CSAA PRACTICE TEST 3

Attempt	6	**Completed on**	Sunday , 13 January 2019 , 03:01 PM
Marks Obtained	63 / 65	**Time Taken**	01 H 46 M 36 S
Your score is	96.92%	**Result**	Pass

Domains / Topics wise Quiz Performance Report

S.No.	Topic	Total Questions	Correct	Incorrect	Unattempted
1	Specify Secure Applications and Architectures	9	8	1	0
2	Define Operationally-Excellent Architectures	25	24	1	0
3	Define Performant Architectures	11	11	0	0
4	Design Resilient Architectures	14	14	0	0
5	Design Cost-Optimized Architectures	6	6	0	0

65 Questions	63 Correct	2 Incorrect	0 Unattempted

Show Answers: All

QUESTION 1 CORRECT SPECIFY SECURE APPLICATIONS AND ARCHITECTURES

A customer planning on hosting an AWS RDS instance, needs to ensure that the underlying data is encrypted. How can this be achieved? Choose 2 answers from the options given below.

- [x] **A.** Ensure that the right instance class is chosen for the underlying instance. ✔
- [ ] **B.** Choose only General Purpose SSD since only this volume type supports encryption ofdata.

- [x] **C.** Encrypt the database during creation. ✔
- [ ] **D.** Enable encryption of the underlying EBS Volume.

Explanation :

Answer – A and C
Encryption for the database can be done during the creation of the database. Also, you need to ensure that the underlying instance type supports DB encryption.
For more information on database encryption, please refer to the below URL:
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html
(https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html)
Encryption at Rest is not available for DB instances running SQL Server Express Edition.
For more information on encryption, please refer to the below URL:
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html
(https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html)

Ask our Experts

QUESTION 2 CORRECT DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

You are developing a new mobile application which is expected to be used by thousands of customers. You are considering storing user preferences in AWS, and need a data store to save the same. Each data item is expected to be 20KB in size. The solution needs to be cost-effective, highly available, scalable and secure. How would you design the data layer?

- **A.** Create a new AWS MySQL RDS instance and store the user data there.
- **B.** Create a DynamoDB table with the required Read and Write capacity and use it as the data layer. ✔
- **C.** Use Amazon Glacier to store the user data.
- **D.** Use an Amazon Redshift Cluster for managing the user preferences.

Explanation :

Answer – B
In this case, since each data item is 20KB and given the fact that DynamoDB is an ideal data layer for storing user preferences, this would be an ideal choice. Also, DynamoDB is a highly scalable and available service.
For more information on AWS DynamoDB, please refer to the below URL:
https://aws.amazon.com/dynamodb/ (https://aws.amazon.com/dynamodb/)

Ask our Experts

QUESTION 3 CORRECT DEFINE PERFORMANT ARCHITECTURES

Your Operations department is using an incident based application hosted on a set of EC2 Instances. These instances are placed behind an Auto Scaling Group to ensure the right number of instances are in place to support the application. The Operations department has expressed dissatisfaction with regard to poor application performance at 9:00 AM each day. However, it is also noted that the system performance returns to optimal at 9:45 AM.

What can be done to ensure that this issue gets fixed?

- A. Create another Dynamic Scaling Policy to ensure that the scaling happens at 9:00 AM.
- B. Add another Auto Scaling group to support the current one.
- C. Change the Cool Down Timers for the existing Auto Scaling Group.
- D. Add a Scheduled Scaling Policy at 8:30 AM. ✔

Explanation :

Answer - D
Scheduled Scaling can be used to ensure that the capacity is peaked before 9:00 AM each day.
AWS Documentation further mentions the following on Scheduled Scaling:
Scaling based on a schedule allows you to scale your application in response to predictable load changes. For example, every week the traffic to your web application starts to increase on Wednesday, remains high on Thursday, and starts to decrease on Friday. You can plan your scaling activities based on the predictable traffic patterns of your web application.
For more information on Scheduled Scaling, please refer to the below URL:
https://docs.aws.amazon.com/autoscaling/ec2/userguide/schedule_time.html
(https://docs.aws.amazon.com/autoscaling/ec2/userguide/schedule_time.html)

Ask our Experts

QUESTION 4 MARKED AS REVIEW CORRECT

DEFINE PERFORMANT ARCHITECTURES

A database hosted in AWS is currently encountering an extended number of write operations and is not able to handle the load. What can be done to the architecture to ensure that the write operations are not lost under any circumstance?

- A. Add more IOPS to the existing EBS Volume used by the database.
- B. Consider using DynamoDB instead of AWS RDS.
- C. Use SQS FIFO to queue the database writes. ✔
- D. Use SNS to send notification on missed database writes and then add them manuallyat a later stage.

Explanation :

Answer – C

SQS Queues can be used to store the pending database writes, and these writes can then be added to the database. It is the perfect queuing system for such architecture.

Note that adding more IOPS may help the situation but will not totally eliminate the chances of losing database writes.

For more information on AWS SQS, please refer to the URL below:

https://aws.amazon.com/sqs/faqs/ (https://aws.amazon.com/sqs/faqs/)

Note:

The scenario in the question is that the database is unable to handle the write operations and the requirement is that with out loosing any data we need to perform data writes on to the database.

For this requirement, we can use an SQS queue to store the pending write requests, which will ensure the delivery of these messages.

Increasing IOPS can handle the traffic bit more efficiently but it has a limit of .40,000 IOPS where as SQS queues can handle 120,000 messages inflight.

Ask our Experts

QUESTION 5 CORRECT SPECIFY SECURE APPLICATIONS AND ARCHITECTURES

You have created an AWS Lambda function that will write data to a DynamoDB table. Which of the following must be in place to ensure that the Lambda function can interact with the DynamoDB table?

- **A.** Ensure an IAM Role is attached to the Lambda function which has the required DynamoDB privileges. ✔
- **B.** Ensure an IAM User is attached to the Lambda function which has the required DynamoDB privileges.
- **C.** Ensure the Access keys are embedded in the AWS Lambda function.
- **D.** Ensure the IAM user password is embedded in the AWS Lambda function.

Explanation :

Answer – A

AWS Documentation mentions the following to support this requirement:
Each Lambda function has an IAM role (execution role) associated with it. You specify the IAM role when you create your Lambda function. Permissions you grant to this role determine what AWS Lambda can do when it assumes the role. There are two types of permissions that you grant to the IAM role:

- If your Lambda function code accesses other AWS resources, such as to read an object from an S3 bucket or write logs to CloudWatch Logs, you need to grant permissions for relevant Amazon S3 and CloudWatch actions to the role.
- If the event source is stream-based (Amazon Kinesis Data Streams and DynamoDB streams), AWS Lambda polls these streams on your behalf. AWS Lambda needs permissions to poll the stream and read new records on the stream so you need to grant the relevant permissions to this role.

For more information on the Permission Role model for AWS Lambda, please refer to the URL below.
https://docs.aws.amazon.com/lambda/latest/dg/intro-permission-model.html
(https://docs.aws.amazon.com/lambda/latest/dg/intro-permission-model.html)

Ask our Experts

QUESTION 6 CORRECT DESIGN RESILIENT ARCHITECTURES

Your company currently has data hosted in an Amazon Aurora MySQL DB. Since this data is critical, there is a need to ensure that it can be made available in another region in case of a disaster. How can this be achieved?

- A. Make a copy of the underlying EBS Volumes in the Amazon Cluster in another region.
- B. Enable Multi-AZ for the Aurora database.
- C. Creating a read replica of Amazon Aurora in another region. ✔
- D. Create an EBS Snapshot of the underlying EBS Volumes in the Amazon Cluster and thencopy them to another region.

Explanation :

Answer - C
Amazon RDS provides high availability and failover support for DB instances using Multi-AZ deployments. Amazon RDS uses several different technologies to provide failover support.

MultiAZ deployments for Oracle, PostgreSQL, MySQL, and MariaDB DB instances use Amazon's failover technology. SQL Server DB instances use SQL Server Mirroring.

Amazon Aurora instances stores copies of the data in a DB cluster across multiple Availability Zones in a single AWS Region, regardless of whether the instances in the DB cluster span multiple Availability Zones.

Hence, the right term used for AWS Aurora is Read Replica for the databases.
AWS Documentation mentions the following:
You can create an Amazon Aurora MySQL DB cluster as a Read Replica in a different AWS Region than the source DB cluster. Taking this approach can improve your disaster recovery capabilities, let you scale read operations into a region that is closer to your users, and make it easier to migrate from one region to another.
For more information on Amazon Aurora Cross-Region Replication, please refer to the URL below.
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/AuroraMySQL.Replication.CrossRegion.html (https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/AuroraMySQL.Replication.CrossRegion.html)

Ask our Experts

QUESTION 7 CORRECT DESIGN COST-OPTIMIZED ARCHITECTURES

Your company has a requirement to host a static web site in AWS. Which of the following steps would help implement a quick and cost-effective solution for this requirement? Choose 2 answers from the options given below. Each answer forms a part of the solution.

- [x] **A.** Upload the static content to an S3 bucket. ✔
- [ ] **B.** Create an EC2 Instance and install a web server.
- [x] **C.** Enable web site hosting for the S3 bucket. ✔
- [ ] **D.** Upload the code to the web server on the EC2 Instance.

Explanation :

Answer – A and C
S3 would be an ideal, cost-effective solution for the above requirement.
AWS Documentation mentions the following on using S3 for static web site hosting:
You can host a static website on Amazon Simple Storage Service (Amazon S3). On a static website, individual webpages include static content. They might also contain client-side scripts.
For more information on static web site hosting using S3, please refer to the URL below.
https://docs.aws.amazon.com/AmazonS3/latest/dev/WebsiteHosting.html
(https://docs.aws.amazon.com/AmazonS3/latest/dev/WebsiteHosting.html)

Ask our Experts

QUESTION 8 CORRECT DESIGN RESILIENT ARCHITECTURES

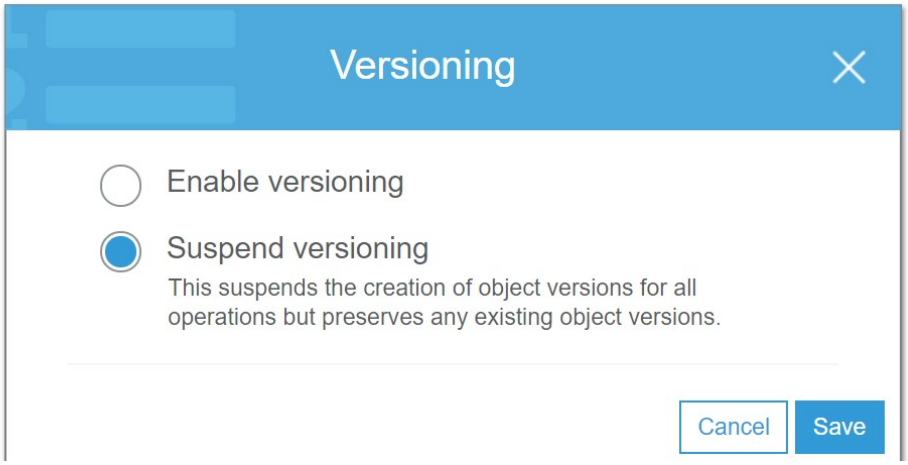
A company currently storing a set of documents in the AWS Simple Storage Service, is worried about the potential loss if these documents are ever deleted. Which of the following can be used to ensure protection from loss of the underlying documents in S3?

- ○ **A.** Enable Versioning for the underlying S3 bucket. ✔
- ○ **B.** Copy the bucket data to an EBS Volume as a backup.
- ○ **C.** Create a Snapshot of the S3 bucket.
- ○ **D.** Enable an IAM Policy which does not allow deletion of any document from the S3 bucket.

Explanation :

Answer - A

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 S3 Versioning, please refer to the below URL:
https://docs.aws.amazon.com/AmazonS3/latest/dev/Versioning.html
(https://docs.aws.amazon.com/AmazonS3/latest/dev/Versioning.html)

Ask our Experts

QUESTION 9 CORRECT DESIGN COST-OPTIMIZED ARCHITECTURES

An application with a 150 GB relational database runs on an EC2 Instance. This application will be used frequently with a high database reads and writes requests. What is the most cost-effective storage type for this application?

- A. Amazon EBS Provisioned IOPS SSD ✔
- B. Amazon EBS Throughput Optimized HDD

- C. Amazon EBS General Purpose SSD
- D. Amazon EFS

Explanation :

Answer – A

The question is focusing on the most cost effective storage option for the application. As per AWS documentation Provisioned IOPS (SSD) are used for applications that require high Inputs/Outputs Operations per sec and is mainly used in large databases such as Mongo, Cassandra, Microsoft SQL Server, MySQL, PostgreSQL, Oracle where as Throughput optimized HDD although it is cheaper compared to PIOPS is used for dataware houses where it is designed to work with throughput intensive workloads such as big data, log processing etc.

So Option A is the right choice for this case.

AWS Documentation mentions the following:

Provisioned IOPS SSD (io1) volumes are designed to meet the needs of I/O-intensive workloads, particularly database workloads that are sensitive to storage performance and consistency.

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

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumes.html (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumes.html)

Note:

as a solutions architect we need to understand the nature of the application and requirement. The question also says that "An application with a 150 GB relational database runs on an EC2 Instance. This application will be used frequently with a lot of database reads and writes."

It also requires high reads and writes, in order to satisfy the application need, we need to go with Provisioned IOPS.

The question also states that the application will be frequently used for heavy read and write operations. So in that case General Purpose SSD won't be able to handle that workload. Hence option A seems to be the right choice.

Ask our Experts

QUESTION 10 CORRECT DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

A company has a set of EC2 Linux based instances hosted in AWS. There is a need to have a standard file interface for files to be used across all Linux based instances. Which of the following can be used for this purpose?

- A. Consider using the Simple Storage Service.
- B. Consider using Amazon Glacier.
- C. Consider using AWS RDS.
- D. Consider using AWS EFS. ✔

Explanation :

Answer - D
AWS Documentation mentions the following:
When mounted on Amazon EC2 instances, an Amazon EFS file system provides a standard file system interface and file system access semantics, allowing you to seamlessly integrate Amazon EFS with your existing applications and tools. Multiple Amazon EC2 instances can access an Amazon EFS file system at the same time, allowing Amazon EFS to provide a common data source for workloads and applications running on more than one Amazon EC2 instance.
For more information on AWS EFS, please visit the following URL:
https://aws.amazon.com/efs/ (https://aws.amazon.com/efs/)

Ask our Experts

QUESTION 11 CORRECT DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

Your company is planning on using Route 53 as the DNS provider. There is a need to ensure that the company's domain name points to an existing CloudFront distribution. How can this be achieved?

- A. Create an Alias record which points to the CloudFront distribution. ✔
- B. Create a host record which points to the CloudFront distribution.
- C. Create a CNAME record which points to the CloudFront distribution.
- D. Create a Non-Alias Record which points to the CloudFront distribution.

Explanation :

Answer - A

AWS Documentation mentions the following:

While ordinary Amazon Route 53 records are standard DNS records, *alias records* provide a Route 53 –specific extension to DNS functionality. Instead of an IP address or a domain name, an alias record contains a pointer to a CloudFront distribution, an Elastic Beanstalk environment, an ELB Classic, Application, or Network Load Balancer, an Amazon S3 bucket that is configured as a static website, or another Route 53 record in the same hosted zone. When Route 53 receives a DNS query that matches the name and type in an alias record, Route 53 follows the pointer and responds with the applicable value.

For more information on Route 53 Alias records, please visit the following URL:

- https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-choosing-alias-non-alias.html (https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-choosing-alias-non-alias.html)

Note:

Route 53 uses "Alias Name" to connect to the CloudFront, reason Alias Record is a Route 53 extension to DNS. Also, alias record is similar to CNAME record, but the main difference is - you can create alias record for both root domain & subdomain, where as CNAME record can be created only to subdomain. Check the below link from Amazon: -

- https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-to-cloudfront-distribution.html (https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-to-cloudfront-distribution.html)

Ask our Experts

QUESTION 12 CORRECT DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

A company needs to extend their storage infrastructure to the AWS Cloud. The storage needs to be available as iSCSI devices for on-premises application servers. Which of the following would be able to fulfill this requirement?

- **A.** Create a Glacier vault. Use a Glacier Connector and mount it as an iSCSI device.
- **B.** Create an S3 bucket. Use an S3 Connector and mount it as an iSCSI device.
- **C.** Use the EFS file service and mount the different file systems to the on-premises servers.
- **D.** Use the AWS Storage Gateway-cached volumes service. ✔

Explanation :

Answer - D

AWS Documentation mentions the following:

By using cached volumes, you can use Amazon S3 as your primary data storage, while retaining frequently accessed data locally in your storage gateway. Cached volumes minimize the need to scale your on-premises storage infrastructure, while still providing your applications with low-latency access to their frequently accessed data. You can create storage volumes up to 32 TiB in size and attach to them as iSCSI devices from your on-premises application servers. Your gateway stores data that you write to these volumes in Amazon S3 and retains recently read data in your on-premises storage gateway's cache and upload buffer storage.

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

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

Ask our Experts

QUESTION 13 CORRECT DEFINE PERFORMANT ARCHITECTURES

Your infrastructure in AWS currently consists of a private and public subnet. The private subnet consists of database servers and the public subnet has a NAT Instance which helps the instances in the private subnet to communicate with the Internet. The NAT Instance is now becoming a bottleneck. Which of the following changes to the current architecture can help prevent this issue from occurring in the future?

- A. Use a NAT Gateway instead of the NAT Instance. ✔
- B. Use another Internet Gateway for better bandwidth.
- C. Use a VPC connection for better bandwidth.
- D. Consider changing the instance type for the underlying NAT Instance.

Explanation :

Answer – A

The NAT Gateway is a managed resource which can be used in place of a NAT Instance. While you can consider changing the instance type for the underlying NAT Instance, this does not guarantee that the issue will not reoccur in the future.

For more information on the NAT Gateway, please visit the following 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 14 CORRECT SPECIFY SECURE APPLICATIONS AND ARCHITECTURES

Your current setup in AWS consists of the following architecture: 2 public subnets, one subnet which has web servers accessed by users across the Internet and another subnet for the database server. Which of the following changes to the architecture adds a better security boundary to the resources hosted in this setup?

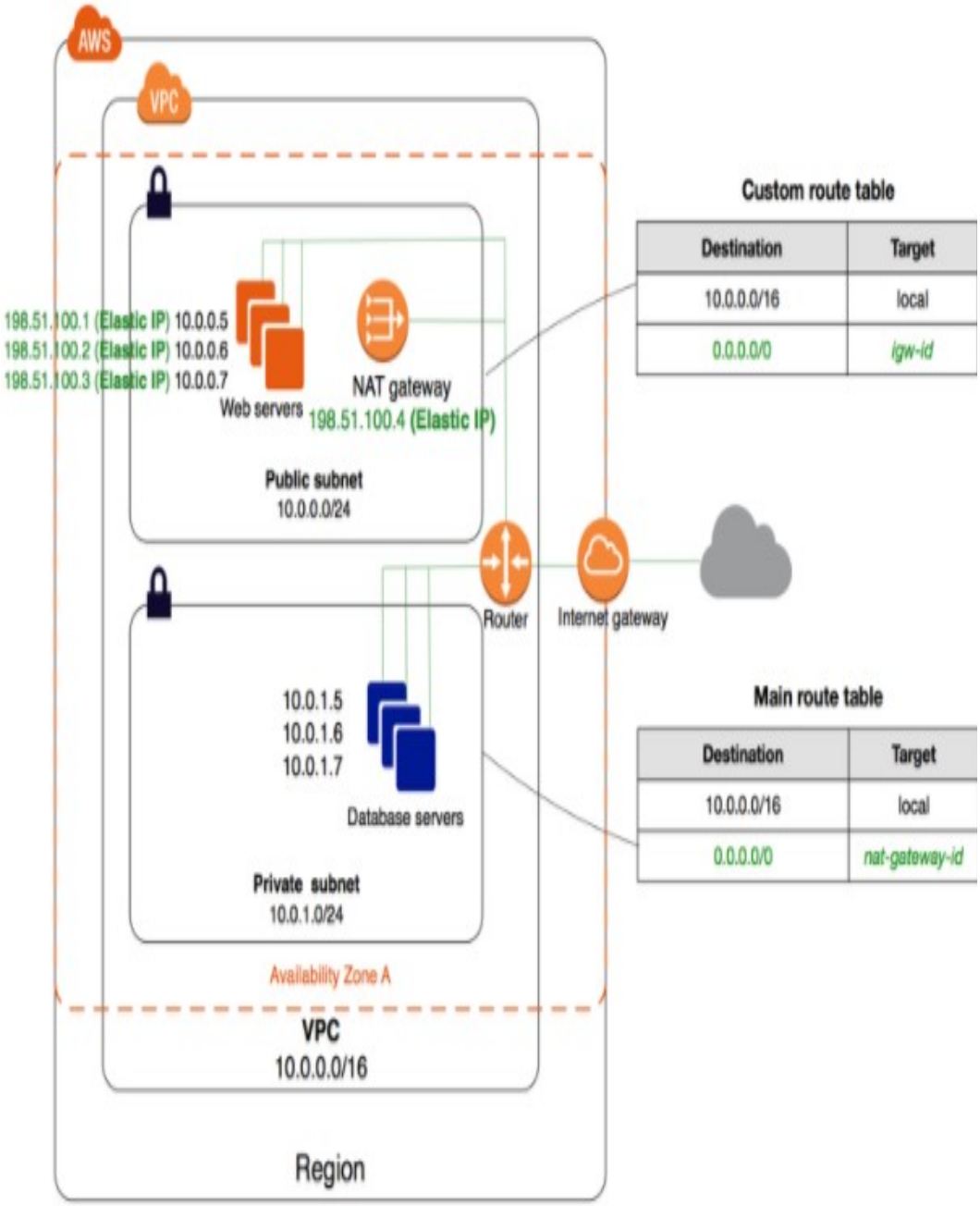
- A. Consider moving the web server to a private subnet.
- B. Create a private subnet and move the database server to a private subnet. ✔
- C. Consider moving both the web and database servers to a private subnet.
- D. Consider creating a private subnet and adding a NAT Instance to that subnet.

Explanation :

Answer – B

The ideal setup is to host the web server in the public subnet so that it can be accessed by users on the Internet. The database server can be hosted in the private subnet.

The below diagram from AWS Documentation shows how this can be set up:



Ask our Experts

QUESTION 15 CORRECT DESIGN RESILIENT ARCHITECTURES

Your company has a set of applications that make use of Docker containers used by the Development team. There is a need to move these containers to AWS. Which of the following methods could be used to set up these Docker containers in a separate environment in AWS?

- A. Create EC2 Instances, install Docker and then upload the containers.
- B. Create EC2 Container registries, install Docker and then upload the containers.
- C. Create an Elastic Beanstalk environment with the necessary Docker containers. ✔
- D. Create EBS Optimized EC2 Instances, install Docker and then upload the containers.

Explanation :

Answer - C

The Elastic Beanstalk service can be used to host Docker containers.

AWS Documentation further mentions the following:

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

For more information on using Elastic Beanstalk for Docker containers, please visit the following URL:

- https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/create_deploy_docker.html (https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/create_deploy_docker.html)

Note:

Option A could be partly correct as we need to install docker on EC2 instance. In addition to this, you need to create an ECS Task definition which details the docker image that we need to use for containers and how many containers to be used as well as the resource allocation for each container.

But with Option C, we have the added advantage that, If a Docker container running in an Elastic Beanstalk environment crashes or is killed for any reason, Elastic Beanstalk restarts it automatically.

In the question we have been asked about the best method to set up docker containers, hence Option C seems o be more appropriate.

More information is available at:

- https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/create_deploy_docker.html (https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/create_deploy_docker.html)
- https://aws.amazon.com/getting-started/tutorials/deploy-docker-containers/ (https://aws.amazon.com/getting-started/tutorials/deploy-docker-containers/)

Ask our Experts

QUESTION 16 CORRECT DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

Instances in your private subnet hosted in AWS, need access to important documents in S3. Due to the confidential nature of these documents, you have to ensure that this traffic does not traverse through the internet. As an architect, how would you you implement this solution?

- A. Consider using a VPC Endpoint. ✔
- B. Consider using an EC2 Endpoint.
- C. Move the instances to a public subnet.
- D. Create a VPN connection and access the S3 resources from the EC2 Instance.

Explanation :

Answer – A
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 services does not leave the Amazon network.
For more information on VPC Endpoints, please visit the following URL:
https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-endpoints.html
(https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-endpoints.html)

Ask our Experts

QUESTION 17 CORRECT DESIGN COST-OPTIMIZED ARCHITECTURES

You have a video transcoding application running on Amazon EC2. Each instance polls a queue to find out which video should be transcoded, and then runs a transcoding process. If this process is interrupted, the video gets transcoded by another instance based on the queuing system. You have a large backlog of videos that need to be transcoded and you would like to reduce this backlog by adding more

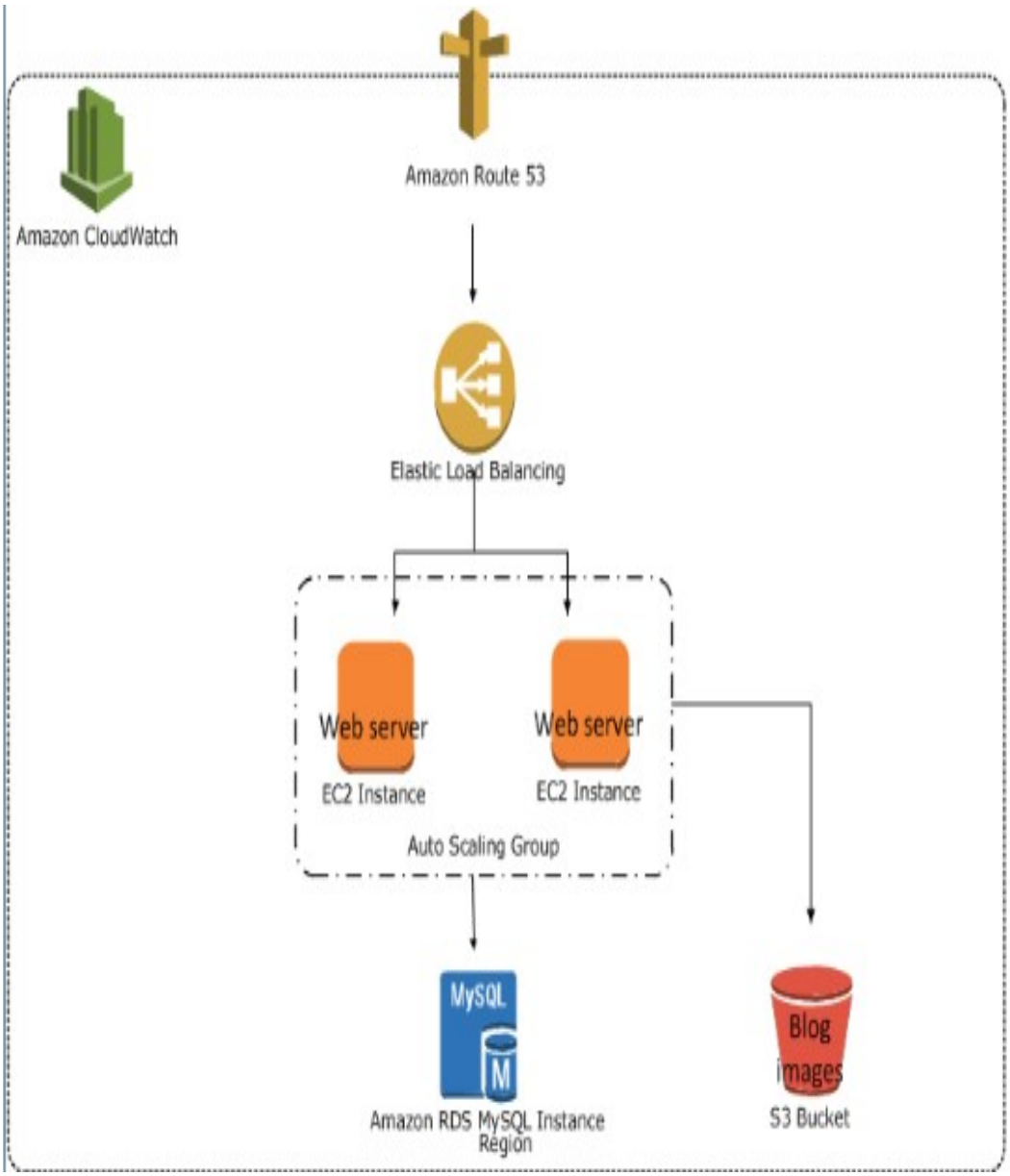
instances. These instances will only be needed until the backlog is reduced. What Amazon EC2 Instance type should you use to reduce the backlog in the most cost-efficient way?

- A. Reserved Instances
- B. Spot Instances ✔
- C. Dedicated Instances
- D. On-Demand Instances

Explanation :

Answer – B

Since the above scenario is similar to a batch processing job, the best instance type to use is a Spot Instance. Spot Instances are normally used in batch processing jobs. Since these jobs don't last for an entire year, they can be bid upon and allocated and deallocated as requested.



Reserved Instances/Dedicated Instances cannot be used since this is not a 100% used application.
There is no mention on a continuous demand of work in the above scenario, hence there is no need to use On-Demand Instances.
For more information on Spot Instances, please visit the following URL:
https://aws.amazon.com/ec2/spot/ (https://aws.amazon.com/ec2/spot/)

Ask our Experts

QUESTION 18 CORRECT DEFINE PERFORMANT ARCHITECTURES

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

- A. SQS guarantees the order of the messages.
- B. SQS synchronously provides transcoding output.
- C. SQS checks the health of the worker instances.
- D. SQS helps to facilitate horizontal scaling of encoding tasks. ✔

Explanation :

Answer - D
Even though SQS guarantees the order of messages for FIFO queues, the main reason for using it is because it helps in horizontal scaling of AWS resources and is used for decoupling systems.
SQS can neither be used for transcoding output nor for checking the health of worker instances. The health of worker instances can be checked via ELB or CloudWatch.
For more information on SQS, please visit the following URL:
https://aws.amazon.com/sqs/faqs/ (https://aws.amazon.com/sqs/faqs/)

Ask our Experts

QUESTION 19 CORRECT DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

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

- A. Remove public read access and use signed URLs with expiry dates. ✔
- B. Use CloudFront distributions for static content.
- C. Block the IPs of the offending websites in Security Groups.
- D. Store photos on an EBS Volume of the web server.

Explanation :

Answer – A

Option B is incorrect, because CloudFront is only used for the distribution of content across edge or region locations, and not for restricting access to content.

Option C is not feasible. Because of their dynamic nature, blocking IPs is challenging and you will not know which sites are accessing your main site.

Option D is incorrect since storing photos on an EBS Volume is neither a good practice nor an ideal architectural approach for an AWS Solutions Architect.

For more information on Pre-Signed URLs, please visit the following URL:

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

Ask our Experts

QUESTION 20 CORRECT DESIGN RESILIENT ARCHITECTURES

A company wants to create standard templates for deployment of their Infrastructure. These would also be used to provision resources in another region during disaster recovery scenarios. Which AWS service can be used in this regard?

- A. Amazon Simple Workflow Service
- B. AWS Elastic Beanstalk
- C. AWS CloudFormation ✔
- D. AWS OpsWorks

Explanation :

Answer – C

AWS CloudFormation gives developers and systems administrators an easy way to create and manage a collection of related AWS resources, provisioning and updating them in an orderly and predictable fashion.

You can use AWS CloudFormation's sample templates (https://aws.amazon.com/cloudformation/aws-cloudformation-templates/) or create your own templates to describe the AWS resources, and any associated dependencies or runtime parameters, required to run your application. You don't need to figure out the order for provisioning AWS services or the subtleties of making those dependencies work. CloudFormation takes care of this for you. After the AWS resources are deployed, you can modify and update them in a controlled and predictable way, in effect applying version control to your AWS infrastructure the same way you do with your software. You can also visualize your templates as diagrams and edit them using a drag-and-drop interface with the AWS CloudFormation Designer (https://aws.amazon.com/cloudformation/details/#designer).

For more information on AWS CloudFormation, please visit the following URL:
https://aws.amazon.com/cloudformation/ (https://aws.amazon.com/cloudformation/)

Ask our Experts

QUESTION 21 CORRECT DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

A company currently hosts their architecture in the US region. They now need to duplicate this architecture to the Europe region and extend the application hosted on this architecture to the new region. In order to ensure that users across the globe get the same seamless experience from either setups, what among the following needs to be done?

- **A.** Create a Classic Elastic Load Balancer setup to route traffic to both locations.
- **B.** Create a weighted Route 53 policy to route the policy based on the weightage for eachlocation.
- **C.** Create an Application Elastic Load Balancer setup to route traffic to bothlocations.
- **D.** Create a Geolocation Route 53 Policy to route the policy based on the location. ✔

Explanation :

Answer - D
AWS Documentation mentions the following with respect to this requirement:
Geolocation routing lets you choose the resources that serve your traffic based on the geographic location of your users, meaning the location that DNS queries originate from.
For more information on AWS Route 53 Routing Policies, please visit the following URL:
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html
(https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html)

Ask our Experts

QUESTION 22 CORRECT DESIGN RESILIENT ARCHITECTURES

You have a set of EC2 Instances that support an application. They are currently hosted in the US Region. In the event of a disaster, you need a way to ensure that you can quickly provision the resources in another region. How could this be accomplished? Choose 2 answers from the options given below.

- [ ] **A.** Copy the underlying EBS Volumes to the destination region.
- [x] **B.** Create EBS Snapshots and then copy them to the destination region. ✔
- [x] **C.** Create AMIs for the underlying instances. ✔
- [ ] **D.** Copy the metadata for the EC2 Instances to S3.

Explanation :

Answer – B and C
AMIs can be used to create a snapshot or template of the underlying instance. You can then copy the AMI to another region. You can also make snapshots of the volumes and then copy them to the destination region.
For more information on AMIs and EBS Snapshots, please visit the following URLs:

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

Ask our Experts

QUESTION 23 CORRECT DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

A company wants to have a NoSQL database hosted on the AWS Cloud, but do not have the necessary staff to manage the underlying infrastructure. Which of the following choices would be ideal for this requirement?

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

Explanation :

Answer – C
AWS Documentation mentions the following:
Amazon DynamoDB is a fully managed NoSQL database service that provides fast and predictable performance with seamless scalability. DynamoDB lets you offload the administrative burdens of operating and scaling a distributed database, so that you don't have to worry about hardware provisioning, setup and configuration, replication, software patching, or cluster scaling.
For more information on AWS DynamoDB, please visit the following URL:
https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Introduction.html (https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Introduction.html)

Ask our Experts

QUESTION 24 CORRECT DESIGN COST-OPTIMIZED ARCHITECTURES

You are building an automated transcription service in which Amazon EC2 worker instances process an uploaded audio file and generate a text file. You must store both of these files in the same durable storage until the text file is retrieved. You do not know what the storage capacity requirements are. Which storage option is both cost-efficient and scalable?

- A. Multiple Amazon EBS Volume with snapshots
- B. A single Amazon Glacier Vault
- C. A single Amazon S3 bucket ✔
- D. Multiple instance stores

Explanation :

Answer – C
Amazon S3 is the perfect storage solution for audio and text files. It is a highly available and durable storage device.
For more information on Amazon S3, please visit the following URL:
https://aws.amazon.com/s3/ (https://aws.amazon.com/s3/)

Ask our Experts

QUESTION 25 MARKED AS REVIEW CORRECT
DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

A customer has an instance hosted in the AWS Public Cloud. The VPC and subnet used to host the instance have been created with the default settings for the Network Access Control Lists. An IT Administrator needs to be provided secure access to the underlying instance. How can this be accomplished?

- A. Ensurethe Network Access Control Lists allow Inbound SSH traffic from the ITAdministrator's Workstation.
- B. Ensurethe Network Access Control Lists allow Outbound SSH traffic from the ITAdministrator's Workstation.
- C. Ensurethat the security group allows Inbound SSH traffic from the IT Administrator'sWorkstation. ✔
- D. Ensurethat the security group allows Outbound SSH traffic from the IT Administrator'sWorkstation.

Explanation :

Answer - C
Ensure that the security group allows Inbound SSH traffic from the IT Administrator's Workstation. Since Security groups are stateful, we do not have to configure outbound traffic. What enters the inbound traffic is allowed in the outbound traffic too.
Note: The default network ACL is configured to allow all traffic to flow in and out of the subnets to which it is associated. Since the question does not mention that it is a custom VPC we would assume it to be the default one.

Based on that Option C is the correct answer.
Since the IT administrator need to be provided ssh access to the instance. The traffic would be inbound to the instance. Security group being stateful means that return response to the allowed inbound request will be allowed and vice-versa.

Allowing the outbound traffic would mean that instance would ssh into the IT admin's server and this server will send the response to the instance but it does not mean that IT admin would also be able to ssh into instance. SSh does not work like that.

To allow ssh you need to allow inbound ssh access over port 22 you can refer this:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/authorizing-access-to-an-instance.html (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/authorizing-access-to-an-instance.html)

Prerequisites for ssh

Before you connect to your Linux instance, complete the following prerequisites:

- **Install an SSH client**

  Your Linux computer most likely includes an SSH client by default. You can check for an SSH client by typing **ssh** at the command line. If your computer doesn't recognize the command, the OpenSSH project provides a free implementation of the full suite of SSH tools. For more information, see http://www.openssh.com (http://www.openssh.com/).

- **Install the AWS CLI Tools**

  (Optional) If you're using a public AMI from a third party, you can use the command line tools to verify the fingerprint. For more information about installing the AWS CLI, see Getting Set Up (https://docs.aws.amazon.com/cli/latest/userguide/cli-chap-getting-set-up.html) in the *AWS Command Line Interface User Guide*.

- **Get the ID of the instance**

  You can get the ID of your instance using the Amazon EC2 console (from the **Instance ID** column). If you prefer, you can use the describe-instances (https://docs.aws.amazon.com/cli/latest/reference/ec2/describe-instances.html) (AWS CLI) or Get-EC2Instance (https://docs.aws.amazon.com/powershell/latest/reference/items/Get-EC2Instance.html) (AWS Tools for Windows PowerShell) command.

- **Get the public DNS name of the instance**

  You can get the public DNS for your instance using the Amazon EC2 console. Check the **Public DNS (IPv4)** column. If this column is hidden, choose the **Show/Hide** icon and select **Public DNS (IPv4)**. If you prefer, you can use the describe-instances (https://docs.aws.amazon.com/cli/latest/reference/ec2/describe-instances.html) (AWS CLI) or Get-EC2Instance (https://docs.aws.amazon.com/powershell/latest/reference/items/Get-EC2Instance.html)(AWS Tools for Windows PowerShell) command.

- **(IPv6 only) Get the IPv6 address of the instance**

  If you've assigned an IPv6 address to your instance, you can optionally connect to the instance using its IPv6 address instead of a public IPv4 address or public IPv4 DNS hostname. Your local computer must have an IPv6 address and must be configured to use IPv6. You can get the IPv6 address of your instance using the Amazon EC2 console. Check the **IPv6 IPs**field. If you prefer, you can use the describe-instances (https://docs.aws.amazon.com/cli/latest/reference/ec2/describe-instances.html) (AWS CLI) or Get-EC2Instance (https://docs.aws.amazon.com/powershell/latest/reference/items/Get-EC2Instance.html) (AWS Tools for Windows PowerShell) command. For more information about IPv6, see IPv6 Addresses (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-instance-addressing.html#ipv6-addressing).

- **Locate the private key and verify permissions**

Get the fully-qualified path to the location on your computer of the `.pem` file for the key pair that you specified when you launched the instance. Verify that the `.pem` file has permissions of 0400, not 0777. For more information, see Error: Unprotected Private Key File (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/TroubleshootingInstancesConnecting.html#troublesh unprotected-key).

- **Get the default user name for the AMI that you used to launch your instance**
  - For Amazon Linux 2 or the Amazon Linux AMI, the user name is `ec2-user`.
  - For a Centos AMI, the user name is `centos`.
  - For a Debian AMI, the user name is `admin` or `root`.
  - For a Fedora AMI, the user name is `ec2-user` or `fedora`.
  - For a RHEL AMI, the user name is `ec2-user` or `root`.
  - For a SUSE AMI, the user name is `ec2-user` or `root`.
  - For an Ubuntu AMI, the user name is `ubuntu`.
  - Otherwise, if `ec2-user` and `root` don't work, check with the AMI provider.
- **Enable inbound SSH traffic from your IP address to your instance**

  Ensure that the security group associated with your instance allows incoming SSH traffic from your IP address. The default security group for the VPC does not allow incoming SSH traffic by default. The security group created by the launch wizard enables SSH traffic by default. For more information, see Authorizing Inbound Traffic for Your Linux Instances (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/authorizing-access-to-an-instance.html).

Ask our Experts

QUESTION 26 CORRECT DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

A company has an on-premises infrastructure which they want to extend to the AWS Cloud. There is a need to ensure that communication across both environments is possible over the Internet. What would you create in this case to fulfill this requirement?

- **A.** Create a VPC peering connection between the on-premises and the AWS Environment.
- **B.** Create an AWS Direct connection between the on-premises and the AWS Environment.
- **C.** Create a VPN connection between the on-premises and the AWS Environment. ✔
- **D.** Create a Virtual private gateway connection between the on-premises and the AWS Environment.

Explanation :

Answer - C
AWS Documentation mentions the following:
One can create a Virtual private connection to establish communication across both environments over the Internet.
For more information on Virtual private connection, please visit the following URL:

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

Option A is invalid because A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. It is not used for connection between on-premise environment and AWS.

Option D is invalid because A virtual private gateway is the Amazon VPC side of a VPN connection. For the communication to take place between the on-premise servers to AWS EC2 instances with in the VPC, we need to set up the customer gateway at the on-premise location.

Note: The question says that "There is a need to ensure that communication across both environments is possible **over the Internet.**" AWS Direct Connect does not involve the Internet.

A VPC VPN Connection utilizes IPSec to establish encrypted network connectivity between your intranet and Amazon VPC over the Internet. VPN Connections can be configured in minutes and are a good solution if you have an immediate need, have low to modest bandwidth requirements, and can tolerate the inherent variability in Internet-based connectivity. **AWS Direct Connect does not involve the Internet;** instead, it uses dedicated, private network connections between your intranet and Amazon VPC.

Ask our Experts

A company wants to build a brand new application on the AWS Cloud. They want to ensure that this application follows the Microservices architecture. Which of the following services can be used to build this sort of architecture? Choose 3 answers from the options given below.

- [x] **A.** AWS Lambda ✔
- [x] **B.** AWS ECS ✔
- [x] **C.** AWS API Gateway ✔
- [ ] **D.** AWS Config

Explanation :

Answer – A, B and C
AWS Lambda is a serverless compute service that allows you to build independent services.
The Elastic Container service (ECS) can be used to manage containers.
The API Gateway is a serverless component for managing access to APIs.
For more information about Microservices on AWS, please visit the following URL:
https://aws.amazon.com/microservices/ (https://aws.amazon.com/microservices/)

Ask our Experts

QUESTION 28 CORRECT DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

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

- ○ **A.** Amazon Kinesis ✔
- ○ **B.** AWS Data Pipeline
- ○ **C.** Amazon AppStream

D. Amazon Simple Queue Service

Explanation :

Answer - A
AWS Documentation mentions the following:
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. Amazon Kinesis enables you to process and analyze data as it arrives and respond instantly instead of having to wait until all your data is collected before the processing can begin.
For more information on Amazon Kinesis, please visit the following URL:
https://aws.amazon.com/kinesis/ (https://aws.amazon.com/kinesis/)

Ask our Experts

QUESTION 29 CORRECT DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

A company is planning on hosting a set of EC2 Instances on the AWS Cloud. They also need to ensure that data can be stored on the EC2 Instances. Which block level storage device could make this possible?

A. Amazon S3
B. Amazon Glacier
C. Amazon Storage Gateway
D. Amazon EBS Volumes ✔

Explanation :

Answer - D
AWS Documentation mentions the following:
An Amazon EBS Volume is a durable, block-level storage device that you can attach to a single EC2 instance. You can use EBS Volumes as primary storage for data that requires frequent updates, such as the system drive for an instance or storage for a database application. You can also use them for throughput-intensive applications that perform continuous disk scans.
For more information on Amazon EBS Volumes, please visit the following URL:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumes.html
(https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumes.html)

Ask our Experts

QUESTION 30 CORRECT DESIGN COST-OPTIMIZED ARCHITECTURES

A company is planning on using the AWS Redshift service. The Redshift service and data on it would be used continuously for the next 3 years as per the current business plan. Which of the following would be the most cost-effective solution in this scenario?

- A. Consider using On-demand instances for the Redshift Cluster.
- B. Enable Automated backup.
- C. Consider using Reserved Instances for the Redshift Cluster. ✔
- D. Consider not using a cluster for the Redshift nodes.

Explanation :

Answer - C
AWS Documentation mentions the following:
If you intend to keep your Amazon Redshift cluster running continuously for a prolonged period, you should consider purchasing reserved node offerings. These offerings provide significant savings over on-demand pricing, but they require you to reserve compute nodes and commit to paying for those nodes for either a one-year or three-year duration.
For more information on Reserved Nodes in Redshift, please visit the following URL:
https://docs.aws.amazon.com/redshift/latest/mgmt/purchase-reserved-node-instance.html
(https://docs.aws.amazon.com/redshift/latest/mgmt/purchase-reserved-node-instance.html)

Ask our Experts

QUESTION 31 CORRECT DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

A company is planning to run a number of Admin related scripts using the AWS Lambda service. There is a need to detect errors that occur while the scripts run. How can this be accomplished in the most effective manner?

- A. Use CloudWatch metrics and logs to watch for errors. ✔
- B. Use CloudTrail to monitor for errors.
- C. Use the AWS Config service to monitor for errors.
- D. Use the AWS Inspector service to monitor for errors.

Explanation :

Answer – A
AWS Documentation mentions the following:
AWS Lambda automatically monitors Lambda functions on your behalf, reporting metrics through Amazon CloudWatch. To help you troubleshoot failures in a function, Lambda logs all requests handled by your function and also automatically stores logs generated by your code through Amazon CloudWatch Logs.
For more information on Monitoring Lambda functions, please visit the following URL:
https://docs.aws.amazon.com/lambda/latest/dg/monitoring-functions-logs.html
(https://docs.aws.amazon.com/lambda/latest/dg/monitoring-functions-logs.html)

Ask our Experts

QUESTION 32 CORRECT SPECIFY SECURE APPLICATIONS AND ARCHITECTURES

A CloudFront distribution is being used to distribute content from an S3 bucket. It is required that only a particular set of users get access to certain content. How can this be accomplished?

- A. Create IAM Users for each user and then provide access to the S3 bucket content.
- B. Create IAM Groups for each set of users and then provide access to the S3 bucketcontent.
- C. Create CloudFront signed URLs and then distribute these URLs to the users. ✔
- D. Use IAM Polices for the underlying S3 buckets to restrict content.

Explanation :

Answer - C
AWS Documentation mentions the following:
Many companies that distribute content via the internet want to restrict access to documents, business data, media streams, or content that is intended for selected users, for example, users who have paid a fee. To securely serve this private content using CloudFront, you can do the following:

- Require that your users access your private content by using special CloudFront signed URLs or signed cookies.
- Require that your users access your Amazon S3 content using CloudFront URLs, not Amazon S3 URLs. Requiring CloudFront URLs isn't required, but we recommend it to prevent users from bypassing the restrictions that you specify in signed URLs or signed cookies.

For more information on serving private content via CloudFront, please visit the following URL:
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/PrivateContent.html#
(https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/PrivateContent.html)

Ask our Experts

QUESTION 33 CORRECT DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

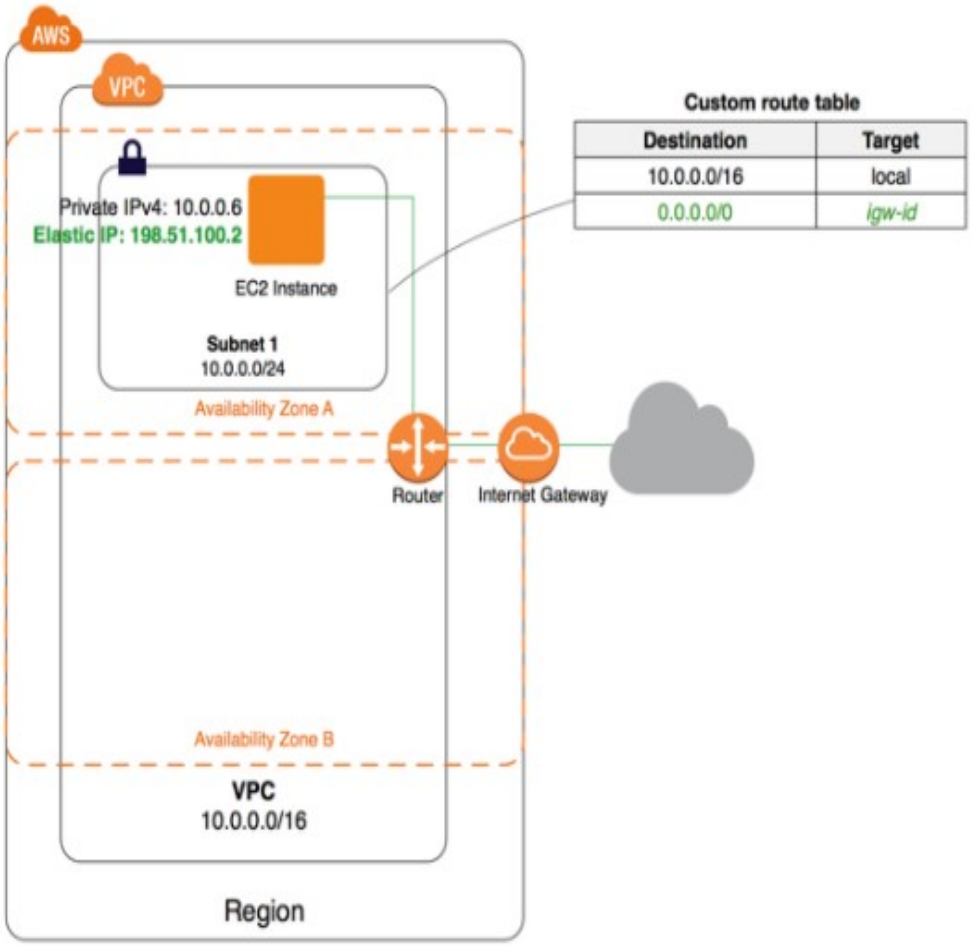
You plan on creating a VPC from scratch and launching EC2 Instances in the subnet. What should be done to ensure that the EC2 Instances are accessible from the Internet?

- **A.** Attach an Internet Gateway to the VPC and add a route for 0.0.0.0/0 to the Route table. ✔
- **B.** Attach an NAT Gateway to the VPC and add a route for 0.0.0.0/0 to the Route table.
- **C.** Attach an NAT Gateway to the VPC and add a route for 0.0.0.0/32 to the Route table.
- **D.** Attach an Internet Gateway to the VPC and add a route for 0.0.0.0/32 to the Routetable.

Explanation :

Answer - A

The below diagram shows the Internet Gateway and the Route table:



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 34 CORRECT DEFINE PERFORMANT ARCHITECTURES

Your company currently has an entire data warehouse of assets that needs to be migrated to the AWS Cloud. Which of the following services should this be migrated to?

- **A.** AWS DynamoDB

- B. AWS S3
- C. AWS RDS
- D. AWS Redshift ✔

Explanation :

Answer – D
AWS Documentation mentions the following:
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.
For more information on AWS Redshift, please visit the following URL:
https://docs.aws.amazon.com/redshift/latest/mgmt/welcome.html
(https://docs.aws.amazon.com/redshift/latest/mgmt/welcome.html)

Ask our Experts

QUESTION 35 CORRECT DESIGN RESILIENT ARCHITECTURES

Your company has confidential documents stored in the Simple Storage Service. Due to compliance requirements, there is a need for the data in the S3 bucket to be available in a different geographical location. As an architect, what change would you make to comply with this requirement?

- A. Apply Multi-AZ for the underlying S3 bucket.
- B. Copy the data to an EBS Volume in another region.
- C. Create a snapshot of the S3 bucket and copy it to another region.
- D. Enable Cross-Region Replication for the S3 bucket. ✔

Explanation :

Answer – D
This is mentioned clearly as a use case for S3 Cross-Region Replication.
You might configure Cross-Region Replication on a bucket for various reasons, including the following:

- Compliance requirements – Although, by default, Amazon S3 stores your data across multiple geographically distant Availability Zones, compliance requirements might dictate that you store data at

even further distances. Cross-region replication allows you to replicate data between distant AWS Regions to satisfy these compliance requirements.

For more information on S3 Cross-Region Replication, please visit the following URL:
https://docs.aws.amazon.com/AmazonS3/latest/dev/crr.html
(https://docs.aws.amazon.com/AmazonS3/latest/dev/crr.html)

Ask our Experts

QUESTION 36 CORRECT DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

A company's requirement is to have a Stack-based model for its resources in AWS. There is a need to have different stacks for the Development and Production environments. Which of the following can be used to fulfill this required methodology?

- A. Use EC2 tags to define different stack layers for your resources.
- B. Define the metadata for the different layers in DynamoDB.
- C. Use AWS OpsWorks to define the different layers for your application. ✔
- D. Use AWS Config to define the different layers for your application.

Explanation :

Answer - C
The requirement can be fulfilled via the OpsWorks service. The AWS Documentation given below supports this requirement:
AWS OpsWorks Stacks lets you manage applications and servers on AWS and on-premises. With OpsWorks Stacks, you can model your application as a stack containing different layers, such as load balancing, database, and application server. You can deploy and configure Amazon EC2 instances in each layer or connect other resources such as Amazon RDS databases.
For more information on OpsWorks stacks, please visit the following URL:

- https://aws.amazon.com/opsworks/stacks/ (https://aws.amazon.com/opsworks/stacks/)

A stack is basically a collection of instances that are managed together for serving a common task.

Consider a sample stack whose purpose is to serve web applications. It will be comprised of the following instances.

- A set of application server instances, each of which handles a portion of the incoming traffic.
- A load balancer instance, which takes incoming traffic and distributes it across the application servers.

- A database instance, which serves as a back-end data store for the application servers.

A common practice is to have multiple stacks that represent different environments. A typical set of stacks consists of:

- A development stack to be used by developers to add features, fix bugs, and perform other development and maintenance tasks.
- A staging stack to verify updates or fixes before exposing them publicly.
- A production stack, which is the public-facing version that handles incoming requests from users.

For more information, please see the link given below:

- https://docs.aws.amazon.com/opsworks/latest/userguide/workingstacks.html (https://docs.aws.amazon.com/opsworks/latest/userguide/workingstacks.html)

Ask our Experts

QUESTION 37 INCORRECT DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

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

- **A.** Use Multipart upload.
- **B.** Add a random prefix to the key names. ✖
- **C.** Amazon S3 will automatically manage performance at this scale. ✔
- **D.** Use a predictable naming scheme, such as sequential numbers or date time sequences in the key names.

Explanation :

Answer – C
##############################

Request Rate and Performance Guidelines

Amazon S3 automatically scales to high request rates. For example, your application can achieve at least 3,500 PUT/POST/DELETE and 5,500 GET requests per second per prefix in a bucket. There are no limits to the number of prefixes in a bucket. It is simple to increase your read or write performance exponentially. For example, if you create 10 prefixes in an Amazon S3 bucket to parallelize reads, you could scale your read performance to 55,000 read requests per second.
##############################
Please refere to the below AWS docs for more infromation:

- **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)**

Ask our Experts

QUESTION 38 CORRECT DEFINE PERFORMANT ARCHITECTURES

An infrastructure is being hosted in AWS using the following resources:

a) A couple of EC2 Instances serving a Web-Based application

b) An Elastic Load Balancer in front of the EC2 Instances

c) An AWS RDS which has Multi-AZ enabled

Which of the following can be added to the setup to ensure scalability?

- **A.** Add another ELB to the setup.
- **B.** Add more EC2 Instances to the setup.
- **C.** Enable Read Replicas for the AWS RDS.

D. Add an Auto Scaling Group to the setup. ✔

Explanation :

Answer – D
AWS Documentation mentions the following:
AWS Auto Scaling enables you to configure automatic scaling for the scalable AWS resources for your application in a matter of minutes. AWS Auto Scaling uses the Auto Scaling and Application Auto Scaling services to configure scaling policies for your scalable AWS resources.
For more information on AWS Auto Scaling, please visit the URL below.
https://docs.aws.amazon.com/autoscaling/plans/userguide/what-is-aws-auto-scaling.html
(https://docs.aws.amazon.com/autoscaling/plans/userguide/what-is-aws-auto-scaling.html)

Ask our Experts

QUESTION 39 CORRECT DEFINE PERFORMANT ARCHITECTURES

A company wants to store their documents in AWS. Initially, these documents will be used frequently, and after a duration of 6 months, they will need to be archived. How would you architect this requirement?

A. Store the files in Amazon EBS and create a Lifecycle Policy to remove the files after 6 months.

B. Store the files in Amazon S3 and create a Lifecycle Policy to archive the files after 6 months. ✔

C. Store the files in Amazon Glacier and create a Lifecycle Policy to remove the files after 6 months.

D. Store the files in Amazon EFS and create a Lifecycle Policy to remove the files after 6 months.

Explanation :

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

- Transition actions – In which you define when objects transition to another storage class (http://docs.aws.amazon.com/AmazonS3/latest/dev/storage-class-intro.html). For example, you may choose to transition objects to the STANDARD_IA (IA, for infrequent access) storage class 30 days after creation, or archive objects to the GLACIER storage class one year after creation.

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

For more information on AWS S3 Lifecycle Policies, please visit the following URL:
https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html
(https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html)

Ask our Experts

QUESTION 40 CORRECT SPECIFY SECURE APPLICATIONS AND ARCHITECTURES

When managing permissions for the API Gateway, what can be used to ensure that the right level of permissions are given to Developers, IT Admins and users? These permissions should be easily managed.

- A. Use the secure token service to manage the permissions for different users.
- B. Use IAM Policies to create different policies for different types of users. ✔
- C. Use the AWS Config tool to manage the permissions for different users.
- D. Use IAM Access Keys to create sets of keys for different types of users.

Explanation :

Answer – B
AWS Documentation mentions the following:
You control access to Amazon API Gateway with IAM permissions
(http://docs.aws.amazon.com/IAM/latest/UserGuide/access_permissions.html) by controlling access to the following two API Gateway component processes:

- To create, deploy, and manage an API in API Gateway, you must grant the API developer permissions to perform the required actions supported by the API management component of API Gateway.
- To call a deployed API or to refresh the API caching, you must grant the API caller permissions to perform required IAM actions supported by the API execution component of API Gateway.

For more information on permissions with the API Gateway, please visit the following URL:
https://docs.aws.amazon.com/apigateway/latest/developerguide/permissions.html
(https://docs.aws.amazon.com/apigateway/latest/developerguide/permissions.html)

Ask our Experts

QUESTION 41 CORRECT DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

Your Development team wants to start making use of EC2 Instances to host their Application and Web servers. In the space of automation, they want the Instances to always download the latest version of the Web and Application servers when they are launched. As an architect, what would you recommend for this scenario?

- **A.** Ask the Development team to create scripts which can be added to the User Data section when the instance is launched. ✔
- **B.** Ask the Development team to create scripts which can be added to the Meta Data section when the instance is launched.
- **C.** Use Auto Scaling Groups to install the Web and Application servers when the instances are launched.
- **D.** Use EC2 Config to install the Web and Application servers when the instances are launched.

Explanation :

Answer - A
AWS Documentation mentions the following:
When you launch an instance in Amazon EC2, you have the option of passing user data to the instance that can be used to perform common automated configuration tasks and even run scripts after the instance starts. You can pass two types of user data to Amazon EC2: shell scripts and cloud-init directives. You can also pass this data into the launch wizard as plain text, as a file (this is useful for launching instances using the command line tools), or as base64-encoded text (for API calls).
For more information on User Data, please visit the following URL:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/user-data.html
(https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/user-data.html)

Ask our Experts

QUESTION 42 CORRECT DEFINE PERFORMANT ARCHITECTURES

Your company has an application that takes care of uploading, processing and publishing videos posted by users. The current architecture for this application includes the following:

a) A set of EC2 Instances to transfer user uploaded videos to S3 buckets

b) A set of EC2 worker processes to process and publish the videos

c) An Auto Scaling Group for the EC2 worker processes

Which of the following can be added to the architecture to make it more reliable?

- A. Amazon SQS ✔
- B. Amazon SNS
- C. Amazon CloudFront
- D. Amazon SES

Explanation :

Answer - A
Amazon SQS is used to decouple systems. It can store requests to process videos to be picked up by the worker processes.
AWS Documentation mentions the following:
Amazon Simple Queue Service (Amazon SQS) offers a reliable, highly scalable hosted queue for storing messages as they travel between applications or microservices. It moves data between distributed application components and helps you decouple these components.
For more information on AWS SQS, please visit the following URL:
https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/Welcome.html
(https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/Welcome.html)

Ask our Experts

QUESTION 43 CORRECT DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

There is an urgent requirement to monitor some database metrics for a database hosted on AWS and send notifications. Which AWS services can accomplish this? Choose 2 answers from the options given below.

- [ ] **A.** Amazon Simple Email Service
- [x] **B.** Amazon CloudWatch ✔
- [ ] **C.** Amazon Simple Queue Service
- [ ] **D.** Amazon Route 53
- [x] **E.** Amazon Simple Notification Service ✔

Explanation :

Answer – B and E
Amazon CloudWatch will be used to monitor the IOPS metrics from the RDS Instance and Amazon Simple Notification Service will be used to send the notification if any alarm is triggered.
For more information on CloudWatch and SNS, please visit the URLs below.

https://aws.amazon.com/cloudwatch/ (https://aws.amazon.com/cloudwatch/)
https://aws.amazon.com/sns/ (https://aws.amazon.com/sns/)

Ask our Experts

QUESTION 44 CORRECT DESIGN RESILIENT ARCHITECTURES

You have a business-critical two-tier web application currently deployed in 2 Availability Zones in a single region, using Elastic Load Balancing and Auto Scaling. The app depends on synchronous replication at the database layer. The application needs to remain fully available even if one application AZ goes offline and if Auto Scaling cannot launch new instances in the remaining AZ. How can the current architecture be enhanced to ensure this?

- ○ **A.** Deploy in 2 regions using Weighted Round Robin with Auto Scaling minimums set at 50%peak load per region.

- **B.** Deploy in 3 AZ with Auto Scaling minimum set to handle 33 percent peak load per zone.
- **C.** Deploy in 3 AZ with Auto Scaling minimum set to handle 50 percent peak load per zone. ✔
- **D.** Deploy in 2 regions using Weighted Round Robin with Auto Scaling minimums set at 100%peak load per region.

Explanation :

Answer – C
Since the requirement states that the application should never go down even if an AZ is not available, we need to maintain 100% availability.
Options A and D are incorrect because region deployment is not possible for ELB. ELBs can manage traffic within a region and not between regions.
Option B is incorrect because even if one AZ goes down, we would be operating at only 66% and not the required 100%.
For more information on Auto Scaling, please visit the below URL:
https://aws.amazon.com/autoscaling/ (https://aws.amazon.com/autoscaling/)
NOTE:
In the question, it clearly mentioned that " The application needs to remain fully available even if one application AZ goes offline and if Auto Scaling cannot launch new instances in the remaining AZ."

Here you need to maintain 100% availability.

In option B, when you create 3 AZs with minimum 33% load on each, If any failure occurs in one AZ then

33% + 33% =66% . Here you can handle only 66% and remaining 34% of load not handeling.

But when you select option C, when you create 3 AZs with minimum 50% load on each, If any failure occurs in one AZ then

50% + 50% =100% . Here you can handle full load i.e 100%.

Ask our Experts

QUESTION 45 CORRECT DESIGN RESILIENT ARCHITECTURES

You have been tasked with creating a VPC network topology for your company. The VPC network must support both internet-facing applications and internal-facing applications accessed only over VPN. Both Internet-facing and internal-facing

applications must be able to leverage at least 3 AZs for high availability. At a minimum, how many subnets must you create within your VPC to accommodate these requirements?

- A. 2
- B. 3
- C. 4
- D. 6 ✔

Explanation :

Answer - D

Since each subnet corresponds to one Availability Zone and you need 3 AZs for both the internet and intranet applications, you will need 6 subnets.

For more information on VPC and subnets, please visit the below URL:

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html (http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html)

Ask our Experts

QUESTION 46 CORRECT DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

You have the following architecture deployed in AWS:

a) A set of EC2 Instances which sit behind an ELB

b) A database hosted in AWS RDS

Of late, the performance on the database has been slacking due to a high number of read requests. Which of the following can be added to the architecture to alleviate the performance issue? Please select 2 correct options.

- [x] A. Add read replica to the primary database to offload read traffic. ✔
- [x] B. Use ElastiCache in front of the database. ✔
- [ ] C. Use AWS CloudFront in front of the database.

☐ **D.** Use DynamoDB to offload all the reads. Populate the common read items in a separatetable.

Explanation :

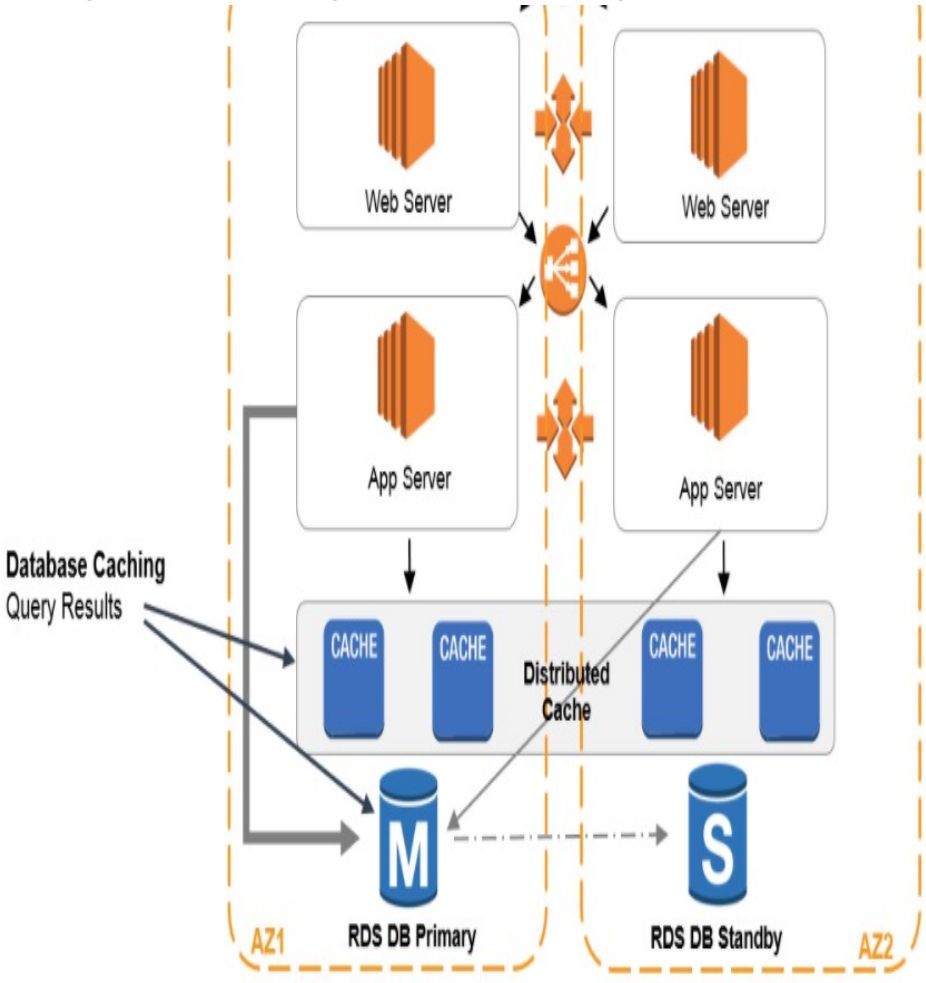
Answer - A and B

Option A is correct.

AWS says "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."

Amazon ElastiCache is an in-memory cache which can be used to cache common read requests.

The below diagram shows how caching can be added to an existing architecture:



For more information on database caching, please visit the below URL:
https://aws.amazon.com/caching/database-caching/ (https://aws.amazon.com/caching/database-caching/)

Note:

Option C is incorrect because, CloudFront is a valuable component of scaling a website, especially for

geo-location workloads and queries. And more advanced for given architecture.

Option D is incorrect because it will have latency and additional changes as well.

Ask our Experts

QUESTION 47 CORRECT DEFINE PERFORMANT ARCHITECTURES

An application is currently hosted on an EC2 Instance which has attached EBS Volumes. The data on these volumes is frequently accessed. But after a duration of a week, the documents need to be moved to infrequent access storage. Which of the following EBS volume type provides cost efficiency for the moved documents?

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

Explanation :

Answer - D

AWS Documentation mentions the following:

Cold HDD (sc1) volumes provide low-cost magnetic storage that defines performance in terms of throughput rather than IOPS. With a lower throughput limit than st1, sc1 is a good fit ideal for large, sequential cold-data workloads. If you require infrequent access to your data and are looking to save costs, sc1 provides inexpensive block storage.

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

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

Ask our Experts

QUESTION 48 CORRECT DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

A customer wants to import their existing virtual machines to the cloud. Which service can they use for this? Choose one answer from the options given below.

- A. VM Import/Export ✔
- B. AWS Import/Export
- C. AWS Storage Gateway
- D. DB Migration Service

Explanation :

Answer – A
VM Import/Export enables customers to import Virtual Machine (VM) images in order to create Amazon EC2 instances. Customers can also export previously imported EC2 instances to create VMs. Customers can use VM Import/Export to leverage their previous investments in building VMs by migrating their VMs to Amazon EC2.
For more information on AWS VM Import, please visit the URL:
https://aws.amazon.com/ec2/vm-import/ (https://aws.amazon.com/ec2/vm-import/)

Ask our Experts

QUESTION 49 CORRECT DESIGN RESILIENT ARCHITECTURES

A company website is set to launch in the upcoming weeks. There is a probability that the traffic will be quite high during the initial weeks. In the event of a load failure, how can you set up DNS failover to a static website? Choose the correct answer from the options given below.

- A. Duplicate the exact application architecture in another region and configure DNSWeight-based routing.
- B. Enable failover to an on-premises data center to the application hosted there.
- C. Use Route 53 with the failover option to failover to a static S3 website bucket orCloudFront distribution. ✔
- D. Add more servers in case the application fails.

Explanation :

Answer – C

Amazon Route 53 health checks monitor the health and performance of your web applications, web servers, and other resources.

If you have multiple resources that perform the same function, you can configure DNS failover so that Amazon Route 53 will route your traffic from an unhealthy resource to a healthy resource. For example, if you have two web servers and one web server becomes unhealthy, Amazon Route 53 can route traffic to the other web server. So you can route traffic to a website hosted on S3 or to a cloudFront distribution.

For more information on DNS failover using Route 53, please refer to the link below.

http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover.html (http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover.html)

Ask our Experts

QUESTION 50 CORRECT DESIGN RESILIENT ARCHITECTURES

A company is running three production web server reserved EC2 Instances with EBS-backed root volumes. These instances have a consistent CPU load of 80%. Traffic is being distributed to these instances by an Elastic Load Balancer. They also have production and development Multi-AZ RDS MySQL databases. What recommendation would you make to reduce cost in this environment without affecting availability of mission-critical systems? Choose the correct answer from the options given below.

- A. Consider using On-demand instances instead of Reserved EC2 instances.
- B. Consider not using a Multi-AZ RDS deployment for the development database. ✔
- C. Consider using Spot instances instead of Reserved EC2 instances.
- D. Consider removing the Elastic Load Balancer.

Explanation :

Answer – B

Multi-AZ databases are better for production environments rather than for development environments, so you can reduce costs by not using these for development environments.

Amazon RDS Multi-AZ deployments provide enhanced availability and durability for Database (DB) Instances, making them a natural fit for production database workloads. When you provision a Multi-AZ DB Instance, Amazon RDS automatically creates a primary DB Instance and synchronously

replicates the data to a standby instance in a different Availability Zone (AZ). Each AZ runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby (or to a read replica in the case of Amazon Aurora), so that you can resume database operations as soon as the failover is complete. Since the endpoint for your DB Instance remains the same after a failover, your application can resume database operation without the need for manual administrative intervention.
For more information on Multi-AZ RDS, please refer to the link below.

- https://aws.amazon.com/rds/details/multi-az/ (https://aws.amazon.com/rds/details/multi-az/)

Note:
Mission Critical system refers to production Instances and Databases. However, if you notice, they have Multi-AZ RDS on Development environment also which is not necessary. Because management always concerned about production environment should be perfect.

In order to reduce the cost, we can disable the Multi-AZ RDS for Development environment and keep it only for the Production environment.

Ask our Experts

QUESTION 51 CORRECT DESIGN RESILIENT ARCHITECTURES

An application consists of a couple of EC2 Instances. One EC2 Instance hosts a web application and the other Instance hosts the database server. Which of the following changes can be made to ensure high availability of the database layer?

- **A.** Enable Read Replicas for the database.
- **B.** Enable Multi-AZ for the database.
- **C.** Have another EC2 Instance in the same Availability Zone with replication configured.
- **D.** Have another EC2 Instance in the another Availability Zone with replicationconfigured. ✔

Explanation :

Answer – D
Since this is a self-managed database and not an AWS RDS instance, options A and B are incorrect.
To ensure high availability, have the EC2 Instance in another Availability Zone, so even if one goes down, the other one will still be available.
One can refer to the following media link for achieving high availability in AWS.

- https://media.amazonwebservices.com/architecturecenter/AWS_ac_ra_ftha_04.pdf (https://media.amazonwebservices.com/architecturecenter/AWS_ac_ra_ftha_04.pdf)

Note:

In the question, they clearly mentioned that **"One EC2 Instance hosts a web application and the other Instance hosts the database server."** So here the database server hosted on EC2 instances (self-managed). When you host a database server on EC2 instance, there are no direct options available to enable the read-replica and multi-AZ.

So based on this Option A and B are the wrong answers.

Ask our Experts

QUESTION 52 CORRECT DESIGN RESILIENT ARCHITECTURES

You are designing an architecture on AWS with disaster recovery in mind. Currently the architecture consists of an ELB and underlying EC2 Instances in a primary and secondary region. How can you establish a switchover in case of failure in the primary region?

- **A.** Use Route 53 Health Checks and then do a failover. ✔
- **B.** Use CloudWatch metrics to detect the failure and then do a failover.
- **C.** Use scripts to scan CloudWatch logs to detect the failure and then do a failover.
- **D.** Use CloudTrail to detect the failure and then do a failover.

Explanation :

Answer - A
AWS Documentation mentions the following:
If you have multiple resources that perform the same function, you can configure DNS failover so that Route 53 will route your traffic from an unhealthy resource to a healthy resource. For example, if you have two web servers and one web server becomes unhealthy, Route 53 can route traffic to the other web server.
For more information on configuring DNS failover using Route 53, one can refer to the below link:
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover.html
(https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover.html)

Ask our Experts

QUESTION 53 MARKED AS REVIEW CORRECT
DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

A company has assigned two web server instances to an Elastic Load Balancer inside a custom VPC. However, the instances are not accessible via URL to the elastic load balancer serving the web app data from the EC2 instances. How might you resolve the issue so that your instances are serving the web app data to the public internet? Choose the correct answer.

- A. Attach an Internet Gateway to the VPC and route it to the subnet. ✔
- B. Add an Elastic IP address to the instance.
- C. Use Amazon Elastic Load Balancer to serve requests to your instances located in the internal subnet.
- D. None of the above

Explanation :

Answer – A

If the Internet Gateway is not attached to the VPC, which is a prerequisite for the instances to be accessed from the Internet, the instances will not be reachable.
For more information on Internet Gateways, please refer to the below link:
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Internet_Gateway.html
(http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Internet_Gateway.html)

Ask our Experts

QUESTION 54 CORRECT DEFINE PERFORMANT ARCHITECTURES

You want to host a static website on aws. As a Solutions architect, you have been given a task to establish a serverless architecture for that. Which of the following could be included in proposed architecture? Choose 2 answers from the options given below.

- [x] A. Use DynamoDB to store data in tables. ✔
- [ ] B. Use EC2 to host the data on EBS Volumes.
- [x] C. Use the Simple Storage Service to store data. ✔
- [ ] D. Use AWS RDS to store the data.

Explanation :

Answer – A and C
Both the Simple Storage Service and DynamoDB are complete serverless offerings from AWS which You don't need to maintain servers, and your applications have automated high availability.
For more information on S3 and DynamoDB, please refer to the links below.

https://aws.amazon.com/s3/ (https://aws.amazon.com/s3/)
https://aws.amazon.com/dynamodb/ (https://aws.amazon.com/dynamodb/)
https://aws.amazon.com/serverless/ (https://aws.amazon.com/serverless/)

Ask our Experts

QUESTION 55 CORRECT DEFINE PERFORMANT ARCHITECTURES

Currently, you're helping design and architect a highly available application. After building the initial environment, you discover that a part of your application does not work correctly until port 443 is added to the security group. After adding port 443 to the appropriate security group, how much time will it take before the changes are applied and the application begins working correctly? Choose the correct answer from the options below.

- **A.** Generally, it takes 2-5 minutes in order for the rules to propagate.
- **B.** Immediately after a reboot of the EC2 Instances belong to that security group.
- **C.** Changes apply instantly to the security group, and the application should be able torespond to 443 requests. ✔
- **D.** It will take 60 seconds for the rules to apply to all Availability Zones withinthe region.

Explanation :

Answer – C
This is given in the AWS Documentation:
"Some systems for setting up firewalls let you filter on source ports. Security groups let you filter only on destination ports.
When you add or remove rules, they are automatically applied to all instances associated with the

security group".

For more information on Security Groups, please refer to the below link:
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html
(http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html)

Ask our Experts

QUESTION 56 MARKED AS REVIEW INCORRECT
SPECIFY SECURE APPLICATIONS AND ARCHITECTURES

A company hosts data in S3. There is now a mandate that going forward, all data in the S3 bucket needs to be encrypted at rest. How can this be achieved?

- A. Use AWS Access Keys to encrypt the data. ✖
- B. Use SSL Certificates to encrypt the data.
- C. Enable Server-side encryption on the S3 bucket. ✔
- D. Enable MFA on the S3 bucket.

Explanation :

Answer – C
AWS Documentation mentions the following:
Server-side encryption is about data encryption at rest—that is, Amazon S3 encrypts your data at the object level as it writes it to disks in its data centers and decrypts it for you when you access it. As long as you authenticate your request and you have access permissions, there is no difference in the way you access encrypted or unencrypted objects.
For more information on S3 Server-side encryption, please refer to the below link:
https://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html
(https://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html)

Ask our Experts

QUESTION 57 CORRECT SPECIFY SECURE APPLICATIONS AND ARCHITECTURES

A company hosts data in S3. There is a requirement to control access to the S3 buckets. Which are the 2 ways in which this can be achieved?

- [x] **A.** Use Bucket Policies. ✔
- [ ] **B.** Use the Secure Token Service.
- [x] **C.** Use IAM user policies. ✔
- [ ] **D.** Use AWS Access Keys.

Explanation :

Answer – A and C
AWS Documentation mentions the following:
Amazon S3 offers access policy options broadly categorized as resource-based policies and user policies. Access policies you attach to your resources (buckets and objects) are referred to as resource-based policies. For example, bucket policies and access control lists (ACLs) are resource-based policies. You can also attach access policies to users in your account. These are called user policies. You may choose to use resource-based policies, user policies, or some combination of these to manage permissions to your Amazon S3 resources.
For more information on S3 access control, please refer to the below link:
https://docs.aws.amazon.com/AmazonS3/latest/dev/s3-access-control.html
(https://docs.aws.amazon.com/AmazonS3/latest/dev/s3-access-control.html)

Ask our Experts

QUESTION 58 CORRECT DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

Your application provides data transformation services. Files containing data to be transformed are first uploaded to Amazon S3 and then transformed by a fleet of Spot EC2 Instances. Files submitted by your premium customers must be transformed with the highest priority. How would you implement such a system?

- ○ **A.** Use a DynamoDB table with an attribute defining the priority level. Transformation instances will scan the table for tasks, sorting the results by priority level.
- ○ **B.** Use Route 53 latency-based routing to send high priority tasks to the closest transformation instances.

- **C.** Use two SQS queues, one for high priority messages, the other for default priority. Transformation instances first poll the high priority queue; if there is no message, they poll the default priority queue. ✔
- **D.** Use a single SQS queue. Each message contains the priority level. Transformation instances poll high-priority messages first.

Explanation :

Answer – C
The best way is to use 2 SQS queues. Each queue can be polled separately. The high priority queue can be polled first.
For more information on AWS SQS, please refer to the link below:
https://aws.amazon.com/sqs/ (https://aws.amazon.com/sqs/)

Ask our Experts

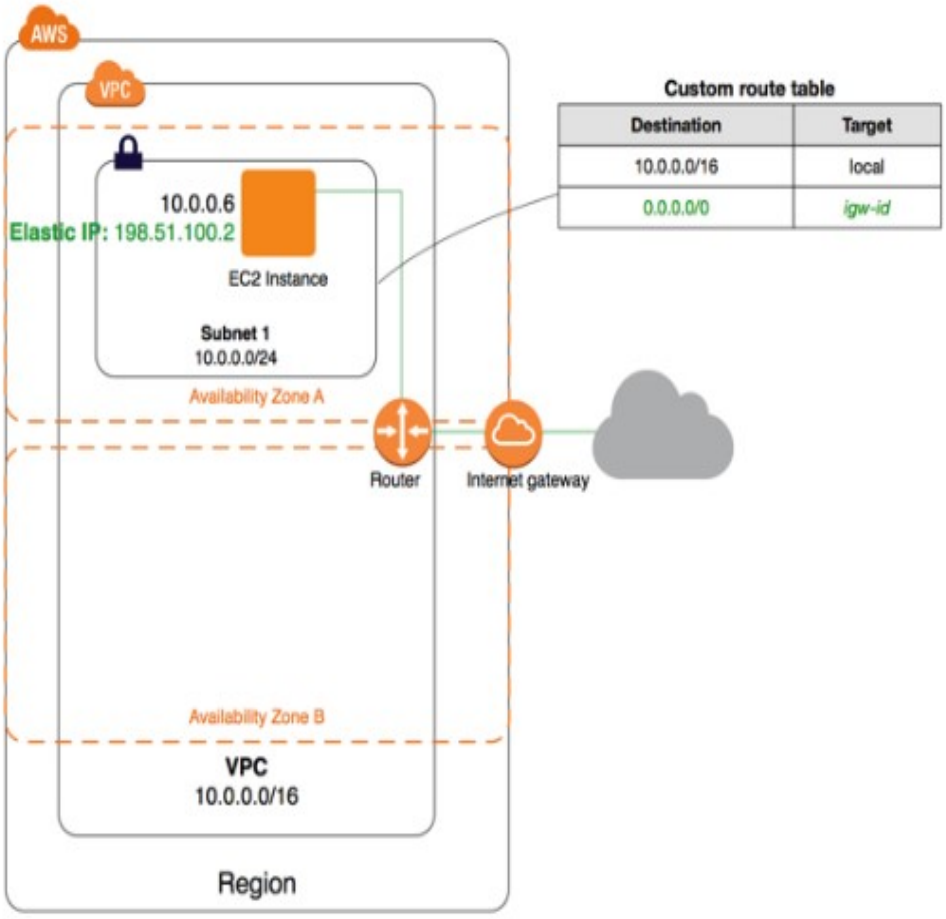
QUESTION 59 CORRECT DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

A VPC has been setup with a subnet and an internet gateway. The EC2 instance is set up with a public IP but you are still not able to connect to it via the Internet. The right security groups are also in place. What should you do to connect to the EC2 Instance from the Internet?

- **A.** Set an Elastic IP Address to the EC2 Instance.
- **B.** Set a Secondary Private IP Address to the EC2 Instance.
- **C.** Ensure the right route entry is there in the Route table. ✔
- **D.** There must be some issue in the EC2 Instance. Check the system logs.

Explanation :

Answer – C
You have to ensure that the Route table has an entry to the Internet Gateway because this is required for instances to communicate over the Internet. The diagram shows the configuration of the public subnet in a VPC:



Option A is incorrect. Since you already have a public IP assigned to the instance, this should have been enough to connect to the Internet.
Option B is incorrect. Private IPs cannot be accessed from the Internet.
Option D is incorrect. The Route table is causing the issue and not the system.
For more information on AWS public subnet, please visit the link below.
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario1.html
(http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario1.html)

Ask our Experts

QUESTION 60 CORRECT DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

A customer has a single 3-TB volume on-premises that is used to hold a large repository of images and print layout files. This repository is growing at 500GB a year and must be presented as a single logical volume. The customer is becoming

increasingly constrained with their local storage capacity and wants an offsite backup of this data, while maintaining low-latency access to their frequently accessed data. Which AWS Storage Gateway configuration meets the customer requirements?

- **A.** Gateway-Cached Volumes with snapshots scheduled to Amazon S3 ✔
- **B.** Gateway-Stored Volumes with snapshots scheduled to Amazon S3
- **C.** Gateway-Virtual Tape Library with snapshots to Amazon S3
- **D.** Gateway-Virtual Tape Library with snapshots to Amazon Glacier

Explanation :

Answer - A

Gateway-cached volumes let you use Amazon Simple Storage Service (Amazon S3) as your primary data storage while retaining frequently accessed data locally in your storage gateway. Gateway-cached volumes minimize the need to scale your on-premises storage infrastructure, while still providing your applications with low-latency access to their frequently accessed data. You can create storage volumes up to 32 TiB in size and attach to them as iSCSI devices from your on-premises application servers. Your gateway stores data that you write to these volumes in Amazon S3 and retains recently read data in your on-premises storage gateway's cache and upload buffer storage.
For more information on Storage Gateways, please visit the link:

- http://docs.aws.amazon.com/storagegateway/latest/userguide/storage-gateway-cached-concepts.html (http://docs.aws.amazon.com/storagegateway/latest/userguide/storage-gateway-cached-concepts.html)

Note:

The two requirements of the question are low latency access to frequently accessed data and an offsite back up of the data.
Option A is correct because your primary data is written to S3 while retaining your frequently accessed data locally in a cache for low-latency access.
Option B is incorrect because it is storing the primary data locally (but we have a storage constraint hence this is not a viable solution) and your entire dataset is available for low-latency access while asynchronously backed up to AWS.
Options C & D are incorrect it cannot provide low latency access to frequently accessed data.

Ask our Experts

A company is planning to use the AWS ECS service to work with containers. There is a need for the least amount of administrative overhead while launching containers. How can this be achieved?

- A. Use the Fargate launch type in AWS ECS. ✔
- B. Use the EC2 launch type in AWS ECS.
- C. Use the Auto Scaling launch type in AWS ECS.
- D. Use the ELB launch type in AWS ECS.

Explanation :

Answer - A
AWS Documentation mentions the following:
The Fargate launch type allows you to run your containerized applications without the need to provision and manage the backend infrastructure. Just register your task definition and Fargate launches the container for you.
For more information on the different launch types, please visit the link:
https://docs.aws.amazon.com/AmazonECS/latest/developerguide/launch_types.html
(https://docs.aws.amazon.com/AmazonECS/latest/developerguide/launch_types.html)

Ask our Experts

QUESTION 62 CORRECT DESIGN RESILIENT ARCHITECTURES

You currently manage a set of web servers hosted on EC2 Servers with public IP addresses. These IP addresses are mapped to domain names. There was an urgent maintenance activity that had to be carried out on the servers and the servers had to be stopped and restarted. Now the web application hosted on these EC2 Instances is not accessible via the domain names configured earlier. Which of the following could be a reason for this?

- A. The Route 53 hosted zone needs to be restarted.
- B. The network interfaces need to initialized again.
- C. The public IP addresses need to associated to the ENI again.
- D. The public IP addresses have changed after the instance was stopped and started. ✔

Explanation :

Answer – D
By default, the public IP address of an EC2 Instance is released after the instance is stopped and started. Hence, the earlier IP address which was mapped to the domain names would have become invalid now.
For more information on public IP addressing, please visit the below URL:
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-instance-addressing.html#concepts-public-addresses (http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-instance-addressing.html#concepts-public-addresses)

Ask our Experts

QUESTION 63 CORRECT SPECIFY SECURE APPLICATIONS AND ARCHITECTURES

You are responsible for deploying a critical application to AWS. It is required to ensure that the controls set for this application meet PCI compliance. Also, there is a need to monitor web application logs to identify any malicious activity. Which of the following services can be used to fulfill this requirement? Choose 2 answers from the options given below.

- [x] A. Amazon CloudWatch Logs ✔
- [ ] B. Amazon VPC Flow Logs
- [ ] C. Amazon AWS Config
- [x] D. Amazon CloudTrail ✔

Explanation :

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

You can use Amazon CloudWatch Logs to monitor, store, and access your log files from Amazon Elastic Compute Cloud (Amazon EC2) instances, AWS CloudTrail, Amazon Route 53, and other sources. You can then retrieve the associated log data from CloudWatch Logs.
For more information on CloudWatch logs, please refer to below URL:
http://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/WhatIsCloudWatchLogs.html
(http://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/WhatIsCloudWatchLogs.html)

Ask our Experts

QUESTION 64 CORRECT DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

There is a requirement to host a database server. This server should not be able to connect to the Internet except while downloading required database patches. Which of the following solutions would best satisfy all the above requirements? Choose the correct answer from the options below.

- **A.** Setup the database in a private subnet with a security group which only allowsoutbound traffic.
- **B.** Setup the database in a public subnet with a security group which only allows inboundtraffic.
- **C.** Setup the database in a local data center and use a private gateway to connect theapplication to the database.
- **D.** Setup the database in a private subnet which connects to the Internet via a NATInstance. ✔

Explanation :

Answer – D
This setup coincides with Scenario 2 of setting up a VPC as per AWS documentation:
Scenario 2: VPC with Public and Private Subnets (NAT)
The configuration for this scenario includes a virtual private cloud (VPC) with a public subnet and a private subnet. We recommend this scenario if you want to run a public-facing web application, while maintaining back-end servers that aren't publicly accessible. A common example is a multi-tier website, with the web servers in a public subnet and the database servers in a private subnet. You can set up security and routing so that the web servers can communicate with the database servers.
For more information on the VPC Scenario for public and private subnets, please see the below link:
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2.html
(http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2.html)

Ask our Experts

QUESTION 65 CORRECT SPECIFY SECURE APPLICATIONS AND ARCHITECTURES

You have both production and development based instances running on your VPC. It is required to ensure that people responsible for the development instances do not have access to work on production instances for better security. Which of the following would be the best way to accomplish this using policies? Choose the correct answer from the options given below.

- **A.** Launch the test and production instances in separate VPCs and use VPC Peering.
- **B.** Create an IAM Policy with a condition that allows access to only those instances which are used for production or development.
- **C.** Launch the test and production instances in different Availability Zones and use Multi-Factor Authentication.
- **D.** Define the tags on the Development and production servers and add a condition to the IAMPolicy which allows access to specific tags. ✔

Explanation :

Answer – D

You can easily add tags to define which instances are production and which ones are development instances. These tags can then be used while controlling access via an IAM Policy.
For more information on tagging your resources, please refer to the link below.
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html
(http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html)

Note:

It can be done with the help of option B as well. However, the question is looking for the "best way to accomplish this using policies".

By using the option D, you can reduce usage of different IAM policies on each instance.

Ask our Experts

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/)

Mobile App

- Android Coming Soon
- iOS Coming Soon

Company

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

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)