CSAA PRACTICE TEST 7

Attempt	9
Marks Obtained	63 / 65
Your score is	96.92%
Completed on	Thursday , 17 January 2019 , 07:48 PM
Time Taken	00 H 32 M 22 S
Result	Pass

Domains / Topics wise Quiz Performance Report

S.No.	Topic	Total Questions	Correct	Incorrect	Unattempted
1	Other	64	62	2	0
2	Design Cost-Optimized Architectures	1	1	0	0

65 Questions	**63** Correct	**2** Incorrect	**0** Unattempted

Show Answers

All

QUESTION 1 CORRECT

Your company is planning on the following architecture for their application

A set of EC2 Instances hosting the web part of the application.
A relational database for the backend
A Load balancer for distribution of traffic
A NAT gateway for routing traffic from the database server to the Internet

Which of the following architecture ensure high availability across all components?

- **A.** A Load balancer with one public subnets. The EC2 Instances placed in one Availability Zone. RDS with Multi-AZ Enabled. NAT Gateway in 2 availability zones.
- **B.** A Load balancer with 2 public subnets. The EC2 Instances placed across 2 Availability Zones. RDS with Multi-AZ Enabled. NAT Gateway in 2 availability zones. ✔
- **C.** A Load balancer with 2 public subnets. The EC2 Instances placed across 2 Availability Zones. RDS with Multi-AZ Enabled. NAT Gateway in one availability zone
- **D.** A Load balancer with 2 public subnets. The EC2 Instances placed in one Availability Zone. RDS with Multi-AZ Enabled. NAT Gateway in one availability zone

Explanation :

Answer – B
The AWS Documentation mentions the following
When you enable an Availability Zone for your load balancer, Elastic Load Balancing creates a load balancer node in the Availability Zone. If you register targets in an Availability Zone but do not enable the Availability Zone, these registered targets do not receive traffic. Note that your load balancer is most effective if you ensure that each enabled Availability Zone has at least one registered target. We recommend that you enable multiple Availability Zones. (Note that with an Application Load Balancer, we require you to enable multiple Availability Zones.) With this configuration, if one Availability Zone becomes unavailable or has no healthy targets, the load balancer can continue to route traffic to the healthy targets in another Availability Zone.
In a Multi-AZ deployment, Amazon RDS automatically provisions and maintains a synchronous standby replica in a different Availability Zone. The primary DB instance is synchronously replicated across Availability Zones to a standby replica to provide data redundancy, eliminate I/O freezes, and minimize latency spikes during system backups. Running a DB instance with high availability can enhance availability during planned system maintenance, and help protect your databases against DB instance failure and Availability Zone disruption.

Option A is invalid because the Load balancer should have multiple subnets and EC2 Instances should be placed across multiple availability zones
Option C is invalid because the NAT gateway should be placed in multiple availability zone
Option D is invalid because the NAT gateway should be placed in multiple availability zone and EC2 Instances should be placed across multiple availability zones
For more information on Elastic Load Balancing , Multi-AZ and NAT gateway , please refer to the below URL's
https://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/how-elastic-load-balancing-works.html (https://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/how-elastic-load-balancing-works.html)
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html (https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html)
https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html (https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html)

Ask our Experts

QUESTION 2 CORRECT

Your company has an AWS account and a lot of resources defined in the Frankfurt region. They want to track the resources to monitor if any changes are made to the resources. Which of the following should be used for this purpose?

- **A.** AWS Config ✔
- **B.** AWS CloudTrail
- **C.** AWS CloudWatch
- **D.** AWS Opswork

Explanation :

Answer – A
The AWS Documentation mentions the following

AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. With Config, you can review changes in configurations and relationships between AWS resources, dive into detailed resource configuration histories, and determine your overall compliance against the configurations specified in your internal guidelines. This enables you to simplify compliance auditing, security analysis, change management, and operational troubleshooting.
Option B is invalid because this is an API monitoring service
Option C is invalid because this is a metric and logging service
Option D is invalid because is used to deploy stacks of resources
For more information on AWS Config , please refer to the below URL

- https://aws.amazon.com/config/ (https://aws.amazon.com/config/)

CloudWatch and Config serve distinct use cases for monitoring and complements each other from AWS ecosystem.

Config is typically used for auditing and compliance purposes across organizations to verify whether AWS resource changes being made are per compliance rules. Some of the typical compliance rules are as follows:

- IAM user should be part of one of the IAM groups
- None of the S3 bucket should be publicly accessible
- EC2 resources should be launched in private subnets only, so that it cannot be accessed outside VPC
- Server access logging should be enabled on S3 buckets
- Certain IAM policy should not be modified or it should not be attached to any user. For e.g AdministratorAccess IAM policy

Above compliance rules vary from one organization to another depending upon legal agreements signed between organization/client and government/customers

CloudWatch is designed to provide performance information about AWS resources such as EC2, Lambda etc. Developers can use information from CloudWatch to identify bottlenecks in applications or workflows.

Cloudwatch will help you to send alerts when *CPU /Memory utilization reaches a certain threshold* and browse metrics associated with CPU/Network to identify operational and security issues , if any

Please find below sample config rule for S3 service:

Rules > Rule details

s3-bucket-public-read-config_rule

Description Checks that your S3 buckets do not allow public read access. If an S3 bucket policy or bucket ACL allows public read access, the bucket is noncompliant.

Trigger type Configuration changes

Scope of changes Resources

Resource types S3 Bucket

Config rule ARN arn:aws:config:us-east-1:[redacted]:config-rule/config-rule-pvgdiy

Parameters *null*

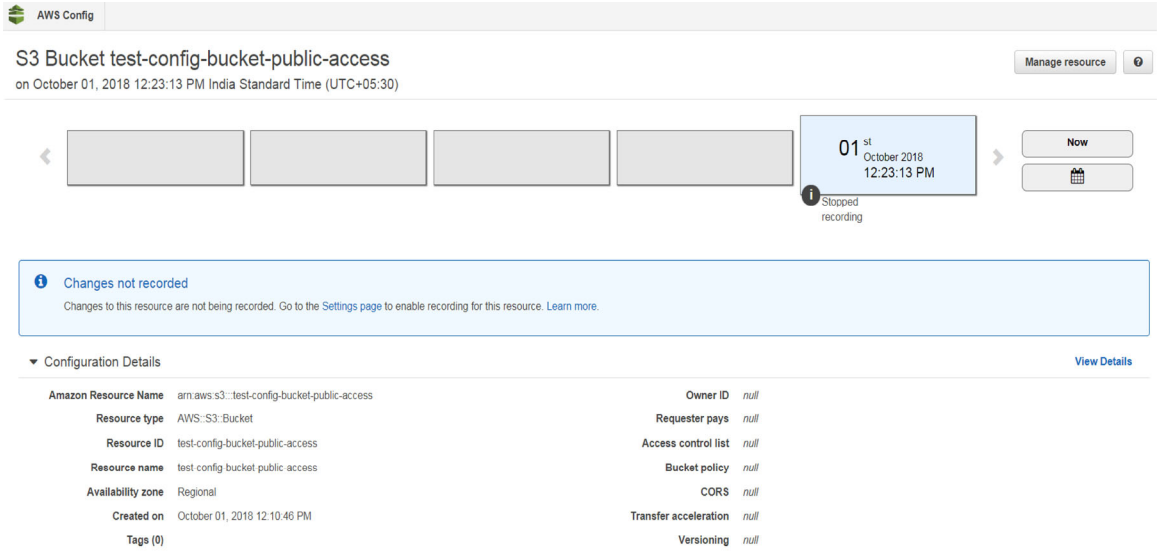
Overall rule status Last successful invocation on October 1, 2018 at 12:23:58 PM
Last successful evaluation on October 1, 2018 at 12:23:58 PM

Resources evaluated

Click on the icon to view configuration details for the resource when it was last evaluated with this rule.

Resource type	Config timeline	Compliance	Last successful invocation	Last successful evaluation	Manage resource
S3 Bucket	cf-templates-1xnurd1kjervw-us-east-1	Compliant	October 01, 2018 12:17:20 PM	October 01, 2018 12:17:20 PM	
S3 Bucket	config-bucket-[redacted]	Compliant	October 01, 2018 12:17:20 PM	October 01, 2018 12:17:20 PM	
S3 Bucket	test-config-bucket-public-access	Compliant	October 01, 2018 12:23:58 PM	October 01, 2018 12:23:58 PM	
S3 Bucket	whizlabstestbucket	Compliant	October 01, 2018 12:17:20 PM	October 01, 2018 12:17:20 PM	

Here is the screenshot, where you could see the changes/revisions made on one of the S3 buckets over a period of time



Cloudwatch would help to monitor AWS resource "metric/event" changes , however Cloudtrail is used for monitoring AWS resource "configuration" changes.

Ask our Experts

QUESTION 3 CORRECT

A company is planning on hosting an application with the below architecture

· A set of EC2 Instances which would host a front-end web page for allowing users to uploaded images.

· The Images would be processed by a backend set of EC2 Instances

Which of the following can be added to decouple the various components of this architecture?

- **A.** AWS SQS ✔
- **B.** AWS SNS
- **C.** AWS Storage Gateway
- **D.** AWS Cognito

Explanation :

Answer – A
The AWS Documentation mentions the following
Amazon Simple Queue Service (SQS) is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SQS eliminates the complexity and overhead associated with managing and operating message oriented middleware, and empowers developers to focus on differentiating work. Using SQS, you can send, store, and receive messages between software components at any volume, without losing messages or requiring other services to be available.
Option B is invalid because this is a notification service
Option C is invalid because this is used to extend the storage options for on-premise servers
Option D is invalid because this is used to provide an authentication and authorization module for web and mobile based applications
For more information on AWS SQS, please refer to the below URL
https://aws.amazon.com/sqs/ (https://aws.amazon.com/sqs/)

Ask our Experts

QUESTION 4 CORRECT

A company is planning on hosting an application with the below architecture

· A lambda function which reads metadata of objects from an S3 bucket

· The Lambda function then stores the metadata in DynamoDB and AWS RDS - MySQL

Which of the following needs to be in place to high availability of all components in the system?

- **A.** Enable Cross Region Replication for the S3 bucket
- **B.** Enable Lambda functions in Multiple Availability Zones
- **C.** Enabling Multi-AZ for the MySQL database ✔
- **D.** Enable Autoscaling for the DynamoDB table

Explanation :

Answer – C
The AWS Documentation mentions the following
In a Multi-AZ deployment, Amazon RDS automatically provisions and maintains a synchronous standby replica in a different Availability Zone. The primary DB instance is synchronously replicated across Availability Zones to a standby replica to provide data redundancy, eliminate I/O freezes, and minimize latency spikes during system backups. Running a DB instance with high availability can enhance availability during planned system maintenance, and help protect your databases against DB instance failure and Availability Zone disruption.
Option A is invalid because the S3 service is already a highly available service within a particular region
Options B and D are invalid because these are already a highly available services in AWS
For more information on Multi-AZ, please refer to the below URL
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html
(https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html)

Ask our Experts

QUESTION 5 CORRECT

A company has a set of EC2 Instances hosting a revenue generating applications. Some of the data on the attached EBS volumes are critical to retain. Hence it has to be ensured that even after the instances are terminated, the EBS volumes will still remain intact. Which of the following needs to be done to ensure this requirement can be met?

- A. Enable the DisableApiTermination for the EC2 Instance
- B. Make the attribute of DeleteOnTermination for the EBS volume to false ✔
- C. Make a copy of the root volume on the EC2 Instance
- D. Make a copy of the volume in another availability zone.

Explanation :

Answer – B
The AWS Documentation mentions the following
When an instance is terminated, Amazon Elastic Compute Cloud (Amazon EC2) uses the value of the DeleteOnTermination attribute for each attached EBS volume to determine whether to preserve or delete the volume when the instance is terminated. By default, the DeleteOnTermination attribute for the root volume of an instance is set to true, but it is set to false for all other volume types.
To preserve the root volume when an instance is terminated, change the DeleteOnTermination attribute for the root volume to false.
Option A is invalid since the flag needs to be set on the EBS volume
Options C and D are invalid since these are really inefficient ways to manage the preservation of volumes
For more information on the Delete on termination flag, please refer to the below URL
https://aws.amazon.com/premiumsupport/knowledge-center/deleteontermination-ebs/
(https://aws.amazon.com/premiumsupport/knowledge-center/deleteontermination-ebs/)

Ask our Experts

QUESTION 6 CORRECT

A company has a set of EC2 Instances hosted in a VPC. The IT Security department has specified that they need to ensure they get a list of IP addresses for all sources that are making requests to the EC2 Instances. Which one of the following could help achieve this requirement?

- A. AWS VPC Flow Logs ✔
- B. AWS Cloudwatch
- C. AWS CloudTrail
- D. AWS Trusted Advisor

Explanation :

Answer – A
The AWS Documentation mentions the following
VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. Flow log data can be published to Amazon CloudWatch Logs and Amazon S3. After you've created a flow log, you can retrieve and view its data in the chosen destination.
Option B is invalid since this is a monitoring service which can only give metrics and not the detailed IP address tracing for traffic flowing into EC2 Instances
Option C is invalid since this is an API monitoring service
Option D is invalid since this is only used as a recommendation service
For more information on VPC Flow logs, please refer to the below URL
https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html
(https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html)

Ask our Experts

QUESTION 7 CORRECT

A company has a requirement for a data store in AWS. Below are the key requirements

- Offer petabyte storage options
- Ability to do queries by business Intelligence tools

Which of the following would be best fit for this purpose?

- A. AWS Aurora
- B. AWS Redshift ✔

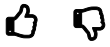
- **C.** AWS DynamoDB
- **D.** AWS Simple Storage Service

Explanation :

Answer – B
The AWS Documentation mentions the following
Amazon Redshift is a fully managed, petabyte-scale data warehouse service in the cloud. You can start with just a few hundred gigabytes of data and scale to a petabyte or more. This enables you to use your data to acquire new insights for your business and customers. Regardless of the size of the data set, Amazon Redshift offers fast query performance using the same SQL-based tools and business intelligence applications that you use today.
Option A is invalid since this is more of a MySQL or PostgreSQL database compliant based service
Option C is invalid since this is a NoSQL database
Option D is invalid since this is an object-based storage service
For more information on AWS Redshift, please refer to the below 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 8 CORRECT

Your company has just started using the AWS RDS service. They have an application making requests to a MySQL instance on this service. Due to the sudden surge of high requests, you need to ensure that the backup activities on the database do not interface with the normal operation of the database. Which of the following would help in this requirement?

- **A.** Ensure that the underlying instance type RDS instance is using General Purpose SSD storage. This type of storage will give minimal impact for such operations.
- **B.** Ensure that the underlying instance type RDS instance is using Enhanced Networking. This type of setting will give minimal impact for such operations.

C. Ensure that Multi-AZ feature has been enabled for the underlying RDS Instance. ✔

D. Ensure that cross region replication is enabled for the underlying RDS Instance.

Explanation :

Answer – C
The AWS Documentation mentions the following
During the automatic backup window, storage I/O might be suspended briefly while the backup process initializes (typically under a few seconds). You may experience elevated latencies for a few minutes during backups for Multi-AZ deployments. For MariaDB, MySQL, Oracle, and PostgreSQL, I/O activity is not suspended on your primary during backup for Multi-AZ deployments, because the backup is taken from the standby. For SQL Server, I/O activity is suspended briefly during backup for Multi-AZ deployments.
Options A and B are incorrect since these features will not help in reducing the impact.
Option D is incorrect since there is no said feature as such for the AWS RDS service
For more information on Automated backups, please refer to the below URL
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_WorkingWithAutomatedBackups.html
(https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_WorkingWithAutomatedBackups.html)

Ask our Experts

QUESTION 9 CORRECT

A company has an application that needs to be hosted on an EC2 Instance. The general amount of throughput data will be in the range of 400-500 MiB/s from the application. Which of the following should be used as the storage type for the underlying EC2 Instance with Cost-effective manner?

A. EBS - General Purpose SSD

B. EBS - Provisioned IOPS SSD

C. EBS - Throughput Optimized HDD ✔

D. EBS - Cold HDD

Explanation :

Answer – C

When you want high throughput, you should choose using the Throughput Optimized EBS volume. The below snapshot from the AWS Documentation shows the features of the different types of volumes.

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

Because of the features mentioned , all other options are invalid

For more information on the EBS volume types, please refer to 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 10 CORRECT

A company has setup their application in AWS. It consists of a web tier hosted on a set of EC2 Instances. These instances interact with a MongoDB database server located in a private subnet. The web tier also interacts with many service-based applications in the private subnet. A NAT Instance is being used to route traffic from the instances in the private subnet to the Internet. The IT Administrative team is now getting Cloudwatch alerts that the NAT Instance is going beyond its threshold value for Network Activity. Which of the following would you advise to increase the performance of this architecture?

○ **A.** Place the database server and application servers in the public subnet.

- **B.** Place the NAT instance closer to the database servers by placing them in the private subnet
- **C.** Use the NAT gateway service instead of the NAT Instance ✔
- **D.** Use a VPN connection for the Instances in the private subnet

Explanation :

Answer – C

The below snapshot from the AWS Documentation shows a partial comparison of the NAT Instance and NAT Gateway. You should consider using the NAT gateway for higher bandwidth requirements

Comparison of NAT Instances and NAT Gateways

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

Attribute	NAT gateway	NAT instance
Availability	Highly available. NAT gateways in each Availability Zone are implemented with redundancy. Create a NAT gateway in each Availability Zone to ensure zone-independent architecture.	Use a script to manage failover between instances.
Bandwidth	Can scale up to 45 Gbps.	Depends on the bandwidth of the instance type.

Option A is incorrect since you should not change the architecture of the database or application servers since this would result in security issues

Option B is incorrect since this would still alleviate the current network issue

Option D is incorrect since the NAT instance should be used to route traffic to the Internet from the Instances in the private subnet

For more information on the comparison between NAT Instances and the NAT gateway, please refer to the below URL

https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-comparison.html (https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-comparison.html)

Ask our Experts

QUESTION 11 CORRECT

Your company is currently hosting an application on their On-premise environment. The company has developed this application inhouse. Consulting companies then use this application via API calls. You now need to consider moving this application to AWS. Which of the following services would best be suited in the architecture design, which would also help deliver a cost-effective solution. Choose 2 answers from the options given below

- [x] **A.** AWS Lambda ✔
- [x] **B.** AWS API Gateway ✔
- [ ] **C.** AWS Config
- [ ] **D.** AWS EC2

Explanation :

Answer – A and B
The AWS Documentation mentions the following
AWS Lambda lets you run code without provisioning or managing servers. You pay only for the compute time you consume - there is no charge when your code is not running.
With Lambda, you can run code for virtually any type of application or backend service - all with zero administration. Just upload your code and Lambda takes care of everything required to run and scale your code with high availability. You can set up your code to automatically trigger from other AWS services or call it directly from any web or mobile app.

Amazon API Gateway is a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale. With a few clicks in the AWS Management Console, you can create an API that acts as a "front door" for applications to access data, business logic, or functionality from your back-end services, such as workloads running on Amazon Elastic Compute Cloud (Amazon EC2), code running on AWS Lambda, or any web application.
Option C is incorrect since this is a configuration service available from AWS
Option D is incorrect since this is less cost effective than using AWS Lambda
For more information on AWS Lambda and the API gateway, please refer to the below URL
https://aws.amazon.com/api-gateway/ (https://aws.amazon.com/api-gateway/)
https://aws.amazon.com/lambda/ (https://aws.amazon.com/lambda/)

Ask our Experts

QUESTION 12 CORRECT

Your company is planning on the following architecture for their application

- A set of EC2 Instances hosting the web part of the application.
- A relational database for the backend

- A Load balancer for distribution of traffic

Now due to the critical nature of the data stored on the underlying EBS volumes for the EC2 Instances, it needs to ensured that the data is available in another region for disaster recovery purposes. Which of the of the following would you consider complying with this requirement?

- **A.** Create a copy of the volume in another region.
- **B.** Create a snapshot from the volume in another region.
- **C.** Create a snapshot. Copy the snapshot to the new region. ✔
- **D.** Create a copy of the volume. Copy the volume to the new region.

Explanation :

Answer – C
The AWS Documentation showcases the use cases of EBS snapshots
Use Cases

- Geographic expansion: Launch your applications in a new region.
- Migration: Move an application to a new region, to enable better availability and to minimize cost.
- Disaster recovery: Back up your data and logs across different geographical locations at regular intervals. In case of disaster, you can restore your applications using point-in-time backups stored in the secondary region. This minimizes data loss and recovery time.
- Encryption: Encrypt a previously unencrypted snapshot, change the key with which the snapshot is encrypted, or, for encrypted snapshots that have been shared with you, create a copy that you own in order to restore a volume from it.
- Data retention and auditing requirements: Copy your encrypted EBS snapshots from one AWS account to another to preserve data logs or other files for auditing or data retention. Using a different account helps prevent accidental snapshot deletions, and protects you if your main AWS account is compromised.

Options A and D are incorrect , since you need to create a snapshot
Option B is incorrect since you cannot directly create a snapshot in another region
For more information on EBS Snapshot copy, please refer to the below URL
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-copy-snapshot.html
(https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-copy-snapshot.html)

Ask our Experts

QUESTION 13 CORRECT

An application consists of a fleet of EC2 Instances. These Instances are launched in the Oregon region which consists of 3 availability zones (us-west-2a, us-west-2b, us-west-2c). This application needs 6 Instances running at all times. As an architect you need to distribute the instances in such a way that the application could still maintain its capacity if any one availability zone were to go down. Also, you need to ensure that the cost is kept to a minimum? Which of the following configurations would you consider?

- **A.** 6 Instances running in us-west-2a, 6 Instances running in us-west-2b, 6 Instances running in us-west-2c
- **B.** 3 Instances running in us-west-2a, 3 Instances running in us-west-2b, 3 Instances running in us-west-2c ✔
- **C.** 4 Instances running in us-west-2a, 2 Instances running in us-west-2b, 2 Instances running in us-west-2c
- **D.** 6 Instances running in us-west-2a, 3 Instances running in us-west-2b, 3 Instances running in us-west-2c

Explanation :

Answer – B
So now let's look at Option A
If any availability zone goes down, we will have a total of 12 instances running. This is an additional 6 over the requirement of the question and will result in a higher cost.
So now let's look at Option C
If the availability zone us-west-2a goes down, then you will have only 4 instances running. His does not meet our minimum requirement for 6 instances running.
So now let's look at Option D
if either us-west-2b or us-west-2c availability zone goes down, we will have a total of 9 instances running. This is an additional 3 over the requirement of the question and will result in a higher cost.
For more information on Regions and Availability zones, please refer to the below URL
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html)

Ask our Experts

QUESTION 14 CORRECT

You have a set of EC2 Instances in a custom VPC. You have installed a web application and need to ensure that only HTTP and secure traffic is allowed into the instance. Which of the following would you consider for this requirement?

- **A.** Add a security group rule to allow HTTP and HTTPS Traffic ✔
- **B.** Place an explicit DENY rule on all traffic and a default allow on HTTP and HTTPS Traffic
- **C.** Add a security group rule to deny explicit traffic on HTTP and HTTPS Traffic
- **D.** Add a security group rule to allow all traffic

Explanation :

Answer – A
The below snapshot from the AWS Documentation shows the security groups examples for web servers

The kind of rules you add can depend on the purpose of the instance. The following table describes example rules for a security group for web servers. The web servers can receive HTTP and HTTPS traffic from all IPv4 and IPv6 addresses, and send SQL or MySQL traffic to a database server.

Inbound			
Source	**Protocol**	**Port Range**	**Comments**
0.0.0.0/0	TCP	80	Allow inbound HTTP access from all IPv4 addresses
::/0	TCP	80	Allow inbound HTTP access from all IPv6 addresses
0.0.0.0/0	TCP	443	Allow inbound HTTPS access from all IPv4 addresses
::/0	TCP	443	Allow inbound HTTPS access from all IPv6 addresses
Your network's public IPv4 address range	TCP	22	Allow inbound SSH access to Linux instances from IPv4 IP addresses in your network (over the Internet gateway)
Your network's public IPv4 address range	TCP	3389	Allow inbound RDP access to Windows instances from IPv4 IP addresses in your network (over the Internet gateway)

Options B and C are incorrect since the default option is to DENY all traffic
Option D is incorrect since this would be a security issue
For more information on VPC Security groups, please refer to the below URL
https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html
(https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html)

Ask our Experts

QUESTION 15 CORRECT

A company has an application defined with the following architecture

- A fleet of EC2 Instances which are used to accept video uploads from users

- A fleet of EC2 Instances which are used to process the video uploads

Which of the following would help architect an operationally excellent architecture?

- **A.** Create an SQS queue to store the information for Video uploads. Spin up the processing servers via an Autoscaling Group. Ensure the Group scales based on the Memory utilization of the underlying processing servers
- **B.** Create an SQS queue to store the information for Video uploads. Spin up the processing servers via an Autoscaling Group. Ensure the Group scales based on the size of the queue ✔
- **C.** Create an SNS topic to store the information for Video uploads. Spin up the processing servers via an Autoscaling Group. Ensure the Group scales based on the Memory utilization of the underlying processing servers
- **D.** Create an SNS topic to store the information for Video uploads. Spin up the processing servers via an Autoscaling Group. Ensure the Group scales based on the size of the queue messages

Explanation :

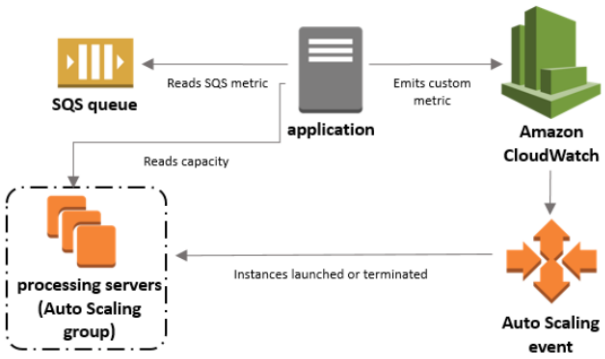
Answer – B

This architecture is also given in the AWS Documentation

There are three main parts to this configuration:

- An Auto Scaling group to manage EC2 instances for the purposes of processing messages from an SQS queue.
- A custom metric to send to Amazon CloudWatch that measures the number of messages in the queue per EC2 instance in the Auto Scaling group.
- A target tracking policy that configures your Auto Scaling group to scale based on the custom metric and a set target value. CloudWatch alarms invoke the scaling policy.

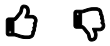
The following diagram illustrates the architecture of this configuration.



Option A is incorrect the ideal approach is to scale the instances based on the size of queue.
Options C and D are incorrect since you should be using SQS queues. SNS topics are used for notification purposes.
For more information on using SQS queues for Autoscaling, please refer to the below URL

https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-using-sqs-queue.html (https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-using-sqs-queue.html)

Ask our Experts



QUESTION 16 CORRECT

A company has an application that currently processes a lot of data streams that need to be processed in real time. You need to process these streams and create dashboards based after the processing is complete. Which of the following can be used to help fulfil this requirement?

- A. AWS ElasticSearch
- B. AWS Kinesis Data Streams ✔
- C. AWS Athena
- D. AWS Redshift

Explanation :

Answer - B
The AWS Documentation mentions the following
You can use Amazon Kinesis Data Streams to collect and process large streams (https://aws.amazon.com/streaming-data/) of data records in real time. You can create data-processing applications, known as *Kinesis Data Streams applications*. A typical Kinesis Data Streams application reads data from a *data stream* as data records. These applications can use the Kinesis Client Library, and they can run on Amazon EC2 instances. You can send the processed records to dashboards, use them to generate alerts, dynamically change pricing and advertising strategies, or send data to a variety of other AWS services

- Option A is incorrect since this is a search service which is available in AWS
- Option C is incorrect since is used for getting data via SQL queries from data sources such as S3
- Option D is incorrect since is used for petabyte data storage

- For more information on AWS Data Streams, please refer to the below URL???????????
  - https://docs.aws.amazon.com/streams/latest/dev/introduction.html (https://docs.aws.amazon.com/streams/latest/dev/introduction.html)

Ask our Experts

QUESTION 17 MARKED AS REVIEW CORRECT

A company has an Amazon Aurora cluster setup. They have setup a Lambda function which needs to insert records into a DynamoDB table. The Amazon Aurora cluster needs to invoke the Lambda as a stored procedure. Which of the following need to be in place for this setup to work. Choose 2 answers from the options given below

- [ ] **A.** Ensure that the Lambda function has an IAM Role assigned to it which can be used to invoke functions on Amazon Aurora
- [x] **B.** Ensure that the Amazon Aurora cluster has an IAM Role which allows it to invoke Lambda functions ✔
- [ ] **C.** Allow the Lambda function to allow outbound communication to Amazon Aurora
- [x] **D.** Allow the Amazon Aurora cluster to allow outbound communication to the Lambda function ✔

Explanation :

Answer – B and D

The below snapshot from the AWS Documentation shows what are the different steps required to ensure that the Lambda function has access to Amazon Aurora

Giving Aurora Access to Lambda

Before you can invoke Lambda functions from an Aurora MySQL, you must first give your Aurora MySQL DB cluster permission to access Lambda.

To give Aurora MySQL access to Lambda

1. Create an AWS Identity and Access Management (IAM) policy that provides the permissions that allow your Aurora MySQL DB cluster to invoke Lambda functions. For instructions, see Creating an IAM Policy to Access AWS Lambda Resources.
2. Create an IAM role, and attach the IAM policy you created in Creating an IAM Policy to Access AWS Lambda Resources to the new IAM role. For instructions, see Creating an IAM Role to Allow Amazon Aurora to Access AWS Services.
3. Set the `aws_default_lambda_role` DB cluster parameter to the Amazon Resource Name (ARN) of the new IAM role.

   For more information about DB cluster parameters, see Amazon Aurora DB Cluster and DB Instance Parameters.
4. To permit database users in an Aurora MySQL DB cluster to invoke Lambda functions, associate the role that you created in Creating an IAM Role to Allow Amazon Aurora to Access AWS Services with the DB cluster. For information about associating an IAM role with a DB cluster, see Associating an IAM Role with an Amazon Aurora MySQL DB Cluster.
5. Configure your Aurora MySQL DB cluster to allow outbound connections to Lambda. For instructions, see Enabling Network Communication from Amazon Aurora MySQL to Other AWS Services.

Options A and C are incorrect since the configurations need to be the other way around
For more information on integrating AWS Lambda with Aurora, please refer to the below URL
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/AuroraMySQL.Integrating.Lambda.html
(https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/AuroraMySQL.Integrating.Lambda.html)

Ask our Experts

QUESTION 18 CORRECT

Your application consists of a set of EC2 Instances which are spun up as part of an Autoscaling Group. These Instances need to access objects in an S3 bucket. Which of the following is the ideal approach to ensure this access is set in place?

- **A.** Ensure that the Access Keys are picked up from another S3 bucket. The Access Keys can be embedded in the User data during Instance Launch.
- **B.** Ensure that the Autoscaling Group attaches an IAM Role attached to the underlying EC2 Instances. ✔
- **C.** Ensure that an IAM policy is attached to the S3 bucket which allows access to the S3 buckets.
- **D.** Ensure that the Autoscaling Group attaches an IAM User attached to the underlying EC2 Instances.

Explanation :

Answer – B
Applications must sign their API requests with AWS credentials. Therefore, if you are an application developer, you need a strategy for managing credentials for your applications that run on EC2 instances. For example, you can securely distribute your AWS credentials to the instances, enabling the applications on those instances to use your credentials to sign requests, while protecting your credentials from other users. However, it's challenging to securely distribute credentials to each instance, especially those that AWS creates on your behalf, such as Spot Instances or instances in Auto Scaling groups. You must also be able to update the credentials on each instance when you rotate your AWS credentials.
We designed IAM roles so that your applications can securely make API requests from your instances, without requiring you to manage the security credentials that the applications use.
Option A is incorrect since using Access keys is the least secure option
Option C is incorrect since the IAM policy is not the right option , you have to use IAM Roles instead
Option D is incorrect since you need to use IAM Roles and not IAM Users
For more information on IAM Roles for EC2, please refer to the below URL
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html
(https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html)

Ask our Experts

QUESTION 19 CORRECT

You are an architect for a company that is going to be hosting an application in AWS. They want to load balance the traffic based on which route the user chooses. The 2 possible routes for the application are /customer and /orders. Which of the following would you include in the design?

- **A.** Application Load Balancer ✔
- **B.** EC2 Container service
- **C.** Classic Load Balancer
- **D.** Docker containers on EC2 Instances

Explanation :

Answer – A
The below snapshot from the AWS Documentation shows the benefits of using the Application Load

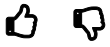
balancer

Using an Application Load Balancer instead of a Classic Load Balancer has the following benefits:

- Support for path-based routing. You can configure rules for your listener that forward requests based on the URL in the request. This enables you to structure your application as smaller services, and route requests to the correct service based on the content of the URL.
- Support for host-based routing. You can configure rules for your listener that forward requests based on the host field in the HTTP header. This enables you to route requests to multiple domains using a single load balancer.
- Support for routing requests to multiple applications on a single EC2 instance. You can register each instance or IP address with the same target group using multiple ports.
- Support for registering targets by IP address, including targets outside the VPC for the load balancer.
- Support for containerized applications. Amazon Elastic Container Service (Amazon ECS) can select an unused port when scheduling a task and register the task with a target group using this port. This enables you to make efficient use of your clusters.
- Support for monitoring the health of each service independently, as health checks are defined at the target group level and many CloudWatch metrics are reported at the target group level. Attaching a target group to an Auto Scaling group enables you to scale each service dynamically based on demand.
- Access logs contain additional information and are stored in compressed format.
- Improved load balancer performance.

Options B and D are incorrect since we don't have enough information on the question to decide on whether to use Docker containers or not.
Option C is invalid since Classic Load balancers will not fit the requirement for route-based load balancing
For more information on the Application Load Balancer, please refer to the below URL
https://docs.aws.amazon.com/elasticloadbalancing/latest/application/introduction.html
(https://docs.aws.amazon.com/elasticloadbalancing/latest/application/introduction.html)

Ask our Experts



QUESTION 20 CORRECT

Your company is planning on the following architecture for their application

- A set of EC2 Instances hosting the web part of the application.
- A relational database for the backend using the AWS RDS MySQL service
- A Load balancer for distribution of traffic

There is a requirement to ensure that all data hosted in the database service is encrypted at rest. How can you achieve this requirement in the easiest manner?

- **A.** Encrypt the underlying EBS volumes for the database
- **B.** Use the Encryption feature for RDS at database creation time. ✔
- **C.** Use S3 server-side encryption
- **D.** Use AWS Managed keys

Explanation :

Answer – B
The AWS Documentation mentions the following
You can encrypt your Amazon RDS instances and snapshots at rest by enabling the encryption option for your Amazon RDS DB instance. Data that is encrypted at rest includes the underlying storage for a DB instance, its automated backups, Read Replicas, and snapshots.
Options C and D are invalid because this is used for encryption of objects in S3.
Option A is incorrect since this can be easily achieved using the encryption feature for AWS RDS
For more information on Encryption for AWS RDS, 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 21 CORRECT

Your company is planning on hosting an application that will be based on Docker containers. They need to setup an orchestration service that would automatically scale based on the load. As much as possible , the company does not want the burden of managing the underlying infrastructure. Which of the following can assist in this scenario?

- **A.** AWS ECS with service autoscaling ✔
- **B.** Use an Elastic Load Balancer in front of an EC2 Instance. Use Docker containers on the EC2 Instance.

- **C.** Use Autoscaling with Spot Instances for the Orchestration Service.
- **D.** Use an Elastic Load Balancer in front of an EC2 Instance. Install and use Kubernetes on the EC2 Instance

Explanation :

Answer – A
The AWS Documentation mentions the following
Your Amazon ECS service can optionally be configured to use Service Auto Scaling to adjust its desired count up or down in response to CloudWatch alarms. Service Auto Scaling leverages the Application Auto Scaling service to provide this functionality. Service Auto Scaling is available in all regions that support Amazon ECS.
Amazon ECS publishes CloudWatch metrics with your service's average CPU and memory usage. You can use these service utilization metrics to scale your service out to deal with high demand at peak times, and to scale your service in to reduce costs during periods of low utilization.
Options B and D are incorrect since this would involve a lot of manual maintenance
Option C is incorrect since Spot Instances are volatile and should not be used for the orchestration service
For more information on AWS ECS with Autoscaling, please refer to the below URL
https://docs.aws.amazon.com/AmazonECS/latest/developerguide/service-auto-scaling.html
(https://docs.aws.amazon.com/AmazonECS/latest/developerguide/service-auto-scaling.html)

Ask our Experts

QUESTION 22 CORRECT

Your team has an application hosted on AWS. This application currently interacts with a DynamoDB table which has the Read capacity set to 10. Based on recent cloudwatch alarms which indicated that throttling was occurring in the requests to the DynamoDB table. Which of the following would help ensure the issue was resolved now and also help ensure the issue does not occur in the future?

- **A.** Add an Elastic Load Balancer in front of the DynamoDB table.
- **B.** Change the Read Capacity for the table to 20.
- **C.** Change the Write capacity for the table to offset the Read capacity.
- **D.** Enable Autoscaling for the underlying DynamoDB table. ✔

Explanation :

Answer – D
The AWS Documentation mentions the following
DynamoDB auto scaling uses the AWS Application Auto Scaling service to dynamically adjust provisioned throughput capacity on your behalf, in response to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read and write capacity to handle sudden increases in traffic, without throttling. When the workload decreases, Application Auto Scaling decreases the throughput so that you don't pay for unused provisioned capacity.
Option A is incorrect since the Elastic Load balancer in front of the DynamoDB table would be a wrong architecture decision
Option B is incorrect since this would only help in temporarily resolving the situation
Option C is incorrect since provisioning Write capacity would not help in this case
For more information on DynamoDB Autoscaling, please refer to the below URL
https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/AutoScaling.html
(https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/AutoScaling.html)

Ask our Experts

QUESTION 23 CORRECT

Your team is developing Lambda functions. These functions would need to interact with databases belonging to different environments. Which of the following is the ideal approach to ensuring that the Lambda functions are designed in the right way to interact with Databases in multiple environments?

- **A.** Create a lambda function for each environment
- **B.** Create a lambda function for each environment and ensure each has a different programming language
- **C.** Make use of environment variables to store the database connecting strings ✔
- **D.** Make use of AWS Lambda tags to store the database connecting strings

Explanation :

Answer – C
The AWS Documentation mentions the following

Environment variables for Lambda functions enable you to dynamically pass settings to your function code and libraries, without making changes to your code. Environment variables are key-value pairs that you create and modify as part of your function configuration, using either the AWS Lambda Console, the AWS Lambda CLI or the AWS Lambda SDK. AWS Lambda then makes these key value pairs available to your Lambda function code using standard APIs supported by the language, like process.env for Node.js functions.
You can use environment variables to help libraries know what directory to install files in, where to store outputs, store connection and logging settings, and more. By separating these settings from the application logic, you don't need to update your function code when you need to change the function behavior based on different settings.
For more information on AWS Lambda environment variables, please refer to the below URL
https://docs.aws.amazon.com/lambda/latest/dg/env_variables.html
(https://docs.aws.amazon.com/lambda/latest/dg/env_variables.html)

Ask our Experts

QUESTION 24 CORRECT

Your team has been instructed to develop an application that will make use of a DynamoDB table. During the design stage, you have to give you inputs to ensure that an optimal strategy is employed for a high read and write expectancy on the underlying DynamoDB table. Which of the following would you consider?

- **A.** Consider a lesser number of partition keys for the underlying table
- **B.** Use partition keys with a large number of distinct values for the underlying table ✔
- **C.** Use partition keys with a small number of distinct values for the underlying table
- **D.** Use partition keys with the number data type only

Explanation :

Answer – B
The AWS Documentation mentions the following

Recommendations for partition keys

Use high-cardinality attributes. These are attributes that have distinct values for each item like e-mail id, employee_no, customerid, sessionid, ordered, and so on.

Use composite attributes. Try to combine more than one attribute to form a unique key, if that meets your access pattern. For example, consider an orders table with **customerid+productid+countrycode** as the partition key and **order_date** as the sort key.

Cache the popular items when there is a high volume of read traffic. The cache acts as a low-pass filter, preventing reads of unusually popular items from swamping partitions. For example, consider a table that has deals information for products. Some deals are expected to be more popular than others during major sale events like Black Friday or Cyber Monday.

Add random numbers/digits from a predetermined range for write-heavy use cases. If you expect a large volume of writes for a partition key, use an additional prefix or suffix (a fixed number from predeternmined range, say 1-10) and add it to the partition key. For example, consider a table of invoice transactions. A single invoice can contain thousands of transactions per client. How do we enforce uniqueness and ability to query/update the invoice details for high-volumetric clients?

For more information on how to choose your partition key wisely, please refer to the below URL
https://aws.amazon.com/blogs/database/choosing-the-right-dynamodb-partition-key/
(https://aws.amazon.com/blogs/database/choosing-the-right-dynamodb-partition-key/)

Ask our Experts

QUESTION 25 CORRECT

Your company needs to have a data store in AWS to store data documents. These documents are not accessed that frequently. But when the document does get requested, it needs to be available within 20 minutes. Which of the following would be an ideal cost effective data store?

- A. S3 Infrequent Access ✔

- B. Glacier – Bulk retrieval
- C. Glacier – Standard Retrieval
- D. S3 Standard Storage

Explanation :

Answer – A
The AWS Documentation mentions the following
Amazon S3 Standard-Infrequent Access (S3 Standard-IA) is an Amazon S3 storage class for data that is accessed less frequently but requires rapid access when needed. S3 Standard-IA offers the high durability, high throughput, and low latency of S3 Standard, with a low per GB storage price and per GB retrieval fee. This combination of low cost and high performance make S3 Standard-IA ideal for long-term storage, backups, and as a data store for disaster recovery.
Options B and C are incorrect since the data retrieval time is more than 20 minutes and does not meet the requirements of the question
Option D is incorrect since this would not be a cost-effective option
For more information on the different storage classes, please refer to the below URL
https://aws.amazon.com/s3/storage-classes/ (https://aws.amazon.com/s3/storage-classes/)

Ask our Experts

QUESTION 26 CORRECT

Your company has a set of applications hosted on AWS. Currently, the IT administrators manually check for the size of the databases to see if the space is getting over. Which of the following can be used to automate these checks?

- A. CloudTrail
- B. Cloudwatch ✔
- C. VPC Flow Logs
- D. AWS Trusted Advisor

Explanation :

Answer – B

The AWS Documentation mentions the following

Monitoring Tools

AWS provides various tools that you can use to monitor Amazon RDS. You can configure some of these tools to do the monitoring for you, while some of the tools require manual intervention. We recommend that you automate monitoring tasks as much as possible.

Automated Monitoring Tools

You can use the following automated monitoring tools to watch Amazon RDS and report when something is wrong:

- **Amazon RDS Events** - Subscribe to Amazon RDS events to be notified when changes occur with a DB instance, DB snapshot, DB parameter group, or DB security group. For more information, see Using Amazon RDS Event Notification.
- **Database log files** - View, download, or watch database log files using the Amazon RDS console or Amazon RDS API actions. You can also query some database log files that are loaded into database tables. For more information, see Amazon RDS Database Log Files.
- **Amazon RDS Enhanced Monitoring** — Look at metrics in real time for the operating system. For more information, see Enhanced Monitoring.

In addition, Amazon RDS integrates with Amazon CloudWatch for additional monitoring capabilities:

- **Amazon CloudWatch Metrics** - Amazon RDS automatically sends metrics to CloudWatch every minute for each active database. You are not charged additionally for Amazon RDS metrics in CloudWatch. For more information, see Viewing DB Instance Metrics.
- **Amazon CloudWatch Alarms** - You can watch a single Amazon RDS metric over a specific time period, and perform one or more actions based on the value of the metric relative to a threshold you set. For more information, see Monitoring with Amazon CloudWatch
- **Amazon CloudWatch Logs** - Most DB engines enable you to monitor, store, and access your database log files in CloudWatch Logs. For more information, see Amazon CloudWatch Logs User Guide

Option A is incorrect since this is only used for API monitoring

Option C is incorrect since this is used for monitoring network traffic to your EC2 Instances
Option D is incorrect this only gives recommendations
For more information on monitoring for databases, please refer to the below URL
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/MonitoringOverview.html
(https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/MonitoringOverview.html)

Ask our Experts

QUESTION 27 CORRECT

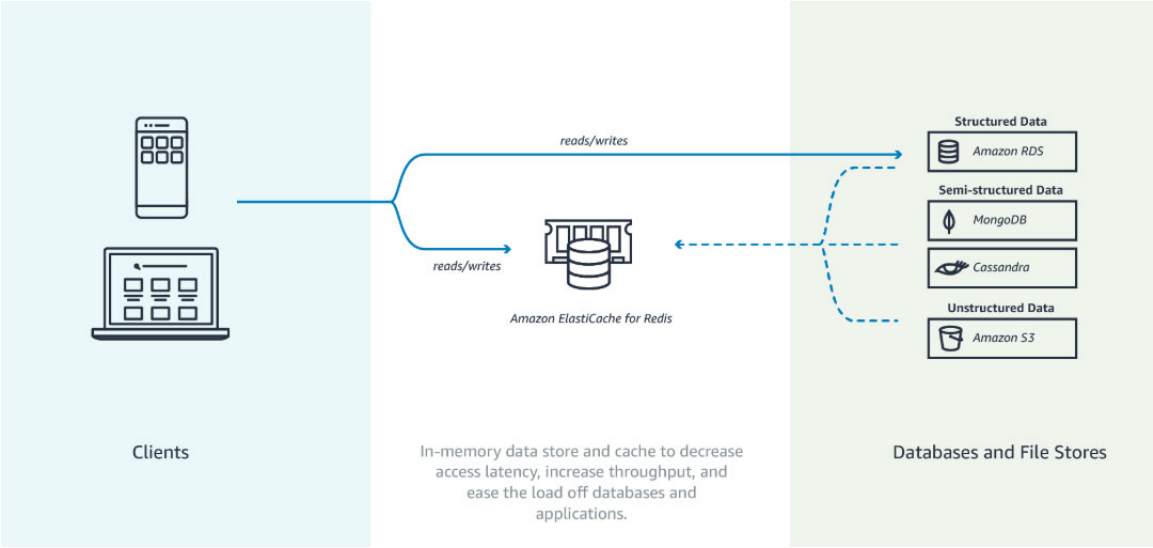
Your company has an application hosted in AWS. This application consists of a web tier and database tier. The web tier is hosted on EC2 Instances. The database is hosted in the AWS RDS service. Recently performance issues have been encountered in the application and this is due to the advanced latency of requests due to the high number of read requests. Which of the following can be used to help resolve the issue?

- A. Enable Multi-AZ for the database
- B. Place an Elastic Load Balancer in front of the database service
- C. Place an Autoscaling Group in front of the database server
- D. Place an Elastic Cache service in front of the database service ✔

Explanation :

Answer -D

The below diagram from the AWS Documentation shows the architecture of how ElastiCache can be used to reduce the latency of requests to the AWS RDS service



Option A is incorrect since this is used for high availability for the databases

Option B is incorrect since this will only divert the traffic but not reduce the load

Option C is incorrect since the Autoscaling Group would not reduce the latency of requests

For more information on ElastiCache use cases, please refer to the below URL

https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/elasticache-use-cases.html (https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/elasticache-use-cases.html)

Ask our Experts

QUESTION 28 CORRECT

Your company is developing an application for a restaurant. The application will basically record the list of people waiting to be given tables at the restaurant. It needs to ensured that the order of requests are maintained when they are recorded in the application. Which of the following service would you have in the architecture?

- A. Simple Notification Service
- B. Elastic Cache
- C. FIFO queues in Simple Queue Service ✔
- D. Standard Queues in Simple Queue Service

Explanation :

Answer – C
The AWS Documentation mentions the following
FIFO (First-In-First-Out) queues are designed to enhance messaging between applications when the order of operations and events is critical, or where duplicates can't be tolerated, for example:

- Ensure that user-entered commands are executed in the right order.
- Display the correct product price by sending price modifications in the right order.
- Prevent a student from enrolling in a course before registering for an account.

Option A is incorrect since this is a notification service
Option B is incorrect since this is used as a caching service
Option D is incorrect since Standard queues does not guarantee the order of requests
For more information on FIFO queues, please refer to the below URL
https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/FIFO-queues.html
(https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/FIFO-queues.html)

Ask our Experts

QUESTION 29 CORRECT

Your company has an application that has been developed and needs to be hosted on an EC2 Instance. The EC2 Instance is located in a private subnet and needs to access AWS Kinesis streams without passing into the Internet. How can you achieve this in the best manner possible?

- A. Attach a NAT gateway to the VPC
- B. Attach an Internet gateway to the VPC
- C. Create a VPC Gateway Endpoint that would allow access to Kinesis Streams
- D. Create a VPC Interface Endpoint that would allow access to Kinesis Streams ✔

Explanation :

Answer – D
The AWS Documentation mentions the following
You can use an interface VPC endpoint to keep traffic between your Amazon VPC and Kinesis Data Streams from leaving the Amazon network. Interface VPC endpoints don't require an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Interface VPC endpoints are powered by AWS PrivateLink, an AWS technology that enables private communication between AWS services using an elastic network interface with private IPs in your Amazon VPC
Options A and B are incorrect since it is mentioned in the question that traffic should not go via the Internet
Option C is incorrect since this is mostly used for S3 and DynamoDB access from Instances in the private subnet
For more information on VPC Endpoints Interfaces, please refer to the below URL
https://docs.aws.amazon.com/streams/latest/dev/vpc.html
(https://docs.aws.amazon.com/streams/latest/dev/vpc.html)

Ask our Experts

QUESTION 30 CORRECT

A company is planning to store sensitive documents in an S3 bucket. They want to ensure that documents are encrypted at rest. They want to ensure they manage the underlying keys which are used for encryption but not the encryption/decryption process. Which of the following can be used for this purpose? Choose 2 answers from the options given below

- [x] **A.** Use S3 server-side encryption with Customer keys ✔
- [ ] **B.** Use S3 client-side encryption
- [ ] **C.** Use S3 server-side encryption with AWS managed keys
- [ ] **D.** Use S3 server-side encryption with AWS KMS keys with Key policy document of size 40kb.
- [x] **E.** Use S3 server-side encryption with AWS KMS keys with the keys uploaded by the company to KMS ✔

Explanation :

Answer – A and E
The AWS Documentation mentions the following
Server-side encryption is about protecting data at rest. Using server-side encryption with customer-provided encryption keys (SSE-C) allows you to set your own encryption keys. With the encryption key you provide as part of your request, Amazon S3 manages both the encryption, as it writes to disks, and decryption, when you access your objects. Therefore, you don't need to maintain any code to perform data encryption and decryption. The only thing you do is manage the encryption keys you provide.

Options C is incorrect since here you will still not manage the complete lifecycle of the keys.
Options D is incorrect, because the maximum key policy document size is 32kb.
https://docs.aws.amazon.com/kms/latest/developerguide/limits.html (https://docs.aws.amazon.com/kms/latest/developerguide/limits.html)
Option E is correct since your own keys can be uploaded to the Key management service.
https://aws.amazon.com/blogs/aws/new-bring-your-own-keys-with-aws-key-management-service/ (https://aws.amazon.com/blogs/aws/new-bring-your-own-keys-with-aws-key-management-service/)
For more information on Server side encryption with customer keys and Client side encryption, please refer to the below URL

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

Ask our Experts

QUESTION 31 CORRECT

Your company currently has the following architecture for their ecommerce application

- EC2 Instances hosting the application
- An Autoscaling group for the EC2 Instances

The users who use the application keep on complaining that the application is slow in the morning from 9:00 – 9:30, after which there are no issues which occur. Which of the following can be done to ensure the issue is not encountered during the morning times?

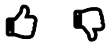
- **A.** Ensure that a dynamic scaling policy is added to the Autoscaling Group
- **B.** Ensure that a step scaling policy is added to the Autoscaling Group
- **C.** Ensure that a scheduled scaling policy is added to the Autoscaling Group ✔
- **D.** Ensure that a static scaling policy is added to the Autoscaling Group

Explanation :

Answer – C
The AWS Documentation mentions the following

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.
The other options will not work because the main issue is that the high-performance issues are because of the high number of users early in the morning. The option is to add a scheduled scaling policy to increase the number of servers before 9:00 itself to handle the high load.
For more information on scaling policies for Autoscaling, please refer to the below URL's
https://docs.aws.amazon.com/autoscaling/ec2/userguide/schedule_time.html (https://docs.aws.amazon.com/autoscaling/ec2/userguide/schedule_time.html)
https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scale-based-on-demand.html#as-scaling-types (https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scale-based-on-demand.html#as-scaling-types)

Ask our Experts



QUESTION 32 CORRECT

An application consists of the following architecture. EC2 Instances in multiple Availability Zones behind an Elastic Load Balancer. A NAT Instance in the public subnet which is used to download updates from the Internet. A database hosted in the AWS RDS service with Multi-AZ enabled. Which of the following is a bottleneck in the above architecture?

- A. EC2 Instances
- B. Elastic Load Balancer
- C. NAT Instance ✔
- D. The database

Explanation :

Answer – C
Here since the NAT instance itself is a single instance, it is a bottleneck in the architecture. Consider

adding the instance as part of an Autoscaling Group or replacing it with a NAT gateway.
For more information on the NAT gateway, please refer to the below URL
https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html
(https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html)

Ask our Experts

QUESTION 33 CORRECT

A company needs to develop an application that will do the following

- Upload images posted by users
- Store the Images in a durable location
- Store the metadata about that image in another durable data store

Which of the following should be consider in the design phase?

- **A.** Store the Images in Amazon Glacier and store the metadata in DynamoDB
- **B.** Store the Images in Amazon S3 and store the metadata in Amazon Glacier
- **C.** Store the Images in DynamoDB and store the metadata in Amazon S3
- **D.** Store the Images in Amazon S3 and store the metadata in DynamoDB ✔

Explanation :

Answer – D
Amazon S3 is used for object level storage and should be used to store files such as Images, videos etc. The metadata can be in JSON format which can then be stored in DynamoDB tables.
Options A and B are incorrect since Amazon Glacier is used for archive storage
Option C is incorrect since you cannot store images in DynamoDB
For more information on Amazon S3 and DynamoDB, please refer to the below URL
https://docs.aws.amazon.com/AmazonS3/latest/dev/Welcome.html
(https://docs.aws.amazon.com/AmazonS3/latest/dev/Welcome.html)
https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Introduction.html
(https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Introduction.html)

Ask our Experts

QUESTION 34 CORRECT

Your development team currently has a web application which they are working with in their on-premise environment. They need to port this to AWS in the easiest way possible with less maintenance overhead. But they still need to ensure they have control over the configuration of the web server itself. Which of the following service from AWS can be used to fulfil this requirement?

- A. AWS Elastic Compute Cloud
- B. AWS Lambda
- C. AWS Elastic Beanstalk ✔
- D. AWS Simple Queue Service

Explanation :

Answer – C
The AWS Documentation mentions the following
With Elastic Beanstalk, you can quickly deploy and manage applications in the AWS Cloud without worrying about the infrastructure that runs those applications. AWS Elastic Beanstalk reduces management complexity without restricting choice or control. You simply upload your application, and Elastic Beanstalk automatically handles the details of capacity provisioning, load balancing, scaling, and application health monitoring
Option A is incorrect since this would involve more effort in setting up the EC2 Instances and the applications
Option B is incorrect since here you want to have control over the web environment
Option D is incorrect since this is a messaging service
For more information on AWS Elastic beanstalk, please refer to the below URL
https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/Welcome.html
(https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/Welcome.html)
Note: We understand that you want better clarity on how is it possible to have control over web server configuration using Elastic Beanstalk.

With Elastic Beanstalk, AWS has provided the ability to either use preconfigured(with a variety of configurations) or create custom platform for web server deployments.

- Preconfigured platform: Platforms published and maintained by AWS Elastic Beanstalk
- Custom Platform: Platform owned and created by us

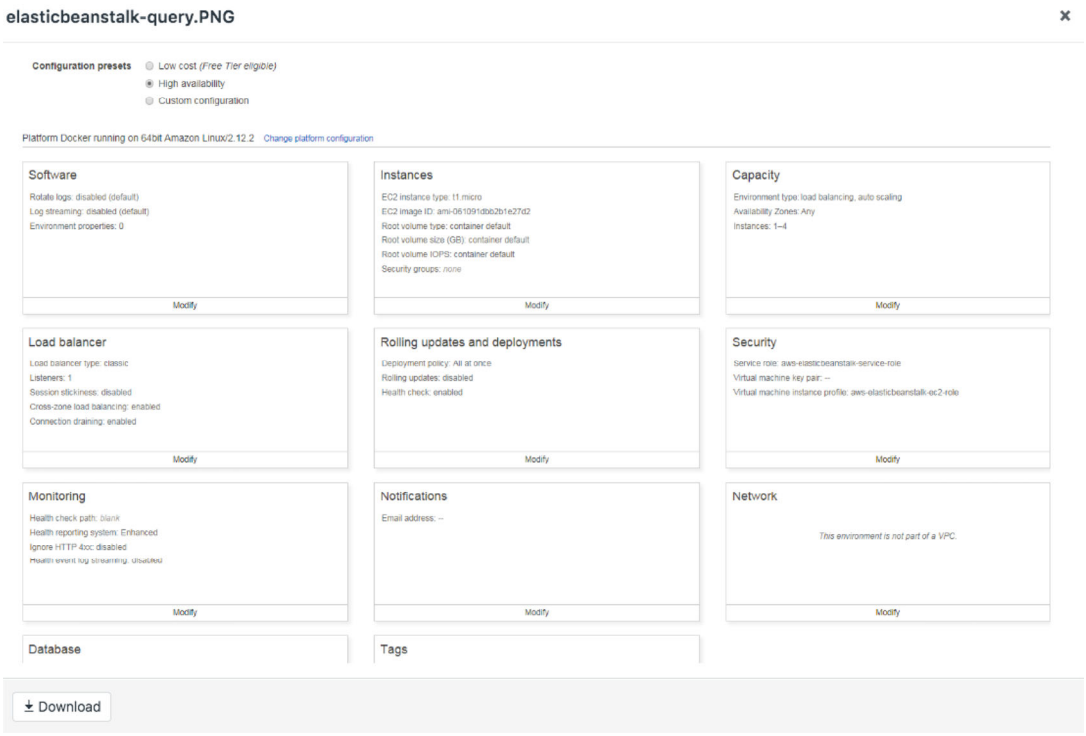
Here is the detailed guide to Elastic Beanstalk Supported platforms:
Supported Platforms Elastic BeanStalk
(https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/customize-containers.html)

We do get an option to choose below web server configurations while creating pre-configured platforms:

- EC2 Instance Types and various properties
- Notifications to Set of users
- Setup load balancer(Classic and ALB) and Autoscaling (if High Availability is enabled) and many more

Here is the detailed guide to different configurations available as part of the Elastic Beanstalk Web server environment:
Custom Configurations Elastic Beanstalk
(https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/customize-containers.html)

Attaching screenshot for different configurations options you get while creating ElasticBeanStalk Environments



Ask our Experts

QUESTION 35 CORRECT

A company has a requirement to monitor API activity for audit purposes for their AWS account. This audit would be conducted in the future as well and should be applicable to all regions. How would you design your solution to meet the present and future needs?

- **A.** Ensure Cloudtrail logs is enabled for each region and then enable for each future region.
- **B.** Ensure one Cloudtrail log is enabled for all regions ✔
- **C.** Enable Cloudtrail and AWS Config to record the events in all regions.
- **D.** Enable Cloudtrail and AWS Inspector to record the events in all regions.

Explanation :

Answer – B
The AWS Documentation mentions the following
When you create a trail that applies to all regions, CloudTrail records events in each region and delivers the CloudTrail event log files to an S3 bucket that you specify. If a region is added after you create a trail that applies to all regions, that new region is automatically included, and events in that region are logged.
Option A is incorrect since this is an overhead to enable it each time for every new region
Options C and D are incorrect since the AWS Config and AWS Inspector services are used for different purposes.
For more information on AWS CloudTrail, please refer to the below URL
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/how-cloudtrail-works.html (https://docs.aws.amazon.com/awscloudtrail/latest/userguide/how-cloudtrail-works.html)

Ask our Experts

QUESTION 36 CORRECT

Your team is planning on developing and deploying an application onto AWS with the following architecture

- A set of EC2 Instances in a VPC hosting the web tier
- A database hosted using the AWS RDS MySQL instance

Which of the following should ideally be set for users to be able to access the web application and for the web application to access the database. Choose 2 answers from the options given below?

- [x] **A.** An Inbound Security group rule for the web EC2 Instances allowing traffic from the source of 0.0.0.0/0 ✔
- [ ] **B.** An Inbound Security group rule for the database layer allowing traffic from the source of 0.0.0.0/0
- [ ] **C.** An Inbound Security group rule for the web EC2 Instances allowing traffic from the source of the database on port 3306
- [x] **D.** An Inbound Security group rule for the database layer allowing traffic from the source of the web layer on port 3306 ✔

Explanation :

Answer – A and D
The AWS Documentation gives an example of this scenario and the recommended security group rules

WebServerSG: Recommended Rules

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

DBServerSG: Recommended Rules

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

Option B is invalid since the database should not be exposed to the Internet
Option C is invalid since the database security group should allow incoming traffic on port 3306
For more information on this scenario, please refer to the below URL
https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Scenario2.html
(https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Scenario2.html)

Ask our Experts

QUESTION 37 CORRECT

Your company is planning on setting up the following architecture in AWS

- A set of EC2 Instances behind a Classic ELB for the presentation layer.
- A set of proxy servers hosted on EC2 Instances
- A set of backend instances

Which of the following can be used to enhance the scalability of the above architecture? Choose 2 answers from the options given below

- [x] **A.** Use Autoscaling for the proxy servers ✔
- [x] **B.** Use Autoscaling for the backend instances ✔
- [ ] **C.** Replace the Classic ELB with Application ELB
- [ ] **D.** Replace the Classic ELB with Network ELB

Explanation :

Answer – A and B

You can increase scalability by ensuring that your proxy servers and backend instances are part of an Autoscaling Group
The AWS Documentation mentions the following
Amazon EC2 Auto Scaling helps you ensure that you have the correct number of Amazon EC2 instances available to handle the load for your application. You create collections of EC2 instances, called Auto Scaling groups. You can specify the minimum number of instances in each Auto Scaling group, and Amazon EC2 Auto Scaling ensures that your group never goes below this size. You can specify the maximum number of instances in each Auto Scaling group, and Amazon EC2 Auto Scaling ensures that your group never goes above this size. If you specify the desired capacity, either when you create the group or at any time thereafter, Amazon EC2 Auto Scaling ensures that your group has this many instances. If you specify scaling policies, then Amazon EC2 Auto Scaling can launch or terminate instances as demand on your application increases or decreases.
Options C and D are incorrect since the Classic Load balancer is also a scalable service
For more information on Autoscaling, please refer to the below URL
https://docs.aws.amazon.com/autoscaling/ec2/userguide/what-is-amazon-ec2-auto-scaling.html (https://docs.aws.amazon.com/autoscaling/ec2/userguide/what-is-amazon-ec2-auto-scaling.html)

Ask our Experts

QUESTION 38 CORRECT

A Company is currently hosting an application which connects to a MySQL AWS RDS Instance. Of late there have been many performance issues being encountered. After careful analysis, it has been determined that the issue is occurring as a result of similar queries being fired against the database. Which of the following can be added to the architecture to alleviate the performance issue?

- A. Enable Multi-AZ for the database
- B. Use the Elastic Cache Service ✔
- C. Place a Load balancer in front of the database
- D. Use Cloudfront in front of the database

Explanation :

Answer – B
The AWS Documentation mentions the following

Amazon ElastiCache offers fully managed Redis and Memcached. Seamlessly deploy, operate, and scale popular open source compatible in-memory data stores. Build data-intensive apps or improve the performance of your existing apps by retrieving data from high throughput and low latency in-memory data stores. Amazon ElastiCache is a popular choice for Gaming, Ad-Tech, Financial Services, Healthcare, and IoT apps.
Option A is incorrect since this is used for high availability of the database
Option C is incorrect since this will only distribute the load but not reduce it
Option D is incorrect since Cloudfront should be used with Web distributions
For more information on ElastiCache, please refer to the below URL
https://aws.amazon.com/elasticache/ (https://aws.amazon.com/elasticache/)

Ask our Experts

QUESTION 39 MARKED AS REVIEW INCORRECT

A company has a set of EC2 Instances hosting a custom based application which is listening on port 3308. All of a sudden there seems to be a barrage of requests coming in from a source IP address of 52.0.9.10. Which of the following can be used to stop requests from entering the VPC from this IP address.

- A. Network ACL's ✔
- B. Security Groups ✖
- C. VPC Flow Logs
- D. AWS CloudTrail

Explanation :

Answer – A
The AWS Documentation mentions the following
A *network access control list (ACL)* is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC.
Option B is incorrect since the Security Groups can only allow, but not deny traffic.
Option C is incorrect since this is used for monitoring your network traffic into the VPC
Option D is incorrect since this is used for API Monitoring

For more information on Network Security Group Rules, please refer to the below URL
https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html
(https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html)

Ask our Experts

QUESTION 40 INCORRECT

A Company is currently hosting an application which connects to a MySQL AWS RDS Instance The application behaves fine when there are 20 lookups against the database. When the lookups start to increase, the performance of the application starts to degrade. Which of the following can be added to the architecture to alleviate the performance issue?

- A. Create a Read Replica for the database ✔
- B. Enable Multi-AZ for the database ✖
- C. Place the database behind a Cloudfront distribution
- D. Create a snapshot of the database

Explanation :

Answer – A
Option B is incorrect since this is used for high availability of the database
Option C is incorrect since Cloudfront is used for web distributions
Option D is incorrect since this is used for backups of databases
The AWS Documentation mentions the following
Amazon RDS Read Replicas provide enhanced performance and durability for database (DB) instances. This feature makes it easy to elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads. You can create one or more replicas of a given source DB Instance and serve high-volume application read traffic from multiple copies of your data, thereby increasing aggregate read throughput.
For more information on AWS Read Replica's, please refer to the below URL
https://aws.amazon.com/rds/details/read-replicas/ (https://aws.amazon.com/rds/details/read-replicas/)

Ask our Experts

QUESTION 41 CORRECT

Your company needs to develop an application that needs to have a login module in place. They key requirement is to ensure that users can also use their current identities which they have with various providers such as facebook to log into the application. Which of the following can help you accomplish this?

- A. Using the AWS Cognito service ✔
- B. Using the AWS Config service
- C. Using the AWS SQS service
- D. Using the AWS WAF service

Explanation :

Answer – A
The AWS Documentation mentions the following
Amazon Cognito provides authentication, authorization, and user management for your web and mobile apps. Your users can sign in directly with a user name and password, or through a third party such as Facebook, Amazon, or Google.
The two main components of Amazon Cognito are user pools and identity pools. User pools are user directories that provide sign-up and sign-in options for your app users. Identity pools enable you to grant your users access to other AWS services. You can use identity pools and user pools separately or together.
Option B is incorrect since this is a configuration service
Option C is incorrect since this is a messaging service
Option D is incorrect since this is a web application firewall service
For more information on AWS Cognito, please refer to the below URL
https://docs.aws.amazon.com/cognito/latest/developerguide/what-is-amazon-cognito.html
(https://docs.aws.amazon.com/cognito/latest/developerguide/what-is-amazon-cognito.html)

Ask our Experts

QUESTION 42 CORRECT

A company is currently hosting a web application on an EC2 Instance. The number of requests on the application is increasing now there is a latency being experience by users when requesting for the web pages. Which of the following can be used to reduce the latency?

- **A.** Place an Elastic Load balancer in front of the EC2 Instance
- **B.** Place the EC2 Instance as an origin behind Cloudfront. ✔
- **C.** Add more EBS volumes for the instance
- **D.** Add more read replica's for the EC2 Instance

Explanation :

Answer – B
The AWS Documentation mentions the following
Amazon CloudFront is a web service that speeds up distribution of your static and dynamic web content, such as .html, .css, .js, and image files, to your users. CloudFront delivers your content through a worldwide network of data centers called edge locations. When a user requests content that you're serving with CloudFront, the user is routed to the edge location that provides the lowest latency (time delay), so that content is delivered with the best possible performance.
Option A is incorrect since this can only distribute requests and is useless without the addition of more instances to the architecture.
Option C is incorrect since this can only be used to increase the storage space
Option D is incorrect since this is normally used for the AWS RDS service
For more information on AWS Cloudfront, please refer to the below URL
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html
(https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html)

Ask our Experts

QUESTION 43 CORRECT

Your current architecture consist of a set of web servers that are spun up as part of an Autoscaling group. These web servers then communicate with a set of database servers. You need to ensure that the security groups of the database servers are set properly to accept traffic from the web servers. Which of the following is the best way to accomplish this?

- **A.** Ensure that the Private IP addresses of the web servers are put as sources for the incoming rules in the database server security group
- **B.** Ensure that the Public IP addresses of the web servers are put as sources for the incoming rules in the database server security group
- **C.** Ensure that the web server security group is placed as the source for the incoming rules in the database server security group ✔
- **D.** Ensure that the Instance ID of the web servers are put as sources for the incoming rules in the database server security group

Explanation :

Answer – C

The below example from the AWS Documentation also shows the Source of the database security group involving the ID of the web server security groups.

DBServerSG: Recommended Rules

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

Options A and B are invalid or not the best practise. Since they are part of the Autoscaling Group , the IP addresses of the instances can change.

Option D is incorrect since normally you don't specify the Instance ID in security Groups

For more information on the Security Groups for the VPC, please refer to the below URL

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Scenario2.html

(https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Scenario2.html)

Ask our Experts

QUESTION 44 CORRECT

Your company needs to host an application on an EC2 Instance. There is a requirement based on the compliance rules for the application that you need to have control over the number of cores allocated to the application. Which of the following should be used in such a case?

- A. AWS Lambda
- B. EC2 - Dedicated Hosts ✔
- C. EC2 – Reserved Instances
- D. Elastic Beanstalk

Explanation :

Answer – B
The AWS Documentation mentions the following
When you launch instances on a Dedicated Host, the instances run on a physical server that is dedicated for your use. While Dedicated instances also run on dedicated hardware, Dedicated Hosts provide further visibility and control by allowing you to place your instances on a specific, physical server. This enables you to deploy instances using configurations that help address corporate compliance and regulatory requirements.
You have visibility of the number of sockets and physical cores that support your instances on a Dedicated Host. You can use this information to manage licensing for your own server-bound software that is licensed per-socket or per-core.
Because of what is mentioned in the AWS Documentation , all other options are invalid
For more information on Dedicated Hosts, please refer to the below URL
https://aws.amazon.com/ec2/dedicated-hosts/ (https://aws.amazon.com/ec2/dedicated-hosts/)

Ask our Experts

QUESTION 45 MARKED AS REVIEW CORRECT

Your company is planning to store sensitive documents in a bucket in the Simple Storage service. They need to ensure that all objects are encrypted at rest in the bucket. Which of the following can help accomplish this? Choose 2 answers from the options given below

- [x] A. Ensure that the default encryption is enabled for the S3 bucket ✔
- [ ] B. Ensure that the bucket policy is set to encrypt all objects that are added to the bucket
- [ ] C. Ensure that the bucket ACL is set to encrypt all objects that are added to the bucket

☑ **D.** Ensure to change the configuration of the bucket to use a KMS key to encrypt the objects ✔

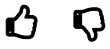
Explanation :

Answer – A and D
Options B and C are incorrect since these options cannot be used to actually encrypt the objects
The AWS Documentation mentions the following
You have three mutually exclusive options depending on how you choose to manage the encryption keys:

- Use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3) – Each object is encrypted with a unique key employing strong multi-factor encryption. As an additional safeguard, it encrypts the key itself with a master key that it regularly rotates..
- Use Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS) – Similar to SSE-S3, but with some additional benefits along with some additional charges for using this service. There are separate permissions for the use of an envelope key (that is, a key that protects your data's encryption key) that provides added protection against unauthorized access of your objects in S3.
- Use Server-Side Encryption with Customer-Provided Keys (SSE-C) – You manage the encryption keys and Amazon S3 manages the encryption, as it writes to disks, and decryption, when you access your objects.

For more information on Server - Side encryption, please refer to the below URL
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 46 MARKED AS REVIEW CORRECT

Your company has a series of web sites hosted in AWS. They need to ensure that users from the Europe region are directed to the website www.demo.com (http://www.demo.com) for regulatory purposes. Which of the following can help in this regard?

- A. Using the Elastic Load balancer service
- B. Using the Route 53 service ✔
- C. Using the Autoscaling service
- D. Using the AWS Config service

Explanation :

Answer – B
You have to use the GeoLocation routing policy in Route 53
The AWS Documentation mentions the following
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 example, you might want all queries from Europe to be routed to an ELB load balancer in the Frankfurt region.
When you use geolocation routing, you can localize your content and present some or all of your website in the language of your users. You can also use geolocation routing to restrict distribution of content to only the locations in which you have distribution rights. Another possible use is for balancing load across endpoints in a predictable, easy-to-manage way, so that each user location is consistently routed to the same endpoint.
Option A is incorrect since this can only distribute traffic and not direct traffic
Option C is incorrect since this is used to scale infrastructure
Option D is incorrect since this is used as a configuration service
For more information on a Routing policy, please refer to the below 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 47 CORRECT

A company is planning to host an active-active site. One site will be located in AWS and the other one on their On-premise data centre. They need to ensure that traffic is distributed accordingly between both the sites. Which of the following routing policy would you use for this purpose?

- A. Simple Routing
- B. Failover Routing

- C. Latency Routing
- D. Weighted Routing ✔

Explanation :

Answer – D
The AWS Documentation mentions the following
Weighted routing lets you associate multiple resources with a single domain name (example.com) or subdomain name (acme.example.com) and choose how much traffic is routed to each resource. This can be useful for a variety of purposes, including load balancing and testing new versions of software.
To configure weighted routing, you create records that have the same name and type for each of your resources. You assign each record a relative weight that corresponds with how much traffic you want to send to each resource. Amazon Route 53 sends traffic to a resource based on the weight that you assign to the record as a proportion of the total weight for all records in the group
Option A is incorrect since this should be used when you want to configure standard DNS records
Option B is incorrect since this should be used when you want to route traffic to a resource when the resource is healthy or to a different resource when the first resource is unhealthy
Option C is incorrect since this should be used when you want to improve performance for your users by serving their requests from the AWS Region that provides the lowest latency.
For more information on a Routing policy, please refer to the below 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 48 CORRECT

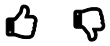
Your company is planning to store sensitive documents in a bucket in the Simple Storage service. They want to keep the documents as private but serve content only to select users based on a particular time frame. Which of the following can help you accomplish this?

- A. Enable CORS for the S3 bucket
- B. Use KMS and enable encryption for the files
- C. Create pre-signed URL's ✔
- D. Enable versioning for the S3 bucket

Explanation :

Answer – C
The AWS Documentation mentions the following
A pre-signed URL gives you access to the object identified in the URL, provided that the creator of the pre-signed URL has permissions to access that object. That is, if you receive a pre-signed URL to upload an object, you can upload the object only if the creator of the pre-signed URL has the necessary permissions to upload that object.
All objects and buckets by default are private. The pre-signed URLs are useful if you want your user/customer to be able to upload a specific object to your bucket, but you don't require them to have AWS security credentials or permissions. When you create a pre-signed URL, you must provide your security credentials and then specify a bucket name, an object key, an HTTP method (PUT for uploading objects), and an expiration date and time. The pre-signed URLs are valid only for the specified duration.
Option A is incorrect since this is used for Cross origin access
Option B is incorrect since this is used for encryption purposes.
Option D is incorrect since this is used for versioning
For more information on pre-signed URL's, please refer to the below 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 49 CORRECT

A company currently is hosting a Redshift cluster. As part of the disaster recovery drill , you need to ensure that the cluster would be made available even if the primary region goes down. How can you accomplish this?

- **A.** Use the Elastic Beanstalk service to copy the cluster to another region
- **B.** Use Cloudformation templates to copy the cluster to another region
- **C.** Configure cross-region snapshots for the underlying Redshift cluster. ✔

D. Use the snapshots stored in S3 to create a new Redshift cluster in another region

Explanation :

Answer - C
The AWS Documentation mentions the following
You can configure Amazon Redshift to automatically copy snapshots (automated or manual) for a cluster to another region. When a snapshot is created in the cluster's primary region, it will be copied to a secondary region; these are known respectively as the *source region* and *destination region*. By storing a copy of your snapshots in another region, you have the ability to restore your cluster from recent data if anything affects the primary region.
Because this is clearly mentioned in the AWS Documentation , all other options are invalid.
For more information on working with snapshots, please refer to the below URL
https://docs.aws.amazon.com/redshift/latest/mgmt/working-with-snapshots.html
(https://docs.aws.amazon.com/redshift/latest/mgmt/working-with-snapshots.html)

Ask our Experts

QUESTION 50 CORRECT

Your company is planning on hosting a batch processing workload on a large set of EC2 Instances. These batch processing workloads are not consistent in nature and they can be interrupted at any point in time. Which of the following is the ideal pricing type for the underlying EC2 Instance?

A. Spot Instances ✔

B. Dedicated Hosts

C. On-Demand Instances

D. Reserved Instances

Explanation :

Answer - A

The AWS Documentation mentions the following
A Spot Instance is an unused EC2 instance that is available for less than the On-Demand price.
Because Spot Instances enable you to request unused EC2 instances at steep discounts, you can lower your Amazon EC2 costs significantly. The hourly price for a Spot Instance is called a Spot price.
The Spot price of each instance type in each Availability Zone is set by Amazon EC2, and adjusted gradually based on the long-term supply of and demand for Spot Instances. Your Spot Instance runs whenever capacity is available and the maximum price per hour for your request exceeds the Spot price.
Spot Instances are a cost-effective choice if you can be flexible about when your applications run and if your applications can be interrupted
Because this is clearly mentioned in the AWS Documentation , all other options are invalid.
For more information on Spot Instances, please refer to the below URL
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-spot-instances.html
(https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-spot-instances.html)

Ask our Experts

QUESTION 51 MARKED AS REVIEW CORRECT

Your company currently has a set of web servers in a public subnet and database servers in the private subnet. You need to ensure administrators from your on-premises environment can access the database servers. Which of the following is a secure way to access the database servers?

- **A.** Create a bastion host in the private subnet as the database servers. Ask the IT administrators to log into the database servers via the bastion host
- **B.** Create a bastion host in the public subnet. Ask the IT administrators to log into the database servers via the bastion host ✔
- **C.** Create a NAT instance in the private subnet as the database servers. Ask the IT administrators to log into the database servers via the NAT Instance
- **D.** Create a NAT instance in the public subnet as the database servers. Ask the IT administrators to log into the database servers via the NAT Instance

Explanation :

Answer – B
The AWS Documentation mentions the following

A bastion host is a server whose purpose is to provide access to a private network from an external network, such as the Internet. Because of its exposure to potential attack, a bastion host must minimize the chances of penetration. For example, you can use a bastion host to mitigate the risk of allowing SSH connections from an external network to the Linux instances launched in a private subnet of your Amazon Virtual Private Cloud (VPC).

- Option A is incorrect since the bastion host needs to be in the public subnet
- Options C and D are incorrect since the NAT instance should not be used as a jump server to the database servers
- For more information on using a bastion host, please refer to the below URL
- https://aws.amazon.com/blogs/security/how-to-record-ssh-sessions-established-through-a-bastion-host/ (https://aws.amazon.com/blogs/security/how-to-record-ssh-sessions-established-through-a-bastion-host/)

Ask our Experts

QUESTION 52 CORRECT

A company needs to access a service provided by a consultant company. The service from the consultant company and the application of the primary company exist in AWS VPC. The VPC's are located in different regions. How can you accomplish this connectivity ensuring that traffic does not pass via the Internet? Choose 2 answers from the options below

- [x] **A.** Create a VPC peering between the VPC's in the primary company and consultant company's account ✔
- [ ] **B.** Create a Network Load Balancer in the consultant VPC in front of the service. Create a VPC Endpoint. Make the application in the other VPC access this endpoint
- [x] **C.** Create an AWS Direct Connect Connection in the primary company's account. Create a private Virtual Interface to the VPC in the consultant company's account. ✔
- [ ] **D.** Create an IPSec Virtual Private connection between both accounts. Access the resources accordingly

Explanation :

Answer – A and C
Option B is incorrect since for VPC Endpoint interfaces, they have to be in the same region
Option D is incorrect since here the traffic will traverse via the Internet
The AWS Documentation mentions the following
A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them privately. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, with a VPC in another AWS account, or with a VPC in a different AWS Region.
AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect, you can establish private connectivity between AWS and your datacenter, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.
For more information on AWS Direct Connect and VPC peering, please refer to the below URL
https://aws.amazon.com/directconnect/ (https://aws.amazon.com/directconnect/)
https://docs.aws.amazon.com/vpc/latest/userguide/vpc-peering.html
(https://docs.aws.amazon.com/vpc/latest/userguide/vpc-peering.html)
the 2 answers provided for the question are correct. Let me explain to you why?

1. Both Primary & Consultant company are existing within there own VPCs in different AWS Regions.
In order to have the connection among them, we create VPC Peering across the region.
Hence, **Option A** is correct answer.

- https://aws.amazon.com/about-aws/whats-new/2017/11/announcing-support-for-inter-region-vpc-peering/ (https://aws.amazon.com/about-aws/whats-new/2017/11/announcing-support-for-inter-region-vpc-peering/)
- https://aws.amazon.com/blogs/aws/new-almost-inter-region-vpc-peering/ (https://aws.amazon.com/blogs/aws/new-almost-inter-region-vpc-peering/)

2. Now to have a good connection ensuring that traffic does not pass via the Internet?
We pick AWS Direct Connect service, reason being it allows us to transfer data through the private network, rather than the Internet.
Hence, **Option C** is the correct answer.

- https://docs.aws.amazon.com/aws-technical-content/latest/aws-vpc-connectivity-options/aws-direct-connect-network-to-amazon.html (https://docs.aws.amazon.com/aws-technical-content/latest/aws-vpc-connectivity-options/aws-direct-connect-network-to-amazon.html)

Ask our Experts

QUESTION 53 CORRECT

Your team has deployed an application which consists of a web and database tier hosted on separate EC2 Instances. Both EC2 Instances are using General Purpose SSD for their underlying volume type. Off late, there are performance issues related to the read and writes of the database EC2 Instance. Which of the following could be used to alleviate the issue?

- A. Change the Instance type to a higher Instance Type
- B. Change the EBS volume to Provisioned IOPS SSD ✔
- C. Enable Enhanced Networking on the Instance
- D. Enable Multi-AZ for the database

Explanation :

Answer – B

The Provisioned IOPS SSD EBS volume type is perfect for these types of workloads. The below excerpt from the documentation shows the key differences between the different volume types

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

Option A is incorrect since the primary issue is that the volume type is not correct

Option C is incorrect since networking is not an issue here

Option D is incorrect since this option is applicable for the AWS RDS service

For more information on EBS volume types, please refer to 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 54 CORRECT

Your company currently stores documents in an S3 bucket. They want to transfer the files to a low-cost storage unit after a duration of 2 months to save on cost. Which of the following can be used to perform this activity automatically?

- **A.** Use the events of the S3 bucket to transfer the files to Amazon Glacier
- **B.** Use the events of the S3 bucket to transfer the files to EBS volumes – Cold HDD
- **C.** Use the lifecycle policies of the S3 bucket to transfer the files to Amazon Glacier ✔
- **D.** Use the lifecycle policies of the S3 bucket to transfer the files to EBS volumes – Cold HDD

Explanation :

Answer – C
The AWS Documentation mentions the following
To manage your objects so that they are stored cost effectively throughout their lifecycle, configure their lifecycle. A *lifecycle configuration* is a set of rules that define actions that Amazon S3 applies to a group of objects. There are two types of actions:

- Transition actions—Define when objects transition to another storage class (http://docs.aws.amazon.com/AmazonS3/latest/dev/storage-class-intro.html). For example, you might choose to transition objects to the STANDARD_IA storage class 30 days after you created them, or archive objects to the GLACIER storage class one year after creating them.
- Expiration actions—Define when objects expire. Amazon S3 deletes expired objects on your behalf.

Options B and D are incorrect because ideally you don't transfer to EBS volumes – Cold HDD
Option A is incorrect because you need to use lifecycle policies
For more information on lifecycle policies, please refer to the below 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 55 CORRECT

You work for a consulting company that needs to design templates. These templates are used to spin up custom environments on the AWS Cloud. Which of the following would you use for this purpose?

- **A.** AWS Cloudformation ✔
- **B.** AWS Elastic Beanstalk
- **C.** AWS Cloudwatch
- **D.** AWS Config

Explanation :

Answer – A
The AWS Documentation mentions the following
AWS CloudFormation provides a common language for you to describe and provision all the infrastructure resources in your cloud environment. CloudFormation allows you to use a simple text file to model and provision, in an automated and secure manner, all the resources needed for your applications across all regions and accounts. This file serves as the single source of truth for your cloud environment.
Option B is incorrect because this is used to quickly provision development environments
Option C is incorrect because this a monitoring service
Option D is incorrect because this a configuration service
For more information on AWS Cloudformation, please refer to the below URL
https://aws.amazon.com/cloudformation/ (https://aws.amazon.com/cloudformation/)

Ask our Experts

QUESTION 56 CORRECT

You have currently contacted an AWS partner to carry out an audit for your AWS account. You need to ensure that the partner can carry out an audit on your resources. Which one of the following steps would you ideally carry out?

- **A.** Create an IAM user for the partner account for login purposes
- **B.** Create a cross account IAM Role ✔
- **C.** Create an IAM group for the partner account for login purposes
- **D.** Create an IAM profile for the partner account for login purposes

Explanation :

Answer - B
The AWS Documentation mentions the following
Cross-account IAM roles (http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_third-party.html) allow customers to securely grant access to AWS resources in their account to a third party, like an APN Partner, while retaining the ability to control and audit who is accessing their AWS account. Cross-account roles reduce the amount of sensitive information APN Partners need to store for their customers, so that they can focus on their product instead of managing keys. In this blog post, I explain some of the risks of sharing IAM keys, how you can implement cross-account IAM roles, and how cross-account IAM roles mitigate risks for customers and for APN Partners, particularly those who are software as a service (SaaS) providers.
Because this is clearly mentioned in the AWS Documentation , all other options are invalid
For more information on cross account roles, please refer to the below URL
https://aws.amazon.com/blogs/apn/securely-accessing-customer-aws-accounts-with-cross-account-iam-roles/ (https://aws.amazon.com/blogs/apn/securely-accessing-customer-aws-accounts-with-cross-account-iam-roles/)

Ask our Experts

QUESTION 57 CORRECT

Your team has a requirement to process a large set of data streams. They want to then persist the data streams in the simple storage service. Which of the following can be used for this purpose?

- **A.** AWS Redshift and S3

- **B.** AWS Kinesis Firehose and DynamoDB
- **C.** AWS Kinesis Firehose and S3 ✔
- **D.** AWS Lambda and S3

Explanation :

Answer – C
The AWS Documentation mentions the following
Amazon Kinesis Data Firehose is a fully managed service for delivering real-time streaming data to destinations such as Amazon Simple Storage Service (Amazon S3), Amazon Redshift, Amazon Elasticsearch Service (Amazon ES), and Splunk. Kinesis Data Firehose is part of the Kinesis streaming data platform, along with Kinesis Data Streams, Kinesis Video Streams, and Amazon Kinesis Data Analytics. With Kinesis Data Firehose, you don't need to write applications or manage resources. You configure your data producers to send data to Kinesis Data Firehose, and it automatically delivers the data to the destination that you specified. You can also configure Kinesis Data Firehose to transform your data before delivering it.
For more information on AWS Kinesis Firehose, please refer to the below URL
https://docs.aws.amazon.com/firehose/latest/dev/what-is-this-service.html
(https://docs.aws.amazon.com/firehose/latest/dev/what-is-this-service.html)

Ask our Experts

QUESTION 58 CORRECT

Your company is planning on making use of the Elastic Container service for managing their container-based applications. They are going to process both critical and non-critical workloads with these applications. Which of the following COST effective setup would they consider?

- **A.** Use ECS orchestration and Spot Instances for processing critical data and On-Demand for the non-critical data
- **B.** Use ECS orchestration and On-Demand Instances for processing critical data and Spot Instances for the non-critical data ✔
- **C.** Use ECS orchestration and Spot Instances for both the processing of critical data and non-critical data

- **D.** Use ECS orchestration and On-Demand Instances for both the processing of critical data and non-critical data

Explanation :

Answer – B
The AWS Documentation mentions the following
A Spot Instance is an unused EC2 instance that is available for less than the On-Demand price. Because Spot Instances enable you to request unused EC2 instances at steep discounts, you can lower your Amazon EC2 costs significantly. The hourly price for a Spot Instance is called a Spot price. The Spot price of each instance type in each Availability Zone is set by Amazon EC2, and adjusted gradually based on the long-term supply of and demand for Spot Instances. Your Spot Instance runs whenever capacity is available and the maximum price per hour for your request exceeds the Spot price.
Options A and C are incorrect since Spot Instances can be taken back or interrupted and should not be used for critical workloads
Option D is not cost effective. You can use Spot Instances for non-critical workloads
For more information on Spot Instances, please refer to the below URL
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-spot-instances.html
(https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-spot-instances.html)

Ask our Experts

QUESTION 59 CORRECT

Your company is planning on setting up an application that will consists of a web layer. This web layer will consist of EC2 Instances sitting behind an Application Load Balancer. The company wants to protect the application against application level attacks. Which of the following can be used for this purpose?

- **A.** AWS Cloudfront
- **B.** AWS WAF ✔
- **C.** AWS Config
- **D.** AWS VPC NACL

Explanation :

Answer – B
The AWS Documentation mentions the following
You use AWS WAF to control how Amazon CloudFront or an Application Load Balancer responds to web requests. You start by creating conditions, rules, and web access control lists (web ACLs). You define your conditions, combine your conditions into rules, and combine the rules into a web ACL.
Option A is invalid because this is used for content delivery
Option C is invalid because this is a configuration service
Option D is invalid because this is used to just block traffic based on simple rules
For more information on how the AWS WAF works, please refer to the below URL
https://docs.aws.amazon.com/waf/latest/developerguide/how-aws-waf-works.html
(https://docs.aws.amazon.com/waf/latest/developerguide/how-aws-waf-works.html)

Ask our Experts

QUESTION 60 CORRECT

Your company is planning on setting up an application that will consist of a presentation layer and a datastore in DynamoDB. The data in DynamoDB will only used frequently within the week in which the data is inserted. After a week, the data would tend to become stale. But the stale data would need to be available on durable storage for future analysis on historical data. Which of the following would be the ideal implementation steps for this sort of architecture? Choose 2 answers from the options given below

- [ ] **A.** Setup DynamoDB tables. Scan the tables for older data and transfer them to another DynamoDB table.
- [x] **B.** Setup DynamoDB tables on a weekly basis. Ensure the most recent week table has a higher throughput setup. ✔
- [ ] **C.** Use the AWS Data Pipeline service to transfer the older data to EBS volumes
- [x] **D.** Use the AWS Data Pipeline service to transfer the older data to Amazon S3 ✔

Explanation :

Answer – B and D
The AWS Documentation mentions the following

AWS Data Pipeline is a web service that you can use to automate the movement and transformation of data. With AWS Data Pipeline, you can define data-driven workflows, so that tasks can be dependent on the successful completion of previous tasks. You define the parameters of your data transformations and AWS Data Pipeline enforces the logic that you've set up.

Design Pattern for Time-Series Data

Consider a typical time-series scenario, where you want to track a high volume of events. Your write access pattern is that all the events being recorded have today's date. Your read access pattern might be to read today's events most frequently, yesterday's events much less frequently, and then older events very little at all.

The read access pattern is best handled by building the current date and time into the primary key. But that is certain to create one or more hot partitions. The latest one is always the *only* partition that is being written to. All other partitions, including all the partitions from previous days, divert provisioned write capacity from where you need it most.

The following design pattern often handles this kind of scenario effectively:

- Create one table per time period, provisioned with write capacity less than 1,000 write capacity units (WCUs) per partition-key value, and minimum necessary read capacity.
- Before the end of each time period, prebuild the table for the next period. Just as the current period ends, direct event traffic to the new table. You can assign names to these tables that specify the time periods that they have recorded.
- As soon as a table is no longer being written to, reduce its provisioned write capacity to 1 WCU and provision whatever read capacity is appropriate. Reduce the provisioned read capacity of earlier tables as they age, and archive or delete the ones whose contents will rarely or never be needed.

Option A is invalid because this would be an inefficient way to handle the data. You will be using too much throughput in the scan process.
Option C is invalid because EBS volumes is not durable storage
For more information on DynamoDB best practises and AWS Data Pipeline, please refer to the below URL
https://docs.aws.amazon.com/datapipeline/latest/DeveloperGuide/what-is-datapipeline.html (https://docs.aws.amazon.com/datapipeline/latest/DeveloperGuide/what-is-datapipeline.html)
https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/best-practices.html (https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/best-practices.html)

Ask our Experts

QUESTION 61 MARKED AS REVIEW CORRECT

A company is going to setup an application that will be based on Docker based containers. The containers will be setup in the Elastic Container Service. You need to also setup load balancing for the underlying services which are based on dynamic port values. Which of the following would be the ideal service to use for this purpose?

- A. Classic Load Balancer
- B. Route 53

C. Network Load Balancer

D. Application Load Balancer ✔

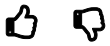
Explanation :

Answer - D
The AWS Documentation mentions the following
Application Load Balancers offer several features that make them attractive for use with Amazon ECS services:

- Application Load Balancers allow containers to use dynamic host port mapping (so that multiple tasks from the same service are allowed per container instance).
- Application Load Balancers support path-based routing and priority rules (so that multiple services can use the same listener port on a single Application Load Balancer).

For more information on Service Load balancing, please refer to the below URL
https://docs.aws.amazon.com/AmazonECS/latest/developerguide/service-load-balancing.html
(https://docs.aws.amazon.com/AmazonECS/latest/developerguide/service-load-balancing.html)

Ask our Experts



QUESTION 62 CORRECT

You've currently have an architecture which consists of a set of web servers in the public subnet. And database servers in the private subnet along with a NAT instance. The NAT instance is now becoming a bottleneck and you are looking to replace it with a NAT gateway. Which of the following would ensure a high availability setup for the NAT device?

A. Disable source/destination check on the NAT Instances

B. Deploy the NAT gateway in 2 availability zones ✔

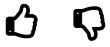
C. Deploy a NAT gateway along with the NAT instance

D. Deploy the NAT Gateway in 2 regions

Explanation :

Answer – B
The AWS Documentation mentions the following
If you have resources in multiple Availability Zones and they share one NAT gateway, in the event that the NAT gateway's Availability Zone is down, resources in the other Availability Zones lose internet access. To create an Availability Zone-independent architecture, create a NAT gateway in each Availability Zone and configure your routing to ensure that resources use the NAT gateway in the same Availability Zone.
Option A is invalid since this is a requirement for the NAT instance to function and will not satisfy the requirement for the question
Option C is invalid since you should just use one type of device
Option D is invalid since you should achieve redundancy via Availability zones
For more information on the NAT gateway, please refer to the below URL
https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html
(https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html)

Ask our Experts



QUESTION 63 CORRECT

Your company is planning on setting up an application with the following architecture

A set of EC2 Instances hosting a web application.
The application will sit behind an Elastic Load balancer
The users will access the application from the internet via the Elastic Load balancer
The application will connect to a backend database server
A NAT Gateway is also implemented.?

Which of the following is the right architecture for the network, keeping high availability and security in mind?

- **A.** 2 public subnets for the Elastic Load balancer, 2 public subnets for the Web server EC2 Instances, 2 private subnets for the database server
- **B.** 2 public subnets for the Elastic Load balancer, 2 private subnets for the Web server EC2 Instances, 2 private subnets for the database server ✔
- **C.** 2 public subnets for the Elastic Load balancer, 2 public subnets for the Web server EC2 Instances, 2 public subnets for the database server
- **D.** 2 public subnets for the Elastic Load balancer, 2 private subnets for the Web server EC2 Instances, 2 public subnets for the database server

Explanation :

Answer – B
You need to have public subnets for the Elastic Load balancer to ensure that traffic can flow via the Internet
The Web servers can be in the private subnet since the communication between the instances and the ELB happens via the private IP
The database servers should be in the private subnet since it does not need to communicate with the Internet
Option A is invalid since the Web servers don't need to be in the public subnet
Option C is invalid since the Web servers and database servers don't need to be in the public subnet
Option D is invalid since the database servers don't need to be in the public subnet
For more information on Elastic Load balancing, please refer to the below URL

- https://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/what-is-load-balancing.html (https://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/what-is-load-balancing.html)

Note: There is no requirement for ec2 instances to be in public subnet as route53 will route the request to elb whose endpoint is exposed as lb(Load Balancer) is in public subnet and the communication between elb and ec2 instances happen via private ip. So its better for security purpose.

Ask our Experts

QUESTION 64 CORRECT

A company currently has the following requirement. They need to develop an application which would take metadata from objects stored in S3 and storing the metadata in DynamoDB. Which of the following can be used to automate the process?

- **A.** AWS Lambda ✔
- **B.** AWS SQS
- **C.** AWS Config
- **D.** AWS SNS

Explanation :

Answer – A

The below diagram from the AWS Documentation shows an example of how AWS Lambda can be used

Data processing

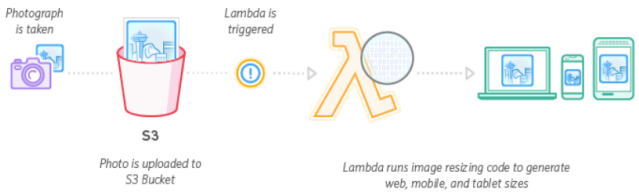
You can use AWS Lambda to execute code in response to triggers such as changes in data, shifts in system state, or actions by users. Lambda can be directly triggered by AWS services such as S3, DynamoDB, Kinesis, SNS, and CloudWatch, or it can be orchestrated into workflows by AWS Step Functions. This allows you to build a variety of real-time serverless data processing systems.

REAL-TIME FILE PROCESSING

You can use Amazon S3 to trigger AWS Lambda to process data immediately after an upload. For example, you can use Lambda to thumbnail images, transcode videos, index files, process logs, validate content, and aggregate and filter data in real-time.

Reference Architecture: Diagram | Sample Code

Example: *Image Thumbnail Creation*



Option B is invalid since this is a messaging service

Option C is invalid since this is a Configuration service

Option D is invalid since this is a notification service

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

https://aws.amazon.com/lambda/ (https://aws.amazon.com/lambda/)

Ask our Experts

An application needs to be setup on AWS. It consists of several components. Two primary components are required to run for 3 hours every day. The other components are required every day for more than 6-8 hours and other servers also running in others instances. Which of the following would you use to ensure COSTS are minimized for the underlying EC2 Instances?

Please select :

- **A.** Reserved instances for the primary components and for the remaining components ,On-Demand Instances.
- **B.** Spot instances for the primary components and for the remaining components ,On-Demand Instances.
- **C.** On-Demand instances for the primary components and for the remaining components ,Spot Instances.
- **D.** On-Demand instances for the primary components and for the remaining components ,Reserved Instances. ✔

Explanation :

Answer – D
The AWS Documentation mentions the following
Reserved Instances provide you with a significant discount compared to On-Demand Instance pricing. Reserved Instances are not physical instances, but rather a billing discount applied to the use of On-Demand Instances in your account. These On-Demand Instances must match certain attributes in order to benefit from the billing discount.
On-Demand Instances – Pay, by the second, for the instances that you launch.
Option A is incorrect since the primary component just runs for 3 hours , you really don't need a reserved instance for it
Options B and C are incorrect since we don't know the type of workload to decide whether Spot Instances are required
For more information on On-Demand and Reserved Instances, please refer to the below URL
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-reserved-instances.html
(https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-reserved-instances.html)

Ask our Experts

Finish Review (https://www.whizlabs.com/learn/course/aws-csaa-practice-tests/quiz/14817)

Certification

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

Company

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

Mobile App

- Android Coming Soon
- iOS Coming Soon

Follow us

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

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

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

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