Flat 15% OFF | Sitewide | Use Coupon - WHIZOFFER15 (https://www.whizlabs.com/)

CSAA PRACTICE TEST 2

Attempt	2
Marks Obtained	47 / 65
Your score is	72.31%
Mode	Practice
Completed on	Saturday , 27 April 2019 , 08:24 AM
Time Taken	N/A
Result	Pass

Domains / Skills wise Quiz Performance Report

S.No.	Skill	Total Questions	Correct	Incorrect	Unattempted	Marked as Review
1	Specify Secure Applications and Architectures	20	16	4	0	4
2	Design Resilient Architectures	18	14	4	0	4
3	Define Performant Architectures	14	8	6	0	7
4	Define Operationally-Excellent Architectures	6	4	2	0	2

	Excellent Architectures					
5	Design Cost-Optimized Architectures	7	5	2	0	2
Total	All Domain	65	47	18	0	19

Show Answers

All

QUESTION 1 CORRECT SPECIFY SECURE APPLICATIONS AND ARCHITECTURES

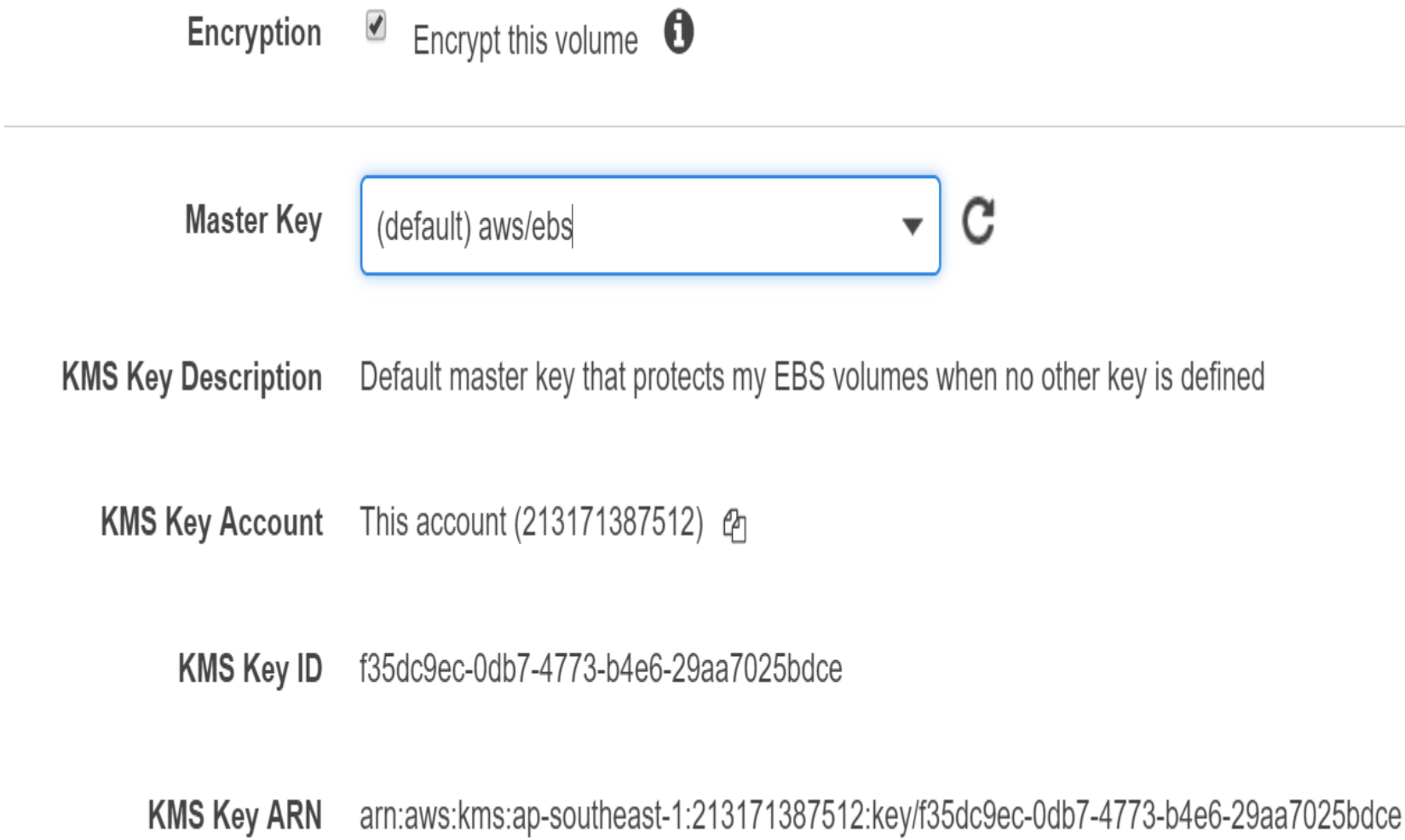
A customer wants to create EBS Volumes in AWS. The data on the volume is required to be encrypted at rest. How can this be achieved?

- A. Create an SSL Certificate and attach it to the EBS Volume.
- B. Use KMS to generate encryption keys which can be used to encrypt the volume. ✔
- C. Use CloudFront in front of the EBS Volume to encrypt all requests.
- D. Use EBS Snapshots to encrypt the requests.

Explanation :

Answer – B

When you create a volume, you have an option to encrypt the volume using keys generated by the Key Management Service.



For more information on using KMS, please refer to the below URL:
https://docs.aws.amazon.com/kms/latest/developerguide/services-ebs.html
(https://docs.aws.amazon.com/kms/latest/developerguide/services-ebs.html)

Option A is incorrect since SSL helps to encrypt data in transit.
Option C is incorrect because it also does not help in encrypting the data at rest.

Option D is incorrect because the snapshot of an unencrypted volume is also unencrypted.

Ask our Experts

QUESTION 2 CORRECT DESIGN RESILIENT ARCHITECTURES

A company has a requirement to store 100TB of data to AWS. This data will be exported using AWS Snowball and needs to then reside in a database layer. The database should have the facility to be queried from a business intelligence application. Each item is roughly 500KB in size. Which of the following is an ideal storage mechanism for the underlying data layer?

- A. AWS DynamoDB
- B. AWS Aurora
- C. AWS RDS
- D. AWS Redshift ✔

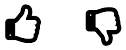
Explanation :

Answer-D

For this sheer data size, the ideal storage unit would be AWS Redshift.
AWS Documentation mentions the following on AWS Redshift:
Amazon Redshift is a fully managed, petabyte-scale data warehouse service in the cloud. You can start with just a few hundred gigabytes of data and scale to a petabyte or more. This enables you to use your data to acquire new insights for your business and customers.
The first step to create a data warehouse is to launch a set of nodes, called an Amazon Redshift cluster. After you provision your cluster, you can upload your data set and then perform data analysis queries. Regardless of the size of the data set, Amazon Redshift offers fast query performance using the same SQL-based tools and business intelligence applications that you use today.
For more information on AWS Redshift, please refer to the URL below.
https://docs.aws.amazon.com/redshift/latest/mgmt/welcome.html (https://docs.aws.amazon.com/redshift/latest/mgmt/welcome.html)

Option A is incorrect because the maximum item size in DynamoDB is 400KB.
Option B is incorrect because Aurora supports 64TB of data.
Option C is incorrect because we can create MySQL, MariaDB, SQL Server, PostgreSQL, and Oracle RDS DB instances with up to **16 TiB** of storage.

Ask our Experts



QUESTION 3 CORRECT DEFINE PERFORMANT ARCHITECTURES

A company is planning on testing a large set of IoT enabled devices. These devices will be streaming data every

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

- A. Use AWS EMR to store and process the streams.
- B. Use AWS Kinesis to process and analyze the data. ✔
- C. Use AWS SQS to store the data.
- D. Use SNS to store the data.

Explanation :

Answer - B

AWS Documentation mentions the following on Amazon Kinesis:

Amazon Kinesis makes it easy to collect, process, and analyze real-time, streaming data so you can get timely insights and react quickly to new information. Amazon Kinesis offers key capabilities to cost-effectively process streaming data at any scale, along with the flexibility to choose the tools that best suit the requirements of your application. With Amazon Kinesis, you can ingest real-time data such as video, audio, application logs, website clickstreams, and IoT telemetry data for machine learning, analytics, and other applications.

- For more information on Amazon Kinesis, please refer to the below URL:
  - https://aws.amazon.com/kinesis/ (https://aws.amazon.com/kinesis/)

- Option A: Amazon EMR can be used to process applications with data-intensive workloads.
- Option B: Amazon Kinesis can be used to store, process and analyze real-time streaming data.
- Option C: SQS is a fully managed message queuing service that makes it easy to decouple and scale microservices, distributed systems, and serverless applications.
- Option D: SNS is a flexible, fully managed pub/sub messaging and mobile notifications service for coordinating the delivery of messages to subscribing endpoints and clients.

Ask our Experts

QUESTION 4 MARKED AS REVIEW INCORRECT DESIGN RESILIENT ARCHITECTURES

Your company currently has a set of EC2 Instances hosted in AWS. The states of these instances need to be monitored and each state change needs to be recorded. Which of the following can help fulfill this requirement? Choose 2 collated steps from the options given below.

- [ ] **A.** Use CloudWatch logs to store the state change of the instances. ✔
- [x] **B.** Use CloudWatch Events to monitor the state change of the events. ✔
- [ ] **C.** Use SQS to trigger a record to be added to a DynamoDB table.
- [x] **D.** Use AWS Lambda to store a change record in a DynamoDB table. ✖

Explanation :

Answer: A and B

- Option C is incorrect as SQS cannot be used for monitoring
- Option D is incorrect as AWS Lambda cannot be used for monitoring

- Using Cloudwatch events metrics we can monitor the changes in state for EC2 instances as given in the link
- https://docs.aws.amazon.com/AmazonCloudWatch/latest/events/CloudWatch-Events-Monitoring-CloudWatch-Metrics.html (https://docs.aws.amazon.com/AmazonCloudWatch/latest/events/CloudWatch-Events-Monitoring-CloudWatch-Metrics.html)

- Using Cloudwatch logs the changes in state for EC2 instances can be recorded as given in the link. Please refer to page 84 on the below link for Cloudwatch logs

Cloudwatch logs

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

Therefore the following options are correct:

A. Use Cloudwatch logs to store the state change of the instances
B. Use Cloudwatch events to monitor the state change of the events

Ask our Experts

QUESTION 5 CORRECT SPECIFY SECURE APPLICATIONS AND ARCHITECTURES

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

- **A.** Create a new public subnet and move the instance to that subnet.
- **B.** Create a new EC2 Instance to download the updates separately and then push them to therequired instance.
- **C.** Use a NAT Gateway to allow the instances in the private subnet to download theupdates. ✔
- **D.** Create a VPC link to the Internet to allow the instances in the private subnet todownload the updates.

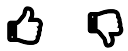
Explanation :

Answer – C

The NAT Gateway is an ideal option to ensure that instances in the private subnet have the ability to download updates from the Internet.
For more information on the NAT Gateway, please refer to the below URL:
https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-nat-gateway.html
(https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-nat-gateway.html)

Option A is not suitable because there may be a security reason for keeping these instances in the private subnet. (for example: db instances)
Option B is also incorrect. The instances in the private subnet may be running various applications and db instances. Hence, it is not advisable or practical for an EC2 Instance to download the updates separately and then push them to the required instance.
Option D is incorrect because a VPC link is not used to connect to the Internet.

Ask our Experts



QUESTION 6 MARKED AS REVIEW INCORRECT DEFINE PERFORMANT ARCHITECTURES

You have created a VPC in Paris region, and one public subnet in each Availability Zone eu-west-3a, eu-west-3b, and eu-west-3c of the same region, and each subnet having one EC2 instance inside it.

Now you want to launch ELB nodes in two AZ's out of three available. How many private IP addresses will be consumed by ELB nodes at initial launch of ELB.

- A. Three nodes in each AZ will consume three private IP addresses

- B. Two nodes in two AZ's will consume two private IP addresses ✔
- C. Two nodes in each AZ's and one for the ELB service, hence total three IP addresses will be consumed. ✖
- D. The ELB services picks the private IP addresses only when the traffic flows through the Elastic Load Balancer.

Explanation :

Answer: Option B

- A.Three nodes in each AZ will consume three private IP addresses

This option is incorrect because problem statement is we would like to launch the ELB nodes in just two subnets out of three. So the third subnet need not, have the ELB node inside it, and hence no IP address will be consumed.

- B. Two nodes in two AZ's will consume two private IP addresses

This is the correct option, as whenever we launch the ELB, the ELB service will create a node in each subnet.

- C. Two nodes in each AZ's and one for the ELB service, hence total three IP addresses will be consumed

This is incorrect option as, whenever, we launch an ELB, the ELB service won't consume an IP address, it's the ELB node which consumes IP address.

- D. The ELB services picks the private IP addresses only when the traffic flows through the Elastic Load Balancer

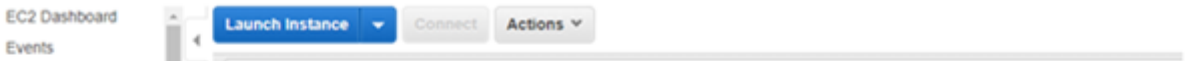
This is incorrect option as the IP addresses are assigned to the nodes at the initial launch of the ELB service.

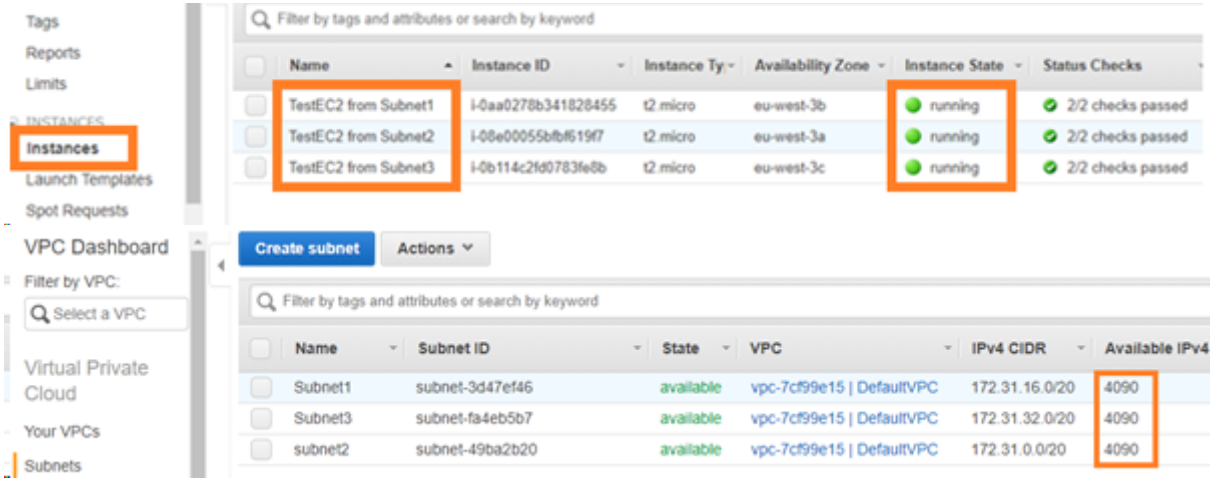
Diagrams:

a. Before creation of ELB and EC2 instances each subnet has 4091 Available IP addresses.

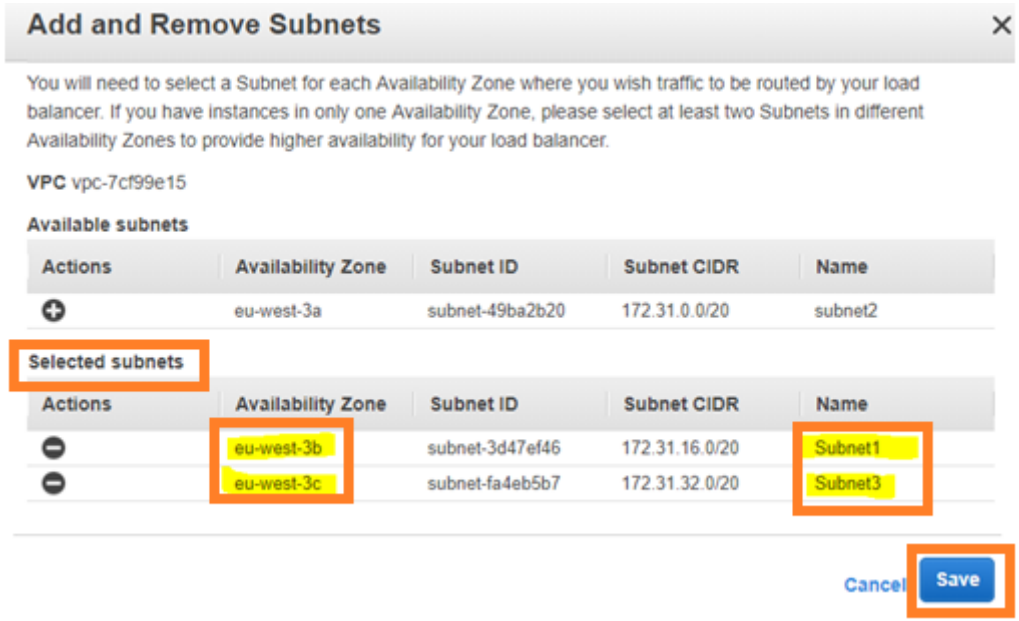
Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4
Subnet1	subnet-3d47ef46	available	vpc-7cf99e15 | DefaultVPC	172.31.16.0/20	4091
subnet2	subnet-49ba2b20	available	vpc-7cf99e15 | DefaultVPC	172.31.0.0/20	4091
Subnet3	subnet-fa4eb5b7	available	vpc-7cf99e15 | DefaultVPC	172.31.32.0/20	4091

b. After creation of EC2 instance, each Subnet holding EC2 will consume one IP hence the resulting Available IP's will be 4090.

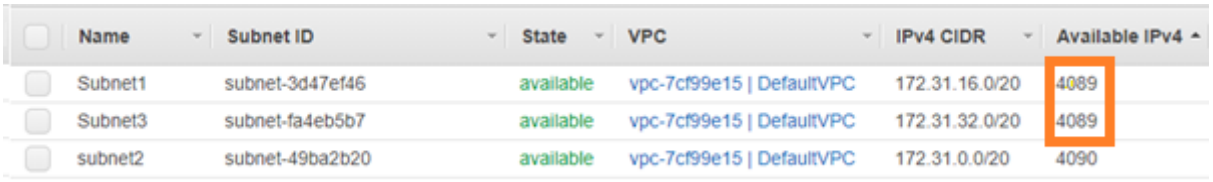




c. Create ELB and add two subnets, (in this case subnet1 and subnet3) out of three to the ELB service and save it.



d. Now the resulting Available IP's will be 4089, 4089 and 4090. Hence **TWO** IP addresses are consumed by the ELB nodes present in Subnet1 and Subnet3.



Ask our Experts

QUESTION 7 CORRECT DESIGN RESILIENT ARCHITECTURES

A company plans to have their application hosted in AWS. This application has users uploading files and then using a public URL for downloading them at a later stage. Which of the following designs would help fulfill this requirement?

- A. Have EBS Volumes hosted on EC2 Instances to store the files.
- B. Use Amazon S3 to host the files. ✔
- C. Use Amazon Glacier to host the files since this would be the cheapest storageoption.
- D. Use EBS Snapshots attached to EC2 Instances to store the files.

Explanation :

Answer – B
If you need storage for the Internet, AWS Simple Storage Service is the best option. Each uploaded file automatically gets a public URL, which can be used to download the file at a later point in time.
For more information on Amazon S3, please refer to the below URL:
https://aws.amazon.com/s3/ (https://aws.amazon.com/s3/)

Options A and D are incorrect because EBS Volumes or Snapshots do not have Public URL.

Option C is incorrect because Glacier is mainly used for data archiving purposes.

Ask our Experts

QUESTION 8 CORRECT SPECIFY SECURE APPLICATIONS AND ARCHITECTURES

You plan on hosting a web application on AWS. You create an EC2 Instance in a public subnet which needs to connect to an EC2 Instance that will host an Oracle database. Which of the following steps should be taken to ensure that a secure setup is in place? Choose 2 answers from the choices below.

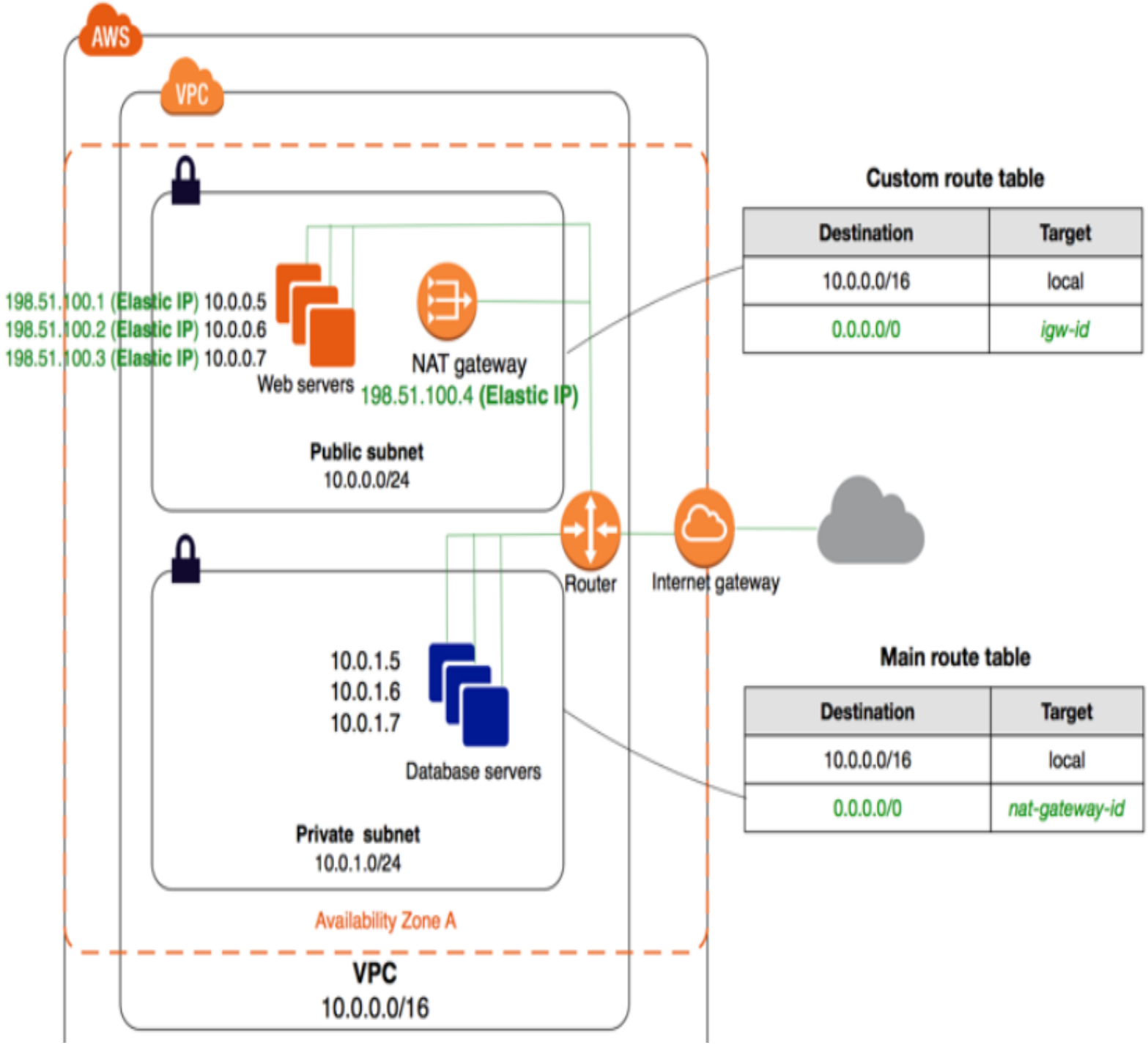
- [ ] **A.** Place the EC2 Instance with the Oracle database in the same public subnet as the Webserver for faster communication.
- [x] **B.** Place the EC2 Instance with the Oracle database in a separate private subnet. ✔
- [x] **C.** Create a database Security group which allows incoming traffic only from the Web server's security group. ✔
- [ ] **D.** Ensure that the database security group allows incoming traffic from 0.0.0.0/0

Explanation :

Answer – B and C

The best and most secure option is to place the database in a private subnet. The below diagram from AWS Documentation shows this

setup. Also, you ensure that access is not allowed from all sources but only from the web servers.



For more information on this type of setup, please refer to the below URL:
https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2.html
(https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2.html)

Option A is incorrect because as per the best practice guidelines, db instances are placed in Private subnets and allowed to communicate with web servers in the public subnet.
Option D is incorrect because allowing all incoming traffic from the Internet to the db instance is a security risk.

Ask our Experts

QUESTION 9 CORRECT SPECIFY SECURE APPLICATIONS AND ARCHITECTURES

An EC2 Instance hosts a Java based application that accesses a DynamoDB table. This EC2 Instance is currently serving production users. Which of the following is a secure way for the EC2 Instance to access the DynamoDB table?

A. Use IAM Roles with permissions to interact with DynamoDB and assign it to the EC2Instance. ✔

- **B.** Use KMS Keys with the right permissions to interact with DynamoDB and assign it tothe EC2 Instance.
- **C.** Use IAM Access Keys with the right permissions to interact with DynamoDB and assignit to the EC2 Instance.
- **D.** Use IAM Access Groups with the right permissions to interact with DynamoDB andassign it to the EC2 Instance.

Explanation :

Answer - A

To ensure secure access to AWS resources from EC2 Instances, always assign a role to the EC2 Instance.

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

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

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

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

Note:

You can attach IAM role to the existing EC2 instance.

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

Ask our Experts

A company planning on building and deploying a web application on AWS, needs to have a data store to store session data. Which of the below services can be used to meet this requirement? Please select 2 correct options.

- [ ] **A.** AWS RDS
- [ ] **B.** AWS SQS
- [x] **C.** DynamoDB ✔
- [x] **D.** AWS ElastiCache ✔

Explanation :

Answer – C and D
AWS Documentation mentions the following:
Amazon ElastiCache offers fully managed Redis (https://aws.amazon.com/redis/) and Memcached. Seamlessly deploy, operate, and scale popular open source compatible in-memory data stores. Build data-intensive apps or improve the performance of your existing apps by retrieving data from high throughput and low latency in-memory data stores. Amazon ElastiCache is a popular choice for Gaming, Ad-Tech, Financial Services, Healthcare, and IoT apps.
For more information on ElastiCache, please refer to the URL below.
https://aws.amazon.com/elasticache/ (https://aws.amazon.com/elasticache/)
Option A is incorrect. RDS is a distributed relational database. It is a web service running "in the cloud" designed to simplify the setup, operation, and scaling of a relational database for use in applications.
Option B is incorrect. SQS is a fully managed message queuing service that makes it easy to decouple and scale microservices, distributed systems, and serverless applications.

Option C is correct.
Consider only storing a unique session identifier in an HTTP cookie and storing more detailed user session information on the server side. Most programming platforms provide a native session management mechanism that works this way. However, user session information is often stored on the local file system by default and results in a stateful architecture. A common solution to this problem is to store this information in a database. Amazon DynamoDB is a great choice because of its scalability, high availability, and durability characteristics. For

many platforms, there are open source drop-in replacement libraries that allow you to store native sessions in Amazon DynamoDB.4
https://d1.awsstatic.com/whitepapers/AWS_Cloud_Best_Practices.pdf
(https://d1.awsstatic.com/whitepapers/AWS_Cloud_Best_Practices.pdf)
AWS best practices white paper - Page:8

Note:
In order to address scalability and to provide a shared data storage for sessions that can be accessible from any individual web server, you can abstract the HTTP sessions from the web servers themselves. A common solution to for this is to leverage an In-Memory Key/Value store such as Redis and Memcached.

In-memory caching improves application performance by storing frequently accessed data items in memory, so that they can be retrieved without access to the primary data store. Properly leveraging caching can result in an application that not only performs better, but also costs less at scale. Amazon ElastiCache is a managed service that reduces the administrative burden of deploying an in-memory cache in the cloud.

Please refer the following white paper for more information.

- https://d0.awsstatic.com/whitepapers/performance-at-scale-with-amazon-elasticache.pdf
(https://d0.awsstatic.com/whitepapers/performance-at-scale-with-amazon-elasticache.pdf)

Ask our Experts

QUESTION 11 MARKED AS REVIEW INCORRECT DEFINE PERFORMANT ARCHITECTURES

A company has setup an application in AWS that interacts with DynamoDB. It is required that when an item is

A company has setup an application in AWS that interacts with DynamoDB. It is required that when an item is modified in a DynamoDB table, an immediate entry is made to the associating application. How can this be accomplished? Choose 2 answers from the choices below.

- [x] **A.** Setup CloudWatch to monitor the DynamoDB table for changes. Then trigger a Lambda function to send the changes to the application. ✖
- [ ] **B.** Setup CloudWatch logs to monitor the DynamoDB table for changes. Then trigger AWS SQS to send the changes to the application.
- [ ] **C.** Use DynamoDB streams to monitor the changes to the DynamoDB table. ✔
- [x] **D.** Trigger a lambda function to make an associated entry in the application as soon as the DynamoDB streams are modified ✔

Explanation :

Answer – C and D

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

Let us try to analyze this with an example:

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

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

AWS Documentation mentions the following:

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

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

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

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

Note:
DynamoDB is integrated with Lambda so that you can create *triggers* to events in DynamoDB Streams.
If you enable DynamoDB Streams on a table, you can associate the stream ARN with a Lambda function that you write. Immediately after an item in the table is modified, a new record appears in the table's stream.

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

- For more information on DynamoDB streams Lambda, please refer to the URL below.
- https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Streams.Lambda.html (https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Streams.Lambda.html)

Ask our Experts

QUESTION 12 CORRECT DESIGN RESILIENT ARCHITECTURES

One of the leading entertainment channel is hosting an audition for popular reality show in India, for which they have published an advertisement to upload images of the participants with certain criteria on their website which is hosted in AWS infrastructure.

The requirement by the channel is that the participants with green card entry should be given a priority and results

for them will be released first. However, results for rest of the users will be released at their (channel's) convenience. Being a popular reality show, number of requests coming to website will increase before the deadline, therefore the solution needs to be scalable and cost effective.

Also, the failure of any layer should not affect the other layer in a multitier environment, in the AWS infrastructure. The technical management has given you few guidelines about the architecture, and they want Web components should allow participants to upload the images on S3 bucket. However, the second component will process these images and store it back to the S3 bucket, by making entries to the database storage.

As a solutions architect for the entertainment channel, how would you design a solution, while considering the priority for the participant is maintained and data is processed and stored as per the requirement.

- **A.** Use web component to get the images and store them on S3 bucket. Have the SQS service read these images with two SQS queues, green card entry queue and non-green card entry queue and EC2 instances with Auto Scaling group, will poll these queues and process these images based on priority requirement and store them to another S3 bucket, making an entry to Amazon RDS database.
- **B.** Use web component to get the images and store them on S3 bucket. Have the SQS service read these images with two SQS queues one green card entry queue and non-green card entry queue and EC2 instances with Auto Scaling group, will poll these queues and process these images based on priority requirement and store them to another S3 bucket, making an entry to Amazon RedShift database.
- **C.** Use web component to get the images and store them on S3 bucket. Have the SQS service read these images with two SQS queues both non-green card entry queues and the fleet of EC2 instances with Auto Scaling group, will poll these queues based on the flags of priority and process these images based on priority requirement and store them to another S3 bucket, making an entry to DynamoDB database.

- **D.** Use web component to get the images and store them on S3 bucket. Have the SQS service read these images with two

SQS queues one green card entry queue and non-green card entry queue and fleet of EC2 instances with Auto Scaling group, will poll these queues and process these images based on priority requirement and store them to another S3 bucket, making an entry to Amazon DynamoDB database. ✔

Explanation :

Answer: D

- A. Use web component to get the images and store them on S3 bucket. Have the SQS service read these images with two SQS queues, one priority and other standard queue and EC2 instances with Auto Scaling group, will poll these queues and process these images based on priority requirement and store them to another S3 bucket, making an entry to Amazon RDS database.

This option is incorrect. Though the solution provides a decoupling but the final metadata updates output cannot be inside Amazon RDS as it holds the transactional data. Also, the fleet of EC2 instances does not have Auto Scaling group, as the solution needs to be scalable as per the company requirement.

- B. Use web component to get the images and store them on S3 bucket. Have the SQS service read these images with two SQS queues one priority and other standard queue and EC2 instances with Auto Scaling group, will poll these queues and process these images based on priority requirement and store them to another S3 bucket, making an entry to Amazon RedShift database.

This option is incorrect. Though the solution provides the decoupling as well as web component and processing part looks good but the final metadata entries cannot be made to the Amazon RedShift which is a analytics databases works on OLAP.

- C. Use web component to get the images and store them on S3 bucket. Have the SQS service read these images with two SQS queues both standard queues and fleet of EC2 instances with Auto Scaling group, will poll these queues based on the flags of priority and process these images based on priority requirement and store them to another S3 bucket, making an entry to DynamoDB database.

This option is incorrect. The solution works well with web component, however the SQS queues used are standard queue, though these standard queues has ability to process the data separately based on green card entry and normal participants but it does not ensure priority, as both queues will be read simultaneously, hence this will not serve the needed requirement. However, storing metadata to DynamoDB table will work fine.

- D. Use web component to get the images and store them on S3 bucket. Have the SQS service read these images with two SQS queues one priority and other standard queue and fleet of EC2 instances with Auto Scaling group, will poll these queues and process these images based on priority requirement and store them to another S3 bucket, making an entry to Amazon DynamoDB database.

This option is CORRECT. As it suits all the requirements mentioned to make the solution decoupled, means even if one web component

fails the database component will always be up and processing these images by reading it from SQS queues based on the priority queue for its green card participants and standard queue for the general participants and fleet of EC2 instances with AUTO scaling will be able to take up the load during peak time. And data will be stored in another S3 bucket making an entry to Amazon DynamoDB table.

Ask our Experts

QUESTION 13 CORRECT DEFINE PERFORMANT ARCHITECTURES

An application currently uses AWS RDS MySQL as its data layer. Due to recent performance issues on the database, it has been decided to separate the querying part of the application by setting up a separate reporting layer. Which of the following additional steps could also potentially assist in improving the performance of the underlying database?

- A. Make use of Multi-AZ to setup a secondary database in another Availability Zone.
- B. Make use of Multi-AZ to setup a secondary database in another region.
- C. Make use of Read Replicas to setup a secondary read-only database. ✔
- D. Make use of Read Replicas to setup a secondary read and write database.

Explanation :

Answer - C
AWS Documentation mentions the following:

Amazon RDS Read Replicas provide enhanced performance and durability for database (DB) instances. This 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 Amazon Read Replicas, please refer to the URL below.

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

Ask our Experts

QUESTION 14 CORRECT DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

As a Solutions Architect for a multinational organization having more than 150000 employees, management has decided to implement a real time analysis for their employees time spent in offices across the globe. You are tasked to design a architecture which will receive the inputs from 10000+ sensors with swipe machine sending in and out data from across the globe, each sending 20KB data every 5 Seconds in JSON format. The application will process and analyze the data and upload the results to dashboards in real time.

Other application requirements will have, ability to apply real time analytics on the captured data, processing of captured data will be parallel and durable, the application must be scalable as per the requirement as the load varies and new sensors are added or removed at various facilities. The analytic processing results are stored in a persistent data storage for data mining.

What combination of AWS services would be used for the above scenario?

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

- **B.** Use Amazon Kinesis Streams to ingest the Swipe data coming from sensors, Custom Kinesis Streams Applications will analyse the data, move analytics outcomes to RedShift using AWS EMR ✔
- **C.** Utilize SQS to receive the data coming from sensors, use Kinesis Firehose to analyse the data from SQS, then save the results to a Multi-AZ RDS instance
- **D.** Use Amazon Kinesis Streams to ingest the sensors' data, custom Kinesis Streams applications will analyse the data, move analytics outcomes to RDS using AWS EMR

Explanation :

Answer: Option B

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

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

- B. Use Amazon Kinesis Streams to ingest the Swipe data coming from sensors, Custom Kinesis Streams Applications will analyse the data, move analytics outcomes to RedShift using AWS EMR

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

- C. Utilize SQS to receive the data coming from sensors, use Kinesis Firehose to analyse the data from SQS, then save the results to a Multi-AZ RDS instance

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

- D. Use Amazon Kinesis Streams to ingest the sensors' data, custom Kinesis Streams applications will analyse the data, move analytics outcomes to RDS using AWS EMR

This option is incorrect, as the AWS EMR can read large amounts of data, however RDS is a transactional database works based on the OLTP,

thus it cannot store the analytical data.

Ask our Experts

QUESTION 15 CORRECT SPECIFY SECURE APPLICATIONS AND ARCHITECTURES

An application running on EC2 Instances processes sensitive information stored on Amazon S3. This information is accessed over the Internet. The security team is concerned that the Internet connectivity to Amazon S3 could be a security risk. Which solution will resolve the security concern?

- A. Access the data through an Internet Gateway.
- B. Access the data through a VPN connection.
- C. Access the data through a NAT Gateway.
- D. Access the data through a VPC endpoint for Amazon S3. ✔

Explanation :

Answer – D
AWS Documentation mentions the following:
A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network.
For more information on VPC endpoints, please refer to the URL below.
https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-endpoints.html

(https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-endpoints.html)

Option A is incorrect. An Internet Gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the Internet.
Option B is incorrect. A VPN, or Virtual Private Network, allows you to create a secure connection to another network over the Internet.
Option C is incorrect. You can use a network address translation (NAT) gateway to enable instances in a private subnet to connect to the Internet or other AWS services, but prevent the internet from initiating a connection with those instances.

Ask our Experts

QUESTION 16 CORRECT SPECIFY SECURE APPLICATIONS AND ARCHITECTURES

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

- **A.** They are the same and just called different things
- **B.** First you sign-in via Cognito then through a federated site, like Google
- **C.** Federated identity providers and identity pools are used to authorize services

D. Sign-in via Cognito user pools and sign-in via federated identity providers are independent of one another ✔

Explanation :

Answer:D

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

Incorrect:

- A. These are separate, independent authentication methods
- B. Only one log-in event is needed, not two
- C. Identity providers authenticate users, not authorize services

Reference:

- https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-user-pools-identity-federation.html (https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-user-pools-identity-federation.html)
- https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_oidc.html (https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_oidc.html)
- https://aws.amazon.com/articles/web-identity-federation-with-mobile-applications/ (https://aws.amazon.com/articles/web-identity-federation-with-mobile-applications/)
- https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-getting-started.html (https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-getting-started.html)

Ask our Experts

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

- A. Add more EC2 Instances to support the load. ✖
- B. Change the Instance type to a higher instance type.
- C. Add Route 53 health checks to improve the performance.
- D. Place the EC2 Instance behind CloudFront. ✔

Explanation :

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

Option A is incorrect. The latency issue is experienced by people from certain parts of the world only. So, increasing the number of EC2 Instances or increasing the instance size does not make much of a difference.
Option C is incorrect. Route 53 health checks are meant to see whether the instance status is healthy or not.

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

CloudFront is a good solution.

Ask our Experts

QUESTION 18 MARKED AS REVIEW INCORRECT DESIGN RESILIENT ARCHITECTURES

Currently, you have a NAT Gateway defined for your private instances. You need to make the NAT Gateway highly available. How can this be accomplished?

- A. Create another NAT Gateway and place is behind an ELB.
- B. Create a NAT Gateway in another Availability Zone. ✔
- C. Create a NAT Gateway in another region.
- D. Use Auto Scaling groups to scale the NAT Gateway. ✖

Explanation :

Answer - B

AWS Documentation mentions the following:

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

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

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

Ask our Experts

QUESTION 19 CORRECT DESIGN RESILIENT ARCHITECTURES

A company wants to have a fully managed data store in AWS. It should be a compatible MySQL database, which is an application requirement. Which of the following databases engines can be used for this purpose?

- A. AWS RDS
- B. AWS Aurora ✔
- C. AWS DynamoDB
- D. AWS Redshift

Explanation :

Answer - B

AWS Documentation mentions the following:

Amazon Aurora (Aurora) is a fully managed, MySQL- and PostgreSQL-compatible, relational database engine. It combines the speed and

reliability of high-end commercial databases with the simplicity and cost-effectiveness of open-source databases. It delivers up to five times the throughput of MySQL and up to three times the throughput of PostgreSQL without requiring changes to most of your existing applications.
For more information on AWS Aurora, please refer to the URL below.

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

Note:
RDS is a generic service to provide Relational Database service which supports 6 database engines. They are Aurora, MySQL, MariaDB, PostgreSQL, Oracle and Microsoft SQL server. Our question is to select MySQL compatible database from the options provided. Out of the options listed **Amazon Aurora** is a MySQL- and PostgreSQL-compatible enterprise-class database.

Hence Option B is the answer.

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

Ask our Experts

QUESTION 20 CORRECT DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

A Solutions Architect is designing an online shopping application running in a VPC on EC2 Instances behind an ELB Application Load Balancer. The instances run in an Auto Scaling group across multiple Availability Zones. The application tier must read and write data to a customer managed database cluster. There should be no access to

the database from the Internet, but the cluster must be able to obtain software patches from the Internet. Which

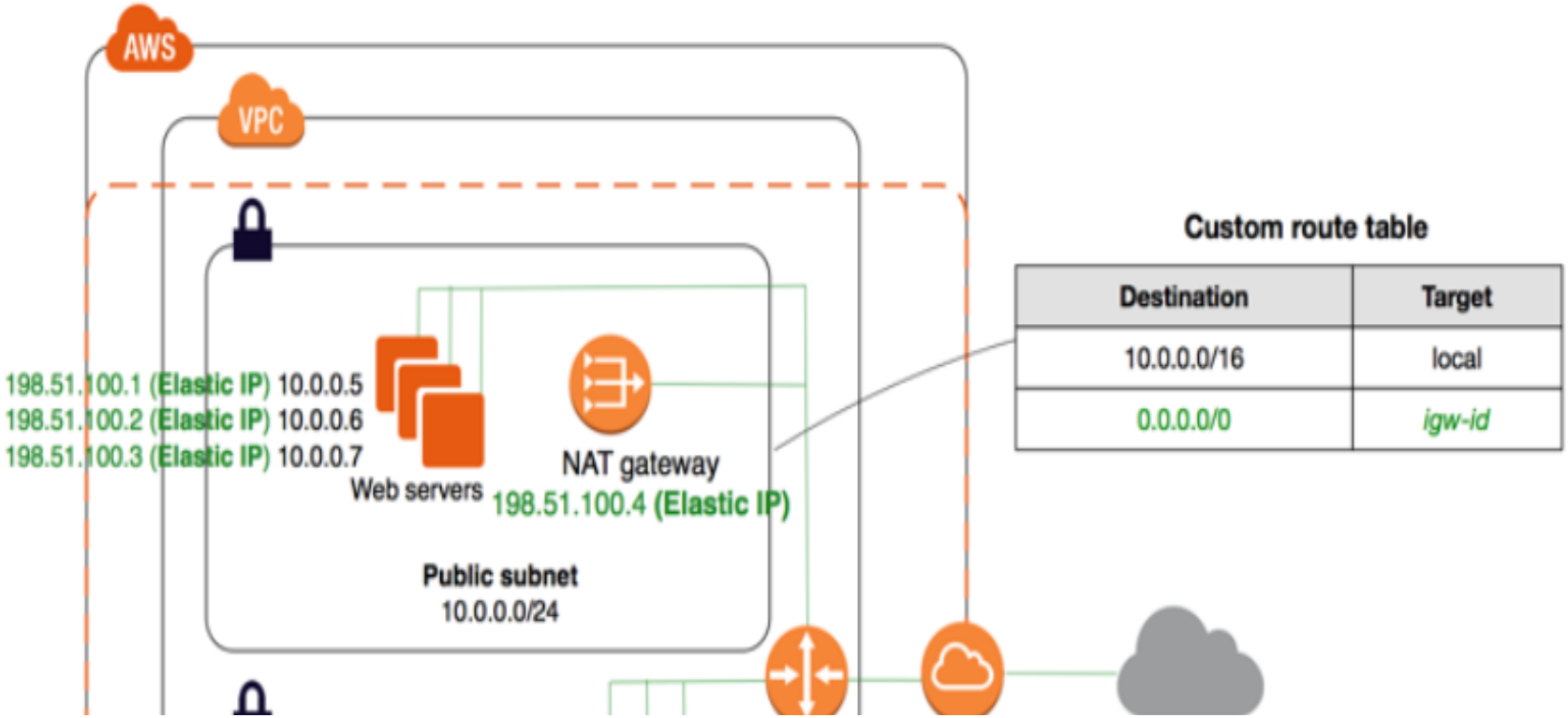
VPC design meets these requirements?

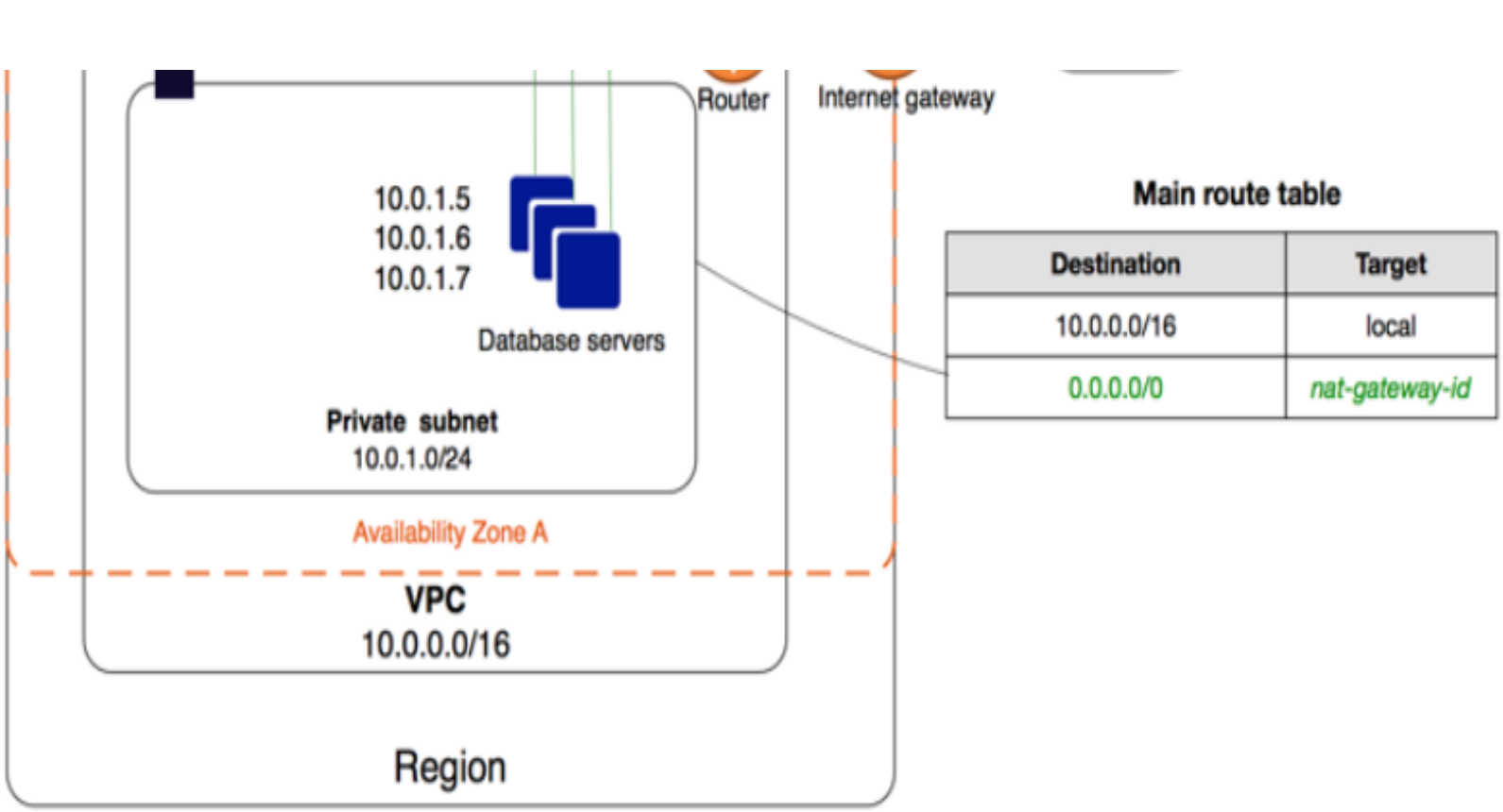
- A. Public subnets for both the application tier and the database cluster
- B. Public subnets for the application tier, and private subnets for the database cluster
- C. Public subnets for the application tier and NAT Gateway, and private subnets for the database cluster ✔
- D. Public subnets for the application tier, and private subnets for the database cluster and NAT Gateway

Explanation :

Answer – C

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





We always need to keep Nat gateway on public Subnet only, because it needs to communicate internet.

Aws says that "To create a NAT gateway, you must specify the public subnet in which the NAT gateway should reside. You must also specify an Elastic IP address (https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-eips.html) to associate with the NAT gateway when you create it. After you've created a NAT gateway, you must update the route table associated with one or more of your private subnets to point Internet-bound traffic to the NAT gateway. This enables instances in your private subnets to communicate with the internet."

- For more information on this setup, please refer to the below URL:
  - https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-nat-gateway.html (https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-nat-gateway.html)

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

patches from the Internet."

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

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

So Option C having these discussed Points and it's a perfect answer.

Ask our Experts

QUESTION 21 MARKED AS REVIEW INCORRECT DEFINE PERFORMANT ARCHITECTURES

It is expected that S3 handles the load when users upload images to it. As an architect what is your suggestion to alleviate this condition?

- **A.** Create a secondary S3 bucket. Then, use an AWS Lambda to sync the contents to the primary bucket.
- **B.** Use Pre-Signed URLs instead to upload the images. ✔
- **C.** Use ECS Containers to upload the images.
- **D.** Upload the images to SQS and then push them to the S3 bucket. ✖

Explanation :

Explanation:

Answer – B

The S3 bucket owner can create Pre-Signed URLs to upload the images to S3.
For more information on Pre-Signed URLs, please refer to the URL below.
https://docs.aws.amazon.com/AmazonS3/latest/dev/PresignedUrlUploadObject.html
(https://docs.aws.amazon.com/AmazonS3/latest/dev/PresignedUrlUploadObject.html)

- Option A is not the correct for this question. Since Amazon has provided us with an inbuilt function for this requirement, using this option is cost expensive and time-consuming. As a Solution Architect, you are supposed to pick the best and cost-effective solution.
- Option C is incorrect. ECS is a highly scalable, fast, container management service that makes it easy to run, stop, and manage Docker containers on a cluster.
- Option D is incorrect. SQS is a message queue service used by distributed applications to exchange messages through a polling model and not through a push mechanism.

Note:

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

You need to understand about pre-signed url - which contains the user login credentials particular resources, such as S3 in this scenario. And user must have permission enabled that other application can use the credential to upload the data (images) in S3 buckets.

AWS definition:

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

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

- Please check the below link to know more about it.
  - https://docs.aws.amazon.com/AmazonS3/latest/dev/PresignedUrlUploadObject.html

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

Hence, option B will solve the concern mentioned in the question.

Ask our Experts

QUESTION 22 CORRECT DEFINE PERFORMANT ARCHITECTURES

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

- A. General Purpose SSD
- B. Provisioned IOPS SSD ✔
- C. Throughput Optimized HDD
- D. Cold HDD

Explanation :

Answer - B

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

	Solid-State Drives (SSD)	Hard disk Drives (HDD)

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

For more information on EBS Volume types, please refer to the URL below.
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html
(https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html)

Ask our Experts

QUESTION 23 CORRECT DEFINE PERFORMANT ARCHITECTURES

You have a set of on-premises virtual machines used to serve a web-based application. You need to ensure that a virtual machine if unhealthy is taken out of the rotation. which of the following option can be used for health checking and DNS failover features for a web application running behind ELB, to increase redundancy and availability.

- A. Use Route 53 health checks to monitor the endpoints. ✔
- B. Move the solution to AWS and use a Classic Load Balancer.
- C. Move the solution to AWS and use an Application Load Balancer.
- D. Move the solution to AWS and use a Network Load Balancer.

Explanation :

Answer - A

Route 53 health checks can be used for any endpoint that can be accessed via the Internet. Hence, this would be an ideal option for monitoring endpoints.

AWS Documentation mentions the following:

You can configure a health check that monitors an endpoint that you specify either by IP address or by the domain name. At regular intervals

that you specify, Route 53 submits automated requests over the internet to your application, server, or other resources to verify that it's reachable, available and functional.

- For more information on Route 53 Health checks, please refer to the URL below.
  - https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-simple-configs.html (https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-simple-configs.html)

Note:

As per AWS,
Once enabled, Route 53 automatically configures and manages health checks for individual ELB nodes. Route 53 also takes advantage of the EC2 instance health checking that ELB performs. By combining the results of health checks of your EC2 instances and your ELBs, Route 53 DNS Failover is able to evaluate the health of the load balancer and the health of the application running on the EC2 instances behind it. In other words, if any part of the stack goes down, Route 53 detects the failure and routes traffic away from the failed endpoint.

- For more information, please visit:
  - https://aws.amazon.com/blogs/aws/amazon-route-53-elb-integration-dns-failover/ (https://aws.amazon.com/blogs/aws/amazon-route-53-elb-integration-dns-failover/)

AWS documentation states, that you can create a Route 53 resource record that points to an address outside AWS, you can set up health checks for parts of your application running outside AWS, and you can fail over to any endpoint that you choose, regardless of location.

For example, you may have a legacy application running in a datacenter outside AWS and a backup instance of that application running within AWS. You can set up health checks of your legacy application running outside AWS, and if the application fails the health checks, you can fail over automatically to the backup instance in AWS.

- Please refer:
  - https://aws.amazon.com/route53/faqs/ (https://aws.amazon.com/route53/faqs/)

Note:

As per AWS,

Route 53 has health checkers in locations around the world. When you create a health check that monitors an endpoint, health checkers start to send requests to the endpoint that you specify to determine whether the endpoint is healthy. You can choose which locations you want Route 53 to use, and you can specify the interval between checks: every 10 seconds or every 30 seconds. Note that Route 53 health checkers in different data centers don't coordinate with one another, so you'll sometimes see several requests per second regardless of the interval you chose, followed by a few seconds with no health checks at all.
Each health checker evaluates the health of the endpoint based on two values:

- Response time
- Whether the endpoint responds to a number of consecutive health checks that you specify (the failure threshold)

Route 53 aggregates the data from the health checkers and determines whether the endpoint is healthy:

- If more than 18% of health checkers report that an endpoint is healthy, Route 53 considers it healthy.
- If 18% of health checkers or fewer report that an endpoint is healthy, Route 53 considers it unhealthy.

The response time that an individual health checker uses to determine whether an endpoint is healthy depends on the type of health check: HTTP and HTTPS health checks, TCP health checks or HTTP and HTTPS health checks with string matching.

Regarding your specific query where we are having more than 2 servers for the website, AWS docs states that:

When you have more than one resource performing the same function—for example, more than one HTTP server or mail server—you can configure Amazon Route 53 to check the health of your resources and respond to DNS queries using only the healthy resources. For example, suppose your website, example.com, is hosted on six servers, two each in three data centers around the world. You can configure Route 53 to check the health of those servers and to respond to DNS queries for example.com using only the servers that are currently healthy. The configuration details are provided in the second link.

Please refer the following links for more information.

- https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-determining-health-of-endpoints.html (https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-determining-health-of-endpoints.html)
- https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-configuring.html (https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-configuring.html)

Ask our Experts

QUESTION 24 CORRECT SPECIFY SECURE APPLICATIONS AND ARCHITECTURES

A company has a set of web servers. It is required to ensure that all the logs from these web servers can be analyzed in real time for any sort of threat detection. Which of the following would assist in this regard?

- A. Upload all the logs to the SQS Service and then use EC2 Instances to scan the logs.
- B. Upload the logs to Amazon Kinesis and then analyze the logs accordingly. ✔
- C. Upload the logs to CloudTrail and then analyze the logs accordingly.
- D. Upload the logs to Glacier and then analyze the logs accordingly.

Explanation :

Answer – B
AWS Documentation provides the following information to support this requirement:
Amazon Kinesis makes it easy to collect, process, and analyze real-time, streaming data so you can get timely insights and react quickly to new information. Amazon Kinesis offers key capabilities to cost-effectively process streaming data at any scale, along with the flexibility to choose the tools that best suit the requirements of your application. With Amazon Kinesis, you can ingest real-time data such as video, audio, application logs, website clickstreams, and IoT telemetry data for machine learning, analytics, and other applications.
For more information on Amazon Kinesis, please refer to the below URL:
https://aws.amazon.com/kinesis/ (https://aws.amazon.com/kinesis/)

Ask our Experts

QUESTION 25 CORRECT DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

You currently have the following architecture in AWS:

a. A couple of EC2 Instances located in us-west-2a

b. The EC2 Instances are launched via an Auto Scaling group.

c. The EC2 Instances sit behind a Classic ELB.

Which of the following additional steps should be taken to ensure the above architecture conforms to a well-architected framework?

- **A.** Convert the Classic ELB to an Application ELB.
- **B.** Add an additional Auto Scaling Group.

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

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

Explanation :

Answer - D

AWS Documentation provides the following information to support this concept:

Balancing resources across Availability Zones (http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html) is a best practice for well-architected (https://aws.amazon.com/blogs/aws/are-you-well-architected/) applications, as this greatly increases aggregate system availability. Auto Scaling automatically balances EC2 instances across zones when you configure multiple zones (http://docs.aws.amazon.com/autoscaling/latest/userguide/as-add-availability-zone.html) in your Auto Scaling group settings. Auto Scaling always launches new instances such that they are balanced between zones as evenly as possible across the entire fleet.

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

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

Ask our Experts

QUESTION 26 CORRECT DESIGN RESILIENT ARCHITECTURES

Your company manages an application that currently allows users to upload images to an S3 bucket. These images

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

- A. AWS Redshift
- B. AWS Glacier
- C. AWS DynamoDB ✔
- D. AWS SQS

Explanation :

Answer - C
Option A is incorrect because this is normally used for petabyte based storage.
Option B is incorrect because this is used for archive storage.
Option D is incorrect because this used for messaging purposes.
AWS DynamoDB is the best, light-weight and durable storage option for metadata.
For more information on DynamoDB, please refer to the URL below.
https://aws.amazon.com/dynamodb/ (https://aws.amazon.com/dynamodb/)

Ask our Experts

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

- A. Create Spot Instances and install the Web and database components.
- B. Create Reserved Instances and install the Web and database components. ✖
- C. Use AWS Lambda to create the web components and AWS RDS for the database layer.
- D. Use Elastic Beanstalk to quickly provision the environment. ✔

Explanation :

Answer – D

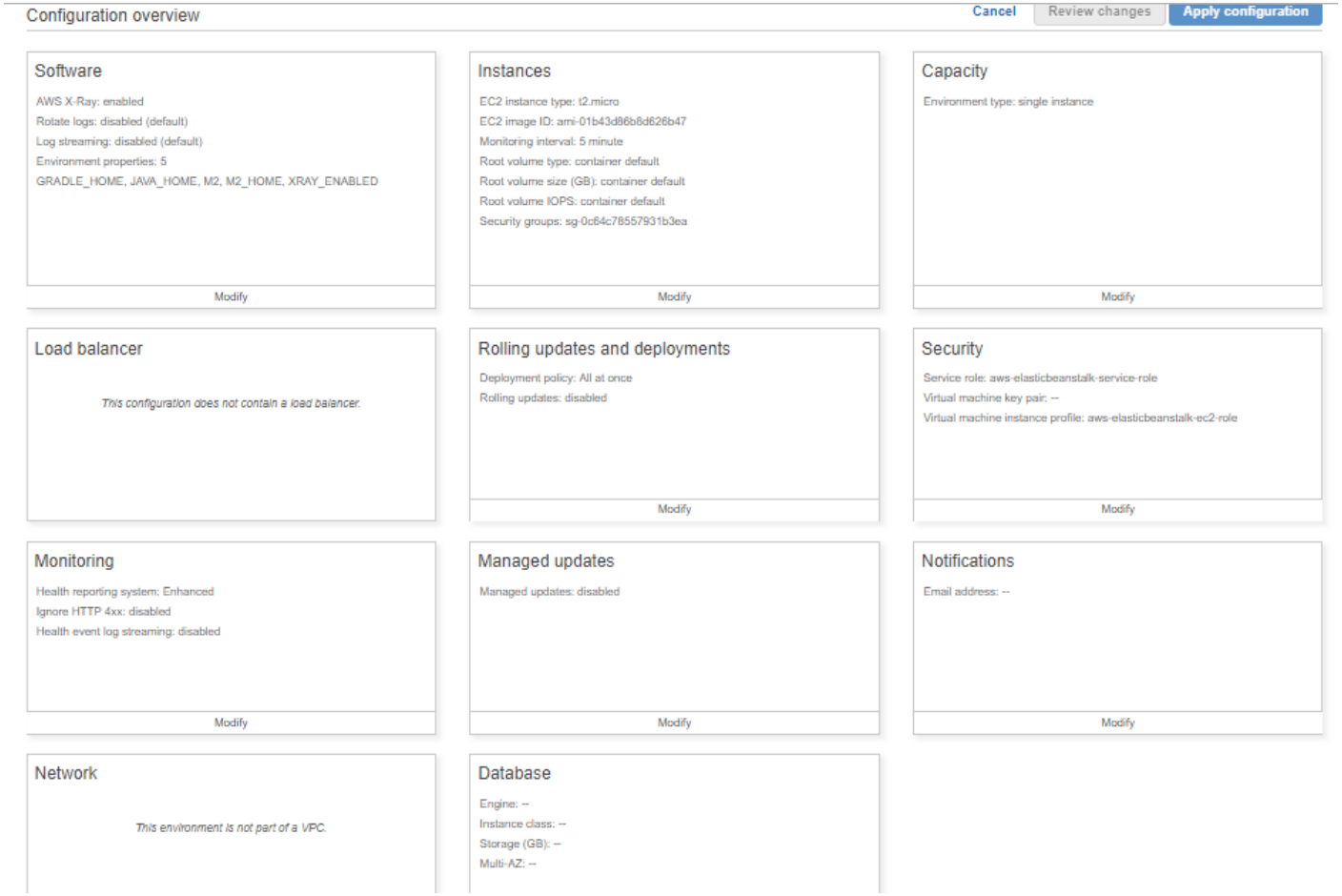
AWS Documentation mentions the following:

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

- For more information on AWS Elastic Beanstalk, please refer to the URL below.
- https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/Welcome.html (https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/Welcome.html)

- Option A is incorrect. Amazon EC2 Spot instances are spare compute capacity in the AWS cloud available to you at steep discounts compared to On-Demand prices.
- Option B is incorrect. A Reserved Instance is a reservation of resources and capacity, for either one or three years, for a particular Availability Zone within a region.
- Option C is incorrect. AWS Lambda is a compute service that makes it easy for you to build applications that respond quickly to new information and not for provisioning a new environment.

Currently, Elastic Beanstalk environment supports the following configurations:



It does support RDS.

Database configuration Setting

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

Ask our Experts

QUESTION 28 MARKED AS REVIEW INCORRECT SPECIFY SECURE APPLICATIONS AND ARCHITECTURES

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

- **A.** IAM policies for resources were changed, thereby restricting access to AWS resources ✔
- **B.** Federation protocols are used to authorize services and needs to be updated ✖
- **C.** AWS changed the services allowed to be accessed via federated login
- **D.** The identity providers no longer allow access to AWS services

Explanation :

Answer: A

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

Incorrect:

- B. Federation is used to authenticate users, not to authorize services
- C. Federation allows for authenticating users, but does not authorize services
- D. The identity providers don't have the capability to authorize services; they authenticate users

Reference:

- https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-user-pools-identity-federation.html (https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-user-pools-identity-federation.html)
- https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_oidc.html (https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_oidc.html)
- https://aws.amazon.com/articles/web-identity-federation-with-mobile-applications/ (https://aws.amazon.com/articles/web-identity-federation-with-mobile-applications/)

Ask our Experts

QUESTION 29 CORRECT DESIGN COST-OPTIMIZED ARCHITECTURES

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

- A. Amazon Glacier with Expedited Retrievals.
- B. Amazon S3 Standard Infrequent Access ✔
- C. Amazon EFS
- D. Amazon S3 Standard

Explanation :

Answer – B

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

- For more information on AWS Storage Classes, please visit the following URL:
  - https://aws.amazon.com/s3/storage-classes/ (https://aws.amazon.com/s3/storage-classes/)

Ask our Experts

QUESTION 30 MARKED AS REVIEW INCORRECT SPECIFY SECURE APPLICATIONS AND ARCHITECTURES

You have an EC2 Instance placed inside a subnet. You have created the VPC from scratch, and added the EC2 Instance to the subnet. It is required to ensure that this EC2 Instance has complete access to the Internet, since it will be used by users on the Internet.

Which of the following options would help accomplish this?

- A. Launch a NAT Gateway and add routes for 0.0.0.0/0 ✖
- B. Attach a VPC Endpoint and add routes for 0.0.0.0/0
- C. Attach an Internet Gateway and add routes for 0.0.0.0/0 ✔
- D. Deploy NAT Instances in a public subnet and add routes for 0.0.0.0/0

Explanation :

Answer – C

AWS Documentation mentions the following:

An Internet Gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the Internet. It therefore imposes no availability risks or bandwidth constraints on your network traffic.
For more information on the Internet Gateway, please visit the following URL:
https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Internet_Gateway.html
(https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Internet_Gateway.html)

Ask our Experts

QUESTION 31 CORRECT DEFINE PERFORMANT ARCHITECTURES

You have an application hosted on AWS consisting of EC2 Instances launched via an Auto Scaling Group. You notice that the EC2 Instances are not scaling out on demand. What checks can be done to ensure that the scaling occurs as expected?

- **A.** Ensure that the right metrics are being used to trigger the scale out. ✔
- **B.** Ensure that ELB health checks are being used.
- **C.** Ensure that the instances are placed across multiple Availability Zones.
- **D.** Ensure that the instances are placed across multiple regions.

Explanation :

Answer – A

If your scaling events are not based on the right metrics and do not have the right threshold defined, then the scaling will not occur as you

want it to happen.

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

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

Ask our Experts

QUESTION 32 CORRECT SPECIFY SECURE APPLICATIONS AND ARCHITECTURES

A company hosts a popular web application that connects to an Amazon RDS MySQL DB instance running in a private VPC subnet created with default ACL settings. The web servers must be accessible only to customers on an SSL connection and the database should only be accessible to web servers in a public subnet. As an architect, which of the following would you not recommend for such an architecture?

- **A.** Create a separate web server and database server security group.
- **B.** Ensure the web server security group allows HTTPS port 443 inbound traffic from anywhere (0.0.0.0/0) and apply it to the web servers.
- **C.** Ensure the web server security group allows MySQL port 3306 inbound traffic from anywhere (0.0.0.0/0) and apply it to the web servers. ✔
- **D.** Ensure the DB server security group allows MySQL port 3306 inbound and specify thesource as the web server security group.

Explanation :

Answer – C

The question is describing a scenario where it has been instructed that the database servers should only be accessible to web servers in the public subnet.

You have been asked which one of the following is not a recommended architecture based on the scenario.

The answer is option C. "Ensure the web server security group allows MySQL port 3306 inbound traffic from anywhere (0.0.0.0/0) and apply it to the web servers."

Here in this Option C, we are allowing all the incoming traffic from the internet to the database port which is not acceptable as per the architecture.?
A similar setup is given in AWS Documentation:
1) To ensure that traffic can flow into your web server from anywhere on secure traffic, you need to allow inbound security at 443.
2) You need to then ensure that traffic can flow from the database server to the web server via the database security group.
The below snapshot from AWS Documentation shows the rules tables for the security groups which relate to the same requirements as the question.

WebServerSG: Recommended Rules

Inbound			
Source	**Protocol**	**Port Range**	**Comments**
0.0.0.0/0	TCP	80	Allow inbound HTTP access to the web servers from any IPv4 address.
0.0.0.0/0	TCP	443	Allow inbound HTTPS access to the web servers from any IPv4 address.

DBServerSG: Recommended Rules

Inbound			
Source	**Protocol**	**Port Range**	**Comments**
The ID of your WebServerSG security group	TCP	1433	Allow inbound Microsoft SQL Server access from the web servers associated with the WebServerSG security group.
The ID of your WebServerSG security group	TCP	3306	Allow inbound MySQL Server access from the web servers associated with the WebServerSG security group.

For more information on this use case scenario, please visit the following URL:

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

The requirement in the question states that the database servers should only be accessible to web servers in the public subnet.
The answer option C - "Ensure the web server security group allows MySQL port 3306 inbound traffic from anywhere (0.0.0.0/0) and apply it to the web servers." is not a recommended architecture for the above scenario. Here, we allow all the incoming traffic from the Internet to the database port which is not acceptable as per the architecture.
The question asks that database should only be accessible to the webservers in the public subnet.

Now in option D database server's sec grp allows inbound at port 3306 and source of the traffic as Webserver sec grp that means request traffic from webserver is allowed to the DB server Since security groups are stateful , response will also be allowed from DB to the webserver. Thus allowing the communication between them So the option D is right.
But wrong in terms of this question as you have to choose an incorrect/wrong option.
Note:
The question asks you to find out which of the following is **not recommend** i.e. incorrect and the option C is not correct because of the incorrect inbound rule. Hence it is the answer.

Ask our Experts

QUESTION 33 CORRECT SPECIFY SECURE APPLICATIONS AND ARCHITECTURES

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

- A. Multi-factor authentication must be used to access DynamoDB
- B. AWS CloudTrail needs to be enabled to audit usage
- C. An IAM role allowing the app to have access to DynamoDB ✔
- D. The user must additionally log into the AWS console to gain database access

Explanation :

Answer: C

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

Incorrect:

- A. Multi-factor authentication is available, but not required
- B. CloudTrail is recommended for auditing but is not required
- D. A second log-in event to the management console is not required

Reference:

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

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

- ttps://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_oidc.html (https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_oidc.html)
- https://aws.amazon.com/articles/web-identity-federation-with-mobile-applications/ (https://aws.amazon.com/articles/web-identity-federation-with-mobile-applications/)

Ask our Experts

QUESTION 34 CORRECT DESIGN RESILIENT ARCHITECTURES

A company has an entire infrastructure hosted on AWS. It wants to create code templates used to provision the same set of resources in another region in case of a disaster in the primary region. Which of the following services can help in this regard?

- A. AWS Beanstalk
- B. AWS CloudFormation ✔
- C. AWS CodeBuild
- D. AWS CodeDeploy

Explanation :

Answer – B

AWS Documentation provides the following information to support this requirement:

AWS CloudFormation provisions your resources in a safe, repeatable manner, allowing you to build and rebuild your infrastructure and

applications, without having to perform manual actions or write custom scripts. CloudFormation takes care of determining the right operations to perform when managing your stack, and rolls back changes automatically if errors are detected.
For more information on AWS CloudFormation, please visit the following URL:
https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/Welcome.html
(https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/Welcome.html)

Ask our Experts

QUESTION 35 MARKED AS REVIEW INCORRECT DESIGN COST-OPTIMIZED ARCHITECTURES

A company has a set of EBS Volumes that need to be catered in case of a disaster. How will you achieve this using existing AWS services effectively?

- **A.** Create a script to copy the EBS Volume to another Availability Zone.
- **B.** Create a script to copy the EBS Volume to another region.
- **C.** Use EBS Snapshots to create the volumes in another region. ✔
- **D.** Use EBS Snapshots to create the volumes in another Availability Zone. ✖

Explanation :

Answer - C

- Options A and B are incorrect because you can't directly copy EBS Volumes.

- Option D is incorrect because disaster recovery always looks at ensuring resources are created in another region.

- AWS Documentation provides the following information to support this requirement:

A snapshot is constrained to the region where it was created. After you create a snapshot of an EBS volume, you can use it to create new volumes in the same region. For more information, see Restoring an Amazon EBS Volume from a Snapshot (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-restoring-volume.html). You can also copy snapshots across regions, making it possible to use multiple regions for geographical expansion, data center migration, and disaster recovery.

- For more information on EBS Snapshots, please visit the following URL:
  - https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html)

NOTE:
It's not possible to provide each and every step in the Options and moreover in AWS exam also you will see these kinds of Options. Option C is not talking about the whole procedure. it's simply giving the idea that we can use snapshots to create the volumes in the other region. That's the reason we also provided the explanation part to understand the concept.

Question: A company has a set of EBS Volumes that need to be catered to in case of a disaster. How can one achieve this in an efficient manner using the existing AWS services?

- **Here catered means - provisioning**

Ask our Experts

QUESTION 36 CORRECT SPECIFY SECURE APPLICATIONS AND ARCHITECTURES

Your recent security review revealed a large spike in attempted logins to your AWS account. With respect to

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

- A. Only KMS generated keys can be used to encrypt or decrypt data
- B. Data is encrypted at rest ✔
- C. KMS allows all users and roles use of the keys by default
- D. Data is decrypted in transit

Explanation :

Answer: B

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

Incorrect:

- A. Data can be encrypted/decrypted using AWS keys or keys provided by your company
- C. Users are granted permissions explicitly, not by default by KMS
- D. Data is not decrypted in transit (while moving to and from S3). Data is encrypted or decrypted while in S3 and then while in transit can be encrypted using SSL.

Reference:

- https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html (https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html)
- ttps://d1.awsstatic.com/whitepapers/AWS_Securing_Data_at_Rest_with_Encryption.pdf (https://d1.awsstatic.com/whitepapers/AWS_Securing_Data_at_Rest_with_Encryption.pdf)
- https://aws.amazon.com/kms/faqs/ (https://aws.amazon.com/kms/faqs/)
- https://docs.aws.amazon.com/general/latest/gr/rande.html#kms_region

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

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

Ask our Experts

QUESTION 37 CORRECT DESIGN RESILIENT ARCHITECTURES

Your company has a set of EC2 Instances hosted in AWS. There is a mandate to prepare for disasters and come up with the necessary disaster recovery procedures. Which of the following would help in mitigating the effects of a disaster for the EC2 Instances?

- A. Place an ELB in front of the EC2 Instances.
- B. Use Auto Scaling to ensure the minimum number of instances are always running.
- C. Use CloudFront in front of the EC2 Instances.
- D. Use AMIs to recreate the EC2 Instances in another region. ✔

Explanation :

Answer – D

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

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

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

the EC2 instance.
For disaster recovery, we have to make sure that we can launch instances in another region when required. Hence, options A,B and C are not feasible solutions.
For more information on AWS AMIs, please visit the following URL:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html
(https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html)

Ask our Experts

QUESTION 38 MARKED AS REVIEW INCORRECT SPECIFY SECURE APPLICATIONS AND ARCHITECTURES

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

- **A.** Enable Amazon Redshift Enhanced VPC Routing. ✔
- **B.** Create a NAT Gateway to route the traffic.
- **C.** Create a NAT Instance to route the traffic.

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

Explanation :

Answer-A
AWS Documentation mentions the following:
When you use Amazon Redshift Enhanced VPC Routing, Amazon Redshift forces all COPY (http://docs.aws.amazon.com/redshift/latest/dg/r_COPY.html) and UNLOAD (http://docs.aws.amazon.com/redshift/latest/dg/r_UNLOAD.html) traffic between your cluster and your data repositories through your Amazon VPC.
If Enhanced VPC Routing is not enabled, Amazon Redshift routes traffic through the Internet, including traffic to other services within the AWS network.
For more information on Redshift Enhanced Routing, please visit the following URL:
https://docs.aws.amazon.com/redshift/latest/mgmt/enhanced-vpc-routing.html (https://docs.aws.amazon.com/redshift/latest/mgmt/enhanced-vpc-routing.html)

Ask our Experts

QUESTION 39 CORRECT DESIGN RESILIENT ARCHITECTURES

A company has a set of Hyper-V machines and VMware virtual machines. They are now planning on migrating

A company has a set of Hyper-V machines and VMware virtual machines. They are now planning on migrating these instances to the AWS Cloud. Which of the following can be used to move these resources to the AWS Cloud?

- A. DB Migration utility
- B. AWS Server Migration Service ✔
- C. Use AWS Migration Tools.
- D. Use AWS Config Tools.

Explanation :

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

Ask our Experts

QUESTION 40 CORRECT SPECIFY SECURE APPLICATIONS AND ARCHITECTURES

You've implemented AWS Key Management Service to protect your data in your applications and other AWS

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

- A. KMS is only offered in North America
- B. AWS CloudTrail has not been enabled to log events
- C. KMS master keys are region-specific and the applications are hitting the wrong api endpoints ✔
- D. The master keys have been disabled

Explanation :

Answer: C

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

Incorrect:

- A. KMS is offered in several regions, but keys are not transferrable out of the region they were created in
- B. CloudTrail is recommended for auditing but is not required
- D. The keys are working as expected where they were created; keys are region specific

Reference:

- https://aws.amazon.com/kms/faqs/ (https://aws.amazon.com/kms/faqs/)
- ttps://docs.aws.amazon.com/general/latest/gr/rande.html#kms_region (https://docs.aws.amazon.com/general/latest/gr/rande.html#kms_region)
- https://www.slideshare.net/AmazonWebServices/encryption-and-key-management-in-aws (https://www.slideshare.net/AmazonWebServices/encryption-and-key-management-in-aws)

Ask our Experts

QUESTION 41 CORRECT DESIGN COST-OPTIMIZED ARCHITECTURES

A company with a set of Admin jobs(.NET core) currently setup in the C# programming language, is moving their infrastructure to AWS. Which of the following would be an efficient means of hosting the Admin related jobs in AWS?

- A. Use AWS DynamoDB to store the jobs and then run them on demand.
- B. Use AWS Lambda functions with C# for the Admin jobs. ✔
- C. Use AWS S3 to store the jobs and then run them on demand.
- D. Use AWS Config functions with C# for the Admin jobs.

Explanation :

Answer - B

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

AWS Documentation mentions the following on AWS Lambda:

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

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

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

Ask our Experts

QUESTION 42 CORRECT DESIGN COST-OPTIMIZED ARCHITECTURES

Your company has a set of resources hosted on the AWS Cloud. As a part of the new governing model, there is a requirement that all activity on AWS resources should be monitored. What is the most efficient way to have this implemented?

- A. Use VPC Flow Logs to monitor all activity in your VPC.
- B. Use AWS Trusted Advisor to monitor all of your AWS resources.
- C. Use AWS Inspector to inspect all of the resources in your account.
- D. Use AWS CloudTrail to monitor all API activity. ✔

Explanation :

Answer – D
AWS Documentation mentions the following on AWS CloudTrail:
AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting.

Visibility into your AWS account activity is a key aspect of security and operational best practices. You can use CloudTrail to view, search,

download, archive, analyze, and respond to account activity across your AWS infrastructure. You can identify who or what took which action, what resources were acted upon, when the event occurred, and other details to help you analyze and respond to activity in your AWS account.
You can integrate CloudTrail into applications using the API, automate trail creation for your organization, check the status of trails you create, and control how users view CloudTrail events.

More information is available at the below URLs:
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html (https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html)
https://aws.amazon.com/cloudtrail/ (https://aws.amazon.com/cloudtrail/)

Ask our Experts

QUESTION 43 MARKED AS REVIEW CORRECT DEFINE PERFORMANT ARCHITECTURES

Below are the requirements for a data store in AWS:

a) Fully Managed

b) Integration with existing business intelligence tools

c) High concurrency workload that generally involves reading and writing all columns for a small number of records at a time

Which of the following would be an ideal data store for the above requirements? Choose 2 answers from the options below.

- [x] **A.** AWS Redshift ✔
- [x] **B.** AWS DynamoDB ✔
- [ ] **C.** AWS Aurora
- [ ] **D.** AWS S3

Explanation :

Answer: A and B

Please refer to the following link for Redshift

- https://docs.aws.amazon.com/redshift/ (https://docs.aws.amazon.com/redshift/)

Please refer to the below link for DynamoDB, on page 25

- https://d1.awsstatic.com/whitepapers/AWS_Cloud_Best_Practices.pdf (https://d1.awsstatic.com/whitepapers/AWS_Cloud_Best_Practices.pdf)

The question says:

a) Fully Managed
b) Integration with existing business intelligence tools

Therefore AWS Redshift would suit this requirement

c) High concurrency workload that generally involves reading and writing all columns for a small number of records at a time

Therefore AWS DynamoDB would suit this requirement

Therefore the following options are correct:

A. AWS Redshift
B. AWS DynamoDB

The following options are incorrect:

C. AWS Aurora - It is a database and it is not suitable for reading and writing small number of records
D. AWS S3 - It cannot be integrated with business intelligence tools

Ask our Experts

QUESTION 44 MARKED AS REVIEW INCORRECT DESIGN COST-OPTIMIZED ARCHITECTURES

A company currently uses Redshift in AWS. The Redshift cluster is required to be used in a cost-effective manner. As an architect, which of the following would you consider to ensure cost-effectiveness?

- **A.** Use Spot Instances for the underlying nodes in the cluster. ✖
- **B.** Ensure that unnecessary manual snapshots of the cluster are deleted. ✔
- **C.** Ensure VPC Enhanced Routing is enabled.
- **D.** Ensure that CloudWatch metrics are disabled.

Explanation :

Answer -B

AWS Documentation mentions the following:
Amazon Redshift provides free storage for snapshots that is equal to the storage capacity of your cluster until you delete the cluster. After you reach the free snapshot storage limit, you are charged for any additional storage at the normal rate. Because of this, you should evaluate how many days you need to keep automated snapshots and configure their retention period accordingly, and delete any manual snapshots that you no longer need.
For more information on working with Redshift Snapshots, please visit the following URL:
https://docs.aws.amazon.com/redshift/latest/mgmt/working-with-snapshots.html
(https://docs.aws.amazon.com/redshift/latest/mgmt/working-with-snapshots.html)

Note:
Redshift pricing is based on the following elements.

- Compute node hours
- Backup Storage
- Data transfer – There is no data transfer charge for data transferred to or from Amazon Redshift and Amazon S3 within the same AWS Region. For all other data transfers into and out of Amazon Redshift, you will be billed at standard AWS data transfer rates.
- Data scanned

There is no additional charge for using Enhanced VPC Routing. Y**ou might incur additional data transfer charges for certain operations, such as UNLOAD to Amazon S3 in a different region or COPY from Amazon EMR or SSH with public IP addresses.**

Enhanced VPC routing does not incur any cost but any Unload operation to a different region will incur a cost.
With Enhanced VPC routing or without it any data transfer to a different region does incur the cost.

But with Storage, increasing your backup retention period or taking additional snapshots increases the backup storage consumed by your data warehouse. There is no additional charge for backup storage up to 100% of your provisioned storage for an active data warehouse cluster. Any amount of storage exceeding this limit does incur the cost.
@@@For Redshift spot Instances is not an option@@@

Amazon Redshift pricing options include:

- On-Demand pricing (https://aws.amazon.com/redshift/pricing/#On-Demand_Pricing): no upfront costs - you simply pay an hourly rate based on the type and number of nodes in your cluster

based on the type and number of nodes in your cluster.

- Amazon Redshift Spectrum pricing (https://aws.amazon.com/redshift/pricing/#Redshift_Spectrum_Pricing): enables you to run SQL queries directly against all of your data, out to exabytes, in Amazon S3 - you simply pay for the number of bytes scanned.
- Reserved Instance pricing (https://aws.amazon.com/redshift/pricing/#Reserved_Instance_Pricing): enables you to save up to 75% over On-Demand rates by committing to using Redshift for a 1 or 3-year term.

Ask our Experts

QUESTION 45 CORRECT SPECIFY SECURE APPLICATIONS AND ARCHITECTURES

A company has a set of resources hosted in an AWS VPC. Having acquired another company with its own set of resources hosted in AWS, it is required to ensure that resources in the VPC of the parent company can access the resources in the VPC of the child company. How can this be accomplished?

- A. Establish a NAT Instance to establish communication across VPCs.
- B. Establish a NAT Gateway to establish communication across VPCs.
- C. Use a VPN Connection to peer both VPCs.
- D. Use VPC Peering to peer both VPCs. ✔

Explanation :

Answer - D

AWS Documentation mentions the following about VPC Peering:

A VPC Peering Connection is a networking connection between two VPCs that enables you to route traffic between them privately.

Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC Peering Connection between your own VPCs, with a VPC in another AWS account, or with a VPC in a different AWS region.
For more information on VPC Peering, please visit the following URL:
https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-peering.html
(https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-peering.html)

NAT Instance, NAT Gateway and VPN do not allow for VPC-VPC connectivitity.

Ask our Experts

QUESTION 46 CORRECT DESIGN RESILIENT ARCHITECTURES

An application consists of the following architecture:

a. EC2 Instances in a single AZ behind an ELB

b. A NAT Instance which is used to ensure that instances can download updates from the Internet

Which of the following can be used to ensure better fault tolerance in this setup? Choose 2 answers from the options given below.

- [ ] **A.** Add more instances in the existing Availability Zone.
- [x] **B.** Add an Auto Scaling Group to the setup. ✔
- [x] **C.** Add more instances in another Availability Zone. ✔
- [ ] **D.** Add another ELB for more fault tolerance.

Explanation :

Answer – B and C
AWS Documentation mentions the following:
Adding Auto Scaling to your application architecture is one way to maximize the benefits of the AWS Cloud. When you use Auto Scaling, your applications gain the following benefits:

- Better fault tolerance. Auto Scaling can detect when an instance is unhealthy, terminate it, and launch an instance to replace it. You can also configure Auto Scaling to use multiple Availability Zones. If one Availability Zone becomes unavailable, Auto Scaling can launch instances in another one to compensate.
- Better availability. Auto Scaling can help you ensure that your application always has the right amount of capacity to handle the current traffic demands.

For more information on the benefits of Auto Scaling, please visit the following URL:
https://docs.aws.amazon.com/autoscaling/ec2/userguide/auto-scaling-benefits.html
(https://docs.aws.amazon.com/autoscaling/ec2/userguide/auto-scaling-benefits.html)

Ask our Experts

QUESTION 47 MARKED AS REVIEW INCORRECT DEFINE PERFORMANT ARCHITECTURES

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

- A. The company could start using Gateway Cached Volumes. ✔
- B. The company could start using Gateway Stored Volumes. ✖
- C. The company could start using the Simple Storage Service.
- D. The company could start using Amazon Glacier.

Explanation :

Answer - A

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

AWS Documentation mentions the following:

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

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

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

Note: The question states that they are running out of storage space and they need a solution to store data with AWS rather than a backup.

So for this purpose, gateway-cached volumes are appropriate which will help them to avoid scaling their on-premises data center and allows them to store on AWS storage service while having the most recent files available for them at low latency.

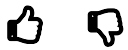
This is the difference between Cached and stored volumes:

- **Cached volumes** – You store your data in S3 and retain a copy of frequently accessed data subsets locally. Cached volumes offer substantial cost savings on primary storage and "minimize the need to scale your storage on-premises. You also retain low-latency access to your frequently accessed data."
- **Stored volumes** – If you need low-latency access to your entire data set, first configure your on-premises gateway to store all your data locally. Then asynchronously back up point-in-time snapshots of this data to Amazon S3. "This configuration provides durable and inexpensive offsite backups that you can recover to your local data center or Amazon EC2." For example, if you need replacement capacity for disaster recovery, you can recover the backups to Amazon EC2.

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

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

Ask our Experts



QUESTION 48 MARKED AS REVIEW INCORRECT DESIGN RESILIENT ARCHITECTURES

A company has a sales team and each member of this team uploads their sales figures daily. A Solutions Architect

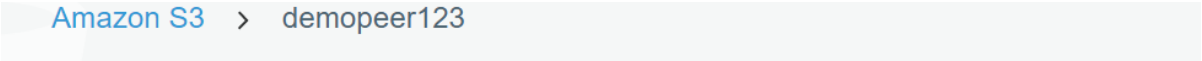
A company has a sales team and each member of this team uploads their sales figures daily. A Solutions Architect needs a durable storage solution for these documents and also a way to preserve documents from accidental deletions. What among the following choices would deliver protection against unintended user actions?

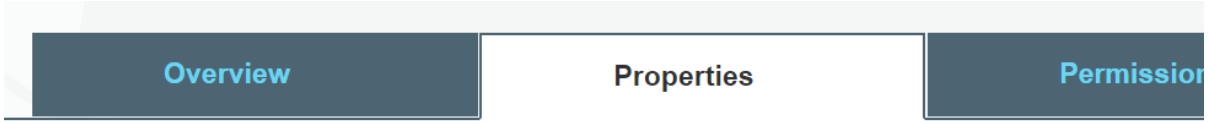
- A. Store data in an EBS Volume and create snapshots once a week.
- B. Store data in an S3 bucket and enable versioning. ✔
- C. Store data in two S3 buckets in different AWS regions. ✖
- D. Store data on EC2 Instance storage.

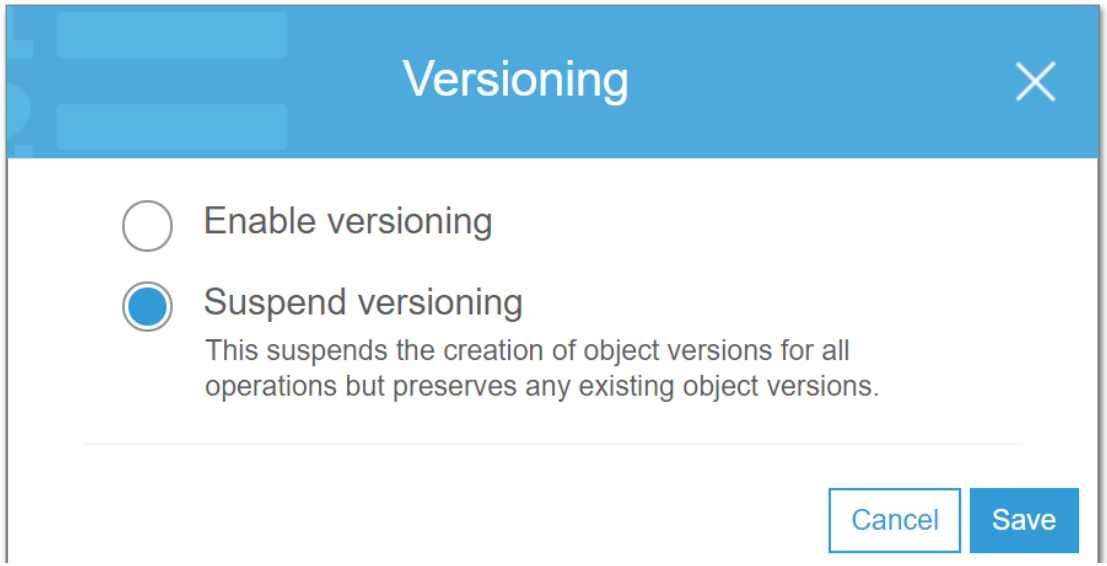
Explanation :

Answer - B

Amazon S3 has an option for versioning as shown below. Versioning is on the bucket level and can be used to recover prior versions of an object.







- For more information on Amazon S3, please visit the following URL:
  - https://aws.amazon.com/s3/ (https://aws.amazon.com/s3/)

Ask our Experts

An application requires a highly available relational database with an initial storage capacity of 8TB. This database will grow by 8GB everyday. To support the expected traffic, at least eight read replicas will be required to handle the database reads. Which of the below options meets these requirements?

- A. DynamoDB
- B. Amazon S3
- C. Amazon Aurora ✔
- D. Amazon Redshift

Explanation :

Answer – C
AWS Documentation mentions the following:
Aurora Replicas
Aurora Replicas are independent endpoints in an Aurora DB cluster, best used for scaling read operations and increasing availability. Up to 15 Aurora Replicas can be distributed across the Availability Zones that a DB cluster spans within an AWS Region. The DB cluster volume is made up of multiple copies of the data for the DB cluster. However, the data in the cluster volume is represented as a single, logical volume to the primary instance and to Aurora Replicas in the DB cluster.
As a result, all Aurora Replicas return the same data for query results with minimal replica lag—usually much less than 100 milliseconds after the primary instance has written an update. Replica lag varies depending on the rate of database change. That is, during periods where a large amount of write operations occur for the database, you might see an increase in replica lag.

Aurora Replicas work well for read scaling because they are fully dedicated to read operations on your cluster volume. Write operations are managed by the primary instance. Because the cluster volume is shared among all DB instances in your DB cluster, minimal additional work is required to replicate a copy of the data for each Aurora Replica.

To increase availability, you can use Aurora Replicas as failover targets. That is, if the primary instance fails, an Aurora Replica is promoted to

the primary instance. There is a brief interruption during which read and write requests made to the primary instance fail with an exception, and the Aurora Replicas are rebooted. If your Aurora DB cluster doesn't include any Aurora Replicas, then your DB cluster will be unavailable for the duration it takes your DB instance to recover from the failure event. However, promoting an Aurora Replica is much faster than recreating the primary instance. For high-availability scenarios, we recommend that you create one or more Aurora Replicas. These should be of the same DB instance class as the primary instance and in different Availability Zones for your Aurora DB cluster. For more information on Aurora Replicas as failover targets, see Fault Tolerance for an Aurora DB Cluster.

Note

You can't create an encrypted Aurora Replica for an unencrypted Aurora DB cluster. You can't create an unencrypted Aurora Replica for an encrypted Aurora DB cluster.

For details on how to create an Aurora Replica, see Adding Aurora Replicas to a DB Cluster.

Replication with Aurora MySQL

In addition to Aurora Replicas, you have the following options for replication with Aurora MySQL:

Two Aurora MySQL DB clusters in different AWS Regions, by creating an Aurora Read Replica of an Aurora MySQL DB cluster in a different AWS Region.

Two Aurora MySQL DB clusters in the same region, by using MySQL binary log (binlog) replication.

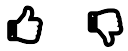
An Amazon RDS MySQL DB instance as the master and an Aurora MySQL DB cluster, by creating an Aurora Read Replica of an Amazon RDS MySQL DB instance. Typically, this approach is used for migration to Aurora MySQL, rather than for ongoing replication.

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

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

(https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Aurora.Replication.html)

Ask our Experts



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

- A. Use S3 Replication to replicate the objects to regions closest to the users.
- B. Ensure S3 Transfer Acceleration is enabled to ensure all users get the desired response times.
- C. Place an ELB in front of S3 to distribute the load across S3.
- D. Place the S3 bucket behind a CloudFront distribution. ✔

Explanation :

Answer - D

AWS Documentation mentions the following:

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

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

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

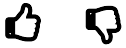
For more information on performance considerations in S3, please visit the following URL:

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

Options A and B are incorrect. S3 Cross-Region Replication and Transfer Acceleration incurs cost.

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

Ask our Experts



QUESTION 51 CORRECT DESIGN RESILIENT ARCHITECTURES

An application needs to have a messaging system in AWS. It is of the utmost importance that the order of messages is preserved and duplicate messages are not sent. Which of the following services can help fulfill this requirement?

- A. AWS SQS FIFO ✔
- B. AWS SNS
- C. AWS Config
- D. AWS ELB

Explanation :

Answer – A
One can use SQS FIFO queues for this purpose.
AWS Documentation mentions the following on SQS FIFO Queues:

Amazon SQS is a reliable and highly-scalable managed message queue service for storing messages in transit between application

components. FIFO queues complement the existing Amazon SQS standard queues, which offer high throughput, best-effort ordering, and at-least-once delivery. FIFO queues have essentially the same features as standard queues, but provide the added benefits of supporting ordering and exactly-once processing. FIFO queues provide additional features that help prevent unintentional duplicates from being sent by message producers or from being received by message consumers. Additionally, message groups allow multiple separate ordered message streams within the same queue.
For more information on SQS FIFO Queues, please visit the following URL:
https://aws.amazon.com/about-aws/whats-new/2016/11/amazon-sqs-introduces-fifo-queues-with-exactly-once-processing-and-lower-prices-for-standard-queues/ (https://aws.amazon.com/about-aws/whats-new/2016/11/amazon-sqs-introduces-fifo-queues-with-exactly-once-processing-and-lower-prices-for-standard-queues/)

Note:

As per AWS, SQS FIFO queues will ensure the delivery of the message only once and it will be delivered in a sequential order. (i.e. First in First Out) where as SNS cannot guarantee the delivery of the message only once.

As per AWS SNS FAQ,
Q: How many times will a subscriber receive each message?
Although most of the time each message will be delivered to your application exactly once, **the distributed nature of Amazon SNS and transient network conditions could result in occasional, duplicate messages at the subscriber end.**Developers should design their applications such that processing a message more than once does not create any errors or inconsistencies.

FIFO FQs states that

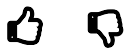
High Throughput: By default, FIFO queues support up to 300 messages per second (300 send, receive, or delete operations per second). When you batch 10 messages per operation (maximum), FIFO queues can support up to 3,000 messages per second. To request a limit increase, file a support request.

Exactly-Once Processing: A message is delivered once and remains available until a consumer processes and deletes it. Duplicates aren't introduced into the queue.

First-In-First-Out Delivery: The order in which messages are sent and received is strictly preserved (i.e. First-In-First-Out).

Using SQS FIFO queues will satisfy both the requirements stated in the question.
i.e. Duplication of message will not occur and the order of messages will be preserved.

Ask our Experts



QUESTION 52 CORRECT DEFINE PERFORMANT ARCHITECTURES

A company is planning on building an application using the services available on AWS. This application will be

A company is planning on building an application using the services available on AWS. This application will be stateless in nature, and the service must have the ability to scale according to the demand. Which of the following would be an ideal compute service to use in this scenario?

- A. AWS DynamoDB
- B. AWS Lambda ✔
- C. AWS S3
- D. AWS SQS

Explanation :

Answer - B
The following content from an AWS Whitepaper supports the usage of AWS Lambda for this requirement:
A stateless application is an application that needs no knowledge of previous interactions and stores no session information. Such an example could be an application that, given the same input, provides the same response to any end user. A stateless application can scale horizontally since any request can be serviced by any of the available compute resources (e.g., EC2 instances, AWS Lambda functions).
For more information on AWS Cloud best practices, please visit the following URL:
https://d1.awsstatic.com/whitepapers/AWS_Cloud_Best_Practices.pdf
(https://d1.awsstatic.com/whitepapers/AWS_Cloud_Best_Practices.pdf)

Ask our Experts

A company has a set of EC2 Instances hosted on the AWS Cloud. These instances form a web server farm which services a web application accessed by users on the Internet. Which of the following would help make this architecture more fault tolerant? Choose 2 answers from the options given below.

- [x] **A.** Ensure the instances are placed in separate Availability Zones. ✔
- [x] **B.** Ensure the instances are placed in separate regions. ✖
- [ ] **C.** Use an AWS Load Balancer to distribute the traffic. ✔
- [ ] **D.** Use Auto Scaling to distribute the traffic.

Explanation :

Answer – A and C
AWS Documentation mentions the following:
A load balancer distributes incoming application traffic across multiple EC2 Instances in multiple Availability Zones. This increases the fault tolerance of your applications. Elastic Load Balancing detects unhealthy instances and routes traffic only to healthy instances.
For more information on the AWS Classic Load Balancer, please visit the following URL:
https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/introduction.html
(https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/introduction.html)

Note:

Autoscaling will not create an ELB automatically you need to manually create it in the same region as the AutoScaling group.
Once you create an ELB, and attach the load balancer to the autoscaling group, it automatically registers the instances in the group and distributes incoming traffic across the instances.

The following steps provides you information on attaching a load balancer to autoscaling group.

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. On the navigation pane, under **Auto Scaling**, choose **Auto Scaling Groups**.
3. Select your group.
4. On the **Details** tab, choose **Edit**.
5. Do one of the following:
    1. [Classic Load Balancers] For **Load Balancers**, select your load balancer.
    2. [Target groups] For **Target Groups**, select your target group.
6. Choose **Save**.

As per AWS,

You can automatically increase the size of your Auto Scaling group when demand goes up and decrease it when demand goes down. As the Auto Scaling group adds and removes EC2 instances, you must ensure that the traffic for your application is distributed across all of your EC2 instances. **The Elastic Load Balancing service automatically routes incoming web traffic across such a dynamically changing number of EC2 instances.** Your load balancer acts as a single point of contact for all incoming traffic to the instances in your Auto Scaling group.

To use a load balancer with your Auto Scaling group, create the load balancer and then attach it to the group.

For more information:
https://docs.aws.amazon.com/autoscaling/ec2/userguide/autoscaling-load-balancer.html
(https://docs.aws.amazon.com/autoscaling/ec2/userguide/autoscaling-load-balancer.html)
https://docs.aws.amazon.com/autoscaling/ec2/userguide/attach-load-balancer-asg.html
(https://docs.aws.amazon.com/autoscaling/ec2/userguide/attach-load-balancer-asg.html)

Ask our Experts

QUESTION 54 CORRECT DESIGN COST-OPTIMIZED ARCHITECTURES

You plan on hosting an application on EC2 Instances which will be used to process logs. The application is not very critical and can resume operation even after an interruption. Which of the following steps can help provide a cost-effective solution?

- A. Use Reserved Instances for the underlying EC2 Instances.
- B. Use Provisioned IOPS for the underlying EBS Volumes.
- C. Use Spot Instances for the underlying EC2 Instances. ✔
- D. Use S3 as the underlying data layer.

Explanation :

Answer – C

One effective solution would be to use Spot Instances in this scenario.

AWS Documentation mentions the following on Spot Instances:

Spot Instances are a cost-effective choice if you can be flexible about when your applications run and if your applications can be interrupted. For example, Spot Instances are well-suited for data analysis, batch jobs, background processing, and optional tasks.

For more information on using Spot Instances, please visit the following URL:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-spot-instances.html

(https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-spot-instances.html)

Ask our Experts

QUESTION 55 CORRECT DESIGN RESILIENT ARCHITECTURES

A company stores its log data in an S3 bucket. There is a current need to have search capabilities available for the data in S3. How can this be achieved in an efficient and ongoing manner? Choose 2 answers from the options below. Each answer forms a part of the solution.

- [x] **A.** Use AWS Athena to query the S3 bucket. ✔
- [ ] **B.** Create a Lifecycle Policy for the S3 bucket.
- [x] **C.** Load the data into Amazon Elasticsearch. ✔
- [ ] **D.** Load the data into Glacier.

Explanation :

Answer – A and C

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

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

Ask our Experts

QUESTION 56 CORRECT DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

A company plans on deploying a batch processing application in AWS. Which of the following is an ideal way to host this application? Choose 2 answers from the options below. Each answer forms a part of the solution.

- [ ] **A.** Copy the batch processing application to an ECS Container.
- [x] **B.** Create a docker image of your batch processing application. ✔
- [x] **C.** Deploy the image as an Amazon ECS task. ✔
- [ ] **D.** Deploy the container behind the ELB.

Explanation :

Answer – B and C
AWS Documentation mentions the following:
Docker containers are particularly suited for batch job workloads. Batch jobs are often short-lived and embarrassingly parallel. You can package your batch processing application into a Docker image so that you can deploy it anywhere, such as in an Amazon ECS task.
For more information on the use cases for AWS ECS, please visit the following URL:
https://docs.aws.amazon.com/AmazonECS/latest/developerguide/common_use_cases.html
(https://docs.aws.amazon.com/AmazonECS/latest/developerguide/common_use_cases.html)

Ask our Experts

QUESTION 57 CORRECT DESIGN RESILIENT ARCHITECTURES

An architecture consists of the following:

a) A primary and secondary infrastructure hosted in AWS

b) Both infrastructures comprise ELB, Auto Scaling and EC2 resources

How should Route 53 be configured to ensure proper failover in case the primary infrastructure were to go down?

- **A.** Configure a primary routing policy.
- **B.** Configure a weighted routing policy.
- **C.** Configure a Multi-Answer routing policy.
- **D.** Configure a failover routing policy. ✔

Explanation :

Answer - D

AWS Documentation mentions the following:
You can create an active-passive failover configuration by using failover records. Create a primary and a secondary failover record that have the same name and type, and associate a health check with each.
The various Route 53 routing policies are as follows:

- Simple routing policy – Use for a single resource that performs a given function for your domain, for example, a web server that serves content for the example.com website.
- Failover routing policy – Use when you want to configure active-passive failover.
- Geolocation routing policy – Use when you want to route traffic based on the location of your users.
- Geoproximity routing policy – Use when you want to route traffic based on the location of your resources and, optionally, shift traffic from resources in one location to resources in another.
- Latency routing policy – Use when you have resources in multiple locations and you want to route traffic to the resource that provides the best latency.
- Multivalue answer routing policy – Use when you want Route 53 to respond to DNS queries with up to eight healthy records selected at random.
- Weighted routing policy – Use to route traffic to multiple resources in proportions that you specify.

For more information on DNS Failover using Route 53, please visit the following URL:
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-configuring-options.html
(https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-configuring-options.html)

Ask our Experts

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

- **A.** Enable AWS KMS to rotate keys and KMS will manage all encrypt/decrypt actions using the appropriate keys ✔
- **B.** Your company must instruct KMS to re-encrypt all data in all services each time a new key is created
- **C.** You have 30 days to delete old keys after a new one is rotated in
- **D.** Your company must create its own keys and import to them to KMS to enable key rotation

Explanation :

Answer: A

- A. KMS will rotate keys annually and use the appropriate keys to perform cryptographic operations

Incorrect:

- B. This is not necessary. KMS, as a managed service, will keep old keys and perform operations based on the appropriate key
- C. This is not a requirement of KMS
- D. This is not a requirement of KMS

Reference:

- https://aws.amazon.com/kms/faqs/ (https://aws.amazon.com/kms/faqs/)
- ttps://docs.aws.amazon.com/general/latest/gr/rande.html#kms_region (https://docs.aws.amazon.com/general/latest/gr/rande.html#kms_region)
- https://www.slideshare.net/AmazonWebServices/encryption-and-key-management-in-aws (https://www.slideshare.net/AmazonWebServices/encryption-and-key-management-in-aws)

Ask our Experts

QUESTION 59 CORRECT SPECIFY SECURE APPLICATIONS AND ARCHITECTURES

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

- A. Use AWS Cognito although it only supports social identity providers like Facebook
- B. Let each user create an AWS user account to be managed via IAM
- C. Invest heavily in Microsoft Active Directory as it's the industry standard
- D. Use Cognito Identity along with a User Pool to securely save users' profile attributes ✔

Explanation :

Answer: D

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

Incorrect:

- A. Cognitio supports more than just social identity providers, including OIDC, SAML, and its own identity pools
- B. This isn't an efficient means of managing user authentication
- C. This isn't the most efficient means to authenticate and save user information

Reference:

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

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

- https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-user-identity-pools.html (https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-user-identity-pools.html)
- https://aws.amazon.com/cognito/getting-started/ (https://aws.amazon.com/cognito/getting-started/)
- https://docs.aws.amazon.com/cognito/latest/developerguide/concepts.html (https://docs.aws.amazon.com/cognito/latest/developerguide/concepts.html)

Ask our Experts

QUESTION 60 CORRECT DEFINE PERFORMANT ARCHITECTURES

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

- A. MySQL
- B. Microsoft SQL Server
- C. Oracle
- D. Amazon Aurora ✔

Explanation :

Answer – D

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

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

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

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

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

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

NOTE:

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

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

Hence, the best answer would be option D.

Ask our Experts

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

- A. It's too much of a security risk to allow unauthenticated users access to the app
- B. Cognito Identity supports guest users for the ability to enter the app and have limited access ✔
- C. A second version of the app will need to be offered for unauthenticated users
- D. This is possible only if we remove the authentication from everyone

Explanation :

Answer:B

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

Incorrect:

- A. Cognito will allow unauthenticated users without being a security risk
- C. This is not necessary; unauthenticated users are allowed using Cognito
- D. Cognito supports both authenticated and unauthenticated users

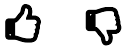
Reference:

- https://aws.amazon.com/cognito/ (https://aws.amazon.com/cognito/)
- http://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-integrate-with-cognito.html (http://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-integrate-with-cognito.html)
- https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-user-identity-pools.html

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

- https://docs.aws.amazon.com/cognito/latest/developerguide/identity-pools.html (https://docs.aws.amazon.com/cognito/latest/developerguide/identity-pools.html)
- https://aws.amazon.com/cognito/getting-started/ (https://aws.amazon.com/cognito/getting-started/)
- https://docs.aws.amazon.com/cognito/latest/developerguide/concepts.html (https://docs.aws.amazon.com/cognito/latest/developerguide/concepts.html)

Ask our Experts



QUESTION 62 CORRECT SPECIFY SECURE APPLICATIONS AND ARCHITECTURES

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

- **A.** This is supported, along with social and SAML based identity providers. ✔
- **B.** This is not supported, only social identity providers can be integrated into User Pools
- **C.** If you want OIDC identity providers, then you must include SAML and social based support as well
- **D.** It's too much effort to add non-Cognito authenticated user information to a User Pool

Explanation :

Explanation:

Answer: A

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

Incorrect:

- B. Cognito supports more than just social identity providers, including OIDC, SAML, and its own identity pools
- C. You can add any combination of federated types, you don't have to add them all
- D. While there is additional coding to develop this, the effort is most likely not too great to add the feature

Reference:

- https://aws.amazon.com/cognito/ (https://aws.amazon.com/cognito/)
- https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-user-pools-oidc-idp.html (https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-user-pools-oidc-idp.html)
- http://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-integrate-with-cognito.html (http://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-integrate-with-cognito.html)
- https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-user-identity-pools.html (https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-user-identity-pools.html)
- https://aws.amazon.com/cognito/getting-started/ (https://aws.amazon.com/cognito/getting-started/)
- https://docs.aws.amazon.com/cognito/latest/developerguide/concepts.html (https://docs.aws.amazon.com/cognito/latest/developerguide/concepts.html)

Ask our Experts

A company is building a Two-Tier web application to serve dynamic transaction-based content. The Data Tier uses an Online Transactional Processing (OLTP) database. What services should you leverage to enable an elastic and scalable Web Tier?

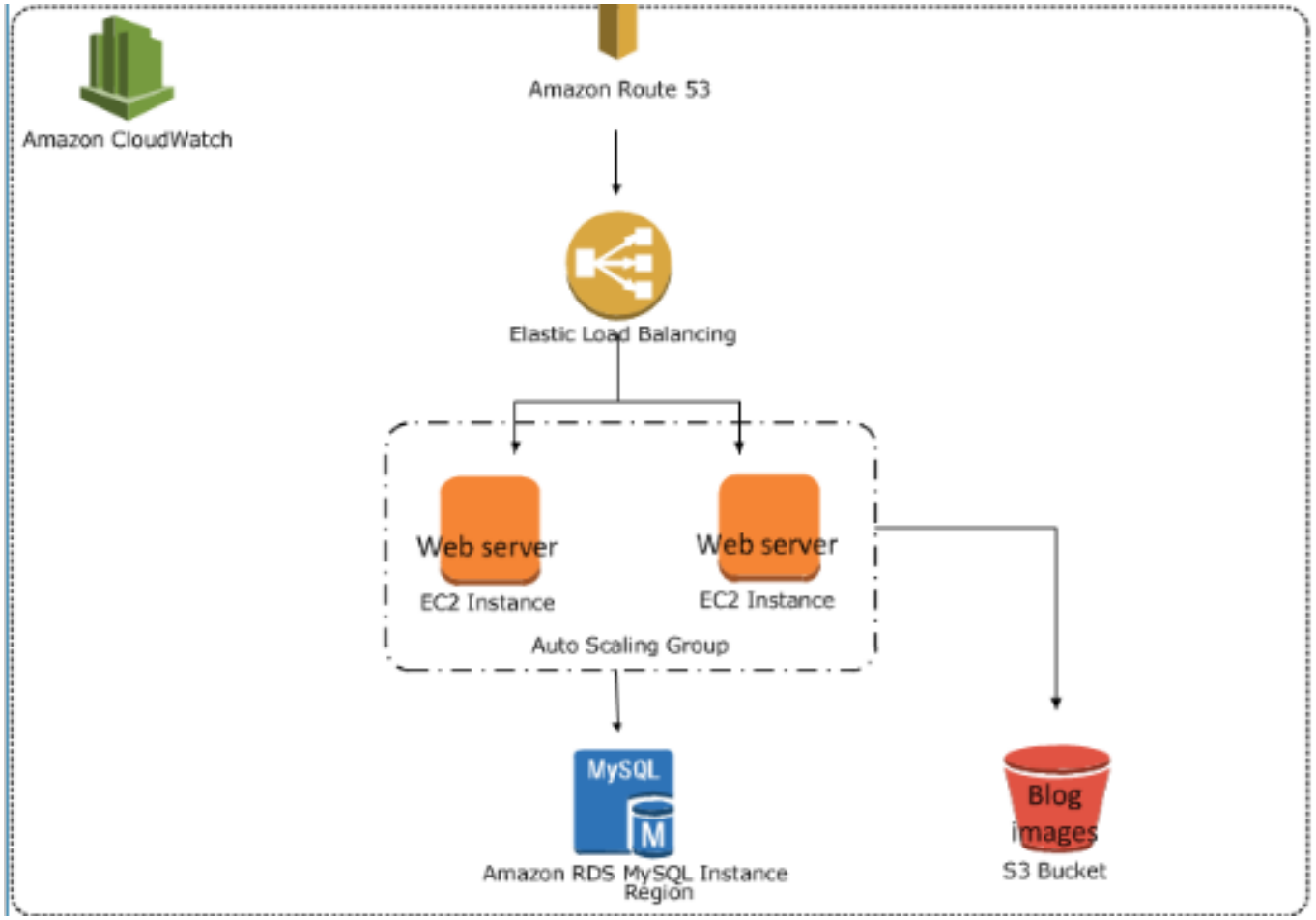
- A. Elastic Load Balancing, Amazon EC2, and Auto Scaling ✔
- B. Elastic Load Balancing, Amazon RDS with Multi-AZ, and Amazon S3
- C. Amazon RDS with Multi-AZ and Auto Scaling ✖
- D. Amazon EC2, Amazon Dynamo DB, and Amazon S3

Explanation :

Answer – A

The question mentions a scalable Web Tier and not a Database Tier. So Option C, D and B can be eliminated since they are database related options.

The below example shows an Elastic Load Balancer connected to 2 EC2 instances via Auto Scaling. This is an example of an elastic and scalable Web Tier. By scalable, we mean that the Auto Scaling process is able to increase or decrease the number of EC2 Instances as required.



For more information on the Elastic Load Balancer, please refer to the link below.
https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/introduction.html
(https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/introduction.html)

Ask our Experts

QUESTION 64 MARKED AS REVIEW INCORRECT SPECIFY SECURE APPLICATIONS AND ARCHITECTURES

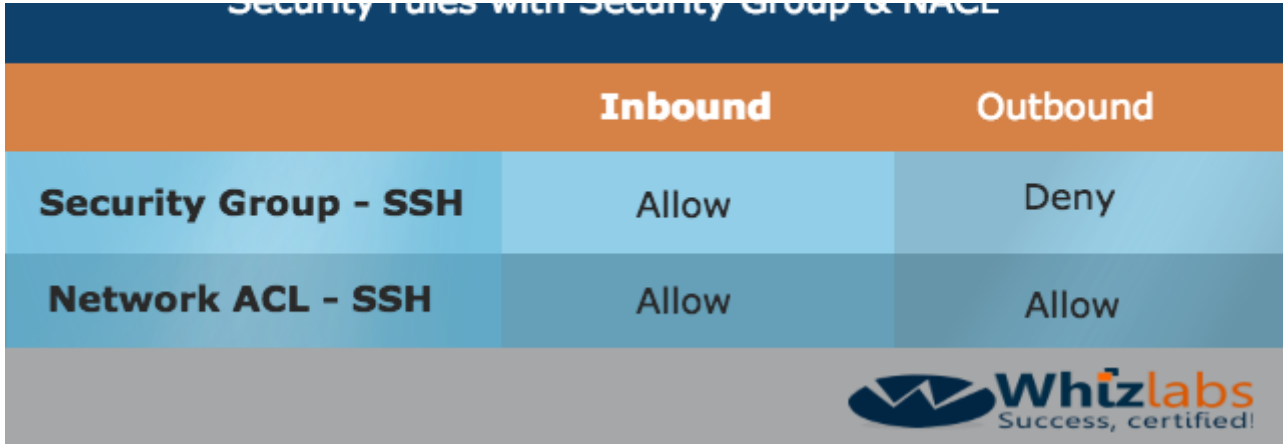
An instance is launched into a VPC subnet with the network ACL configured to allow all inbound traffic and deny all outbound traffic. The instance's security group is configured to allow SSH from any IP address. What changes need to be made to allow SSH access to the instance?

- A. The Outbound Security Group needs to be modified to allow outbound traffic.
- B. The Outbound Network ACL needs to be modified to allow outbound traffic. ✔
- C. Nothing, it can be accessed from any IP address using SSH.
- D. Both the Outbound Security Group and Outbound Network ACL need to be modified toallow outbound traffic. ✖

Explanation :

Answer – B

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



The reason why Network ACL has to have both an Allow for Inbound and Outbound is because network ACLs are stateless. Responses to allowed inbound traffic are subject to the rules for outbound traffic (and vice versa). Whereas for Security groups, responses are stateful. So if an incoming request is granted, by default an outgoing request will also be granted.

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

- For more information on Network ACLs, please refer to the link below.
  - https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html (https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html)

Ask our Experts

QUESTION 65 MARKED AS REVIEW INCORRECT DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

Your company currently has a web distribution hosted using the AWS CloudFront service. The IT Security

department has confirmed that the application using this web distribution now falls under the scope of PCI compliance. What are the possible ways to meet the requirements? Choose two answers from the choices below.

- [x] **A.** Enable CloudFront access logs. ✔
- [ ] **B.** Enable Cache in CloudFront.
- [ ] **C.** Capture requests that are sent to the CloudFront API. ✔
- [x] **D.** Enable VPC Flow Logs ✖

Explanation :

Answer – A and C
AWS Documentation mentions the following:
If you run PCI or HIPAA-compliant workloads based on the AWS Shared Responsibility Model (https://aws.amazon.com/compliance/shared-responsibility-model/), we recommend that you log your CloudFront usage data for the last 365 days for future auditing purposes. To log usage data, you can do the following:

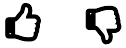
- Enable CloudFront access logs.
- Capture requests that are sent to the CloudFront API.

For more information on compliance with CloudFront, please visit the following URL:
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/compliance.html (https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/compliance.html)

Option B helps to reduce latency.

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

Ask our Experts



Finish Review (https://www.whizlabs.com/learn/course/aws-csaa-practice-tests/quiz/14729)

Certification

- Cloud Certification (https://www.whizlabs.com/cloud-certification-training-courses/)
- Java Certification (https://www.whizlabs.com/oracle-java-certifications/)
- PM Certification (https://www.whizlabs.com/project-management-certifications/)
- Big Data Certification (https://www.whizlabs.com/big-data-certifications/)

Company

- Support (https://help.whizlabs.com/hc/en-us)
- Discussions (http://ask.whizlabs.com/)
- Blog (https://www.whizlabs.com/blog/)

Mobile App

- Android Coming Soon
- iOS Coming Soon

Follow us

(https://www.facebook.com/whizlabs.software/)

(https://in.linkedin.com/company/whizlabs-software)

(https://twitter.com/whizlabs?lang=en)

(https://plus.google.com/+WhizlabsSoftware)

© Copyright 2018. Whizlabs Software Pvt. Ltd. All Rights Reserved.