CSAA Practice Test 4

Completed on 21-October-2020

Attempt	Marks Obtained	Your score
03	0 / 65	0.0%

Time Taken	Result
N/A	Failed

Domains wise Quiz Performance Report

No	1
Domain	Design High-Performing Architectures
Total Question	21
Correct	0
Incorrect	0
Unattempted	21
Marked for review	0

No	2
Domain	Design Resilient Architectures
Total Question	24
Correct	0
Incorrect	0
Unattempted	24
Marked for review	0
No	3
Domain	Design Secure Applications and Architectures
Total Question	12
Correct	0
Incorrect	0
Unattempted	12
Marked for review	0
No	4
Domain	Design Cost-Optimized Architectures
Total Question	8
Correct	0
Incorrect	0
Unattempted	8
Marked for review	0
Total	Total
All Domain	All Domain
Total Question	65
Correct	0
Incorrect	0
Unattempted	65
Marked for review	0

Review the Answers

Sorting by All

Question 1 Unattempted

Domain :Design High-Performing Architectures

A company is planning to build a 2-tier architecture with a web server and a databse server with separate environments for development and testing. The architecture will be hosted on EC2 Instances accordingly, and database server would require less than 16,000 IOPS per volume. Which of the following EBS volumes are optimum for the underlying EC2 Instances? **(Select Two)**

A. General Purpose SSD for the web server

B. Provisioned IOPS for the web server

C. General Purpose SSD for the database server

D. Provisioned IOPS for the database server

Explanation:

Correct Answers – A and C

The General Purpose SSD would be suitable for development and test environments and the IOPS SSD for business critical applications

The below excerpt from AWS documentation shows the different types of EBS Volumes for different workloads:

	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 16,000 IOPS or 250 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

API Name	gp2	io1	st1	sc1
Volume Size	1 GiB - 16 TiB	4 GiB - 16 TiB	500 GiB - 16 TiB	500 GiB - 16 TiB
Max IOPS per Volume	16,000 (16 KiB I/O) *	64,000 (16 KiB I/O) †	500 (1 MiB I/O)	250 (1 MiB I/O)

For more information on EBS Volume types, please visit the following URL:

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

Try now labs related to this question

Introduction to Amazon Elastic Compute Cloud (EC2)

1. This lab walks you through the steps to launch and configure a virtual machine in the Amazon cloud.

2. You will practice using Amazon Machine Images to launch Amazon EC2 Instances and use key pairs for SSH authentication to log into your instance. You will create a web page and publish it.

Credit Needed 10 Time 0 : 30 Try Now

Ask our Experts

Rate this Question?

View Queries open

Question 2 Unattempted

Domain :Design High-Performing Architectures

You are hosting a web server on an EC2 Instance. With the number of requests consuming a large part of the CPU, the response performance for the application is getting degraded. Which of the following would help to alleviate the problem and provide a better response time?

A. **Place the EC2 Instance behind a Classic Load Balancer.**

B. **Place the EC2 Instance behind an Application Load Balancer.**

C. **Place the EC2 Instance in an Auto Scaling Group with the max size as 1.**

D. **Place a CloudFront distribution in front of the EC2 Instance.**

Explanation:

Correct Answer - D

Since there is a mention of only one EC2 instance, placing it behind the ELB would not make much sense, hence Options A and B are invalid.

Having it in an Auto Scaling Group with just one instance would not make much sense.

CloudFront distribution would help to alleviate the load on the EC2 Instance because of its edge location and cache feature.

For more information on CloudFront, please visit the following URL:

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

Try now labs related to this question

Introduction to Amazon Elastic Compute Cloud (EC2)

1. This lab walks you through the steps to launch and configure a virtual machine in the Amazon cloud.

2. You will practice using Amazon Machine Images to launch Amazon EC2 Instances and use key pairs for SSH authentication to log into your instance. You will create a web page and publish it.

Credit Needed 10 Time 0 : 30 Try Now

Ask our Experts

Rate this Question?

View Queries open

Question 3 Unattempted

Domain :Design High-Performing Architectures

A company is hosting a MySQL database in AWS using the AWS RDS service. To offload the reads, a Read Replica has been created and reports are run off the Read Replica database. But at certain times, the reports show stale data. What could be the possible reason behind this?

A. **The Read Replica has not been created properly.**

B. **The backup of the original database has not been set properly.**

C. **This is due to the replication lag.**

D. **The Multi-AZ feature is not enabled.**

Explanation:

Correct Answer – C

An AWS Whitepaper on the caveat for reading Replicas is given below which must be taken into consideration by architects:

Read Replicas are separate database instances that are replicated asynchronously. As a result, they are subject to replication lag and might be missing some of the latest transactions. Application architects need to consider which queries have the tolerance to slightly stale data. Those queries can be executed on a Read Replica, while the rest should run on the primary node. Read Replicas may also not accept any write queries.

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 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 4 Unattempted

Domain :Design Resilient Architectures

A company plan to use SQS queues and AWS Lambda to leverage the serverless aspects of the AWS Cloud. Each invocation to AWS Lambda will send a message to an SQS queue. What should be done to achieve this?

A. The queue must be a FIFO queue.

B. An IAM Role must have the required permissions.

C. The code for Lambda must be written in C#.

D. An IAM Group must have the required permissions.

Explanation:

Correct Answer – B

While working with AWS Lambda functions, if there is a need to access other resources, ensure that an IAM role is in place. The IAM role will have the required permissions to access the SQS queue.

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

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

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 5 Unattempted

Domain :Design Secure Applications and Architectures

You have enabled CloudTrail logs for your company's AWS account. In addition, the IT Security department has mentioned that the logs need to be encrypted. How could this be achieved?

A. Enable SSL certificates for the CloudTrail logs.

B. There is no need to do anything since the logs will already be encrypted.

C. Enable Server-Side Encryption for the trail.

D. Enable Server-Side Encryption for the destination S3 bucket.

Explanation:

Correct Answer – B

AWS Documentation mentions the following:

By default, CloudTrail event log files are encrypted using Amazon S3 server-side encryption (SSE). You can also choose to encrypt your log files with an AWS Key Management Service (AWS KMS) key. You can store your log files in your bucket for as long as you want. You can also define Amazon S3 lifecycle rules to archive or delete log files automatically. If you want notifications about log file delivery and validation, you can set up Amazon SNS notifications.

For more information on how CloudTrail works, please visit the following URL:

https://docs.aws.amazon.com/awscloudtrail/latest/userguide/how-cloudtrail-works.html

Ask our Experts

Rate this Question?

View Queries open

Question 6 Unattempted

Domain :Design High-Performing Architectures

A company has set up its data layer in the Simple Storage Service. There are a number of requests which include read/write and updates to objects in an S3 bucket. Users sometimes complain that updates to an object are not being reflected. What could be the most likely reason for this?

A. Versioning is not enabled for the bucket, so the newer version does not reflect the right data.

B. Updates made to the objects usually take sometime to reflect .

C. Encryption is enabled for the bucket, hence it is taking time for the update to occur.

D. The metadata for the S3 bucket is incorrectly configured.

Explanation:

Correct Answer – B

Updates made to the objects in S3 follow an eventual consistency model. Hence, for object updates, there can be a slight delay when an updated object is provided back to the user on the next read request.

For more information on various aspects of the Simple Storage Service, please visit the following URL:

https://aws.amazon.com/s3/faqs/

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 7 Unattempted

Domain :Design High-Performing Architectures

Your company has enabled CORS on your S3 bucket to allow cross-origin resource sharing. In the CORS configuration, you need to specify the values for the "AllowedMethod" element. What would be

your suggestion to the developer?

A. Those two methods require special permission from AWS

B. The developer's user profile was limited to and required to be updated

C. Only these methods are supported: GET, PUT, POST, DELETE, and HEAD

D. OPTIONS and CONNECT are controlled by other bucket policies

Explanation:

Correct Answer: C

Only these methods are supported: GET, PUT, POST, DELETE, and HEAD

Refer page 163 on the below link under the topic "AllowedMethod Element"

https://docs.aws.amazon.com/AmazonS3/latest/dev/s3-dg.pdf

Reference for CORS:

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

https://docs.aws.amazon.com/apigateway/latest/developerguide/how-to-cors.html

https://aws.amazon.com/blogs/aws/amazon-S3-cross-origin-resource-sharing/

Ask our Experts

Rate this Question?

View Queries open

Question 8 Unattempted

Domain :Design Secure Applications and Architectures

Your company has a MySQL database deployed in an on-premise datacenter. You start using AWS Database Migration Service (AWS DMS) to migrate the database to AWS RDS. You have a replication instance in DMS to run the migration task. Which of the following options assigns permissions that determine who is allowed to manage AWS DMS resources?

A. **Transport Layer Security (TLS) connections between AWS DMS and local datacenter.**

B. **AWS Key Management Service (AWS KMS) encryption used by the replication instance.**

C. **AWS Identity and Access Management (IAM) policies.**

D. **Network Control Lists (NCLs) in VPC subnets.**

Explanation:

Correct Answer – C

There are multiple approaches to secure the AWS DMS resources. Details can be found in

https://docs.aws.amazon.com/dms/latest/userguide/CHAP_Security.html.

Option A is incorrect: TLS protects the network layer however it does not assign permissions.

Option B is incorrect: KMS encrypts data but it cannot manage the permissions.

Option C is CORRECT: Because IAM policies can be assigned to IAM users who need to manage DMS resources.

Option D is incorrect: NCL acts as a firewall to protect the VPC subnets but it does not determine who can access DMS resources.

Ask our Experts

Rate this Question? ☺ ☹

View Queries open

Question 9 Unattempted

Domain :Design Cost-Optimized Architectures

Your company stores a big amount of archive data in expensive on-premises storage systems. You need to move the data to low cost storage such as Amazon S3 Glacier. Which of the following tools is the most suitable to simplify and automate the data transfer from on-premises to S3 Glacier?

A. AWS DataSync

B. Server Migration Service

C. Database Migration Service

D. Direct Connect

Explanation:

Correct Answer – A

AWS DataSync should be selected as it can simplify moving data between on-premises storage and AWS services such as S3 Glacier. Check https://docs.aws.amazon.com/datasync/latest/userguide/what-is-datasync.html.

Option A is CORRECT: With AWS DataSync, users can create a task to specify the data source and destination and then configure the data transfer.

Option B is incorrect: Because Server Migration Service is used to migrate on-premise servers such as VMware.

Option C is incorrect: Database Migration Service is used to migrate a database instead of local storage.

Option D is incorrect: Direct Connect sets up a dedicated network connection to AWS. However it does not automate the data transfer to AWS.

Ask our Experts

Rate this Question?

View Queries open

Question 10 Unattempted

Domain :Design Secure Applications and Architectures

You use an Amazon S3 bucket as the origin for a CloudFront distribution. In order to restrict access to S3 content, you create an Origin Access Identity (XXXX1234567890) in CloudFront and associate it with the distribution. You need to modify the S3 bucket policy so that users cannot bypass CloudFront to access the S3 files. Which of the following options contains the correct S3 bucket policy statement?

A.
```
{
    "Effect": "Deny",
    "Principal": {
        "AWS": "arn:aws:iam::cloudfront:user/CloudFront Origin Access Identity XXXX123456
    },
    "Action": "s3:GetObject",
    "Resource": "arn:aws:s3:::aws-example-bucket/*"
}
```

B.
```
{
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::cloudfront:user/XXXX1234567890"
    },
    "Action": "s3:GetObject",
    "Resource": "arn:aws:s3:::aws-example-bucket"
}
```

C.
```
{
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::cloudfront:user/CloudFront Origin Access Identity XXXX123456
    },
    "Action": "s3:GetObject",
    "Resource": "arn:aws:s3:::aws-example-bucket/*"
}
```

D.
```
{
    "Effect": "Deny",
    "NotPrincipal": {
        "AWS": "arn:aws:iam::cloudfront:user/CloudFront Origin Access Identity XXXX123456
    },
    "Action": "s3:GetObject",
    "Resource": "arn:aws:s3:::aws-example-bucket"
}
```

Explanation:

Correct Answer – C

The S3 bucket policy should allow the "s3:GetObject" action if the Principal comes from the CloudFront Origin Access Identity. Details can be found in https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_notprincipal.html.

Option A is incorrect: Because the "Effect" should be "Allow" instead of "Deny".

Option B is incorrect: Both "Principal" and "Resource" are incorrect according to the above reference.

Option C is CORRECT: Because with this bucket policy, "s3:GetObject" action is only allowed for the CloudFront OAI.

Option D is incorrect: The bucket policy denies the action if the Principal is NOT the Origin Access Identity. However, it still does not allow the action if the Principal comes from the CloudFront OAI. An explicit Allow is required.

Ask our Experts

Rate this Question? ☺ ☹

View Queries open

Question 11 Unattempted

Domain :Design High-Performing Architectures

You are working in a financial company and you need to establish the network connections between on-premises data centers and AWS VPCs. The connectivity needs to be secure with IPsec connections. A predictable and high-performance network is also required over private lines. Which of the following methods would you select?

A. AWS Direct Connect + VPN

B. AWS Managed VPN

C. AWS Direct Connect

D. Software VPN

Explanation:

Correct Answer – A

AWS has provided several connectivity options according to https://d1.awsstatic.com/whitepapers/aws-amazon-vpc-connectivity-options.pdf. VPN is needed as it creates an IPsec connection. AWS Direct Connect is also required because it establishes a private connection with high bandwidth throughput.

Option A is CORRECT: Because with AWS Direct Connect + VPN, you can create IPsec-encrypted private connections.

Option B is incorrect: Because only with VPN, the network performance cannot be guaranteed.

Option C is incorrect: Because AWS Direct Connect does not use IPsec protocol.

Option D is incorrect: Because Software VPN is still based on the internet instead of a dedicated network.

Ask our Experts

Rate this Question?

View Queries open

Question 12 Unattempted

Domain :Design Secure Applications and Architectures

Your IT Supervisor is worried about users, accidentally deleting objects from an S3 bucket. Which of the following can help prevent accidental deletion of objects in an S3 bucket? **(Select Three)**

A. **Enable encryption for the S3 bucket.**

B. **Enable MFA Delete on the S3 bucket.**

C. **Enable Versioning on the S3 bucket.**

D. **Enable IAM Roles on the S3 bucket.**

Explanation:

Correct Answers – B, C, and D

AWS Documentation mentions the following:

When a user performs a DELETE operation on an object, subsequent simple (un-versioned) requests will no longer retrieve the object. However, all versions of that object will continue to be preserved in your Amazon S3 bucket and can be retrieved or restored.

Versioning's MFA Delete capability, which uses multi-factor authentication, can be used to provide an additional layer of security. By default, all requests to your Amazon S3 bucket require your AWS account credentials. If you enable Versioning with MFA Delete on your Amazon S3 bucket, two forms of authentication are required to permanently delete a version of an object: your AWS account credentials and valid six-digit code and serial number from an authentication device in your physical possession.

For more information on the features of S3, please visit the following URL:

https://aws.amazon.com/s3/faqs/

To know more about Option D, Please refer to the below AWS Document.

https://aws.amazon.com/blogs/security/how-to-restrict-amazon-s3-bucket-access-to-a-specific-iam-role/

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 13 Unattempted

Domain :Design Secure Applications and Architectures

A company has been using AWS cloud services for six months and have just finished a security review. Which of the following is considered a best practice in the security pillar of the well-architected framework?

A. Using the root user to create all-new user accounts, at any time

B. Monitoring and using alerts using CloudTrail and CloudWatch

C. Assigning Private IP address ranges to VPCs that do not overlap

D. Designing the system using elasticity to meet changes in demand

Explanation:

Correct Answer: B

Option B is correct. Monitoring and alerting for key metrics and events is the best practice of the Security pillar

Option A is incorrect. For the root user, you should follow the best practice of using this login only to create another, an initial set of IAM users and groups for longer-term identity management operations

Option C is incorrect. Non-overlapping Private IP addresses are in the Reliability pillar.

D. Design using elasticity to meet demand is in the Performance Efficiency pillar (Design for Cloud Operations).

References:

https://d1.awsstatic.com/whitepapers/architecture/AWS_Well-Architected_Framework.pdf

https://d1.awsstatic.com/whitepapers/architecture/AWS-Security-Pillar.pdf

Try now labs related to this question

Creating Events in CloudWatch

This lab walks you through the Creating Rules in the Events Section of Cloudwatch and adding a SNS target. It will tested using EC2 Instance state events

Credit Needed 10 Time 0 : 30 Try Now

Ask our Experts

Rate this Question?

View Queries open

Question 14 Unattempted

Domain :Design Cost-Optimized Architectures

A company has a Redshift Cluster defined in AWS. The IT Operations team have ensured that both automated and manual snapshots are in place. Since the cluster is going to be run for a couple of years, Reserved Instances have been purchased. There has been a recent concern on the cost, being incurred by the cluster. Which step should be carried out to minimize the costs being incurred by the cluster?

A. **Delete the manual snapshots.**

B. **Set the retention period of the automated snapshots to 35 days.**

C. **Choose to use Spot Instances instead of Reserved Instances.**

D. **Choose to use Instance store volumes to store the cluster data.**

Explanation:

Correct Answer - A

AWS Documentation mentions the following:

Regardless of whether you enable automated snapshots, you can take a manual snapshot whenever you want at any time. By default, manual snapshots are retained indefinitely, even after you delete your cluster. You can specify the retention period when you create a manual snapshot or you can change the retention period by modifying the snapshot. If you create a snapshot using the Amazon Redshift console, it defaults the snapshot retention period to 365 days.

Automated snapshots are automatically deleted within the period of 1(Least) to **35(Max)** days (Based on the retention period settings). So we have to take care of the Manual snapshots instead of Automated snapshots. Amazon Redshift never deletes Manual snaphots automatically, like how it does for Automatic Snapshots.

For more information on working with Snapshots, please visit the following URL:

https://docs.aws.amazon.com/redshift/latest/mgmt/working-with-snapshots.html

Try now labs related to this question

Creating New EC2 Instance using Snapshot

This lab walks you through creation of a snapshot of EC2 instance and launch a new EC2 instance using AMI of that snapshot.

Credit Needed 10 Time 0 : 30 Try Now

Ask our Experts

Rate this Question?

View Queries open

Question 15 Unattempted

Domain :Design Resilient Architectures

A website is hosted on two EC2 instances that sit behind an Elastic Load Balancer. The response time of the website has been slowed down dramatically, and customers are placing fewer orders due to the wait time. Troubleshooting showed that one of the EC2 instances has been failed and only one instance is running now. What is the best course of action to prevent this from happening in the future?

A. Change the instance size to the maximum available to compensate for the failure

B. Use CloudWatch to monitor the VPC Flow Logs for the VPC, the instances are deployed in

C. Configure the ELB to perform health checks on the EC2 instances and implement auto-scaling

D. Replicate the existing configuration in several regions for failover

Explanation:

Correct Answer: C

Option C is correct. Using the elastic load balancer to perform health checks will determine whether or not to remove a non-performing or underperforming instance, and have the auto-scaling group launch a new instance.

Option A is incorrect. Increasing the instance size doesn't prevent failure of one or both the instances, therefore the website can still become slow or unavailable.

B. Monitoring the VPC flow logs for the VPC will capture the VPC traffic, not the traffic for the EC2 instance. You would need to create a flow log for a network interface.

D. Replicating the same two instance deployment may not prevent failure of instances and could still result in the website becoming slow or unavailable.

References:

https://media.amazonwebservices.com/AWS_Building_Fault_Tolerant_Applications.pdf

https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/flow-logs.html#working-with-flow-logs

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 16 Unattempted

Domain :Design Resilient Architectures

A company currently hosts a lot of data on its On-premises location. It wants to start storing backups of this data with low latency access to data on AWS. How could this be achieved in the most efficient way?

A. **Create EBS Volumes and store the data.**

B. **Create EBS Snapshots and store the data.**

C. **Make use of Storage Gateway Stored volumes.**

D. **Make use of Amazon Glacier.**

Explanation:

Correct Answer – C

AWS Storage Gateway connects an on-premises software appliance with cloud-based storage to provide seamless integration with data security features between your on-premises IT environment and the AWS storage infrastructure. You can use the service to store data in the AWS Cloud for scalable and cost-effective storage that helps to maintain data security.

It has two types of configuration, cached volumes, and stored volumes.

Our requirement is to **start storing backups of the on-premises data to AWS.**

In **cached** volumes, you store your data in S3 and retain a copy of frequently accessed data subsets locally. It means that we are not storing the backups on S3 but the **actual primary data** itself.

But in the **stored** mode, **your primary data is stored locally** and your entire dataset is available for low-latency access while **asynchronously backed up to AWS S3.**

Ask our Experts

Rate this Question?  

View Queries open

Question 17 Unattempted

Domain :Design Resilient Architectures

As a solutions architect, you need to design a multi-tier architecture for a project in AWS. The application contains three tiers: the frontend layer, business logic layer and storage layer. The frontend

and business logic layers are implemented by Auto Scaling groups and Amazon DynamoDB is selected as the data storage option in the storage layer. Which of the following options is NOT a feature of this architecture?

A. **Each layer is modularized and managed independently.**

B. **The backend and data storage are not exposed to the internet and protected in private subnets.**

C. **The architecture is completely serverless so that users do not need to configure the desired number of servers or capabilities.**

D. **Frontend and backend servers can be configured in different availability zones for high availability.**

Explanation:

Correct Answer – C

The multi-tier architecture in AWS has a number of features such as high availability and scalability, fault tolerant and security. The question asks for the option that is NOT a feature.

Option C should be selected as you still need to configure the min/max/desired number of servers in ASGs and the read/write capabilities in DynamoDB tables.

Option A is incorrect: Because the application is divided into three components and each component works independently.

Option B is incorrect: Because the backend and data storage are located in private subnets. Users can only reach the frontend layer.

Option C is CORRECT: Refer to the above explanations. This architecture is not completely serverless.

Option D is incorrect: Because the servers in ASG can be put into several availability zones so that even if one AZ has an outage, the servers in other AZs can still work as normal.

Ask our Experts

Rate this Question? ☺ ☹

View Queries open

Question 18 Unattempted

Domain :Design High-Performing Architectures

Currently, you have a set of Lambda functions which have business logic embedded in them. You want customers to have the ability to call these functions via HTTPS. How could this be achieved?

A. Use the API Gateway and provide integration with the AWS Lambda functions.

B. Enable HTTP access on the AWS Lambda functions.

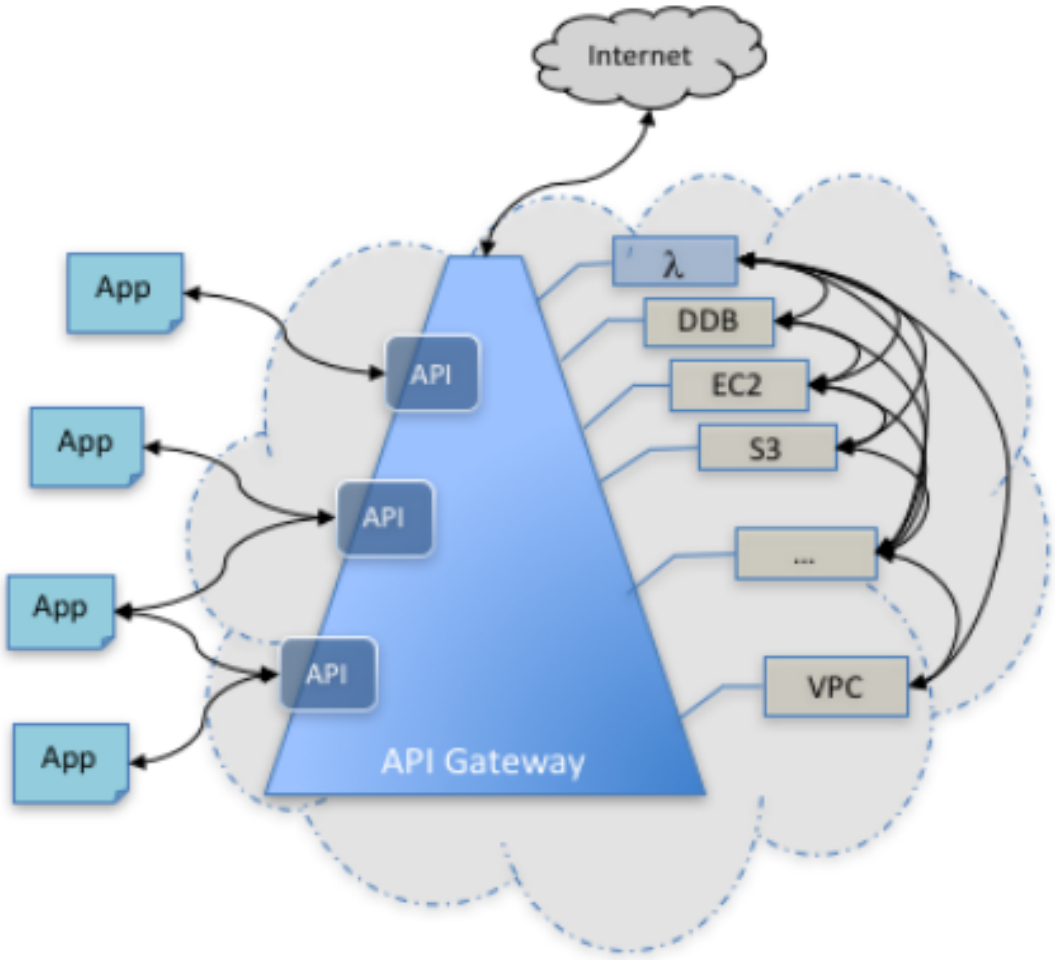
C. Add EC2 Instances with an API server installed. Integrate the server with AWS Lambda functions.

D. Use S3 websites to make calls to the Lambda functions

Explanation:

Correct Answer - A

An API Gateway provides the ideal access to your back end services via APIs.



For more information on the API Gateway service, please visit the following URL:

https://docs.aws.amazon.com/apigateway/latest/developerguide/welcome.html

Ask our Experts

Rate this Question?

View Queries open

Question 19 Unattempted

Domain :Design Resilient Architectures

For a new application, you need to build up the logic tier and data storage tier in AWS. The whole architecture needs to be serverless so that designers can quickly deploy the application without the need to manage servers. Which of the following AWS services would you choose?

A. Logic tier: “Amazon Cognito + Lambda”. Data Storage tier: “Amazon RDS”

B. Logic tier: “API Gateway + Lambda”. Data Storage tier: “Amazon DynamoDB”

C. Logic tier: “API Gateway + Lambda”. Data Storage tier: “Amazon Redshift”

D. Logic tier: “Elastic Beanstalk”. Data Storage tier: “Amazon Aurora”

Explanation:

Correct Answer – B

The key to the question is that the architecture should be severless. For AWS serverless multi-tier architectures, please refer to https://d1.awsstatic.com/whitepapers/AWS_Serverless_Multi-Tier_Architectures.pdf.

Option A is incorrect: Because Amazon Cognito is not suitable for the logic tier and Amazon RDS is not a serverless service.

Option B is CORRECT: Because both API Gateway/Lambda and Amazon DynamoDB are severless so that the process of deploying servers is simplified.

Option C is incorrect: Amazon Redshift is a data warehouse service and is not serverless.

Option D is incorrect: Because Elastic Beanstalk utilizes EC2 instances as its computing resources and is not a serverless service.

Ask our Experts

Rate this Question? ☺ ☹

View Queries open

Question 20 Unattempted

Domain :Design Cost-Optimized Architectures

A Solutions Architect is designing a solution to store and archive corporate documents. He has determined that Amazon Glacier is the right solution. Data has to be retrieved within 3-5 hrs as directed by the management.
Which feature in Amazon Glacier could be helpful to meet this requirement and ensure cost-effectiveness?

A. Vault Lock

B. Expedited retrieval

C. Bulk retrieval

D. Standard retrieval

Explanation:

Correct Answer – D

Option A - Vault Lock

- This feature of Amazon Glacier allows you to lock your vault with a variety of compliance controls that are designed to support such long-term records retention. Due to this reason, this is not the correct answer.

Option B - Expedited retrieval

- It allows you to quickly access your data when occasional urgent requests are required for a subset of archives. The data is available within 1 - 5 minutes. Since our requirement is 3 - 5 hours, we do not need to use this option.

Option C - Bulk retrieval

- They are the lowest-cost retrieval option, enabling you to retrieve large amounts of data within 5 - 12 hours. Due to this reason, it is not the correct answer.

AWS Documentation mentions the following on Standard retrievals:

Standard retrievals are a low-cost way to access your data within just a few hours. For example, you can use Standard retrievals to restore backup data, retrieve archived media content for same-day editing or distribution, or pull and analyze logs to drive business decisions within hours.

For more information on Amazon Glacier retrievals, please visit the following URL:

https://aws.amazon.com/glacier/faqs/#dataretrievals

Ask our Experts

Rate this Question?

View Queries open

Question 21 Unattempted

Domain :Design Resilient Architectures

You have an application running in AWS. The application has the frontend EC2 servers deployed in a public subnet. And the backend EC2 servers are hosted in a private subnet. The frontend servers can communicate with the backend servers properly. One day there is an issue in production and you need to login to one backend EC2 instance to troubleshoot. The connection to the backend servers should be done in the most secure way. Which of the following options is the most secure one to access the instance?

A. Generate a new SSH key and use the key to SSH to the backend instance.

B. SSH to one of the frontend instances and then SSH to the backend.

C. Modify the security group of the instance to allow the SSH inbound traffic from your IP address. Revert the change after you do not need the access.

D. SSH to a bastion host first and then SSH to the backend instance from the bastion.

Explanation:

Correct Answer – D

Bastion host is the most suitable one in this scenario. It is a dedicated server for users to securely SSH to the backend servers in the private subnet.

Option A is incorrect: Since the backend instance is in the private subnet, users cannot directly SSH to it.

Option B is incorrect: Because normally frontend servers should not have the SSH access to the backend. In this scenario, we should use a dedicated jump host rather than the frontend instances.

Option C is incorrect: Same as option A. The backend instance does not have a public IP and you cannot directly SSH to it from your server.

Option D is CORRECT: Through the bastion host, the SSH connection can be safely established and monitored.

Ask our Experts

Rate this Question?

View Queries open

Question 22 Unattempted

Domain :Design Resilient Architectures

Your application has two tiers in AWS: the frontend layer and the backend layer. The frontend includes an Auto Scaling group deployed in a public subnet. The backend Auto Scaling group is located in another private subnet. The backend instances should only allow the incoming traffic from the frontend ASG through a custom port. For the backend security group, how would you configure the source in its inbound rule?

A. **Configure the frontend security group ID as the source.**

B. **Configure the public subnet IP range as the source.**

C. **Configure the frontend Auto Scaling group ARN as the source.**

D. **Configure the frontend Auto Scaling launch configuration as the source.**

Explanation:

Correct Answer – A

Refer to https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-security-groups.html#security-group-rules for how to configure security group rules.

Option A is CORRECT: By configuring the frontend security group as the source, any frontend instances that have the specified security group are allowed to access the backend.

Option B is incorrect: Other instances in this subnet can also access the backend. This option is not as good as option A.

Option C is incorrect: Because Auto Scaling group ARN cannot be configured in the source of a security group inbound rule.

Option D is incorrect: Because launch configuration cannot be configured in the source.

Ask our Experts

Rate this Question?

View Queries open

Question 23 Unattempted

Domain :Design High-Performing Architectures

A company requires an open-source system for automating the deployment, scaling, and management of containerized applications. Which of the following would be ideal for such a requirement?

A. **Use the Amazon Elastic Container Service for Kubernetes.**

B. **Install a custom orchestration tool on EC2 Instances.**

C. **Use SQS to orchestrate the messages between docker containers.**

D. **Use AWS Lambda functions to embed the logic for container orchestration.**

Explanation:

Correct Answer – A

AWS Documentation mentions the following;

Amazon Elastic Container Service for Kubernetes (Amazon EKS) is a managed service that makes it easy for you to run Kubernetes on AWS without the requirement of installing and operating your own Kubernetes clusters. Kubernetes is an open-source system for automating the deployment, scaling, and management of containerized applications. Operating Kubernetes for production applications presents a number of challenges. You need to manage the scaling and availability of your Kubernetes masters and persistence layer by ensuring that you have chosen appropriate instance types, running them across multiple Availability Zones, monitoring their health, and replacing unhealthy nodes. You need to patch and upgrade your masters and worker nodes to ensure that you are running the latest version of Kubernetes. All this requires expertise and a lot of manual work. With Amazon EKS, upgrades and high availability are managed for you by AWS. Amazon EKS runs three Kubernetes masters across three Availability Zones in order to ensure high availability. Amazon EKS automatically

detects and replaces unhealthy masters, and provides automated version upgrades and patching for the masters.

For more information on the Elastic Container Service, please visit the below URL:

https://aws.amazon.com/eks/

Ask our Experts

Rate this Question?

View Queries open

Question 24 Unattempted

Domain :Design Cost-Optimized Architectures

A small company started using EBS backed EC2 instances for the cost improvements over their own running servers. The company's policy is to stop the development servers over weekend and restart them next week. First time when the servers were brought back, none of the developers were able to SSH into them. What did the server most likely overlook?

A. **The associated Elastic IP address has changed and the SSH configurations were not updated**

B. **The security group for a stopped instance needs to be reassigned after the start**

C. **The public IPv4 address has changed on the server start and the SSH configurations were not updated**

D. **EBS backed EC2 instances could not be stopped and were automatically terminated**

Explanation:

Correct Answer: C

Option C is correct. The instance retains its private IPv4 addresses and any IPv6 addresses when stopped and started. AWS releases public IPv4 address and assigns a new one when it is stopped & started.

Option A is incorrect. An EC2 instance retains its associated Elastic IP addresses.

Option B is incorrect. Security groups do not need to be reassigned to instances that are restarted.

Option D is incorrect. EBS backed instances are the only instance type that can be started and stopped.

Reference:

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

Try now labs related to this question

Introduction to Amazon Elastic Compute Cloud (EC2)

1. This lab walks you through the steps to launch and configure a virtual machine in the Amazon cloud.

2. You will practice using Amazon Machine Images to launch Amazon EC2 Instances and use key pairs for SSH authentication to log into your instance. You will create a web page and publish it.

Credit Needed 10 Time 0 : 30 Try Now

Ask our Experts

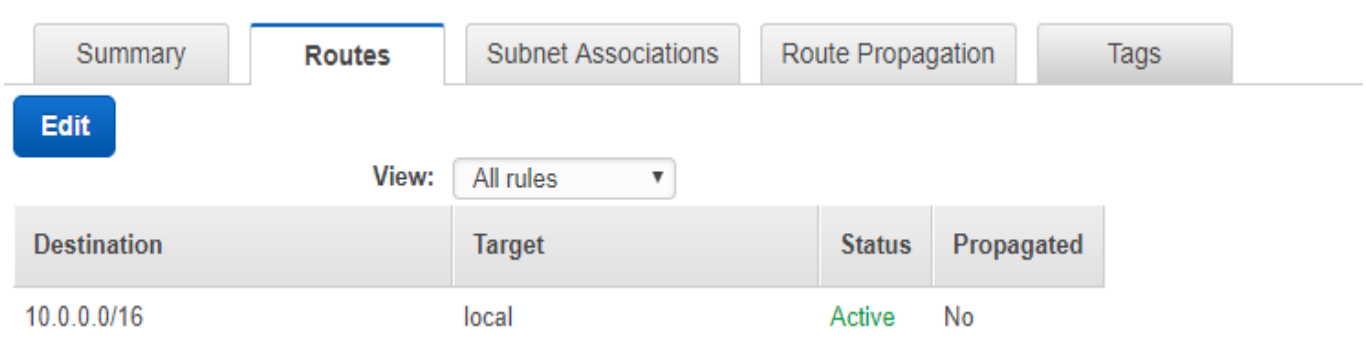
Rate this Question?

View Queries open

Question 25 Unattempted

Domain :Design Secure Applications and Architectures

You created your own VPC and subnet in AWS and launched an instance in that subnet. On attaching an Internet Gateway to the VPC, you see that the instance has a public IP. The route table is shown below:



Still, the instance cannot be **reached from the Internet.** What changes are required to be made to the route table to ensure that the issue is resolved?

A. **Add the following entry to the route table – Destination as 0.0.0.0/0 and Target as Internet Gateway**

B. **Modify the above route table – Destination as 10.0.0.0/16 and Target as Internet Gateway**

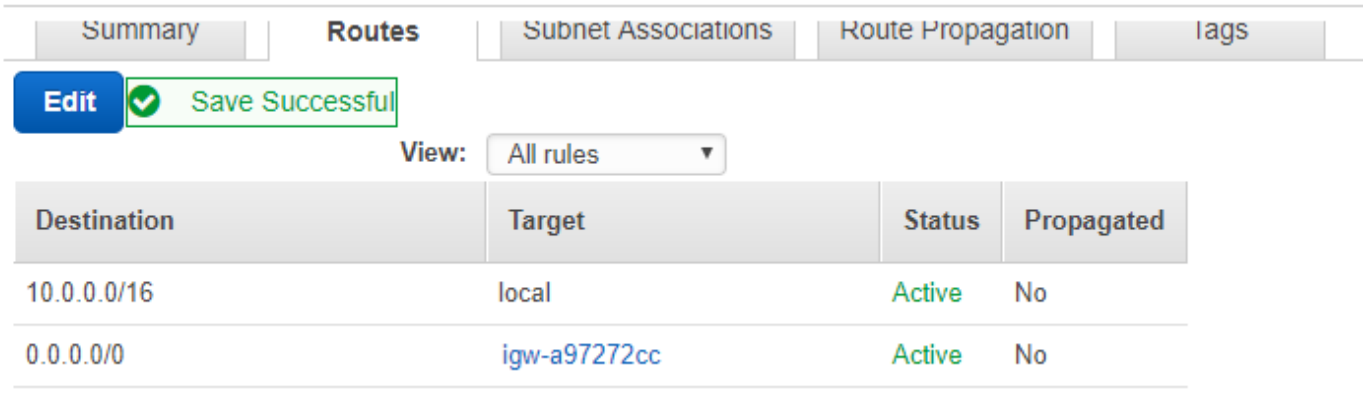
C. **Add the following entry to the route table – Destination as 10.0.0.0/16 and Target as Internet Gateway**

D. **Add the following entry to the route table - Destination as 0.0.0.0/16 and Target as Internet Gateway**

Explanation:

Correct Answer – A

The route table needs to be modified as shown below to ensure that routes from the Internet reach the instance:



Hence by default, all other options become invalid.

For more information on Route Tables, please visit the URL below:

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Route_Tables.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 26 Unattempted

Domain :Design Resilient Architectures

You are building a microservice architecture in AWS for a web application. A Lambda function collects clients' requests and forwards them to a standard SQS queue. Another Lambda function gets messages from the queue and processes them. Your manager is worried about the availability of the SQS queue which may become a single point of failure. How would you address this concern?

A. Create another SQS queue to provide a redundancy.

B. Select multiple availability zones when creating the SQS queue.

C. Configure the SQS queue to be the FIFO queue.

D. No actions are required as Amazon SQS uses redundant infrastructure to provide high availability.

Explanation:

Correct Answer – D

Please check https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/welcome.html for the benefits of Amazon SQS.

Option A is incorrect: Because there is no need of doing that as SQS service is highly available.

Option B is incorrect: Because users cannot select availability zones when configuring the SQS queue.

Option C is incorrect: Because both standard and FIFO queues provide high availability.

Option D is CORRECT: SQS is a highly available system so no actions are required.

Ask our Experts

Rate this Question?

View Queries open

Question 27 Unattempted

Domain :Design High-Performing Architectures

You create an Auto Scaling Group which is used to spin up instances on demand. As an architect, you need to ensure that the instances are pre-installed with software when they are launched. What are the different ways to achieve this? **(Select Two)**

A. Add the software installation to the configuration for the Auto Scaling Group.

B. Add the scripts for the installation in the User data section.

C. Create an AMI and then create a launch configuration.

D. Ask the IT operations team to install the software as soon as the instance is launched.

Explanation:

Correct Answers – B and C

The User data section of an instance launch can be used to pre-configure software after the instance is initially booted.

For more information on User data, please visit the below URL:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/user-data.html

Also, you can create an AMI or a golden image with the already installed software. Then create a launch configuration which can be used by that Auto Scaling Group.

For more information on AMIs, please visit the below URL:

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

Ask our Experts

Rate this Question? ☺ ☹

View Queries open

Question 28 Unattempted

Domain :Design Resilient Architectures

You maintain a DynamoDB table that stores customers' subscription data. High availability is very important for the table and even if there is an outage in an AWS region, the application should still be able to access the data from other regions. Which method would you take to achieve this requirement?

A. **Create a read replica in another region as a backup.**

B. **Configure a Multi-AZ backup for the DynamoDB table.**

C. **Configure a global table to use DynamoDB as a multi-region database.**

D. **No actions required as DynamoDB is a global service.**

Explanation:

Correct Answer – C

Amazon DynamoDB global tables provide a solution for deploying a multi-region, multi-master database. The reference can be found in https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/GlobalTables.html.

Option A is incorrect: Because DynamoDB does not have such a feature.

Option B is incorrect: Because there is no need to configure Multi-AZ for a DynamoDB table and it is highly available by default

Option C is CORRECT: With the DynamoDB global table, when one AWS region becomes unavailable, users can still access the same data in other regions.

Option D is incorrect: Refer to option C.

Ask our Experts

Rate this Question? ☺ ☹

View Queries open

Question 29 Unattempted

Domain :Design High-Performing Architectures

You have a set of IIS Servers running on EC2 Instances. You want to collect and process the log files generated from these IIS Servers. Which service would be ideal to run in this scenario?

A. Amazon S3 for storing the log files and Amazon EMR for processing the log files.

B. Amazon S3 for storing the log files and EC2 Instances for processing the log files.

C. Amazon EC2 for storing and processing the log files.

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

Explanation:

Correct Answer – A

Amazon EMR is a managed cluster platform that simplifies running big data frameworks, such as Apache Hadoop and Apache Spark, on AWS to process and analyze vast amounts of data. By using

these frameworks and related open-source projects, such as Apache Hive and Apache Pig, you can process data for analytics purposes and business intelligence workloads. Additionally, you can use Amazon EMR to transform and move a large amount of data into and out of other AWS data stores and databases, such as Amazon Simple Storage Service (Amazon S3) and Amazon DynamoDB.

Options B and C are partially correct as it would be an overhead for EC2 Instances to process log files when you already have a ready-made service to help in this regard.

Option D is in invalid because DynamoDB is not an ideal option to store log files.

For more information on EMR, please visit the URL below:

http://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-what-is-emr.html

Ask our Experts

Rate this Question?

View Queries open

Question 30 Unattempted

Domain :Design Resilient Architectures

You need to ensure that new objects being uploaded to an S3 bucket are available in another region, due to the criticality of the data hosted in the S3 bucket. How could you achieve this in the easiest way possible?

A. Enable Cross-Region Replication for the bucket.

B. Write a script to copy the objects to another bucket in the destination region.

C. Create an S3 snapshot in the destination region.

D. Enable versioning that will copy the objects to the destination region.

Explanation:

Correct Answer – A

AWS Documentation mentions the following:

Cross-Region Replication is a bucket-level configuration that enables automatic, asynchronous copying of objects across buckets in different AWS Regions.

For more information on Cross-Region Replication in the Simple Storage Service, please visit the URL below:

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

Ask our Experts

Rate this Question?

View Queries open

Question 31 Unattempted

Domain :Design Cost-Optimized Architectures

You want to use AWS to host your own website with a unique domain name that uses the format www.example.com. How would you achieve this?

A. **Register a domain with Route53 and use it to route requests to your website**

B. **Create an auto-scaling group of EC2 instances and manage the web hosting on these instances**

C. **Create one large EC2 instance to host the website and replicate it in every region**

D. **Create a Content Delivery Network (CDN) to deliver your images and files**

Explanation:

Correct Answer: A

Option A is correct. Route53 is used to register a domain and route requests to a website.

Option B is incorrect. Hosting on EC2 is not necessary here as server-side scripting is not needed and S3 will scale automatically.

Option C is incorrect. Hosting on EC2 is not necessary and this particular implementation can lead to different configurations on each server.

Option D is incorrect. A CDN will improve the delivery time of your files and pages to the customer but is not a hosting solution itself.

References:

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

https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/Welcome.html

https://docs.aws.amazon.com/AmazonS3/latest/dev/website-hosting-cloudfront-walkthrough.html

Ask our Experts

Rate this Question?

View Queries open

Question 32 Unattempted

Domain :Design Cost-Optimized Architectures

A storage solution is required in AWS to store videos uploaded by the user. After accessing these videos frequently for a period of a month, these videos can be deleted. How could this be implemented in the most cost-effective manner?

A. **Use EBS Volumes to store the videos. Create a script to delete the videos after a month.**

B. **Configure object expiration on the S3 bucket and the policy will take care of deleting the videos on the completion of 30 days.**

C. **Store the videos in Amazon Glacier and then use Lifecycle Policies.**

D. **Store the videos using Stored Volumes. Create a script to delete the videos after a month.**

Explanation:

Correct Answer – B

AWS Documentation mentions the following on Lifecycle Policies:

Lifecycle configuration enables you to specify the lifecycle management of objects in a bucket. The configuration is a set of one or more rules, where each rule defines an action for Amazon S3 to apply to a group of objects. These actions can be classified as follows:

Transition actions – In which you define when objects transition occurs to another storage class. For example, you may choose transition objects to the STANDARD_IA (IA, for infrequent access) storage class 30 days after creation or archive objects to the GLACIER storage class one year after creation.

Expiration actions – In which you specify when the objects expire. Then Amazon S3 deletes the expired objects on your behalf.

For more information on AWS S3 Lifecycle policies, please visit the following URL:

https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html

Ask our Experts

Rate this Question? ☺ ☹

View Queries open

Question 33 Unattempted

Domain :Design Secure Applications and Architectures

You are working as an AWS Architect for a global media firm. They have web servers deployed on EC2 instances across multiple regions. For audit purposes, you have created a CloudTrail trail to store all CloudTrail event log files to the S3 bucket.
This trail applies to all regions & is stored in S3 buckets at the EU-Central region. During last year's audit, auditors have raised a query on the integrity of log files that are stored in the S3 buckets and tendered as Non-Compliance. Which feature could help you to gain compliance from Auditors for this query?

A. Use Amazon SSE-S3 encryption for the CloudTrail log file while storing it to S3 buckets.

B. Use Amazon SSE-KMS encryption for CloudTrail log file while storing it to S3 buckets.

C. Use an S3 bucket policy to grant access to only Security head for S3 buckets having CloudTrail log files.

D. Enable the CloudTrail log file integrity validation feature.

Explanation:

Correct Answer: D

After you enable CloudTrail log file integrity, it will create a hash file called digest file which refers to logs that are generated. This digest file is saved in a different folder in the S3 bucket where log files are saved. Each of these digest files has the private key of public & private key pair. The DIgest file can be validated using the public key. This feature ensures that all the modifications made to CloudTrail log files are recorded.

Option A is incorrect as by default all CloudTrail log files are delivered to S3 buckets using SSE-S3 encryption, this will not ensure the integrity of log files.

Option B is incorrect as with Amazon SSE-KMS encryption for CloudTrail log file, there would be an additional layer of security for log files, but it won't ensure the integrity of log files.

Option C is incorrect as although this will restrict access to the bucket but won't ensure that no modification has been done to log files post delivering in S3 buckets.

For more information on CloudTrail Log files Integrity, please refer to the following URLs:

https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-log-file-validation-intro.html

https://aws.amazon.com/blogs/aws/aws-cloudtrail-update-sse-kms-encryption-log-file-integrity-verification/

Ask our Experts

Rate this Question? ☺ ☹

View Queries open

Question 34 Unattempted

Domain :Design Resilient Architectures

You have an EC2 Instance in a particular region. This EC2 Instance has a preconfigured software running on it. You have been requested to create a disaster recovery solution in case the instance in the region fails. Which of the following is the best solution?

A. **Create a duplicate EC2 Instance in another AZ. Keep it in the shutdown state. When required, bring it back up.**

B. **Backup the EBS data volume. If the instance fails, bring up a new EC2 instance and attach the volume.**

C. **Store the EC2 data on S3. If the instance fails, bring up a new EC2 instance and restore the data from S3.**

D. **Create an AMI of the EC2 Instance and copy it to another region.**

Explanation:

Answer - D

You can copy an Amazon Machine Image (AMI) within or across an AWS region using the AWS Management Console, the AWS command line tools or SDKs, or the Amazon EC2 API, all of which support the CopyImage action. You can copy both Amazon EBS-backed AMIs and instance store-backed AMIs. You can copy AMIs with encrypted snapshots and encrypted AMIs.

Copying a source AMI results in an identical but distinct target AMI with its own unique identifier. In the case of an Amazon EBS-backed AMI, each of its backing snapshots is, by default, copied to an identical but distinct target snapshot.

Option A is invalid, because it is a maintenance overhead to maintain another non-running instance.

Option B is invalid, because the preconfigured software could have settings on the root volume.

Option C is invalid, because this is a long and inefficient way to restore a failed instance.

For more information on Copying AMIs, please visit the below URL:

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

Ask our Experts

Rate this Question?

View Queries open

Question 35 Unattempted

Domain :Design Secure Applications and Architectures

You work in the media industry and have created a web application where users will be able to upload photos they create, to your website. This web application must be able to call the S3 API in order to function properly. Where would you store your API credentials while maintaining the maximum level of security?

A. Save the API credentials to your PHP files.

B. Don't save your API credentials. Instead, create a role in IAM and assign this role to an EC2 instance when you first create it.

C. Save your API credentials in a public Github repository.

D. Pass API credentials to the instance using instance user data.

Explanation:

Correct Answer – B

Applications must sign their API requests with AWS credentials. Therefore, if you are an application developer, you need a strategy for managing credentials for your applications that run on EC2 instances.

For example, you can securely distribute your AWS credentials to the instances, enabling the applications on those instances to use your credentials to sign requests, while protecting your credentials from other users. However, it's challenging to securely distribute credentials to each instance, especially those that the AWS creates on your behalfs, such as Spot Instances or instances in Auto Scaling groups. You must also be able to update the credentials on each instance when you rotate your AWS credentials.

IAM roles are designed so that your applications can securely make API requests from your instances, without requiring you to manage the security credentials that the applications use.

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

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html

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 36 Unattempted

Domain :Design Resilient Architectures

Your company has a new web application that needs to be deployed in AWS as soon as possible. The application is backed in an AMI and you plan to use an Application Load Balancer to distribute the traffic to an Auto Scaling group. Which of the following methods helps you to achieve a highly available system?

A. Assign an Elastic IP to each instance under the Auto Scaling group.

B. Use the Application Load Balancer to send traffic across instances in multiple availability zones.

C. Configure the Application Load Balancer to distribute traffic to instances in multiple AWS regions.

D. Assign a dedicated IP address to the Application Load Balancer.

Explanation:

Correct Answer – B

Refer to https://d1.awsstatic.com/whitepapers/aws-building-fault-tolerant-applications.pdf for how to build highly available and fault-tolerant software systems in AWS.

Option A is incorrect: It is not necessary to assign Elastic IPs to ASG instances. The instances may be terminated when the ASG scales in and new instances will be created.

Option B is CORRECT: Because this ensures that when one availability zone has an outage, instances in other availability zones can still serve traffic from the Application Load Balancer.

Option C is incorrect: Because Application Load Balancer is a regional service and cannot distribute traffic to instances in multiple regions.

Option D is incorrect: Because users cannot assign IP addresses to an Application Load Balancer.

Ask our Experts

Rate this Question?

View Queries open

Question 37 Unattempted

Domain :Design High-Performing Architectures

An organization is managing a Redshift Cluster in AWS. They need to monitor the performance of this Redshift cluster to ensure that it is performing as efficiently as possible. Which of the following services should be used for achieving this requirement? **(Select Two)**

A. CloudTrail

B. VPC Flow Logs

C. CloudWatch

D. AWS Trusted Advisor

Explanation:

Correct Answers - C and D

AWS Documentation mentions the following on monitoring Redshift Clusters:

Amazon CloudWatch metrics help you monitor the physical aspects of your cluster, such as CPU utilization, latency, and throughput. Metric data is displayed directly in the Amazon Redshift console. You can also view it in the Amazon CloudWatch console, or you can consume it in any other way you work with metrics such as with the Amazon CloudWatch Command Line Interface (CLI) or one of the AWS Software Development Kits (SDKs).

For more information on monitoring Redshift, please visit the URL below:

https://docs.aws.amazon.com/redshift/latest/mgmt/metrics.html

For Option D, please go through the link below:

https://aws.amazon.com/about-aws/whats-new/2016/03/aws-trusted-advisor-adds-checks-for-amazon-s3-amazon-redshift-reserved-instances-security-and-service-limits/

Ask our Experts

Rate this Question? ☺ ☹

View Queries open

Question 38 Unattempted

Domain :Design High-Performing Architectures

You are working as an AWS Architect for a global insurance firm. For the web application, you are using S3 buckets and have configured CloudFront to cache image files. For audit purposes, you have created a CloudTrail trail in each region and the events logs files are logged in S3 bucket in the us-west-1 region.
There have been changes in CloudFront which have caused all traffic being routed to the origin, resulting in increased latency for users in other continents. After scrutinizing CloudTrail logs, you found that there are duplicate CloudFront events being logged. What configuration changes would you perform to eliminate duplicate CloudFront logs?

A. **Using AWS CLI, update CloudTrail trail to disable global service events that are delivered in all regions except US-West-1.**

B. **Using AWS CLI, change the configuration of a trail to logging a single region instead of logging all regions.**

C. **Using AWS console, update CloudTrail trail to disable global service events to be delivered in all regions except US-West-1.**

D. **Using the AWS console, change the configuration of a trail to logging a single region instead of logging all regions.**

Explanation:

Correct Answer – A

Amazon CloudFront is a global service for which events are delivered to CloudTrail trails which include global services. To avoid duplicate Amazon CloudFront events, you can disable these events from delivering to CloudTrail trails in all regions & enable in only one region.

Options B & D is incorrect as if CloudTrail trail is changed to logging a single region, global service event logging is off automatically, this will disable CloudFront events being logged instead of avoiding duplicate logs.

Option C is incorrect as Changes to Global service event logs can be done only via AWS CLI & not via AWS console.

For more information on Global Service Events with CloudTrail, refer to the following URL:

https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-concepts.html#cloudtrail-concepts-regional-and-global-services

Ask our Experts

Rate this Question?

View Queries open

Question 39 Unattempted

Domain :Design High-Performing Architectures

You are working for a start-up firm that developed a new multilingual website for sharing images and video files. You are using EC2 instance to host this web application. To deliver these web content with the lowest latency to end-users, you have configured Amazon CloudFront which forward query strings to origin servers based on selected parameter values and also cache web content based upon these parameter values.
During the trial, it was observed that caching is not happening based upon query strings resulting in these requests hitting origin servers. Which of the following need to be checked if CloudFront is caching properly based upon query strings? **(Select Three)**

A. **Make sure that the distribution is an RTMP distribution.**

B. Make sure that the delimiter character between query string parameters is a '&' character.

C. Check if Parameters' names and values are in the same case.

D. Make sure that the delimiter character between query string parameters is a "/" character.

E. Make sure that the distribution is a Web distribution.

F. Check only that the query parameter names are in the same case

Explanation:

Correct Answers – B, C, E

CloudFront Query String Forwarding only supports Web distribution. For query string forwarding, the delimiter character must be always a '&' character. Parameters' names and values used in the query string are case sensitive.

Option A is incorrect as CloudFront Query String Forwarding does not support RTMP distribution.

Option D is incorrect as Delimiter Character should be always '&', not '\' character.

Option F is incorrect as in the case of Parameters in the query string, both the parameters' names and values are case sensitive.

For more information on Query String forwarding, refer to the following URL:

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/QueryStringParameters.htr

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 40 Unattempted

Domain :Design High-Performing Architectures

IoT sensors monitor the number of bags that are handled at an airport. The data is sent back to a Kinesis stream with default settings. Every alternate day, the data from the stream is sent to S3 for processing. But it is noticed that S3 is not receiving all of the data that is being sent to the Kinesis stream. What could be the reason for this?

A. **The sensors probably stopped working on somedays, hence data is not sent to the stream.**

B. **S3 can only store data for a day.**

C. **The default retention period of the data stream is set to 24 hours only, and hence the failure.**

D. **Kinesis streams are not meant to handle IoT related data.**

Explanation:

Correct Answer – C

Kinesis Streams support changes to the data record retention period of your stream. A Kinesis stream is an ordered sequence of data records, meant to be written to and read from in real-time. Data records are therefore stored in shards in your stream temporarily. The time period from when a record is added to when it is no longer accessible is called the *retention period*. A Kinesis stream stores the records from 24 hours (by default), up to 168 hours.

Option A is incorrect, even though a possibility, cannot be considered as the right option.

Option B is incorrect since S3 can store data indefinitely unless you have a lifecycle policy defined.

Option D is incorrect because the Kinesis service is perfect for this sort of data ingestion.

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

http://docs.aws.amazon.com/streams/latest/dev/kinesis-extended-retention.html

Ask our Experts

Rate this Question?

View Queries open

Question 41 Unattempted

Domain :Design Resilient Architectures

Your company uses an S3 bucket to store data for an application. Sometimes the team also downloads the S3 files for further analysis. As the data is very important, you need to protect against accidental deletions initiated by someone or an application. Which of the following options is appropriate?

A. **Enable the versioning feature in the S3 bucket.**

B. **Modify the S3 bucket to be read-only.**

C. **Use an S3 Lifecycle policy to transfer objects to a lower cost storage.**

D. **Enable the Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS).**

Explanation:

Correct Answer – A

Option A is CORRECT: The versioning feature in Amazon S3 helps to retain prior versions of objects stored in S3. Even if the current version is deleted accidently, the data can still be recovered from the previous version. Check the reference in https://d1.awsstatic.com/whitepapers/aws-building-fault-tolerant-applications.pdf.

Option B is incorrect: The application may still need to write data in the S3 bucket so the option is not appropriate.

Option C is incorrect: This method helps to save cost but not protect the data.

Option D is incorrect: Because the Server-Side Encryption cannot protect against accidental deletions.

Ask our Experts

Rate this Question?

View Queries open

Question 42 Unattempted

Domain :Design Resilient Architectures

You create an Amazon SQS queue to decouple software components. The messages are processed by a Lambda function. Sometimes, the Lambda function fails to process messages in the queue. You need a mechanism to isolate the message failures to determine why the processing was unsuccessful. Which of the following options would you choose?

A. FIFO (First-In-First-Out) queue

B. Visibility timeout

C. SQS dead-letter queue

D. SQS long polling

Explanation:

Correct Answer – C

SQS dead-letter queue should be selected as it is designed to isolate problematic messages in the queue. Details please check https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-dead-letter-queues.html.

Option A is incorrect: Because FIFO queue itself does not isolate the messages that have failures.

Option B is incorrect: Visibility timeout prevents other consumers from processing the message again. It does not resolve the mentioned problem.

Option C is CORRECT: Because users can configure the dead letter queue to isolate the message failures as follows:

Option D is incorrect: SQS long polling reduces the number of empty responses. It cannot handle the problematic messages.

Ask our Experts

Rate this Question?

View Queries open

Question 43 Unattempted

Domain :Design High-Performing Architectures

A company requires to deploy an existing Java-based application to AWS. Which of the following should be used to fulfill this requirement in the quickest way possible?

A. Deploy to an S3 bucket and enable website hosting.

B. Use the Elastic Beanstalk service to provision the environment.

C. Use EC2 with Auto Scaling for the environment.

D. Use AMIs to build EC2 instances for deployment.

Explanation:

Correct Answer - B

AWS Documentation mentions the following:

AWS Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services developed with Java, .NET, PHP, Node.js, Python, Ruby, Go, and Docker on familiar servers such as Apache, Nginx, Passenger, and IIS.

You can simply upload your code and Elastic Beanstalk will automatically handle the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring. At the same time, you retain full control over the AWS resources powering your application and can access the underlying resources at any time.

For more information on the Elastic Beanstalk service, please visit the following URL:

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

Try now labs related to this question

Introduction to AWS Elastic Beanstalk

This lab walks you through to AWS Elastic Beanstalk. In this lab, you will quickly deploy and manage a Java application in the AWS Cloud without worrying about the infrastructure that runs those applications.

Credit Needed 10 Time 0 : 45 Try Now

Ask our Experts

Rate this Question?

View Queries open

Question 44 Unattempted

Domain :Design Secure Applications and Architectures

You are working as an AWS Administrator for a software firm that has a popular Web application hosted on EC2 instance in various regions. You are using AWS CloudHSM for offloading SSL/TLS processing from Web servers. Since this is a critical application for the firm, you need to ensure that proper backups are performed for data in AWS CloudHSM on a daily basis. What does the AWS CloudHSM use to perform a secure & durable backup?

A. **Ephemeral backup key (EBK) is used to encrypt data & Persistent backup key (PBK) is used to encrypt EBK before saving data to the Amazon S3 bucket in the same region as that of AWS CloudHSM cluster.**

B. Data Key is used to encrypt data & Customer Managed Key (CMK) is used to encrypt Data Key before saving data to the Amazon S3 bucket in the same region as that of AWS CloudHSM cluster.

C. Ephemeral Backup Key (EBK) is used to encrypt data & Persistent backup Key (PBK) is used to encrypt EBK before saving data to the Amazon S3 bucket in a different region than the AWS CloudHSM cluster.

D. Data Key is used to encrypt data & Customer Managed Key (CMK) is used to encrypt Data Key before saving data to Amazon S3 bucket in a different region than the AWS CloudHSM cluster.

Explanation:

Correct Answer – A

To backup the AWS CloudHSM data to Amazon S3 buckets in the same region, AWS CloudHSM generates a unique Ephemeral Backup Key (EBK) to encrypt all data using AES 256-bit encryption key. This Ephemeral Backup Key (EBK) is further encrypted using Persistent Backup Key (PBK) which is also AES 256-bit encryption key.

Option B is incorrect as Data Key & Customer Managed Key are not used by AWS CloudHSM for the encryption of data, instead of that EBK & PBK are used.

Option C is incorrect. While taking the backup of data from different AWS CloudHSM clusters to the Amazon S3 bucket, the Amazon S3 bucket should be in the same region as that of the AWS CloudHSM cluster.

Option D is incorrect as Data Key & Customer Managed Key are not used by AWS CloudHSM for the encryption of data, instead of that EBK & PBK are used for encrypting and saving data to the Amazon S3 bucket in the same region.

For more information on backing data from AWS CloudHSM, refer to the following URL:

https://docs.aws.amazon.com/cloudhsm/latest/userguide/backups.html

Ask our Experts

Rate this Question? ☺ ☹

View Queries open

Question 45 Unattempted

Domain :Design Resilient Architectures

You want to build a decoupled, highly available and fault tolerant architecture, including buffered request for your application in AWS. You decide to use EC2, the Classic Load Balancer, Auto Scaling and Route 53. Which one of the following additional services should you involve in this architecture?

A. AWS SNS

B. AWS SQS

C. AWS API Gateway

D. AWS Config

Explanation:

Answer – B

The Simple Queue Service can be used to build a decoupled architecture.

AWS Documentation further mentions the following:

Amazon Simple Queue Service (SQS) is a fully managed message queuing service that makes it easy to decouple and scale microservices, distributed systems, and serverless applications. Building applications from individual components that each perform a discrete function improves scalability and reliability, and is best practice design for modern applications.

• Scalability – Amazon SQS can process each buffered request (p. 202) independently, scaling transparently to handle any load increases or spikes without any provisioning instructions.

For more information on the Simple Queue Service, please visit the following URL:

https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-dg.pdf

Ask our Experts

Rate this Question?

View Queries open

Question 46 Unattempted

Domain :Design Resilient Architectures

You have been assigned the task of architecting an application in AWS. The architecture would consist of EC2, the Classic Load Balancer, Auto Scaling, and Route 53. You need to ensure that Blue-Green deployments are possible in this architecture. Which routing policy should you ideally use in Route 53 in order to achieve Blue-Green deployments?

A. Simple

B. Multivalue Answer

C. Latency

D. Weighted

Explanation:

Correct Answer – D

AWS Documentation mentions that the Weighted routing policy is good for testing new versions of the software. Also, It is the ideal approach for Blue-Green deployments.

Weighted routing lets you associate multiple resources with a single domain name (example.com) or subdomain name (acme.example.com) and choose how much traffic is routed to each resource. This can be useful for a variety of purposes, including load balancing and testing new versions of the software.

For more information on Route 53 routing policies, please visit the following URL:

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

Note: Multivalue-answer is recommended to use only when you want to route traffic randomly to multiple resources, such as web servers, you can create one multivalue answer record for each resource and, optionally, associate an Amazon Route 53 health check with each record.

However, in this case, we need to choose how much traffic is routed to each resource (blue and green). For example, Blue is currently live and we need to send less portion of traffic to Green to check everything works fine. If yes, then we can decide to go with Green resources. If no, we can change the weight for that record to 0. Blue will be completely live again.

NOTE:

When you implement the Blue-Green Deployment, It's not always fixed that the Blue environment is in an Alive state and Green environment in Idle state vice versa. During the testing phase, you can route your traffic to both the Blue and Green environments with a specified traffic load.

For more information, please visit the link below:

https://d1.awsstatic.com/whitepapers/AWS_Blue_Green_Deployments.pdf (11 of 35). AWS explained with the proper diagram.

Ask our Experts

Rate this Question?

View Queries open

Question 47 Unattempted

Domain :Design High-Performing Architectures

A company is planning to deploy an application in AWS. This application requires an EC2 Instance to continuously perform log processing activities requiring Max 500MiB/s of data throughput. Which of the following is the best storage option for this requirement?

A. EBS IOPS

B. EBS SSD

C. EBS Throughput Optimized

D. EBS Cold Storage

Explanation:

Correct Answer – C

While considering storage volume types for batch processing activities with large throughput, consider using the EBS Throughput Optimized volume type.

AWS Documentation mentions this, as shown below:

	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 16,000 IOPS or 250 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
API Name	gp2	io1	st1	sc1
Volume Size	1 GiB - 16 TiB	4 GiB - 16 TiB	500 GiB - 16 TiB	500 GiB - 16 TiB
Max. IOPS/Volume**	16,000***	64,000****	500	250
Max. Throughput/Volume	250 MiB/s***	1,000 MiB/s†	500 MiB/s	250 MiB/s
Max. IOPS/Instance††	80,000	80,000	80,000	80,000
Max. Throughput/Instance††	1,750 MiB/s	1,750 MiB/s	1,750 MiB/s	1,750 MiB/s

For more information on EBS Volume Types, please visit the following URL:

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

Try now labs related to this question

Introduction to Amazon Elastic Compute Cloud (EC2)

1. This lab walks you through the steps to launch and configure a virtual machine in the Amazon cloud.

2. You will practice using Amazon Machine Images to launch Amazon EC2 Instances and use key pairs for SSH authentication to log into your instance. You will create a web

page and publish it.

Credit Needed 10 Time 0 : 30 Try Now

Ask our Experts

Rate this Question?

View Queries open

Question 48 Unattempted

Domain :Design High-Performing Architectures

You are working as an AWS Architect for a start-up company. You have developed an application that will read out AWS Blogs to AWS professionals using "Amazon Polly". You need to perform a trial with the "Amazon S3" blog, in which the first "S3" should be read as "Amazon Simple Storage Service" while all subsequent "S3" should be read as "S3".
This test needs to be done in 2 different regions, us-west-1 & us-east-1. What could be done to perform the test successfully?

A. **Using multiple Lexicons, create different alias for the word “S3” & apply in different orders. Upload Lexicons in us-west-1 region & use for both regions.**

B. **Using multiple Lexicons, create different alias for the word “S3” & apply in different orders. Upload Lexicons in us-west-1 region & us-east-1 region.**

C. **Using a single Lexicon, create different alias for the word “S3” & apply in different orders. Upload Lexicons in us-west-1 region & us-east-1 region.**

D. **Using a single Lexicon, create different alias for the word “S3” & apply in different orders. Upload Lexicons in us-east-1 region & use for both regions.**

Explanation:

Correct Answer – B

Lexicons are specific to a region. You will need to upload Lexicon in each region where you need to use it. For a single text which appears multiple times in the content, you can create an alias using multiple Lexicons to have different speech.

Option A is incorrect as Lexicons needs to upload in all regions where content will be using Amazon Polly.

Option C is incorrect as if a single word is repeating multiple times in content & needs to have different speech, we need to have multiple Lexicons created.

Option D is incorrect as Lexicons needs to upload in all regions where content will be using Amazon Polly & to have a different speech for the single word being repeated multiple times, multiple Lexicons needs to be created.

For more information on managing Lexicons, refer to the following URL:

https://docs.aws.amazon.com/polly/latest/dg/managing-lexicons.html

Ask our Experts

Rate this Question? ☺ ☹

View Queries open

Question 49 Unattempted

Domain :Design Secure Applications and Architectures

You need to ensure that instances in a private subnet can access the Internet. The solution should be highly available and ensure less maintenance overhead. Which of the following would ideally fit this requirement?

A. **Host the NAT Instance in the private subnet.**

B. **Host the NAT Instance in the public subnet.**

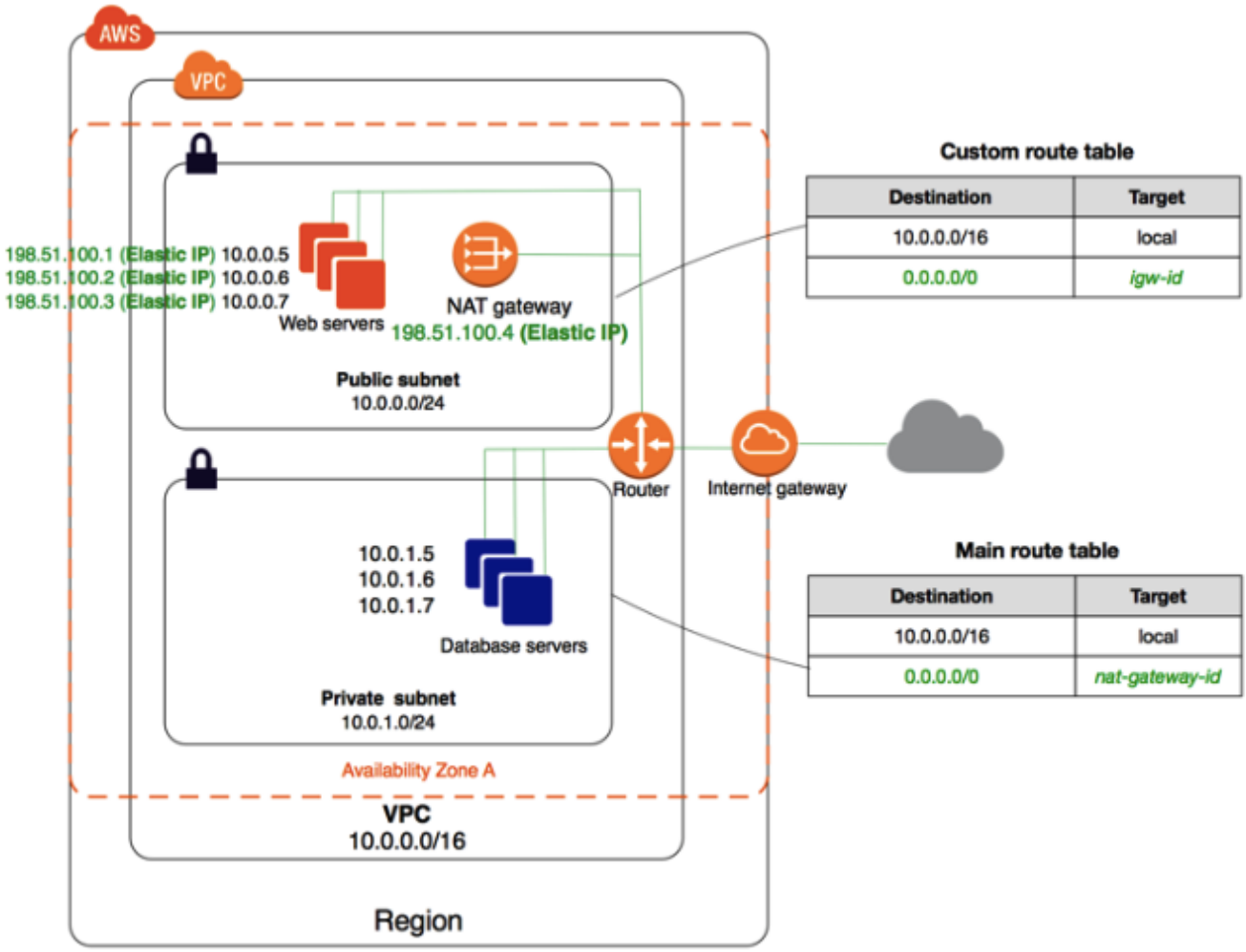
C. **Host the NAT Gateway in the private subnet.**

D. **Host the NAT Gateway in the public subnet.**

Explanation:

Correct Answer – D

NAT gateway is used to enable instances in a private subnet to connect to the internet. However, the **NAT gateway is implemented or placed in the public subnet of a VPC.**



For more information, please check out the following URLs:

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

https://docs.aws.amazon.com/appstream2/latest/developerguide/managing-network-internet-manual.html

Shown below is a comparison of the NAT Gateway and NAT Instances as per the AWS Documentation. The documentation states that the NAT Gateway is highly available and requires less management.

Comparison of NAT Instances and NAT Gateways

The following is a high-level summary of the differences between NAT instances and NAT gateways.

Attribute	NAT gateway	NAT instance
Availability	Highly available. NAT gateways in each Availability Zone are implemented with redundancy. Create a NAT gateway in each Availability Zone to ensure zone-independent architecture.	Use a script to manage failover between instances.
Bandwidth	Supports bursts of up to 10Gbps.	Depends on the bandwidth of the instance type.
Maintenance	Managed by AWS.You do not need to perform any maintenance.	Managed by you, for example, by installing software updates or operating system patches on the instance.

For more information on the above comparison, please visit the following URL:

https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-nat-comparison.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 50 Unattempted

Domain :Design High-Performing Architectures

You need to have a Data storage layer in AWS. Following are the key requirements:
a) Storage of JSON documents
b) Availability of Indexes
c) Automatic scaling
What would be an ideal storage layer for the above requirements?

A. AWS DynamoDB

B. AWS EBS Volumes

C. AWS S3

D. AWS Glacier

Explanation:

Correct Answer – A

AWS Documentation mentions the following:

Amazon DynamoDB is a fully managed NoSQL database service that provides fast and predictable performance with seamless scalability. DynamoDB enables customers to offload the administrative burdens of operating and scaling distributed databases to AWS so that they don't have to worry about hardware provisioning, setup, and configuration, throughput capacity planning, replication, software patching or cluster scaling.

For more information on DynamoDB, please visit the following URL:

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

Try now labs related to this question

Introduction to AWS DynamoDB

This lab walks you through to Amazon DynamoDB features. In this lab, we will create a table in Amazon DynamoDB to store information and then query that information from the DynamoDB table.

Credit Needed 10 Time 0 : 30 Try Now

Ask our Experts

Rate this Question?

View Queries open

Question 51 Unattempted

Domain :Design High-Performing Architectures

You have a set of Docker images that you use for building containers. You want to start using the Elastic Container Service and utilize the Docker images. You need a place to store these Docker images. What would you use for this purpose?

A. Use AWS DynamoDB to store the Docker images.

B. Use AWS RDS to store the Docker images.

C. Use EC2 Instances with EBS Volumes to store the Docker images.

D. Use the ECR Service to store the Docker images.

Explanation:

Correct Answer - D

AWS Documentation mentions the following:

Amazon Elastic Container Registry (ECR) is a fully-managed Docker container registry that makes it easy for developers to store, manage, and deploy Docker container images. Amazon ECR is integrated with Amazon Elastic Container Service (ECS), simplifying your development to production workflow.

For more information on the Elastic Container Service, please visit the following URL:

https://aws.amazon.com/ecr/?nc2=h_m1

Ask our Experts

Rate this Question?

View Queries open

Question 52 Unattempted

Domain :Design High-Performing Architectures

You are working with an educational website that provides online content for professional exams using WordPress. You have recently added Amazon Polly plugins to the website to provide students audio recordings for exam contents.
You are getting customer feedback on the speech rate being too fast & continuous. What changes would you make in your content to resolve this? **(Select Three)**

A. **Add a pause using SSML tag between appropriate words & paragraphs.**

B. **Convert commas in content into the period.**

C. **Convert period in content into commas.**

D. **Add a tag as "Reduced" for appropriate words & paragraphs.**

E. **Add a tag as "Strong" for appropriate words & paragraphs.**

Explanation:

Correct Answers – A, B, E

Using SSML tags, we can control the speech generated by Amazon Polly. In the above example, using SSML tags, convert commas to period & tag words and paragraphs as "Strong", will help to control the speech speed, adds appropriate pause & emphasis on appropriate words slowing speaking rate.

Option C is incorrect as commas will not insert a pause in the speech during the reading text.

Option D is incorrect as adding the tag as "Reduced" will speed up speech rate, along with a decrease in volume.

For more information on SSML Tags supported by Amazon Polly, refer to the following URL:

https://docs.aws.amazon.com/polly/latest/dg/supported-ssml.html

Ask our Experts

Rate this Question?

View Queries open

Question 53 Unattempted

Domain :Design Cost-Optimized Architectures

You are developing a mobile application for your company with DynamoDB as the back end and JavaScript as the front end. During application usage, you notice that there are spikes in the application especially in the DynamoDB write throughput. What would be the most cost-effective and scalable architecture for this application?

A. Autoscale DynamoDB to meet the requirements.

B. Increase write capacity of DynamoDB tables to meet the peak loads.

C. Create a service that pulls SQS messages and writes them to DynamoDB to handle sudden spikes in DynamoDB.

D. Launch DynamoDB in Multi-AZ configuration with a global index to balance writes.

Explanation:

Correct Answer – A

For more information on DynamoDB auto-scaling, please refer to the below URL:

https://aws.amazon.com/blogs/aws/new-auto-scaling-for-amazon-dynamodb/

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

Try now labs related to this question

Introduction to AWS DynamoDB

This lab walks you through to Amazon DynamoDB features. In this lab, we will create a table in Amazon DynamoDB to store information and then query that information from the DynamoDB table.

Credit Needed 10 Time 0 : 30 Try Now

Ask our Experts

Rate this Question?

View Queries open

Question 54 Unattempted

Domain :Design Secure Applications and Architectures

You are building a large-scale confidential documentation web server on AWS such that all of its documentation will be stored on S3. One of the requirements is that it should not be publicly accessible from S3 directly, and CloudFront would be needed to accomplish this. Which method would satisfy the outlined requirements?

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

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

C. **Create individual policies for each bucket the documents are stored in, and grant access only to CloudFront in these policies.**

D. **Create an S3 bucket policy that lists the CloudFront distribution ID as the Principal and the target bucket as the Amazon Resource Name (ARN).**

Explanation:

Correct Answer – B

If you want to use CloudFront signed URLs or signed cookies to provide access to objects in your Amazon S3 bucket, you probably want to prevent users from accessing your Amazon S3 objects using

Amazon S3 URLs. If users access your objects directly in Amazon S3, they bypass the controls provided by CloudFront signed URLs or signed cookies. For example, control over the date and time that a user can no longer access your content and control over which IP addresses can be used to access the content. In addition, if users access objects both through CloudFront and directly by using Amazon S3 URLs, CloudFront access logs are less useful because they're incomplete.

For more information on Origin Access Identity, please visit the link below:

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

Ask our Experts

Rate this Question?

View Queries open

Question 55 Unattempted

Domain :Design Secure Applications and Architectures

Your company is planning on hosting its development, test and production applications on EC2 Instances in AWS. The team is worried about how access control would be given to relevant IT Admins for each of the above environments. As an architect, what would you suggest to manage the relevant accesses?

A. Add tags to the instances marking each environment and then segregate access using IAM Policies.

B. Add Userdata to the underlying instances to mark each environment.

C. Add Metadata to the underlying instances to mark each environment.

D. Add each environment to a separate Auto Scaling Group.

Explanation:

Correct Answer - A

AWS Documentation mentions the following to support this requirement:

Tags enable you to categorize your AWS resources in different ways, for example, by purpose, owner, or environment. This is useful when you have many resources of the same type — you can quickly identify a specific resource based on the tags you've assigned to it.

Each tag consists of a *key* and an optional *value*, both of which you define. For example, you could define a set of tags for your account's Amazon EC2 instances that help you track each instance's owner and stack level.

We recommend you to devise a set of tag keys that meets your needs for each resource type. Using a consistent set of tag keys makes it easier for you to manage your resources. You can search and filter the resources based on the tags you add.

For more information on using tags, please visit the link below:

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

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 56 Unattempted

Domain :Design Resilient Architectures

You want to set up a public website on AWS. Your requirements are as follows:

You want the database and the application server running on AWS VPC.

You want the database to be able to connect to the Internet, specifically for patch upgrades.

You do not want to receive any incoming requests from the Internet to the database.

Which of the following solutions would best satisfy all these requirements?

A. Setup the database in a private subnet with a security group that only allows outbound traffic.

B. Setup the database in a public subnet with a security group that only allows inbound traffic.

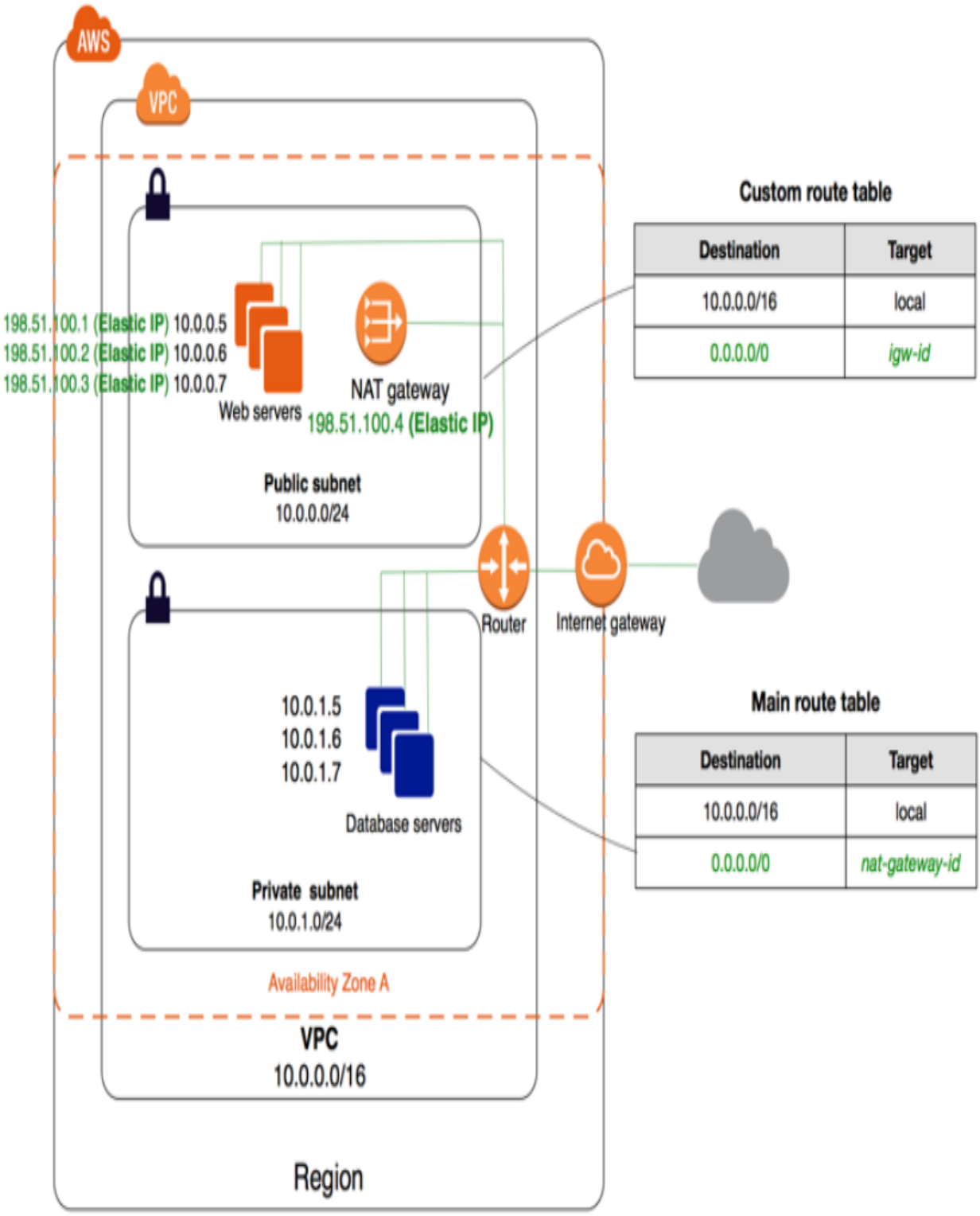
C. Setup the database in a local data center and use a private gateway to connect the application to the database.

D. Setup the public website on a public subnet and setup the database in a private subnet that connects to the Internet via a NAT Gateway.

Explanation:

Correct Answer – D

The below diagram from AWS Documentation showcases this architecture:



For more information on the VPC Scenario for public and private subnets, please visit the link below:

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

Try now labs related to this question

How to Create Virtual Private Cloud (VPC) with AWS CloudFormation

This lab walks you through how to create a VPC using AWS CloudFormation Stack. In this lab we will launch a AWS CloudFormation template to create a four-subnet Amazon VPC that spans two Availability Zones and a NAT that allows servers in the private subnets to communicate with the Internet in order to download packages and updates.

Credit Needed 10 Time 0 : 55 Try Now

Ask our Experts

Rate this Question?

View Queries open

Question 57 Unattempted

Domain :Design Resilient Architectures

Your company has a legacy application that uses the monolithic architecture. You need to design a new microservices architecture for the application and host it in AWS. The application should be dockerized so that it can be easily deployed.
Which of the following AWS services would you choose to host the application?

A. Elastic Kubernetes Engine

B. Amazon Lambda

C. Elastic Container Registry

D. Elastic Container Service

Explanation:

Correct Answer – D

Refer to https://aws.amazon.com/microservices/ for how to build highly available microservices in AWS.

Option A is incorrect: Because the service name should be Elastic Kubernetes Service (EKS).

Option B is incorrect: Because Amazon Lambda cannot run a Docker container.

Option C is incorrect: Because Elastic Container Registry is the service to store Docker images and it cannot run Docker containers.

Option D is CORRECT: Because Elastic Container service (ECS) allows users to easily run applications in Docker containers. ECS is a suitable AWS compute service for microservices.

Ask our Experts

Rate this Question?

View Queries open

Question 58 Unattempted

Domain :Design Resilient Architectures

You have a web application that processes customer orders. The frontend application forwards the order messages to an SQS queue. The backend contains an Elastic Load Balancer and an Auto Scaling group. You want the ASG to auto scale depending on the queue size. Which of the following CloudWatch metrics would you choose to discover the SQS queue length?

A. ApproximateNumberOfMessagesVisible

B. NumberOfMessagesReceived

C. NumberOfMessagesDeleted

D. ApproximateNumberOfMessagesNotVisible

Explanation:

Correct Answer – A

The backend nodes can scale based on the queue length. Check the reference in https://aws.amazon.com/blogs/compute/building-loosely-coupled-scalable-c-applications-with-amazon-sqs-and-amazon-sns/.

Option A is CORRECT: ApproximateNumberOfMessagesVisible describes the number of messages available for retrieval. It can be used to decide the queue length.

Option B is incorrect: Because NumberOfMessagesReceived is the number of messages returned by calls to the ReceiveMessage action. It does not measure the queue length.

Option C is incorrect: Because NumberOfMessagesDeleted is the number of messages deleted from the queue. It is not suitable to be used in this scenario.

Option D is incorrect: Because ApproximateNumberOfMessagesNotVisible measures the number of messages in flight. It should not be used here.

Ask our Experts

Rate this Question?

View Queries open

Question 59 Unattempted

Domain :Design High-Performing Architectures

You are performing a Load Testing exercise on your application that is hosted on AWS. While testing your Amazon RDS MySQL DB Instance, you notice that your application becomes non-responsive when you reach 100% CPU utilization. Your application is read-heavy. Which methods would help scale your data-tier to meet the application's needs? **(Select Three)**

A. **Add Amazon RDS DB Read Replicas, and have your application direct read queries to them.**

B. **Add your Amazon RDS DB instance to Storage Auto Scaling, and set your desired maximum storage limit.**

C. **Use an Amazon SQS queue to throttle data going to the Amazon RDS DB Instance.**

D. **Use ElastiCache to cache common queries of your Amazon RDS DB.**

E. **Shard your data set among multiple Amazon RDS DB Instances.**

F. **Enable Multi-AZ for your Amazon RDS DB Instance.**

Explanation:

Correct Answers - A, D, and E

Amazon RDS Read Replicas provide enhanced performance and durability for database (DB) instances. This replication feature makes it easy to elastically scale out beyond the capacity constraints of a single DB Instance for read-heavy database workloads. You can create one or more

replicas of a given source DB Instance and serve high-volume application read traffic from multiple copies of your data, thereby increasing aggregate read throughput.

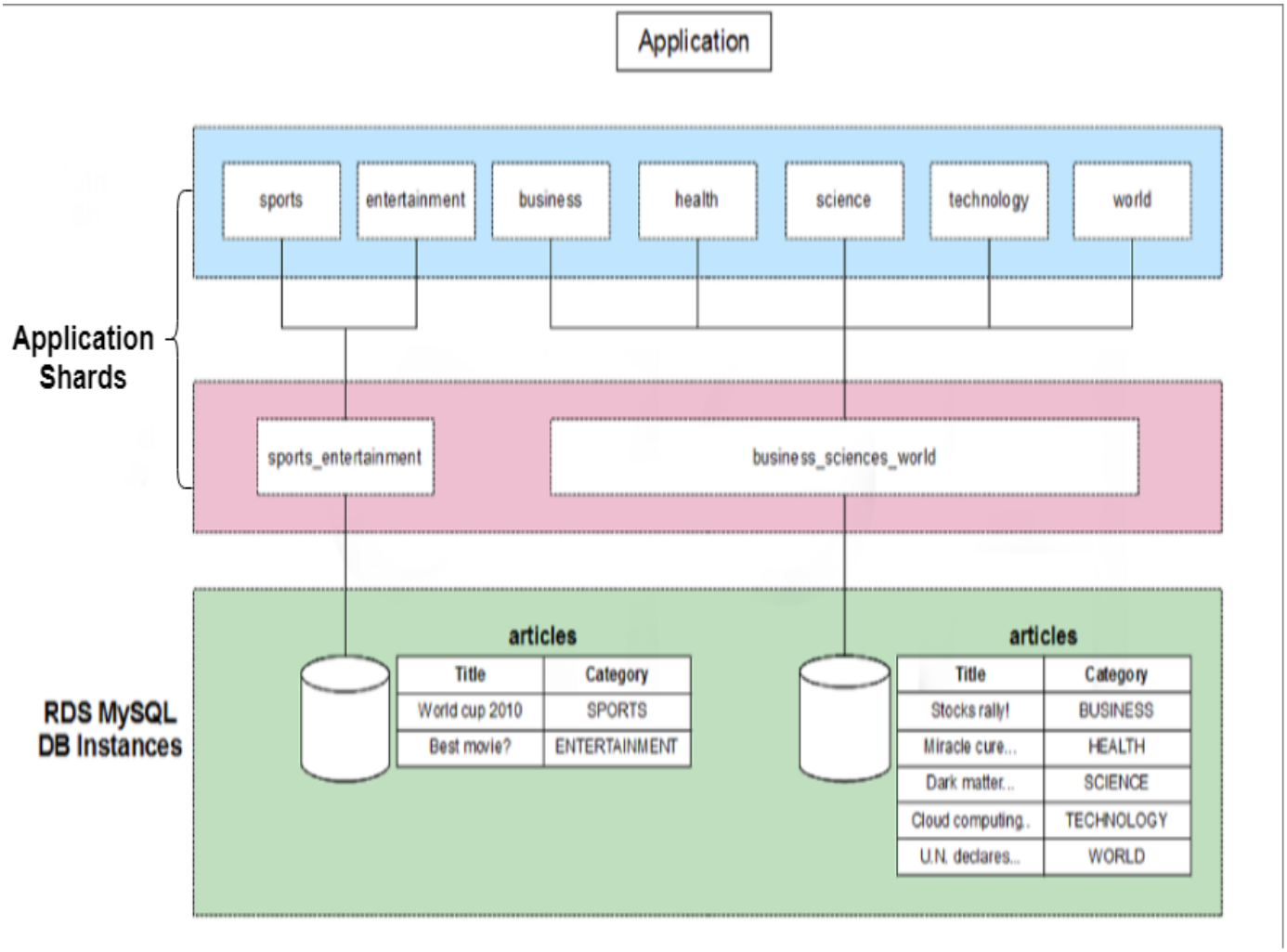
For more information on Read Replicas, please refer to the link below.

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

Sharding is a common concept to split data across multiple tables in a database. Let's consider the following example.

Application Shards

In this example, we assume that our application currently doesn't have enough load to need an application shard for each category, but we want to plan ahead with growth in mind. To make future growth easier we make use of application shards. So our application code will act as if it has seven shards, but Hibernate will map those seven shards onto a smaller number of application shards. Each application shard will map to a MySQL database instance. By using this mapping we can distribute the load to best suit our needs. For our application, assume that sports and entertainment generate as much load as the other five categories combined. These two categories will map to one application shard and the other five categories will map to the other application shard. The two application shards will be mapped as follows.



For more information on sharding, please refer to the link below.

https://forums.aws.amazon.com/thread.jspa?messageID=203052

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

For more information on ElastiCache, please refer to the link below.

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

Option B is incorrect because it is not an ideal way to scale a database. Amazon RDS Auto Scaling is to scale the storage capacity. If the storage capacity threshold is reached, then capacity will be scaled through Auto Scaling. RDS Auto Scaling does not look for the CPU utilization threshold so it cannot be a solution for bottlenecks to read heavy databases.

Option C is not an ideal choice. Because our application is read-heavy and this is the cause of the problem that we are facing with the RDS. So for this issue, Creating Read replicas, Elastic cache implementation, and Sharding the dataset are the ways through which we can tackle this issue. But if we have too may PUT requests for the DB, that is causing the issue then we can create an SQS queue and store these PUT requests in the message queue and then process it accordingly.

Option F is invalid because the Multi-AZ feature is only a failover option.

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 60 Unattempted

Domain :Design Resilient Architectures

You work for a big company having multiple applications that are very different from each other. These applications are built using different programming languages. How could you deploy these applications as quickly as possible?

A. Develop all the apps in a single Docker container and deploy using Elastic Beanstalk

B. Create a Lambda function deployment package consisting of code and any dependencies.

C. Develop each app in a separate Docker container and deploy using Elastic Beanstalk.

D. Develop each app in separate Docker containers and deploy using CloudFormation.

Explanation:

Correct Answer – C

Elastic Beanstalk supports the deployment of web applications from Docker containers. With Docker containers, you can define your own runtime environment. You can choose your own platform, programming language, and any application dependencies (such as package managers or tools), that aren't supported by other platforms. Docker containers are self-contained and include all the configuration information and software your web application requires to run.

Option A is incorrect because the requirement is to deploy multiple apps that are very different from each other and developed with different programming languages.

Option B is ideally used for running code and not packaging the applications and dependencies.

Option D is incorrect as Deploying Docker containers using CloudFormation is also not an ideal choice.

For more information on Docker and Elastic Beanstalk, please visit the URL below:

http://docs.aws.amazon.com/elasticbeanstalk/latest/dg/create_deploy_docker.html

Try now labs related to this question

Introduction to AWS Elastic Beanstalk

This lab walks you through to AWS Elastic Beanstalk. In this lab, you will quickly deploy and manage a Java application in the AWS Cloud without worrying about the infrastructure that runs those applications.

Credit Needed 10 Time 0 : 45 Try Now

Ask our Experts

Rate this Question?

View Queries open

Question 61 Unattempted

Domain :Design Cost-Optimized Architectures

You are designing a system which needs at minimum, 8 m4.large instances operating to service traffic. While designing a system for high availability in the us-east-1 region having 6 Availability Zones, your company needs to be able to handle the death of a full availability zone. How should you distribute the servers to save as much cost as possible, assuming all of the EC2 nodes are properly linked to an ELB? Your VPC account can utilize us-east-1's AZs a through f, inclusive.

A. 3 servers in each of AZs a through d, inclusive.

B. 8 servers in each of AZs a and b.

C. 2 servers in each of AZs a through e, inclusive.

D. 4 servers in each of AZs a through c, inclusive.

Explanation:

Correct Answer – C

The best way is to distribute the instances across multiple AZs to get the best performance and to avoid a disaster scenario.

With this solution, you will always have a minimum of more than 8 servers even if one AZ went down.

Even though options A and D are also valid, the best solution for distribution is Option C.

For more information on High Availability and Fault tolerance, please refer to the link below:

https://media.amazonwebservices.com/architecturecenter/AWS_ac_ra_ftha_04.pdf

Note:
In option A, we need to distribute 3 servers in each AZ.
so, A=3, B=3, C=3, D=3. Total servers used=12.

In option B, we will not get high availability.

In option C, we need to distribute 2 servers in each AZ.
so, A=2, B=2, C=2, D=2, E=2. Total servers used=10.

In option D, we need to distribute 4 servers in each AZ.
so, A=4, B=4, C=4. Total servers used=12.

In the question, it's clearly mentioned that "the company needs to be handle death of full AZ and save as much cost as possible". In option C, we are using fewer servers i.e 10 servers distributed in more AZ's.

The question says" **You are designing a system which needs at minimum, 8 m4.large instances operating to service traffic**". Now it is clear that the number of minimum instances required should be 8. The next part of the question is that "**How should you distribute the servers to save as much cost as possible, assuming all the EC2 nodes are properly linked to an ELB?"**

We have to select the solution that should be cost-effective and more available. Based on this, Option B is not that much available. Because here you are using only 2 availability zones with 8 instances in each i.e. 16 instances.

So, Option C is the correct and more suitable here.

Ask our Experts

Rate this Question? ☺ ☹

View Queries open

Question 62 Unattempted

Domain :Design Resilient Architectures

You create several SQS queues to store different types of customer requests. Each SQS queue has a backend node that pulls messages for processing. Now you need a service to collect messages from the frontend and push them to the related queues using the publish/subscribe model. Which service would you choose?

A. Amazon MQ

B. Amazon Simple Notification Service (SNS)

C. Amazon Simple Queue Service (SQS)

D. AWS Step Functions

Explanation:

Correct Answer – B

AWS SNS is able to push notifications to the related SQS endpoints. SNS uses a publish/subscribe model that provides instant event notifications for applications.

Option A is incorrect: Amazon MQ is a managed message broker service which is not suitable for this scenario.

Option B is CORRECT: Because SNS uses Pub/Sub messaging to provide asynchronous event notifications. Please check https://aws.amazon.com/pub-sub-messaging/.

Option C is incorrect: Because SQS does not use the publish/subscribe model.

Option D is incorrect: AWS Step Functions coordinates application components using visual workflows. The service should not be used in this scenario.

Ask our Experts

Rate this Question?

View Queries open

Question 63 Unattempted

Domain :Design Resilient Architectures

You need a new S3 bucket to store objects using the write-once-read-many (WORM) model. After objects are saved in the bucket, they are not allowed to be deleted or overwritten for a fixed amount of time. Which option would you select to achieve this requirement?

A. Enable the Amazon S3 object lock when creating the S3 bucket.

B. Enable versioning for the S3 bucket.

C. Modify the S3 bucket policy to only allow the read operation.

D. Enable the WORM model in the S3 Access Control List (ACL) configuration.

Explanation:

Correct Answer – A

Amazon S3 object lock should be enabled in order to store objects using the write once, read many (WORM) model. The reference can be found in https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lock.html.

Option A is CORRECT: After the S3 object lock is enabled, you can prevent the S3 objects from being deleted or overwritten for a fixed amount of time or indefinitely.

Option B is incorrect: Because versioning does not prevent objects from being deleted or modified.

Option C is incorrect: Because the S3 bucket should still allow the write operation otherwise new objects cannot be saved in the bucket.

Option D is incorrect: Because there is no such configuration in Access Control List (ACL).

Ask our Experts

Rate this Question? ☺ ☹

View Queries open

Question 64 Unattempted

Domain :Design Resilient Architectures

There are two folders A and B in an S3 bucket. Folder A stores objects that are frequently accessed. Folder B saves objects that are long-lived, infrequently accessed and non-critical. The retrieval time for files in folder B should be within milliseconds. You want to use different storage classes for objects in these two folders to save cost. Which storage classes are proper?

A. Standard for folder A and S3 Glacier for folder B.

B. Intelligent-Tiering for folder A and Reduced Redundancy for folder B.

C. Standard for folder A and One Zone-IA for folder B.

D. Two S3 buckets are required as an S3 bucket cannot have two storage classes at the same time.

Explanation:

Correct Answer – C

About different storage classes of S3 objects, please check https://docs.aws.amazon.com/AmazonS3/latest/dev/storage-class-intro.html.

Folder A should use Standard as objects are frequently accessed. Folder B should use infrequently accessed storage classes such as Standard-IA or One Zone-IA.

Option A is incorrect: Because S3 Glacier is improper as files cannot be retrieved within milliseconds.

Option B is incorrect: Because Reduced Redundancy is not cost-efficient for infrequently accessed objects.

Option C is CORRECT: Check the above explanations.

Option D is incorrect: Each object in an S3 bucket can have a user-defined storage class. There is no need to maintain two S3 buckets in this scenario.

Ask our Experts

Rate this Question? ☺ ☹

View Queries open

Question 65 Unattempted

Domain :Design Resilient Architectures

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

A. Amazon DynamoDB to store the logs and EC2 to run custom log analysis scripts

B. Amazon EC2 for storing and processing the log files

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

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

Explanation:

Correct Answer – D

This question is not that complicated, even if you don't understand the options. If you see “collection of logs and processing of logs”, directly think of AWS EMR.

Amazon EMR provides a managed Hadoop framework that makes it easy, fast, and cost-effective to process a vast amount of data across dynamically scalable Amazon EC2 instances. You can also run other popular distributed frameworks such as Apache Spark, HBase, Presto, and Flink in Amazon EMR, and interact with data in other AWS data stores such as Amazon S3 and Amazon DynamoDB.

Amazon EMR securely and reliably handles a broad set of big data use cases, including log analysis, web indexing, data transformations (ETL), machine learning, financial analysis, scientific simulation, and bioinformatics.

For more information on EMR, please visit the link below.

https://aws.amazon.com/emr/

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