AWS, it is not a quick way to establish connectivity.

Option D is incorrect as this will incur additional management & cost for maintaining Amazon EC2 instance with required VPN software.

For more information on using AWS Direct Connect & VPN, refer to the following URL,

https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/network-to-amazon-vpc-connectivity-options.html

Ask our Experts Rate this Question?

View Queries open

Question 58 **Unattempted**

Domain :Design Secure Applications and Architectures

Your company uses KMS to fully manage the master keys and performing encryption and decryption operations on your data and in your applications. As an additional level of security, you now recommend AWS rotate your keys. What would happen after enabling this additional feature?

A. **Nothing needs to be done. KMS will manage all encrypt/decrypt actions using the appropriate keys**

B. **Your company must instruct KMS to re-encrypt all data in all services each time a new key is created**

C. **You have 30 days to delete old keys after a new one is rotated in**

D. **Your company must create its own keys and import them to KMS to enable key rotation**

Explanation:

Correct Answer: A

Option A is correct. KMS will rotate keys annually and use the appropriate keys to perform cryptographic operations.

Option B is incorrect. This is not necessary. KMS, as a managed service, will keep old keys and

perform operations based on the appropriate key

Option C is incorrect. This is not a requirement of KMS.

Option D is incorrect. This is not a requirement of KMS

References:

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

ttps://docs.aws.amazon.com/general/latest/gr/rande.html#kms_region

https://www.slideshare.net/AmazonWebServices/encryption-and-key-management-in-aws

Ask our Experts

Rate this Question?

View Queries

open

Question 59

Unattempted

Domain :Design Secure Applications and Architectures

You are a Solutions Architect in a startup company that is releasing the first iteration of its app. Your company doesn't have a directory service for its intended users but wants the users to be able to sign in and use the app. What would you advice to implement a solution quickly?

A. Use AWS Cognito although it only supports social identity providers like Facebook

B. Let each user create an AWS user account to be managed via IAM

C. Invest heavily in Microsoft Active Directory as it's the industry standard

D. Use Cognito Identity along with a User Pool to securely save users' profile attributes

Explanation:

Correct Answer: D

Option D is correct. Cognito is a managed service that can be used for this app and scale quickly as usage grows.

Option A is incorrect. Cognitio supports more than just social identity providers, including OIDC, SAML, and its own identity pools

Option B is incorrect. This isn't an efficient means of managing user authentication.

Option C is incorrect. This isn't the most efficient means to authenticate and save user information.

References:

https://aws.amazon.com/cognito/

http://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-integrate-with-cognito.html

https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-user-identity-pools.html

https://aws.amazon.com/cognito/getting-started/

https://docs.aws.amazon.com/cognito/latest/developerguide/concepts.html

Ask our Experts Rate this Question?

View Queries open

Question 60 **Unattempted**

Domain :Design High-Performing Architectures

A company is migrating an on-premises 5TB MySQL database to AWS and expects its database size to increase steadily. Which Amazon RDS engine would meet these requirements?

A. **MySQL**

B. Microsoft SQL Server

C. Oracle

D. Amazon Aurora

Explanation:

Correct Answer – D

AWS Documentation supports the above requirements with regard to AWS Aurora.

Amazon Aurora (Aurora) is a fully managed, MySQL and PostgreSQL compatible, relational database engine. It combines the speed and reliability of high-end commercial databases with the simplicity and cost-effectiveness of open-source databases. It delivers up to five times the throughput of MySQL and up to three times the throughput of PostgreSQL without requiring changes to most of your existing applications.

All Aurora Replicas return the same data for query results with minimal replica lag—usually, much lesser than 100 milliseconds after the primary instance has written an update.

For more information on AWS Aurora, please visit the following URL:

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

NOTE:

On a MySQL DB instance, avoid tables in your database growing too large. Provisioned storage limits restrict the maximum size of a MySQL table file to 16 TB

However, based on database usage, your Amazon Aurora storage will automatically grow, from the minimum of 10 GB up to 64 TB, in 10 GB increments, with no impact on database performance.

Hence, the best answer would be option D.

Try now labs related to this question

Introduction to Amazon Aurora

This lab walks you through the creation and testing of an Amazon Aurora database. We will create an Aurora MySQL Database and and test the connection.

Credit Needed 10 Time 1 : 30 Try Now

Ask our Experts Rate this Question?

View Queries open

Question 61 **Unattempted**

Domain :Design Secure Applications and Architectures

You have implemented AWS Cognito services to require users to sign in and sign up to your app through social identity providers like Facebook, Google, etc. Your marketing department wants users to try out the app anonymously as they think that the current log-in requirement is excessive and will reduce demand for products and services offered through the app. What would you suggest to the marketing department in this regard?

A. It's too much of a security risk to allow unauthenticated users access to the app

B. Cognito Identity supports guest users for the ability to enter the app and have limited access

C. A second version of the app will need to be offered for unauthenticated users

D. This is possible only if we remove the authentication from everywhere

Explanation:

Correct Answer - B

Option B is correct. Amazon Cognito Identity Pools can support unauthenticated identities by providing a unique identifier and AWS credentials for users who do not authenticate with an identity provider. Unauthenticated users can be associated with a role that has limited access to resources as compared to a role for authenticated users.

Option A is incorrect. Cognito will allow unauthenticated users without being a security risk.

Option C is incorrect. Cognito supports both authenticated and unauthenticated users.

References:

https://aws.amazon.com/cognito/

http://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-integrate-with-cognito.html

https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-user-identity-pools.html

https://docs.aws.amazon.com/cognito/latest/developerguide/identity-pools.html

https://aws.amazon.com/cognito/getting-started/

https://docs.aws.amazon.com/cognito/latest/developerguide/concepts.html

Ask our Experts

Rate this Question?

View Queries

open

Question 62

Unattempted

Domain :Design Secure Applications and Architectures

Your app uses AWS Cognito Identity for authentication and stores user profiles in a User Pool. To expand the availability and ease of signing in to the app, your team is requesting advice on allowing the use of OpenID Connect (OIDC) identity providers as additional means of authenticating users and saving the user profile information. What is your recommendation on OIDC identity providers?

A. **This is supported, along with social and SAML based identity providers.**

B. **This is not supported, only social identity providers can be integrated into User Pools**

C. **If you want OIDC identity providers, then you must include SAML and social-based support as well**

D. **It's too much effort to add non-Cognito authenticated user information to a User Pool**

Explanation:

Correct Answer - A

Option A is correct. OpenID Connect (OIDC) identity providers (IdPs) (like Salesforce or Ping Identity) are supported in Cognito, along with social and SAML based identity providers. You can add an OIDC IdP to your user pool in the AWS Management Console, with the AWS CLI, or by using the user pool API method CreateIdentityProvider.

Option B is incorrect. Cognito supports more than just social identity providers, including OIDC, SAML, and its own identity pools.

Option C is incorrect. You can add any combination of federated types, you don't have to add them all.

Option D is incorrect. While there is additional coding to develop this, the effort is most likely not too great to add the feature.

References:

https://aws.amazon.com/cognito/

https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-user-pools-oidc-idp.html

http://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-integrate-with-cognito.html

https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-user-identity-pools.html

https://aws.amazon.com/cognito/getting-started/

https://docs.aws.amazon.com/cognito/latest/developerguide/concepts.html

Try now labs related to this question

Introduction to Amazon CloudFront

This lab walks you through to Amazon CloudFront creation and working. In this lab you will create an Amazon CloudFront distribution. It will distribute a publicly accessible image file stored in an Amazon S3 bucket.

Credit Needed 10 **Time** 1 : 30 Try Now

Ask our Experts Rate this Question?

View Queries open

Question 63 **Unattempted**

Domain :Design High-Performing Architectures

A company is building a two-tier web application to serve dynamic transaction-based content. Which services would you leverage to enable an elastic and scalable Web Tier?

A. Elastic Load Balancing, Amazon EC2, and Auto Scaling

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

C. Amazon RDS with Multi-AZ and Auto Scaling

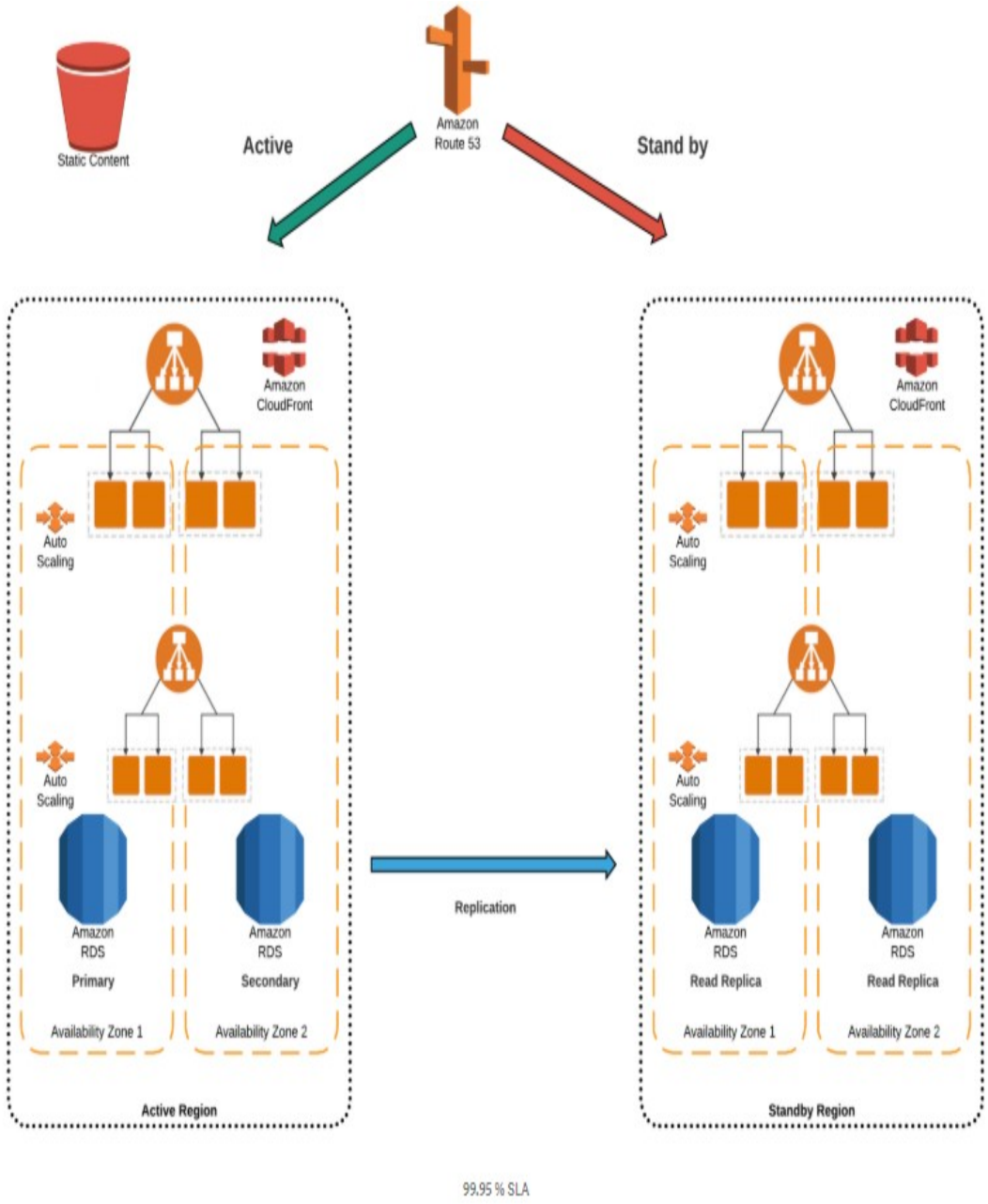
D. Amazon EC2, Amazon Dynamo DB, and Amazon S3

Explanation:

Correct Answer – A

The question mentions a scalable Web Tier. So Option B, C, and D can be eliminated since they are database related options.

The below example (this is a general depiction giving the deployment design of standby architecture having a two tier in them) shows an Elastic Load Balancer connected to 2 EC2 instances via Auto Scaling. This is an example of an elastic and scalable Web Tier. By scalable, we mean that the Auto Scaling process is able to increase or decrease the number of EC2 Instances as required.



For more information on the Elastic Load Balancer, please refer to the URL below.

https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/introduction.html

Try now labs related to this question

Introduction to Amazon Auto Scaling

AWS Auto Scaling will automatically scale resources as needed to align to your selected scaling strategy, This lab walks you through to use Auto Scaling to automatically launch or terminate EC2's instances based on user defined policies, schedules and health checks.

Credit Needed 10 Time 0 : 55 Try Now

Ask our Experts Rate this Question?

View Queries open

Question 64 **Unattempted**

Domain :Design Secure Applications and Architectures

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

A. **The Outbound Security Group needs to be modified to allow outbound traffic.**

B. **The Inbound Network ACL needs to be modified to allow inbound traffic**

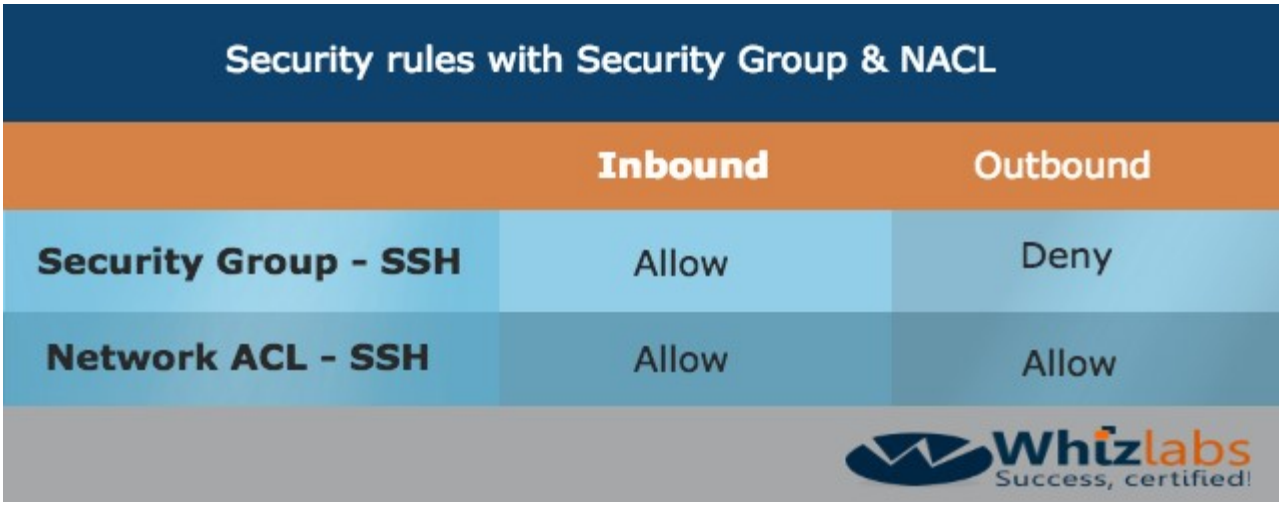
C. **Nothing, it can be accessed from any IP address using SSH**

D. **Both the Outbound Security Group and Outbound Network ACL need to be modified to allow outbound traffic**

Explanation:

Correct Answer – B

For an EC2 Instance to allow SSH, you can have the below configurations for the Security and Network ACL for Inbound and Outbound Traffic.



The reason why Network ACL has to have both an Allow for Inbound and Outbound is that network ACLs 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 an outgoing request will also be granted.

Options A and D are invalid because Security Groups are stateful. Here, any traffic allowed in the Inbound rule is allowed in the Outbound rule too. Option C is also incorrect.

For more information on Network ACLs, please refer to the URL below.

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

Try now labs related to this question

Build Amazon VPC with Public and Private Subnets from Scratch

1. Learn how to build Public and Private subnets from scratch.
2. VPC wizard will not be used. So every component required to build public and private subnets will be created and configured manually.

3. This will give an in-depth understanding of internal components of VPC and subnets.

Credit Needed 10 Time 0 : 30 Try Now

Ask our Experts Rate this Question?

View Queries open

Question 65 **Unattempted**

Domain :Design High-Performing Architectures

Your company currently has a web distribution hosted using the AWS CloudFront service. The IT Security department has confirmed that the application using this web distribution now falls under the scope of PCI compliance. What are the possible ways to meet the requirements? (SELECT TWO)

A. **Enable CloudFront access logs.**

B. **Enable Cache in CloudFront.**

C. **Capture requests that are sent to the CloudFront API.**

D. **Enable VPC Flow Logs**

Explanation:

Correct Answer – A and C

AWS Documentation mentions the following:

If you run PCI or HIPAA-compliant workloads based on the AWS Shared Responsibility Model, we recommend that you log your CloudFront usage data for the last 365 days for future auditing purposes. To log usage data, you can do the following:

Enable CloudFront access logs.

Capture requests that are sent to the CloudFront API.

For more information on compliance with CloudFront, please visit the following URLs:

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/AccessLogs.html

https://aws.amazon.com/blogs/aws/pci-compliance-for-amazon-cloudfront/

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/SERVICENAME-compliance.html

Option B is incorrect. It helps to reduce latency.

Option D is incorrect. VPC flow logs capture information about the IP traffic going to and from network interfaces in a VPC but not for CloudFront.

Try now labs related to this question

Introduction to Amazon CloudFront

This lab walks you through to Amazon CloudFront creation and working. In this lab you will create an Amazon CloudFront distribution. It will distribute a publicly accessible image file stored in an Amazon S3 bucket.

Credit Needed 10 Time 1 : 30 Try Now

Ask our Experts Rate this Question?

View Queries open

Finish Review

Certification

Cloud Certification

Java Certification

PM Certification

Big Data Certification

Company

Become Our Instructor

Support

Discussions

Blog

Business

Support

Contact Us

Help Topics

Join us on Slack!

Join our open **Slack community** and get your queries answered instantly! Our experts are online to answer your questions!

Follow us