PRACTICE TEST V - 2018 VERSION

Attempt	1
Marks Obtained	61 / 65
Your score is	93.85%
Completed on	Saturday , 22 December 2018 , 03:43 PM
Time Taken	00 H 40 M 26 S
Result	Pass

Objective wise Report

S.No.	Topic	Total Questions	Correct	Incorrect	Unattempted
1	Other	65	61	4	0

65 Questions	**61** Right	**4** Wrong	**0** Unattempted

Show Answers

All

QUESTION 1 CORRECT

You are a developer for a company that is planning on using the AWS RDS service. Your Database administrator spins up a new MySQL RDS Instance in AWS. You now need to connect to that instance. How can you achieve this? Choose 2 answers from the options given below.

- [x] **A.** Use the DescribeDBInstances API and get the endpoint for the database instance ✔
- [ ] **B.** Use the DescribeDBInstances API and get the IP address for the database instance
- [x] **C.** Request the DBA for the endpoint for the Instance via the AWS Console ✔
- [ ] **D.** Request the DBA for the IP address for the Instance via the AWS Console

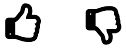
Explanation :

Answer – A and C
The AWS Documentation mentions the following
Before you can connect to a DB instance running the MySQL database engine, you must create a DB instance. For information, seeCreating a DB Instance Running the MySQL Database Engine. Once Amazon RDS provisions your DB instance, you can use any standard MySQL client application or utility to connect to the instance. In the connection string, you specify the DNS address from the DB instance endpoint as the host parameter and specify the port number from the DB instance endpoint as the port parameter.
You can use the AWS Management Console, the AWS CLI describe-db-instances command, or the Amazon RDS API DescribeDBInstances action to list the details of an Amazon RDS DB instance, including its endpoint
Options B and D are incorrect since you need to use the endpoints to connect to the database
For more information on connecting to a database endpoint , please refer to the below URL

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

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

Ask our Experts



QUESTION 2 CORRECT

You are a developer for a company that has been given the responsibility to debug performance issues for an existing application. The application connects to a MySQL RDS Instance in AWS. There is a suspicion that there are performance issues in the underlying queries. Which of the following can help diagnose these issues?

- A. The Cloudtrail logs for the region
- B. Get the slow query logs for the RDS service ✔
- C. Use the AWS Config service to diagnose the problem areas
- D. Use the AWS Inspector service to diagnose the problem areas

Explanation :

Answer – B
The AWS RDS Service contains several logs such as the ones given below

- Error log (https://dev.mysql.com/doc/refman/5.7/en/error-log.html) – contains diagnostic messages generated by the database engine, along with startup and shutdown times.
- General query log (https://dev.mysql.com/doc/refman/5.7/en/query-log.html) – contains a record of all SQL statements received from clients, and also client connect and disconnect times.
- Slow query log (https://dev.mysql.com/doc/refman/5.7/en/slow-query-log.html) – contains a record of SQL statements that took

longer to execute than a set amount of time and that examined more than a defined number of rows. Both thresholds are configurable.

Option A is incorrect because this is used to monitor API activity
Option C is incorrect because this is used as a configuration service
Option D is incorrect because this is used to inspect EC2 Instances for vulnerabilities
For more information on monitoring Amazon RDS , please refer to the below URL

- https://aws.amazon.com/blogs/database/monitor-amazon-rds-for-mysql-and-mariadb-logs-with-amazon-cloudwatch/ (https://aws.amazon.com/blogs/database/monitor-amazon-rds-for-mysql-and-mariadb-logs-with-amazon-cloudwatch/)

Ask our Experts

QUESTION 3 CORRECT

Your team has an application deployed using the Elastic Beanstalk service. A Web environment has been configured for the production environment. There is now a requirement to perform a Blue Green deployment for a new version of the application. How can you achieve this?

- **A.** Create a new application and swap the application environments.
- **B.** Create a new application version and upload the new application version
- **C.** Create a new environment in the application with the updated application version and perform a swap ✔
- **D.** Create a new environment in the application and Load the configuration of an existing environment

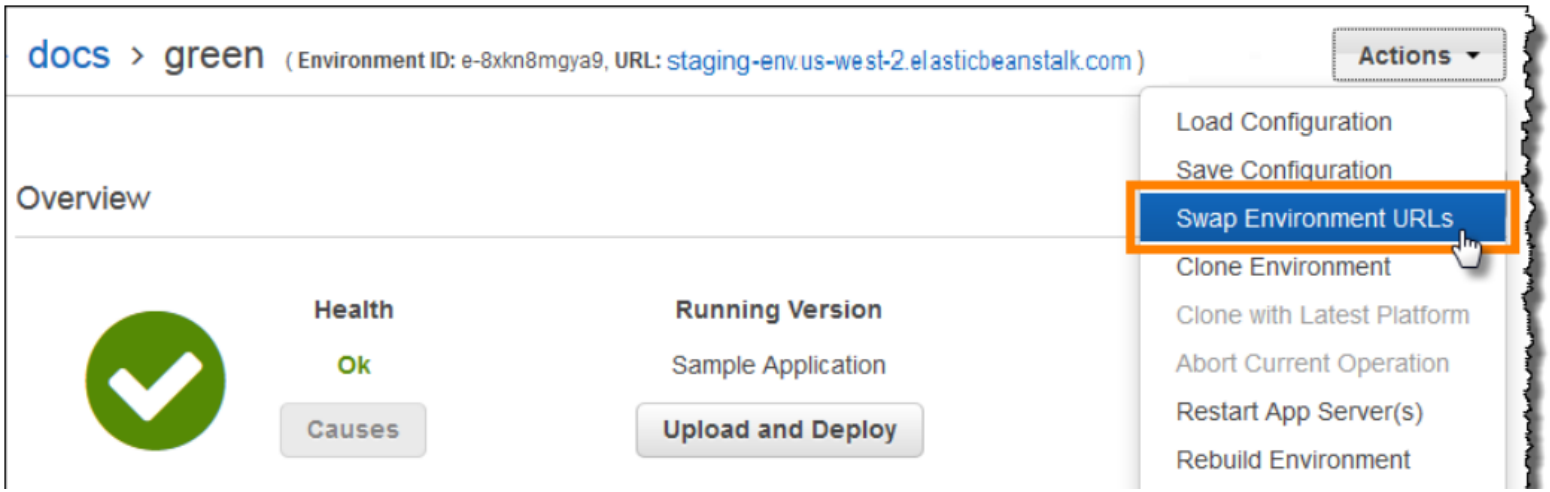
Explanation :

Answer - C

This is mentioned in the AWS Documentation

To perform a blue/green deployment

1. Open the Elastic Beanstalk console.
2. Clone your current environment, or launch a new environment running the configuration you want.
3. Deploy the new application version to the new environment.
4. Test the new version on the new environment.
5. From the new environment's dashboard, choose **Actions**, and then choose **Swap Environment URLs**.



Since this is clearly mentioned in the AWS Documentation, all other options are invalid
For more information on Blue Green deployments in Elastic Beanstalk, please refer to the below URL

- https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.CNAMESwap.html (https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.CNAMESwap.html)

Ask our Experts

QUESTION 4 CORRECT

You are developing an application that consist of the following architecture

- A set of EC2 Instances hosting a web layer
- A database hosting a MySQL instance

You need to add a layer that can be used to ensure that the most frequently accessed data from the database is fetched in a more fast and efficient manner from the database. Which of the following can be used to accomplish this requirement?

- **A.** An SQS queue to store the frequently accessed data
- **B.** An SNS topic to store the frequently accessed data
- **C.** A Cloudfront distribution to store the frequently accessed data
- **D.** A Elasticache instance to store the frequently accessed data ✔

Explanation :

Answer – D
The AWS Documentation mentions the following
Amazon ElastiCache offers fully managed Redis (https://aws.amazon.com/redis/) and Memcached (https://aws.amazon.com/memcached/). Seamlessly deploy, run, 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 because this is a messaging service
Option B is incorrect because this is a notification service
Option C is incorrect because this is a web distribution service

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

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

Ask our Experts

QUESTION 5 CORRECT

You've just started development on an application that will make use of the ElastiCache service. You need to ensure that objects are cached but not kept inadvertently for a long time. Which of the following cache maintenance strategy would you employ for the cache service?

- A. TTL ✔
- B. Lazy Loading
- C. Write Through
- D. Read Through

Explanation :

Answer – A
The AWS Documentation mentions the following

Lazy loading allows for stale data but won't fail with empty nodes. Write through ensures that data is always fresh but may fail with empty

nodes and may populate the cache with superfluous data. By adding a time to live (TTL) value to each write, we are able to enjoy the advantages of each strategy and largely avoid cluttering up the cache with superfluous data.
Option B is incorrect because this is a caching strategy that loads data into the cache only when necessary.
Option C is incorrect because this is a caching strategy that adds data or updates data in the cache whenever data is written to the database.
Option D is incorrect because there is no such caching strategy
For more information on Caching strategies, please refer to the below URL

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

Ask our Experts

QUESTION 6 CORRECT

Your team has been instructed with the development of an application. The backend store needs to store data on which ad-hoc queries can run and table joins are required. Which of the following would you use to host the underlying data store?

- A. AWS RDS ✔
- B. AWS DynamoDB
- C. AWS S3
- D. AWS Athena

Explanation :

Answer – A

The AWS Documentation gives an example comparison of when to use AWS RDS for SQL data and DynamoDB for NoSQL data

Characteristic	Relational Database Management System (RDBMS)	Amazon DynamoDB
Optimal Workloads	Ad hoc queries; data warehousing; OLAP (online analytical processing).	Web-scale applications, including social networks, gaming, media sharing, and IoT (Internet of Things).
Data Model	The relational model requires a well-defined schema, where data is normalized into tables, rows and columns. In addition, all of the relationships are defined among tables, columns, indexes, and other database elements.	DynamoDB is schemaless. Every table must have a primary key to uniquely identify each data item, but there are no similar constraints on other non-key attributes. DynamoDB can manage structured or semi-structured data, including JSON documents.

Option B is incorrect because this should not be used when you have table joins to be carried out.

Option C is incorrect because this is used for object level storage

Option D is incorrect because this is used for querying data in S3

For more information on when to use SQL over NoSQL, please refer to the below URL

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

Ask our Experts

QUESTION 7 MARKED AS REVIEW CORRECT

Your development team is currently working with an application that interacts with the DynamoDB table. Due to the proposed extensive use of the application, the underlying DynamoDB table would undergo a steady growth in size. Which of the following preferred options should be used for retrieving the data? Choose 3 answers from the options given below

- [x] **A.** Use the query operation ✔
- [ ] **B.** Use the Scan operation
- [x] **C.** Use the GetItem API command ✔
- [x] **D.** Use the BatchGetItem API command ✔

Explanation :

Answer – A ,C and D

The AWS Documentation mentions the following

If possible, you should avoid using a Scan operation on a large table or index with a filter that removes many results. Also, as a table or index grows, the Scan operation slows. The Scan operation examines every item for the requested values and can use up the provisioned throughput for a large table or index in a single operation. For faster response times, design your tables and indexes so that your applications can use Query instead of Scan. (For tables, you can also consider using the GetItem and BatchGetItem APIs.)

Option B is incorrect since this would cause performance issues as the amount of items starts to increase.

For more information on best practises for the query and scan operation, please refer to the below URL

- https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/bp-query-scan.html (https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/bp-query-scan.html)

Ask our Experts

QUESTION 8 CORRECT

Your development team is planning on building an application based on the Microservice architecture pattern

Your development team is planning on building an application based on the Microservice architecture pattern. Docker containers would be used to build the application. When deploying the application to AWS, which of the following services should be considered. Choose 2 answers from the options given below?

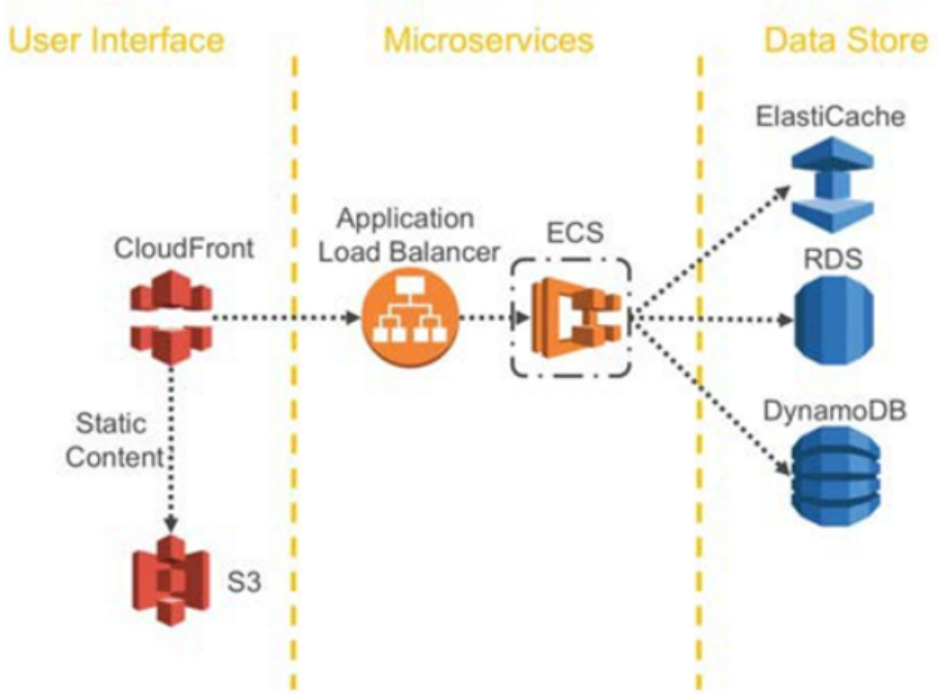
- [ ] **A.** AWS EC2
- [x] **B.** AWS ECS ✔
- [x] **C.** Application Load balancer ✔
- [ ] **D.** Classic Load balancer

Explanation :

Answer – B and C

The below diagram from the AWS Documentation, shows the example of a simple Microservices Architecture

In the past, typical monolithic applications were built using different layers, for example, a user interface (UI) layer, a business layer, and a persistence layer. A central idea of a microservices architecture is to split functionalities into cohesive "verticals"—not by technological layers, but by implementing a specific domain. The following figure depicts a reference architecture for a typical microservices application on AWS.



Option A is incorrect since ECS should be preferred for its ability to provide a serverless architecture for your docker containers
Option D is incorrect since the Application Load balancer has better support for docker containers.
For more information on a simple microservices architecture, please refer to the below URL

- https://docs.aws.amazon.com/aws-technical-content/latest/microservices-on-aws/simple-microservices-architecture-on-aws.html (https://docs.aws.amazon.com/aws-technical-content/latest/microservices-on-aws/simple-microservices-architecture-on-aws.html)

Ask our Experts

QUESTION 9 MARKED AS REVIEW CORRECT

Your team has an application deployed on the AWS platform. This application is making requests to an S3 bucket. There is a surge of increased number of GET requests. After monitoring using Cloudwatch metrics you can see the rate of GET requests going close to 5000 requests per second. Which of the following can be used to ensure the performance and cost are optimized?

- A. Add an Elasticache in front of the S3 bucket
- B. Use DynamoDB instead of using S3
- C. Place a Cloudfront distribution in front of the S3 bucket ✔
- D. Place an Elastic Load balancer in front of the S3 bucket

Explanation :

Answer - C

The AWS Documentation mentions the following

If your workload is mainly sending GET requests, in addition to the preceding guidelines, you should consider using Amazon CloudFront for performance optimization. By integrating CloudFront with Amazon S3, you can distribute content to your users with low latency and a high data transfer rate. You also send fewer direct requests to Amazon S3, which reduces your costs.

Since the documentation clearly mentions this , all other options are invalid

For more information on request rate configurations for S3, please refer to the below URL

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

Ask our Experts

QUESTION 10 CORRECT

Your team is planning on creating a Lambda function which will interact with a DynamoDB stream. Which of the following would need to be in place to ensure the Lambda function can interact with the DynamoDB table.

- A. Access Keys for an IAM user embedded in the function
- B. IAM Role with required permissions to access DynamoDB ✔
- C. The password for an IAM user in the environment variable for the Lambda function
- D. A Security group rule to allow egress traffic into DynamoDB

Explanation :

Answer - B

The AWS Documentation mentions the following

Regardless of what invokes a Lambda function, AWS Lambda always executes a Lambda function on your behalf. If your Lambda function needs to access any AWS resources, you need to grant the relevant permissions to access those resources. You also need to grant AWS Lambda permissions to poll your DynamoDB stream. You grant all of these permissions to an IAM role (execution role) that AWS Lambda can assume to poll the stream and execute the Lambda function on your behalf. You create this role first and then enable it at the time you create the Lambda function

For more information on using Lambda with DynamoDB, please refer to the below URL

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

Ask our Experts

QUESTION 11 MARKED AS REVIEW CORRECT

Your team is looking into the Serverless deployment of an AWS lambda function. The function will be deployed using the Serverless application model. To test this out , you first create a sample function created below.

```
var AWS = require('aws-sdk');
  exports.handler = function(event, context, callback) {
 var bucketName = "Demobucket";
 callback(null, bucketName);
}
```

What should be the next steps in the serverless deployment? Choose 2 answers from the options given below

- [x] **A.** Create a YAML file with the deployment specific's and package that along with the function file. ✔
- [ ] **B.** Upload the application function file onto an S3 bucket.
- [ ] **C.** Upload the function on AWS Lambda
- [x] **D.** Upload the complete package onto an S3 bucket ✔

Explanation :

Answer – A and D

This is given in the AWS Documentation

Packaging and Deployment

After you create your Lambda function handler and your *example.yaml* file, you can use the AWS CLI to package and deploy your serverless application.

Packaging

To package your application, create an Amazon S3 bucket that the `package` command will use to upload your ZIP deployment package (if you haven't specified one in your *example.yaml* file). You can use the following command to create the Amazon S3 bucket:

```
aws s3 mb s3://bucket-name --region region
```

Next, open a command prompt and type the following:

```
sam package \
   --template-file path/example.yaml \
   --output-template-file serverless-output.yaml \
   --s3-bucket s3-bucket-name
```

Option B is incorrect since you need to package both the application function and the YAML file
Option C is incorrect since you have the requirement to deploy this in an automated fashion
For more information on serverless deployment, please refer to the below URL

- https://docs.aws.amazon.com/lambda/latest/dg/serverless-deploy-wt.html (https://docs.aws.amazon.com/lambda/latest/dg/serverless-deploy-wt.html)

Ask our Experts

QUESTION 12 CORRECT

Your team has developed an application that makes use of an SQS queue for distributed messaging. Your team needs to monitor the number of messages in the queue. Which of the following can be used to get this information?

- A. AWS Cloudwatch ✔
- B. AWS Cloudtrail
- C. AWS Config
- D. AWS Inspector

Explanation :

Answer – A
This is given in the AWS Documentation
Amazon SQS and Amazon CloudWatch are integrated so you can use CloudWatch to view and analyze metrics for your Amazon SQS queues. You can view and analyze your queues' metrics from the Amazon SQS console (https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-access-metrics.html#access-cloudwatch-metrics-sqs-console), the CloudWatch console (https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-access-metrics.html#access-metrics-cloudwatch-console), using the AWS CLI (https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-access-metrics.html#access-cloudwatch-metrics-cli), or using the CloudWatch API (https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-access-metrics.html#access-metrics-cloudwatch-api). You can also set CloudWatch alarms (https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/set-cloudwatch-alarms-for-metrics.html) for Amazon SQS metrics.
CloudWatch metrics for your Amazon SQS queues are automatically collected and pushed to CloudWatch every five minutes. These metrics are gathered on all queues that meet the CloudWatch guidelines for being *active*. CloudWatch considers a queue to be active for up to six hours if it contains any messages or if any action accesses it.
Option B is incorrect since this is an API monitoring service
Option C is incorrect since this is resource configuration service

Option D is incorrect since this is used to check EC2 instances for vulnerabilities
For more information on monitoring using Cloudwatch, please refer to the below URL

- https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-monitoring-using-cloudwatch.html (https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-monitoring-using-cloudwatch.html)

Ask our Experts

QUESTION 13 MARKED AS REVIEW CORRECT

Your team is using the AWS CodeBuild service for an application build. As part of Integration testing during the build phase, the application needs to access an RDS instance in a private subnet. How can you ensure this is possible?

- A. Create a VPC Endpoint and ensure the codebuild project configuration is modified with the endpoint information
- B. Provide additional VPC-specific configuration information as part of your AWS CodeBuild project ✔
- C. Mark the subnet as a public subnet during the time of the Integration tests
- D. Use a NAT gateway to relay the requests from AWS CodeBuild to the RDS Instance

Explanation :

Answer - B
This is given in the AWS Documentation

Typically, resources in an VPC are not accessible by AWS CodeBuild. To enable access, you must provide additional VPC-specific

configuration information as part of your AWS CodeBuild project configuration. This includes the VPC ID, the VPC subnet IDs, and the VPC security group IDs. VPC-enabled builds are then able to access resources inside your VPC.
VPC connectivity from AWS CodeBuild builds makes it possible to:

- Run integration tests from your build against data in an Amazon RDS database that's isolated on a private subnet.
- Query data in an Amazon ElastiCache cluster directly from tests.
- Interact with internal web services hosted on Amazon EC2, Amazon ECS, or services that use internal Elastic Load Balancing.

Since the requirements are clearly mentioned in the documentation , all other options are incorrect
For more information on VPC support for AWS CodeBuild, please refer to the below URL

- https://docs.aws.amazon.com/codebuild/latest/userguide/vpc-support.html (https://docs.aws.amazon.com/codebuild/latest/userguide/vpc-support.html)

Ask our Experts

QUESTION 14 MARKED AS REVIEW CORRECT

You've setup an application on a set of EC2 Instances. It is a web-based application. You've also setup a load balancer. During the initial round of testing after deploying, the users complain that they are not able to reach the home page for the web based application. Which of the following must you check? Choose 2 answers from the options given below

- [ ] **A.** Ensure that the load balancer is attached to a private subnet
- [x] **B.** Ensure that the load balancer is attached to a public subnet ✔
- [x] **C.** Ensure that the Security Group of the Load balancer allows traffic from the internet ✔

☐ **D.** Ensure that the Security Group of the EC2 allows traffic from the internet

Explanation :

Answer – B and C

This is given in the AWS Documentation

Clients cannot connect to an Internet-facing load balancer

If the load balancer is not responding to requests, check for the following:

Your Internet-facing load balancer is attached to a private subnet

Verify that you specified public subnets for your load balancer. A public subnet has a route to the Internet Gateway for your virtual private cloud (VPC).

A security group or network ACL does not allow traffic

The security group for the load balancer and any network ACLs for the load balancer subnets must allow inbound traffic from the clients and outbound traffic to the clients on the listener ports.

Option A is invalid since the load balancer should be attached to a public subnet

Option D is invalid since the Security Group for the Load balancer should allow traffic from the internet

For more information on troubleshooting the load balancer, please refer to the below URL

- https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-troubleshooting.html (https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-troubleshooting.html)

Ask our Experts

QUESTION 15 CORRECT

Your team has developed an application that will be launched on EC2 Instances that are part of the an Autoscaling Group. It needs to be ensured that the application can get the IP address of the Instance. How can you achieve this?

- A. Make the application query the Instance Metadata ✔
- B. Make the application query the Instance Userdata
- C. Make the application query the Autoscaling Group
- D. Make the application query the Launch configuration

Explanation :

Answer - A
This is given in the AWS Documentation
Instance metadata is data about your instance that you can use to configure or manage the running instance
Because your instance metadata is available from your running instance, you do not need to use the Amazon EC2 console or the AWS CLI. This can be helpful when you're writing scripts to run from your instance. For example, you can access the local IP address of your instance from instance metadata to manage a connection to an external application.
Since the data can only be retrieved from the Instance Metadata , all other options are invalid
For more information on Instance Metadata, please refer to the below URL

- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html)

Ask our Experts

QUESTION 16 MARKED AS REVIEW CORRECT

You're in charge for creating a cloudformation template. This template needs to create resources for multiple types of environment. The template needs to be flexible so that it can create resources based on the type of environment. How can you achieve this? Choose 2 answers from the options given below.

- [x] **A. Create an Input Parameter to take in the type of environment.** ✔
- [ ] **B. Use the Outputs section to define the type of environment**
- [ ] **C. Use the Custom Resources feature to create resources based on the type of environment**
- [x] **D. Use the Conditions section to create resources based on the type of environment** ✔

Explanation :

Answer – A and D

This is given in the AWS Documentation

The optional Conditions section contains statements that define the circumstances under which entities are created or configured. For example, you can create a condition and then associate it with a resource or output so that AWS CloudFormation only creates the resource or output if the condition is true. Similarly, you can associate the condition with a property so that AWS CloudFormation only sets the property to a specific value if the condition is true. If the condition is false, AWS CloudFormation sets the property to a different value that you specify.

You might use conditions when you want to reuse a template that can create resources in different contexts, such as a test environment versus a production environment. In your template, you can add an EnvironmentType input parameter, which accepts either prod or test as inputs.

Since this is clearly given in the documentation, all other options are incorrect

For more information on conditions in a Cloudformation template, please refer to the below URL

- https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/conditions-section-structure.html (https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/conditions-section-structure.html)

Ask our Experts

QUESTION 17 MARKED AS REVIEW CORRECT

Your team is working on an API definition which will be deployed using the API gateway service. You then need to ensure that control is established on who can access the various resources within the API gateway. Which of the following can help ensure this security requirement is met? Choose 3 Options

- [ ] **A.** Key Policies
- [x] **B.** IAM Policies ✔
- [x] **C.** Resource Policies ✔
- [x] **D.** IAM Roles ✔

Explanation :

Answer - B, C and D
This is given in the AWS Documentation

Control Who Can Call an API Gateway API Method with IAM Policies

To control who can or cannot call a deployed API with IAM permissions, create an IAM policy document with required permissions. A template for such a policy document is shown as follows.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Permission",
      "Action": [
        "execute-api:Execution-operation"
      ],
      "Resource": [
        "arn:aws:execute-api:region:account-id:api-id/stage/METHOD_HTTP_VERB/Resource-path"
      ]
    }
  ]
}
```

For more information on using IAM Policies for controlling access, please refer to the below URL

- https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-control-access-using-iam-policies-to-invoke-api.html (https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-control-access-using-iam-policies-to-invoke-api.html)

Resource policies,Iam roles and policies can controll access to an API.

- https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-control-access-to-api.html (https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-control-access-to-api.html)

Ask our Experts

QUESTION 18 MARKED AS REVIEW CORRECT

You are a developer for a company. You are using planning on using the X-Ray service to trace all incoming HTTP requests for an application being developed. In the X-Ray SDK which of the following feature would you use to fulfil this requirement?

- A. Interceptors ✔
- B. Client handlers
- C. Server handlers
- D. Daemon service

Explanation :

Answer - A
This is given in the AWS Documentation
The X-Ray SDK provides:

- Interceptors to add to your code to trace incoming HTTP requests
- Client handlers to instrument AWS SDK clients that your application uses to call other AWS services
- An HTTP client to use to instrument calls to other internal and external HTTP web services

Since this is clearly given in the documentation, all other options are incorrect
For more information on using AWS X-Ray, please refer to the below URL

- https://docs.aws.amazon.com/xray/latest/devguide/aws-xray.html (https://docs.aws.amazon.com/xray/latest/devguide/aws-xray.html)

Ask our Experts

QUESTION 19 MARKED AS REVIEW CORRECT

You're planning on using the DataPipeline service to transfer data from Amazon S3 to Redshift. You need to define the source and destination locations. Which of the following part of the DataPipeline service allows you to define these locations?

- A. Data Nodes ✔
- B. Task Runner
- C. Activities
- D. Resources

Explanation :

Answer – A
This is given in the AWS Documentation

Data Nodes

In AWS Data Pipeline, a data node defines the location and type of data that a pipeline activity uses as input or output. AWS Data Pipeline supports the following types of data nodes:

DynamoDBDataNode

A DynamoDB table that contains data for HiveActivity or EmrActivity to use.

SqlDataNode

An SQL table and database query that represent data for a pipeline activity to use.

Note

Previously, MySqlDataNode was used. Use SqlDataNode instead.

RedshiftDataNode

An Amazon Redshift table that contains data for RedshiftCopyActivity to use.

S3DataNode

An Amazon S3 location that contains one or more files for a pipeline activity to use.

Option B is incorrect since the Task Runner is an application that polls AWS Data Pipeline for tasks and then performs those tasks.

Option C is incorrect since an activity is a pipeline component that defines the work to perform
Option D is incorrect since a resource is the computational resource that performs the work that a pipeline activity specifies
For more information on Data Nodes, please refer to the below URL

- https://docs.aws.amazon.com/datapipeline/latest/DeveloperGuide/dp-concepts-datanodes.html (https://docs.aws.amazon.com/datapipeline/latest/DeveloperGuide/dp-concepts-datanodes.html)

Ask our Experts

QUESTION 20 MARKED AS REVIEW CORRECT

As a database developer, you have started working with Redshift. Your IT administrator has provisioned a Redshift

As a database developer, you have started working with Redshift. Your IT administrator has provisioned a Redshift cluster. You now need to load data into the Redshift cluster from S3. Which of the following command should you use for this activity?

- A. GET
- B. COPY ✔
- C. MERGE
- D. PUT

Explanation :

Answer - B

This is given in the AWS Documentation

2. Load sample data from Amazon S3 by using the COPY command.

> **Note**
>
> We recommend using the COPY command to load large datasets into Amazon Redshift from Amazon S3 or DynamoDB. For more information about COPY syntax, see COPY in the *Amazon Redshift Database Developer Guide*.

The ideal command to be used is given in the documentation , hence all other options are incorrect

For more information on working with a sample Redshift cluster, please refer to the below URL

- https://docs.aws.amazon.com/redshift/latest/gsg/rs-gsg-create-sample-db.html (https://docs.aws.amazon.com/redshift/latest/gsg/rs-gsg-create-sample-db.html)
- https://docs.aws.amazon.com/redshift/latest/dg/r_COPY.html (https://docs.aws.amazon.com/redshift/latest/dg/r_COPY.html)
- https://docs.aws.amazon.com/datapipeline/latest/DeveloperGuide/dp-template-s3redshift.html (https://docs.aws.amazon.com/datapipeline/latest/DeveloperGuide/dp-template-s3redshift.html)

Ask our Experts

QUESTION 21 MARKED AS REVIEW CORRECT

Your company has a development application that needs to interact with an S3 bucket. There is a requirement that all data in the bucket is encrypted at rest. You also need to ensure that the keys are managed by you. Which of the following can you use for this purpose? Choose 2 answers from the options given below

- [ ] **A.** Server-Side Encryption with AWS Managed Keys
- [ ] **B.** Server-Side Encryption with AWS KMS Keys
- [x] **C.** Server-Side Encryption with Customer-Provided Keys ✔
- [x] **D.** Client-Side Encryption ✔

Explanation :

Answer – C and D

This is given in the AWS Documentation

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.

You can encrypt data client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, the encryption keys, and related tools

Options A and B are incorrect since here the keys are managed by AWS.

For more information on Server-side encryption for S3, 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 22 MARKED AS REVIEW CORRECT

Your developing an application that is going to make use of AWS Cognito. The default sign-in and sign-up features of the AWS Cognito service will be used. There is a security requirement to ensure that if the user's credentials are compromised, then they would need to use a new password. Which of the following needs to be in place for this? Choose 2 answers from the options given below

- [x] **A.** Ensure to create a user pool in AWS Cognito ✔
- [x] **B.** Ensure to "Block use" for compromised credentials in the Advanced Security section ✔
- [ ] **C.** Ensure to "Block use" for compromised credentials in the Basic Security section
- [ ] **D.** Verify sign-in operation on Cognito using Secure Remote Password

Explanation :

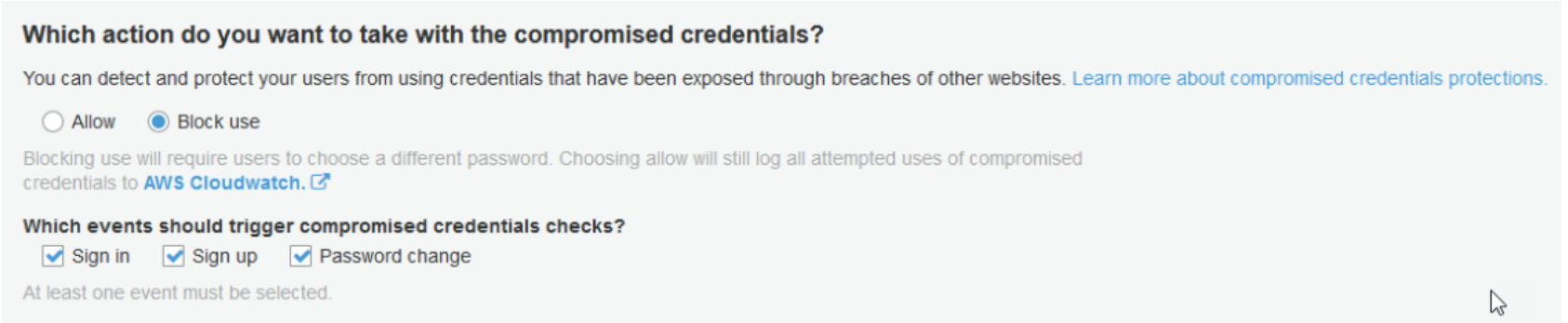
Answer – A and B
This is given in the AWS Documentation

Checking for Compromised Credentials

Amazon Cognito can detect if a user's credentials (user name and password) have been compromised elsewhere. This can happen when users reuse credentials at more than one site, or when they use passwords that are easy to guess.

From the **Advanced security** page in the Amazon Cognito console, you can choose whether to allow, or block the user if compromised credentials are detected. Blocking requires users to choose another password. Choosing **Allow** publishes all attempted uses of compromised credentials to Amazon CloudWatch. For more information, see Viewing Advanced Security Metrics.

You can also choose whether Amazon Cognito checks for compromised credentials during sign-in, sign-up, and password changes.



Option C is incorrect since this configuration needs to be done in the Advanced Security section
Option D is incorrect as Currently, Amazon Cognito doesn't check for compromised credentials for sign-in operations with Secure Remote Password (SRP) flow, which doesn't send the password during sign-in.
For more information on Cognito User pools, please refer to the below URL

- https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-user-pool-settings-compromised-credentials.html (https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-user-pool-settings-compromised-credentials.html)

Ask our Experts

QUESTION 23 MARKED AS REVIEW CORRECT

You are currently a Business Intelligence developer for a company. A lot of data sources that are defined for the Logistics team in your company is hosted in AWS. They are now looking for a quick solution to build visualization screens around the data hosted in AWS. Which of the following can be used to fulfil this requirement?

- A. AWS Redshift
- B. AWS Quicksight ✔
- C. AWS Glue
- D. AWS DynamoDB

Explanation :

Answer – B
This is given in the AWS Documentation
Amazon QuickSight is a business analytics service you can use to build visualizations, perform ad hoc analysis, and get business insights from your data. It can automatically discover AWS data sources and also works with your data sources. Amazon QuickSight enables organizations to scale to hundreds of thousands of users and delivers responsive performance by using a robust in-memory engine (SPICE).
Option A is invalid because this is a datawarehousing solution
Option C is invalid because this service is fully managed ETL (extract, transform, and load) service
Option D is invalid because this is a fully managed NoSQL database
For more information on AWS Quicksight, please refer to the below URL

- https://docs.aws.amazon.com/quicksight/latest/user/welcome.html (https://docs.aws.amazon.com/quicksight/latest/user/welcome.html)

Ask our Experts

QUESTION 24 MARKED AS REVIEW INCORRECT

Your team is currently publishing items to an S3 bucket. You need to record the size of the objects in a separate DynamoDB table. How can you ensure that each uploaded object triggers a record in the DynamoDB table in an ideal manner? Choose 2 answers from the options given below.

- [x] **A.** Create a new SQS queue ✖
- [ ] **B.** Create a new Lambda function ✔
- [ ] **C.** Add the SQS queue to the source event for the S3 bucket
- [x] **D.** Add the Lambda function to the source event for the S3 bucket ✔

Explanation :

Answer – B and D

This is given in the AWS Documentation

Amazon S3 can publish events (for example, when an object is created in a bucket) to AWS Lambda and invoke your Lambda function by passing the event data as a parameter. This integration enables you to write Lambda functions that process Amazon S3 events. In Amazon S3, you add bucket notification configuration that identifies the type of event that you want Amazon S3 to publish and the Lambda function that you want to invoke.

Options A and C are incorrect since the ideal option would be to create a Lambda function that could be used to automatically record the data size and then place a record in the DynamoDB table

For more information on S3 with Lambda, please refer to the below URL

- https://docs.aws.amazon.com/lambda/latest/dg/with-s3.html (https://docs.aws.amazon.com/lambda/latest/dg/with-s3.html)

Ask our Experts

QUESTION 25 CORRECT

Your working on a system that will make use of AWS Kinesis. Here you will various log sources that will send data onto AWS Kinesis. You are looking at creating an initial number of shards for the Kinesis stream. Which of the following can be used in the calculation for the an initial number of shards for the Kinesis stream. Choose 2 answers from the options given below.

- [x] **A.** Incoming write bandwidth ✔
- [ ] **B.** Outgoing write bandwidth
- [ ] **C.** Incoming read bandwidth
- [x] **D.** Outgoing read bandwidth ✔

Explanation :

Answer – A and D

This is given in the AWS Documentation

You can calculate the initial number of shards (`number_of_shards`) that your stream needs by using the input values in the following formula:

```
number_of_shards = max(incoming_write_bandwidth_in_KB/1000, outgoing_read_bandwidth_in_KB/2000)
```

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

- https://docs.aws.amazon.com/streams/latest/dev/amazon-kinesis-streams.html

(https://docs.aws.amazon.com/streams/latest/dev/amazon-kinesis-streams.html)

Ask our Experts

QUESTION 26 CORRECT

Your development team has developed a series of Docker containers that will be part of an application. The deployment team is looking at using the Elastic Container service for hosting these containers. Which of the following are 2 possible data sources for storing the Docker based images?

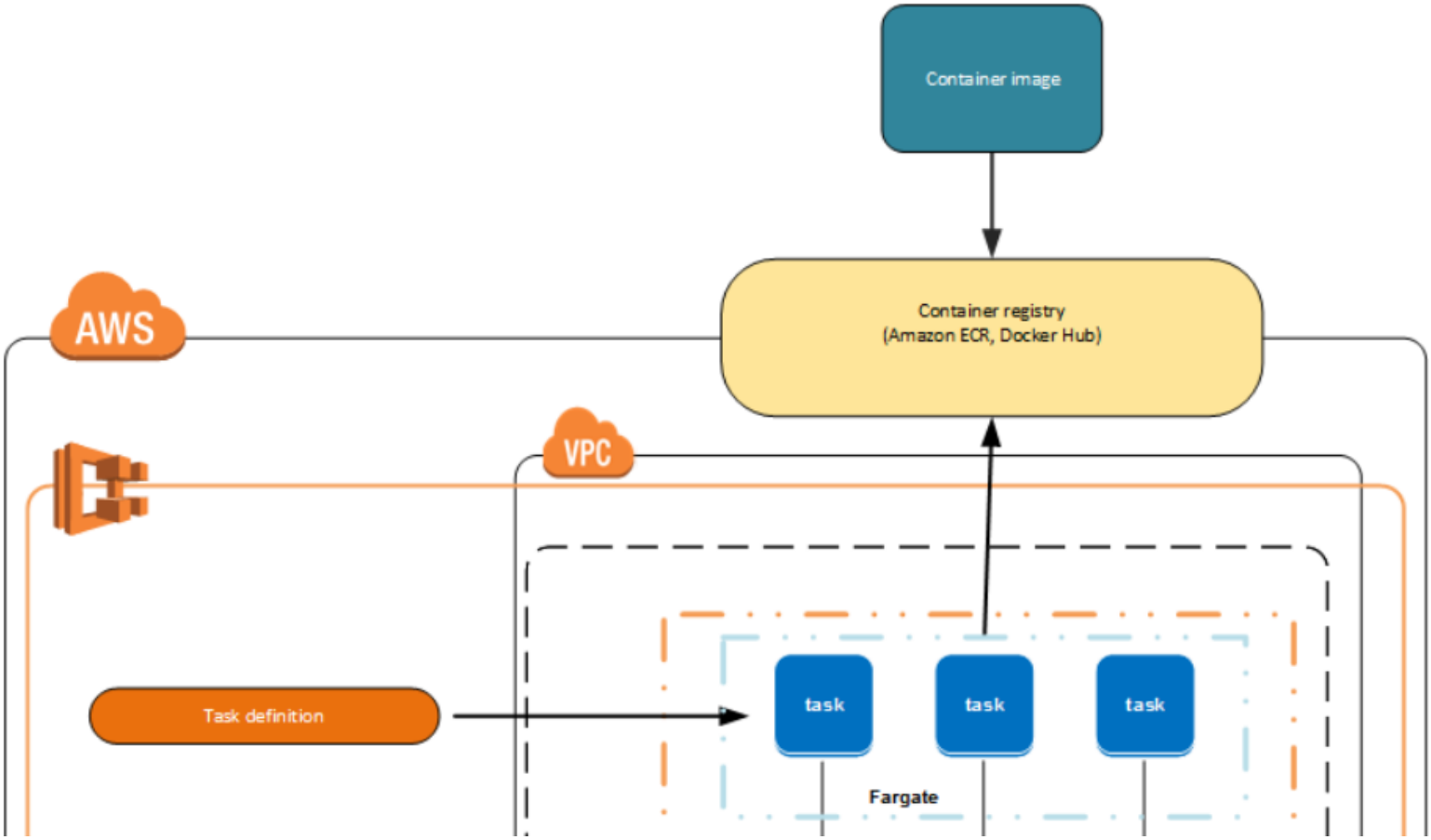
- [ ] **A.** On the EC2 Instances
- [x] **B.** In Docker Hub ✔
- [x] **C.** In the Elastic Container Registry ✔
- [ ] **D.** Store them as Amazon Machine Images

Explanation :

Answer – B and C

The AWS Documentation architecture diagram of the Elastic Container service shows the 2 sources from where you can download the Docker containers

The following diagram shows the architecture of an Amazon ECS environment using the Fargate launch type:



Because the AWS Documentation clearly mentions this , all other options are invalid.
For more information on the Amazon Container Service, please refer to the below URL

- https://docs.aws.amazon.com/AmazonECS/latest/developerguide/Welcome.html (https://docs.aws.amazon.com/AmazonECS/latest/developerguide/Welcome.html)

Ask our Experts

QUESTION 27 CORRECT

You are setting out policies for allowing access to users for objects in an S3 bucket. You have configured a policy for testing which currently works as intended. You try to create a more restrictive policy but find out that the changes are not working as intended. What can you do to resolve the issue in the EASIEST way possible?

- A. Delete the current version of the policy and recreate the older one
- B. Revert back to the previous version of the policy ✔
- C. Recreate the IAM users again
- D. Use the recycle bin to get the deleted policies back

Explanation :

Answer - B

The AWS Documentation mentions the following

You create a customer managed policy that allows users to administer a particular Amazon S3 bucket using the AWS Management Console. Upon creation, your customer managed policy has only one version, identified as v1, so that version is automatically set as the default. The policy works as intended.

Later, you update the policy to add permission to administer a second Amazon S3 bucket. IAM creates a new version of the policy, identified as v2, that contains your changes. You set version v2 as the default, and a short time later your users report that they lack permission to use the Amazon S3 console. In this case, you can roll back to version v1 of the policy, which you know works as intended. To do this, you set version v1 as the default version. Your users are now able to use the Amazon S3 console to administer the original bucket.

Because the AWS Documentation clearly mentions this , all other options are invalid.

For more information on the Amazon Container Service, please refer to the below URL

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

Ask our Experts

QUESTION 28 CORRECT

Your developers have been given access to a CodeCommit Repository. You need to ensure that if any changes are made to a repository, notifications are sent accordingly. Which of the below 2 destinations can be used for the notifications.

- [x] **A.** AWS Lambda ✔
- [x] **B.** AWS SNS ✔
- [ ] **C.** AWS Config
- [ ] **D.** AWS IAM

Explanation :

Answer – A and B

The AWS Documentation mentions the following

You can configure an AWS CodeCommit repository so that code pushes or other events trigger actions, such as sending a notification from Amazon Simple Notification Service (Amazon SNS) or invoking a function in AWS Lambda. You can create up to ten triggers for each AWS CodeCommit repository.

Option C is incorrect since this is used to monitor configuration changes

Option D is incorrect since this is used for managing IAM users

For more information on the notification, please refer to the below URL

- https://docs.aws.amazon.com/codecommit/latest/userguide/how-to-notify.html (https://docs.aws.amazon.com/codecommit/latest/userguide/how-to-notify.html)

Ask our Experts

QUESTION 29 MARKED AS REVIEW CORRECT

Your development team is planning on using the AWS Batch service to process a high number of intensive performance computing jobs. Which of the following integration services with AWS Batch will allow you to monitor the progress of the jobs?

- A. AWS Cloudtrail
- B. AWS Cloudwatch Events ✔
- C. AWS Config
- D. AWS SQS

Explanation :

Answer – B
The AWS Documentation mentions the following
Using CloudWatch Events, you can monitor the progress of jobs, build AWS Batch custom workflows with complex dependencies, generate usage reports or metrics around job execution, or build your own custom dashboards. With AWS Batch and CloudWatch Events, you can eliminate scheduling and monitoring code that continuously polls AWS Batch for job status changes. Instead, handle AWS Batch job state changes asynchronously using any CloudWatch Events target, such as AWS Lambda, Amazon Simple Queue Service, Amazon Simple Notification Service, or Amazon Kinesis Data Streams.
Option A is incorrect since this is an API Monitoring service
Option C is incorrect since this is used to monitor configuration changes
Option D is incorrect since this is used as a messaging service
For more information on Cloudwatch event stream, please refer to the below URL

- https://docs.aws.amazon.com/batch/latest/userguide/cloudwatch_event_stream.html (https://docs.aws.amazon.com/batch/latest/userguide/cloudwatch_event_stream.html)

Ask our Experts

QUESTION 30 CORRECT

Your team is working on an application that it going to work with a DynamoDB table. At the design stage, you are trying to find out the optimum way to define partition keys and secondary indexes. Which of the following are recommendations for defining secondary indexes? Choose 2 answers from the options given below.

- [x] **A.** Keep the number of indexes to a minimum ✔
- [ ] **B.** Define as many indexes as possible to maximize performance
- [x] **C.** Avoid indexing tables that experience heavy write activity ✔
- [ ] **D.** Add indexes to tables that experience heavy write activity

Explanation :

Answer – A and C
The AWS Documentation mentions the following

- Keep the number of indexes to a minimum. Don't create secondary indexes on attributes that you don't query often. Indexes that are seldom used contribute to increased storage and I/O costs without improving application performance

used contribute to increased storage and I/O costs without improving application performance.

- Avoid indexing tables that experience heavy write activity. In a data capture application, for example, the cost of I/O operations required to maintain an index on a table with a very high write load can be significant. If you need to index data in such a table, it may be more effective to copy the data to another table that has the necessary indexes and query it there.

Since the documentation mentions this clearly, all other options are invalid
For more information on working with indexes, please refer to the below URL

- https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/bp-indexes-general.html (https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/bp-indexes-general.html)

Ask our Experts

QUESTION 31 CORRECT

Your team is working on an application that will connect to a MySQL RDS Instance. The security mandate is that the connection to the application needs to be encrypted. How can you accomplish this?

- A. By using Access Keys assigned to an IAM user
- B. By using Private Key pairs
- C. By using SSL ✔
- D. By using KMS Keys

Explanation :

Answer – C

The AWS Documentation mentions the following

Using SSL to Encrypt a Connection to a DB Instance

You can use SSL from your application to encrypt a connection to a DB instance running MySQL, MariaDB, SQL Server, Oracle, or PostgreSQL. Each DB engine has its own process for implementing SSL. To learn how to implement SSL for your DB instance, use the link following that corresponds to your DB engine:

- Using SSL with a MariaDB DB Instance
- Using SSL with a Microsoft SQL Server DB Instance
- Using SSL with a MySQL DB Instance
- Using SSL with an Oracle DB Instance
- Using SSL with a PostgreSQL DB Instance

Option A is incorrect since this is used for programmatic access for a user
Option B is incorrect since this is used for connection to an EC2 Instance
Option D is incorrect since is normally used for encrypting data at rest or before data is sent in transit
For more information on using RDS with SSL, please refer to the below URL

- https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.SSL.html (https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.SSL.html)

Ask our Experts

QUESTION 32 CORRECT

You are planning on developing and deploying a Node.js Lambda function. The code has a dependency on a lot of third-party libraries. Which of the following needs to be done to ensure the code can be executed in the AWS Lambda service?

- A. Install the third-party libraries in the Lambda service
- B. Create a deployment package with your code and the third-party libraries ✔
- C. Use Cloudformation templates to deploy the third-party libraries
- D. Use an IAM Role with the required permissions on those libraries

Explanation :

Answer - B

The AWS Documentation mentions the following

If you are writing code that uses other resources, such as a graphics library for image processing, or you want to use the AWS CLI instead of the console, you need to first create the Lambda function deployment package, and then use the console or the CLI to upload the package.

Because of what is mentioned in the AWS Documentation, all other options are invalid

For more information on creating the deployment package, please refer to the below URL

- https://docs.aws.amazon.com/lambda/latest/dg/nodejs-create-deployment-pkg.html (https://docs.aws.amazon.com/lambda/latest/dg/nodejs-create-deployment-pkg.html)

Ask our Experts

QUESTION 33 CORRECT

You have to create a DynamoDB table called Customers which will have 2 attributes. One is the ID which will be the

You have to create a DynamoDB table called Customers which will have 2 attributes. One is the ID which will be the partition key and the other is the Name which will be the sort key. Which of the following is the right definition for the CLI command that would be used to create the table?

- **A.** aws dynamodb create-table \ --table-name Customer \ --attribute-definitions \ AttributeName=ID,AttributeType=N \ AttributeName=Name,AttributeType=S \ --key-schema \ AttributeName=ID,KeyType=HASH \ AttributeName=Name,KeyType=RANGE \ --provisioned-throughput \ ReadCapacityUnits=10,WriteCapacityUnits=5 ✔
- **B.** aws dynamodb create-table \ --table-name Customer \ --attribute-definitions \ AttributeName=ID,AttributeType=N \ AttributeName=Name,AttributeType=S \ --provisioned-throughput \ ReadCapacityUnits=10,WriteCapacityUnits=5
- **C.** aws dynamodb create-table \ --table-name Customer \ --attribute-definitions \ AttributeName=ID,AttributeType=N \ AttributeName=Name,AttributeType=S \ --key-schema \ AttributeName=Name,KeyType=HASH \ AttributeName=ID,KeyType=RANGE \ --provisioned-throughput \ ReadCapacityUnits=10,WriteCapacityUnits=5
- **D.** aws dynamodb set-table \ --table-name Customer \ --attribute-definitions \ AttributeName=ID,AttributeType=N \ AttributeName=Name,AttributeType=S \ --key-schema \ AttributeName=ID,KeyType=HASH \ AttributeName=Name,KeyType=RANGE \ --provisioned-throughput \ ReadCapacityUnits=10,WriteCapacityUnits=5

Explanation :

Answer - A

An example of this is given in the AWS Documentation

Example

The following AWS CLI example shows how to create a table (*Music*). The primary key consists of *Artist* (partition key) and *SongTitle* (sort key), each of which has a data type of String. The maximum throughput for this table is 10 read capacity units and 5 write capacity units.

```
aws dynamodb create-table \
    --table-name Music \
    --attribute-definitions \
        AttributeName=Artist,AttributeType=S \
        AttributeName=SongTitle,AttributeType=S \
    --key-schema \
        AttributeName=Artist,KeyType=HASH \
        AttributeName=SongTitle,KeyType=RANGE \
    --provisioned-throughput \
        ReadCapacityUnits=10,WriteCapacityUnits=5
```

Option B is incorrect since the keys are not being defined here
Option C is incorrect since the Name key should be RANGE and the ID should be HASH
Option D is incorrect since the right CLI command is create-table
For more information on working with tables, please refer to the below URL

- https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/WorkingWithTables.Basics.html (https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/WorkingWithTables.Basics.html)

Ask our Experts

QUESTION 34 CORRECT

You have to develop an Orders processing system. The system needs to store the Product Information which

You have to develop an Orders processing system. The system needs to store the Product information which contains the image for every product. Which of the following implementation steps should be used when storing the Product related data. Choose 2 answers from the options given below

- [x] **A.** Store the Product ID, Name and price in a DynamoDB table ✔
- [ ] **B.** Store the Product Image as an attribute in the same table
- [ ] **C.** Store the Product ID, Name and price in an S3 bucket
- [x] **D.** Store the Product Image in an S3 bucket ✔

Explanation :

Answer – A and D

This is also mentioned in the AWS Documentation

As mentioned above, you can also take advantage of Amazon Simple Storage Service (Amazon S3) to store large attribute values that cannot fit in a DynamoDB item. You can store them as an object in Amazon S3 and then store the object identifier in your DynamoDB item. You can also use the object metadata support in Amazon S3 to provide a link back to the parent item in DynamoDB. Store the primary key value of the item as Amazon S3 metadata of the object in Amazon S3. Doing this often helps with maintenance of the Amazon S3 objects.

Option B is incorrect since the Images should ideally be stored as an object in S3

Option C is incorrect since the ID and Name data should ideally be stored in a table

For more information on best developer practises for DynamoDB, please refer to the below URL

- 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 35 MARKED AS REVIEW INCORRECT

Your team is planning on delivering content to users by using the Cloudfront service and an S3 bucket as the source. You need to ensure that a custom value is placed for the amount of time the object is stored in the Cloudfront cache. Which of the following 2 options can be used to fulfil this requirement?

- [ ] **A.** Configure the origin to add an Expires header field to the object ✔
- [ ] **B.** Configure the Cloudfront distribution to add an Expires header field to the object
- [x] **C.** Specify a value for Minimum TTL in CloudFront cache behaviors ✔
- [x] **D.** Specify a value for Minimum TTL in the origin object ✖

Explanation :

Answer – A and C
This is also mentioned in the AWS Documentation
For web distributions, to control how long your objects stay in a CloudFront cache before CloudFront forwards another request to your origin, you can:

- Configure your origin to add a Cache-Control or an Expires header field to each object.
- Specify a value for Minimum TTL in CloudFront cache behaviors.
- Use the default value of 24 hours.

Since this is clearly mentioned in the AWS Documentation , the other options are invalid
For more information on request and response behaviour for Cloudfront with S3, please refer to the below URL

- https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/RequestAndResponseBehaviorS3Origin.html (https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/RequestAndResponseBehaviorS3Origin.html)

Ask our Experts

QUESTION 36 CORRECT

You are using a custom tool known as POSTMAN to make API requests to resources in AWS. Part of the job of sending requests is to sign the request. Which of the following would you use to sign the API requests made to AWS?

- A. Your user name and password
- B. A private key file
- C. KMS keys
- D. Access Keys ✔

Explanation :

Answer – D
The AWS Documentation mentions the following
When you send HTTP requests to AWS, you sign the requests so that AWS can identify who sent them. You sign requests with your AWS access key, which consists of an access key ID and secret access key. Some requests do not need to be signed, such as anonymous requests to Amazon Simple Storage Service (Amazon S3) and some API operations in AWS Security Token Service (AWS STS) such as AssumeRoleWithWebIdentity (https://docs.aws.amazon.com/STS/latest/APIReference/API_AssumeRoleWithWebIdentity.html).
Option A is incorrect since this is used for console-based access
Option B is incorrect since this is used for logging onto EC2 Instances
Option C is incorrect since this is use for encrypting data
For more information on signing API requests, please refer to the below URL

- https://docs.aws.amazon.com/general/latest/gr/signing_aws_api_requests.html (https://docs.aws.amazon.com/general/latest/gr/signing_aws_api_requests.html)

Ask our Experts

QUESTION 37 CORRECT

A company is making use of the Simple Notification service to send notifications to various subscribers for their service. There is a user requirement for the subscriber to only receive certain types of messages and not all messages published to the topic. How can you achieve this?

- A. By adding a filter policy to the topic ✔
- B. By adding an IAM policy to the topic
- C. Publish the messages to an SQS queue
- D. Publish the messages to a Lambda function

Explanation :

Answer - A

The AWS Documentation mentions the following

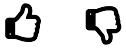
By default, a subscriber of an Amazon SNS topic receives every message published to the topic. To receive only a subset of the messages, a subscriber assigns a filter policy to the topic subscription.

A filter policy is a simple JSON object. The policy contains attributes that define which messages the subscriber receives. When you publish

a message to a topic, Amazon SNS compares the message attributes to the attributes in the filter policy for each of the topic's subscriptions. If there is a match between the attributes, Amazon SNS sends the message to the subscriber. Otherwise, Amazon SNS skips the subscriber without sending the message to it. If a subscription lacks a filter policy, the subscription receives every message published to its topic.
Since the documentation clearly mentions this , all other options are incorrect
For more information on message filtering, please refer to the below URL

- https://docs.aws.amazon.com/sns/latest/dg/message-filtering.html (https://docs.aws.amazon.com/sns/latest/dg/message-filtering.html)

Ask our Experts



QUESTION 38 CORRECT

Your company has an existing Redshift cluster. The sales team currently store historical data in the cluster. There is now a requirement to ensure that all data is encrypted at rest. How can you achieve this?

- A. Enable the Encryption feature for the cluster
- B. Enable encryption for the underlying EBS volumes
- C. Use SSL certificates to encrypt the data at rest
- D. Create a new cluster with encryption enabled ✔

Explanation :
Answer – D

The AWS Documentation mentions the following

In Amazon Redshift, you can enable database encryption for your clusters to help protect data at rest. When you enable encryption for a cluster, the data blocks and system metadata are encrypted for the cluster and its snapshots.

Encryption is an optional, immutable setting of a cluster. If you want encryption, you enable it during the cluster launch process.To go from an unencrypted cluster to an encrypted cluster or the other way around, unload your data from the existing cluster and reload it in a new cluster with the chosen encryption setting.

Option A is invalid since you cannot enable Encryption for an existing cluster

Option B is invalid since the encryption needs to be enabled at the cluster level

Option C is invalid since SSL certificates are used for encryption of data in transit

For more information on database encryption with Redshift, please refer to the below URL

- https://docs.aws.amazon.com/redshift/latest/mgmt/working-with-db-encryption.html (https://docs.aws.amazon.com/redshift/latest/mgmt/working-with-db-encryption.html)

Note: Latest Update

You can enable encryption for an existing Redshift cluster.

- https://docs.aws.amazon.com/redshift/latest/mgmt/working-with-db-encryption.html (https://docs.aws.amazon.com/redshift/latest/mgmt/working-with-db-encryption.html)

AWS Docs Above mentions "When you modify your cluster to enable KMS encryption, Amazon Redshift automatically migrates your data to a new encrypted cluster."

Since this is a recent announcement, Questions in exam won't be updated yet. We'll update the question and options once we get the confirmation that exam questions are updated.

Ask our Experts

QUESTION 39 MARKED AS REVIEW CORRECT

Your team has developed a web application that will run on an EC2 Instance. There is a deployment requirement

Your team has developed a web application that will run on an EC2 instance. There is a deployment requirement wherein if the primary application fails, the requests need to be routed to a static web site. Which of the following can help you achieve this?

- A. A Classic Load balancer placed in front of the EC2 Instances
- B. An Application Load balancer placed in front of the EC2 Instances
- C. A health check in Route 53 ✔
- D. The swap URL feature in Elastic Beanstalk

Explanation :

Answer – C
The AWS Documentation mentions the following
Amazon Route 53 health checks monitor the health and performance of your web applications, web servers, and other resources. Each health check that you create can monitor one of the following:

- The health of a specified resource, such as a web server
- The status of other health checks
- The status of an Amazon CloudWatch alarm

Options A and B are incorrect since the Load balancers are used to distribute traffic and not divert traffic
Option D is incorrect since the application is not being hosted on Elastic Beanstalk
For more information on DNS failover, please refer to the below URL

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

Ask our Experts

QUESTION 40 MARKED AS REVIEW CORRECT

Your team has decided to host a static web site using the Simple Storage Service. A bucket has been defined with the domain name, the objects uploaded, and the static web site hosting enabled for the bucket. But you are still not able to able to access the web site. Which of the following could be the underlying issue?

- A. You need to enable versioning for the bucket as well
- B. The bucket must have public read access ✔
- C. You need to ensure the storage class is infrequent access
- D. You need to use AWS Managed Keys

Explanation :

Answer – B
The AWS Documentation mentions the following
To host a static website, you configure an Amazon S3 bucket for website hosting, and then upload your website content to the bucket. This bucket must have public read access. It is intentional that everyone in the world will have read access to this bucket.
Option A is incorrect since this feature is used to avoid accidental deletion of objects
Option C is incorrect since this the storage class should ideally be standard storage
Option D is incorrect since this is used for encryption of objects at rest
For more information on static web site hosting, please refer to the below URL

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

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

Ask our Experts

QUESTION 41 MARKED AS REVIEW CORRECT

As a developer you are looking at making use of AWS Cognito Sync. Which of the below are features of this service. Choose 3 answers from the options given below.

- [x] **A.** Cross-device syncing of application-related user data ✔
- [x] **B.** Synching of offline data back to AWS ✔
- [x] **C.** Push Sync Notification ✔
- [ ] **D.** Sync data with DynamoDB

Explanation :

Answer – A, B and C
The AWS Documentation mentions the following
Amazon Cognito Sync is an AWS service and client library that enable cross-device syncing of application-related user data. You can use it to synchronize user profile data across mobile devices and web applications. The client libraries cache data locally so your app can read and write data regardless of device connectivity status. When the device is online, you can synchronize data, and if you set up push sync,

notify other devices immediately that an update is available.

Since the documentation clearly gives the features of this service, all other options are invalid
For more information on AWS Cognito Sync, please refer to the below URL

- https://docs.aws.amazon.com/cognito/latest/developerguide/getting-started-with-cognito-sync.html (https://docs.aws.amazon.com/cognito/latest/developerguide/getting-started-with-cognito-sync.html)

Ask our Experts

QUESTION 42 CORRECT

You've developed an application that is going to be hosted on an EC2 Instance. The company has decided to use Cloudfront to distribute the content. The IT Security department has mandated that the traffic is encrypted between Cloudfront and the Viewer and Cloudfront and the origin as well. How can you achieve this? Choose 2 answers from the options given below.

- [ ] **A.** Ensure that HTTP is mapped to port 443 at the origin
- [ ] **B.** Ensure that KMS keys are used to encrypt the traffic
- [x] **C.** Ensure that the Viewer Protocol policy is set to HTTPS only or Redirect HTTP to HTTPS ✔
- [x] **D.** Ensure that the Origin Protocol policy is set to HTTPS only ✔

Explanation :

Answer – C and D

This is given in the AWS Documentation

To require HTTPS between viewers and CloudFront for one or more cache behaviors, perform the following procedure.

To configure CloudFront to require HTTPS between viewers and CloudFront

1. Sign in to the AWS Management Console and open the CloudFront console at https://console.aws.amazon.com/cloudfront/.
2. In the top pane of the CloudFront console, choose the ID for the distribution that you want to update.
3. On the **Behaviors** tab, choose the cache behavior that you want to update, and then choose **Edit**.
4. Specify one of the following values for **Viewer Protocol Policy**:

   Redirect HTTP to HTTPS

   Viewers can use both protocols. HTTP `GET` and `HEAD` requests are automatically redirected to HTTPS requests. CloudFront returns HTTP status code 301 (Moved Permanently) along with the new HTTPS URL. The viewer then resubmits the request to CloudFront using the HTTPS URL.

   Important

   If you send `POST`, `PUT`, `DELETE`, `OPTIONS`, or `PATCH` over HTTP with an HTTP to HTTPS cache behavior and a request protocol version of HTTP 1.1 or above, CloudFront redirects the request to a HTTPS location with a HTTP status code 307 (Temporary Redirect). This guarantees that the request is sent again to the new location using the same method and body payload.

   If you send `POST`, `PUT`, `DELETE`, `OPTIONS`, or `PATCH` requests over HTTP to HTTPS cache behavior with a request protocol version below HTTP 1.1, CloudFront returns a HTTP status code 403 (Forbidden).

   When a viewer makes an HTTP request that is redirected to an HTTPS request, CloudFront charges for both requests. For the HTTP request, the charge is only for the request and for the headers that CloudFront returns to the viewer. For the HTTPS request, the charge is for the request, and for the headers and the object that are returned by your origin.

   HTTPS Only

To configure CloudFront to require HTTPS between CloudFront and your custom origin

1. Sign in to the AWS Management Console and open the CloudFront console at https://console.aws.amazon.com/cloudfront/.

2. In the top pane of the CloudFront console, choose the ID for the distribution that you want to update.

3. On the **Origins** tab, choose the origin that you want to update, and then choose **Edit**.

4. Update the following settings:

Origin Protocol Policy

Change the **Origin Protocol Policy** for the applicable origins in your distribution:

- **HTTPS Only** – CloudFront uses only HTTPS to communicate with your custom origin.
- **Match Viewer** – CloudFront communicates with your custom origin using HTTP or HTTPS, depending on the protocol of the viewer request. For example, if you choose **Match Viewer** for **Origin Protocol Policy** and the viewer uses HTTPS to request an object from CloudFront, CloudFront also uses HTTPS to forward the request to your origin.
  Choose **Match Viewer** only if you specify **Redirect HTTP to HTTPS** or **HTTPS Only** for **Viewer Protocol Policy**.
  CloudFront caches the object only once even if viewers make requests using both HTTP and HTTPS protocols.

Since this is clearly given in the documentation, all other options are incorrect
For more information on configuring HTTPS between the Viewer and Cloudfront and the Origin and Cloudfront, please refer to the below URL

- https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/using-https-viewers-to-cloudfront.html (https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/using-https-viewers-to-cloudfront.html)
- https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/using-https-cloudfront-to-custom-origin.html (https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/using-https-cloudfront-to-custom-origin.html)

Ask our Experts

QUESTION 43 MARKED AS REVIEW CORRECT

Your application is currently configured to interact with an S3 bucket. Now you are getting errors that the bucket

Your application is currently configured to interact with an S3 bucket. Now you are getting errors that the bucket does not exist. Which of the following is the best way to understand how the bucket was deleted?

- A. Use the Cloudwatch logs to see the Bucket Deletion API request
- B. Use the Cloudtrail logs to see the Bucket Deletion API request ✔
- C. Use the AWS Inspector service to see the Bucket Deletion API request
- D. Use the AWS Trusted Advisor service to see the Bucket Deletion API request

Explanation :

Answer – B

You can use the Cloudtrail service to see when the bucket was deleted and who initiated the bucket deletion request.

Amazon S3 Bucket-Level Actions Tracked by CloudTrail Logging

By default, CloudTrail logs bucket-level actions. Amazon S3 records are written together with other AWS service records in a log file. CloudTrail determines when to create and write to a new file based on a time period and file size.

The tables in this section list the Amazon S3 bucket-level actions that are supported for logging by CloudTrail.

Amazon S3 Bucket-Level Actions Tracked by CloudTrail Logging

REST API Name	API Event Name Used in CloudTrail Log
DELETE Bucket	DeleteBucket
DELETE Bucket cors	DeleteBucketCors
DELETE Bucket encryption	DeleteBucketEncryption
DELETE Bucket lifecycle	DeleteBucketLifecycle
DELETE Bucket policy	DeleteBucketPolicy
DELETE Bucket replication	DeleteBucketReplication
DELETE Bucket tagging	DeleteBucketTagging
DELETE Bucket website	DeleteBucketWebsite

Option A is incorrect since the logs will not have the detailed information about the bucket deletion request

Option C is incorrect since this service is only used to check the vulnerabilities on servers

Option D is incorrect since this service is only used to provide recommendations
For more information on Cloudtrail logging, please refer to the below URL

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

Ask our Experts

QUESTION 44 MARKED AS REVIEW CORRECT

Your team is developing an application makes use of Docker containers. These containers will be deployed to the Elastic Container Service. The applications on these containers need to interact with DynamoDB tables. Which of the following is the most secure way to ensure the containers can interact with DynamoDB?

- A. Create an IAM Role for the ECS Tasks ✔
- B. Embed the Access Keys in the containers
- C. Embed the Access Keys in the cluster
- D. Use an IAM user's credentials to spin up the cluster

Explanation :

Answer - A
The AWS Documentation mentions the following

With IAM roles for Amazon ECS tasks, you can specify an IAM role that can be used by the containers in a task. Applications must sign their

AWS API requests with AWS credentials, and this feature provides a strategy for managing credentials for your applications to use, similar to the way that Amazon EC2 instance profiles provide credentials to EC2 instances. Instead of creating and distributing your AWS credentials to the containers or using the EC2 instance's role, you can associate an IAM role with an ECS task definition or RunTask API operation. The applications in the task's containers can then use the AWS SDK or CLI to make API requests to authorized AWS services.
All other options are invalid since the most secure way is to use IAM Roles for accessing AWS services
For more information on IAM Roles for tasks, please refer to the below URL

- https://docs.aws.amazon.com/AmazonECS/latest/developerguide/task-iam-roles.html (https://docs.aws.amazon.com/AmazonECS/latest/developerguide/task-iam-roles.html)

Ask our Experts

QUESTION 45 CORRECT

An application is making calls to a DynamoDB table. The queries are taking on a lot of read capacity. The table has a large number of attributes. Not all of the attributes are used in the query. Which of the following can be used to minimize the read capacity being used by the queries?

- A. Use global secondary indexes with projected attributes ✔
- B. Use an Application Load balancer in front of the DynamoDB table
- C. Consider using parallel scans on the table
- D. Use a cloudfront distribution in front of the DynamoDB table

Explanation :

Answer – A

You can use Global secondary indexes and use only those attributes which will be queried. This can help reduce the amount of read throughput used on the table.
Options B and D are invalid because these are invalid architecture designs
Option C is incorrect since using queries is more effective
For more information on general guidelines for indexes, please refer to the below URL

- https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/bp-indexes-general.html (https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/bp-indexes-general.html)

Ask our Experts

QUESTION 46 MARKED AS REVIEW CORRECT

Your team is developing a set of Lambda functions. You need to ensure the team uses the best practices for working with AWS Lambda. What is the advantage of initializing any external dependencies of your Lambda function code? Choose one of the options given below.

- A. Ability to decode errors better
- B. Ability to instantiate an object for each invocation
- C. Ability to reuse Execution Context ✔
- D. Ability to call functions faster

Explanation :

Explanation :

Answer - C

This is given as one of the best practises for AWS Lambda in the documentation

Take advantage of Execution Context reuse to improve the performance of your function. Make sure any externalized configuration or dependencies that your code retrieves are stored and referenced locally after initial execution. Limit the re-initialization of variables/objects on every invocation. Instead use static initialization/constructor, global/static variables and singletons. Keep alive and reuse connections (HTTP, database, etc.) that were established during a previous invocation.

Since this is clearly given in the AWS Documentation, all other options are invalid

For more information on Best practices, please refer to the below URL

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

Ask our Experts

QUESTION 47 MARKED AS REVIEW INCORRECT

Your team is transitioning a stateful based web application to AWS. You need to decide the services which will be used to host the application. Which of the following would be included in the design? Choose 2 answers from the options given below

- [x] **A.** DynamoDB to store the session data ✔
- [ ] **B.** AWS Lambda to store the session data
- [ ] **C.** An Application Load balancer to distribute traffic ✔
- [x] **D.** An API gateway to distribute traffic ✖

Explanation :

Answer – A and C

The below example from the AWS Documentation shows how DynamoDB can be used to store session data

DynamoDB Session Handler

Introduction

The **DynamoDB Session Handler** is a custom session handler for PHP that allows developers to use Amazon DynamoDB as a session store. Using DynamoDB for session storage alleviates issues that occur with session handling in a distributed web application by moving sessions off of the local file system and into a shared location. DynamoDB is fast, scalable, easy to setup, and handles replication of your data automatically.

The DynamoDB Session Handler uses the `session_set_save_handler()` function to hook DynamoDB operations into PHP's native session functions to allow for a true drop in replacement. This includes support for features like session locking and garbage collection which are a part of PHP's default session handler.

For more information on the Amazon DynamoDB service, please visit the Amazon DynamoDB homepage.

And the application load balancer can be used to distribute traffic for the application

Option B is incorrect since this service is used as a Compute Service

Option D is incorrect since this is an API management service

For more information on AWS Cloud Best practises, please refer to the below URL

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

Ask our Experts

QUESTION 48 CORRECT

An application consists of an Autoscaling Group. It has been determined that the best way to scale the group is

An application consists of an Autoscaling Group. It has been determined that the best way to scale the group is based on the number of concurrent users. How can you achieve this?

- A. Create a tag for the Group to contain the number of concurrent users
- B. Create a custom metric for the number of concurrent users ✔
- C. Since concurrent user metrics are not available, base the scaling of the group on CPU percentage
- D. Since concurrent user metrics are not available, base the scaling of the group on Memory percentage

Explanation :

Answer – B
The AWS Documentation mentions the following
With target tracking scaling policies, you select a predefined metric or configure a customized metric and set a target value. Application Auto Scaling creates and manages the CloudWatch alarms that trigger the scaling policy and calculates the scaling adjustment based on the metric and the target value. The scaling policy adds or removes capacity as required to keep the metric at, or close to, the specified target value. In addition to keeping the metric close to the target value, a target tracking scaling policy also adjusts to changes in the metric due to a changing load pattern and minimizes changes to the capacity of the scalable target.
Since you can define a custom metric based on concurrent usage, you can scale the Autoscaling group based on that. Based on this all other options are invalid.
For more information on auto scaling based on target tracking, please refer to the below URL
https://docs.aws.amazon.com/autoscaling/application/userguide/application-auto-scaling-target-tracking.html
(https://docs.aws.amazon.com/autoscaling/application/userguide/application-auto-scaling-target-tracking.html)

Ask our Experts

QUESTION 49 CORRECT

As a developer, you need your operations team to monitor a set of metrics for an application. They also need to be notified in case any of the metrics crosses the threshold. How can you achieve this?

- A. Publish custom metrics for the application that can be monitored via Cloudwatch. Create Alarms for notifications. ✔
- B. Ask the System administrators to monitor the Cloudwatch logs
- C. Ask the System administrators to monitor the Cloudtrail logs
- D. Use the inbuilt metrics for Cloudwatch. Create Alarms for notifications.

Explanation :

Answer – A

The AWS Documentation mentions the following

You can create a CloudWatch alarm that watches a single metric. The alarm performs one or more actions based on the value of the metric relative to a threshold over a number of time periods. The action can be an Amazon EC2 action, an Amazon EC2 Auto Scaling action, or a notification sent to an Amazon SNS topic. You can also add alarms to CloudWatch dashboards and monitor them visually. When an alarm is on a dashboard, it turns red when it is in the ALARM state, making it easier for you to monitor its status proactively.

You can publish your own metrics to CloudWatch using the AWS CLI or an API. You can view statistical graphs of your published metrics with the AWS Management Console.

Option B is invalid since this is used for logging purposes and here you need to view the metrics

Option C is invalid since this is used for API monitoring purposes

Option D is invalid since here we have to assume that we need to monitor metrics for an application and hence you would need to publish custom metrics

For more information on publishing custom metrics and alarms, please refer to the below URL

- https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/publishingMetrics.html (https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/publishingMetrics.html)
- https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/AlarmThatSendsEmail.html (https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/AlarmThatSendsEmail.html)

Ask our Experts

QUESTION 50 CORRECT

Your company has a SOAP service that receives requests in XML. The service is going to be placed behind the API gateway service. Which of the following must be done to ensure that requests made to the API gateway service can be consumed by the SOAP service?

- A. Create a mapping template ✔
- B. Setup a gateway response
- C. Enable support for binary workloads
- D. Setup Private integrations

Explanation :

Answer – A
The AWS Documentation mentions the following
In API Gateway, an API's method request can take a payload in a different format from the corresponding integration request payload, as required in the backend. Similarly, the backend may return an integration response payload different from the method response payload, as expected by the frontend. API Gateway lets you use mapping templates to map the payload from a method request to the corresponding integration request and from an integration response to the corresponding method response.
A *mapping template* is a script expressed in Velocity Template Language (VTL) (http://velocity.apache.org/engine/devel/vtl-reference-guide.html) and applied to the payload using JSONPath expressions (http://goessner.net/articles/JsonPath/). The payload can have a data model according to the JSON schema draft 4 (https://tools.ietf.org/html/draft-zyp-json-schema-04). You must define the model in order

to have API Gateway to generate a SDK or to enable basic request validation for your API. You do not have to define any model to create a

mapping template. However, a model can help you create a template because API Gateway will generate a template blueprint based on a provided model.
Option B is incorrect since this is used to customize gateway responses
Option C is incorrect since this is used specifically for binary workloads
Option D is incorrect since this is used for use within a VPC
For more information on models and mappings, please refer to the below URL

- https://docs.aws.amazon.com/apigateway/latest/developerguide/models-mappings.html (https://docs.aws.amazon.com/apigateway/latest/developerguide/models-mappings.html)

Ask our Experts

QUESTION 51 CORRECT

An application needs to make use of the SQS service for sending and receiving messages. The application takes 60 seconds to process a message. Assuming that a queue has been created with the default settings, which one of the following must be implemented?

- **A.** Call the ChangeMessageVisibility API and increase the timeout. Call the DeleteMessage API to delete the message. ✔
- **B.** Call the DeleteMessage API to increase the timeout.
- **C.** Call the ChangeMessageVisibility API and decrease the timeout. Call the DeleteMessage API to delete the message.
- **D.** Call the DeleteMessage API to delete the message from the queue first. Call the ChangeMessageVisibility API and increase the timeout

Explanation :

Explanation:

Answer – A

The AWS Documentation mentions the following

Changes the visibility timeout of a specified message in a queue to a new value. The default visibility timeout for a message is 30 seconds. The minimum is 0 seconds. The maximum is 12 hours.

For example, you have a message with a visibility timeout of 5 minutes. After 3 minutes, you call ChangeMessageVisibility with a timeout of 10 minutes. You can continue to call ChangeMessageVisibility to extend the visibility timeout to the maximum allowed time. If you try to extend the visibility timeout beyond the maximum, your request is rejected.

Options B and D are incorrect since you first need to call ChangeMessageVisibility API

Option C is incorrect since the ChangeMessageVisibility API should be used to increase the timeout

For more information on the visibility timeout, please refer to the below URL

- https://docs.aws.amazon.com/AWSSimpleQueueService/latest/APIReference/API_ChangeMessageVisibility.html (https://docs.aws.amazon.com/AWSSimpleQueueService/latest/APIReference/API_ChangeMessageVisibility.html)

Ask our Experts

QUESTION 52 MARKED AS REVIEW INCORRECT

As a programmer you have been hired to develop an application for a company. The application needs to first encrypt the data at the client side before sending it to a destination location. How can you achieve this? The size of the data is generally around 1 – 4 MB. Each object needs to have its own key to encrypt the data.

- A. Upload the data to KMS and use the CMK key to encrypt the data
- B. Use the CMK key ARN to get the key and encrypt the data ✖
- C. Use the GenerateDataKey API to get the key from a CMK ✔

○ **D.** Upload the data to an S3 bucket with encryption enabled

Explanation :

Answer – C

The AWS Documentation mentions the following

We recommend that you use the following pattern to encrypt data locally in your application:

1. Use this operation (GenerateDataKey) to get a data encryption key.
2. Use the plaintext data encryption key (returned in the Plaintext field of the response) to encrypt data locally, then erase the plaintext data key from memory.
3. Store the encrypted data key (returned in the CiphertextBlob field of the response) alongside the locally encrypted data.

Option A is incorrect since you don't upload the data to KMS to encrypt it.

Option B is incorrect since you don't use the CMK key to encrypt large data objects

Option D is incorrect since here the data would only be encrypted at rest and the question states that the object needs to be encrypted at the client side.

For more information on the Generate Data Key API, please refer to the below URL

- https://docs.aws.amazon.com/kms/latest/APIReference/API_GenerateDataKey.html (https://docs.aws.amazon.com/kms/latest/APIReference/API_GenerateDataKey.html)

Ask our Experts

QUESTION 53 MARKED AS REVIEW CORRECT

As a developer, you have the requirement to access resources in another account. Which of the following is the

As a developer, you have the requirement to access resources in another account. Which of the following is the best way to achieve this?

- A. Create a cross account role and call the AssumeRole API ✔
- B. Create a user in the destination account and share the password
- C. Create a user in the destination account and share the Access Keys
- D. Create an IAM Role and attach it to an EC2 Instance

Explanation :

Answer - A

The AWS Documentation mentions the following

For cross-account access, imagine that you own multiple accounts and need to access resources in each account. You could create long-term credentials in each account to access those resources. However, managing all those credentials and remembering which one can access which account can be time consuming. Instead, you can create one set of long-term credentials in one account and then use temporary security credentials to access all the other accounts by assuming roles in those accounts.

All other options are incorrect since the right option is to use cross account roles

For more information on Assuming a Role, please refer to the below URL

- https://docs.aws.amazon.com/STS/latest/APIReference/API_AssumeRole.html (https://docs.aws.amazon.com/STS/latest/APIReference/API_AssumeRole.html)

Ask our Experts

QUESTION 54 CORRECT

You are a developer for an application. The application needs to make use of AWS for managing authentication.

The users should be able to authenticate using identity providers such as Facebook and Google. At the same time, you also need to enable guest user access to limited resources. How can you achieve this in the best possible way?

- A. Use IAM users and groups
- B. Use AWS Cognito and identity pools with both authenticated and unauthenticated identities ✔
- C. Use AWS federated identities
- D. Use AWS Cognito App Sync

Explanation :

Answer – B
The AWS Documentation mentions the following
Amazon Cognito identity pools support both authenticated and unauthenticated identities. Authenticated identities belong to users who are authenticated by any supported identity provider. Unauthenticated identities typically belong to guest users.
Option A is incorrect since this would be too much of a maintenance overhead to maintain the users
Option C is incorrect since we don't need federation access over here
Option D is incorrect since we don't need Sync capabilities here
For more information on Identity pools, please refer to the below URL

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

Ask our Experts

QUESTION 55 CORRECT

You are currently working on a function for AWS Lambda. When uploading the package for your AWS Lambda function, you are receiving the following error

CodeStorageExceededException

What can you do to surpass this error?

- A. Raise a call with AWS Support to raise the limit on storage
- B. Change the code to Node.js for taking up less storage
- C. Reduce the size for your code ✔
- D. Change the memory limit

Explanation :

Answer - C
The AWS Documentation mentions the following

AWS Lambda Limit Errors

Functions that exceed any of the limits listed in the previous limits tables will fail with an `exceeded limits` exception. These limits are fixed and cannot be changed at this time. For example, if you receive the exception `CodeStorageExceededException` or an error message similar to `"Code storage limit exceeded"` from AWS Lambda, you need to reduce the size of your code storage.

To reduce the size of your code storage

1. Remove the functions that you no longer use.
2. Reduce the code size of the functions that you do not want to remove. You can find the code size of a Lambda function by using the AWS Lambda console, the AWS Command Line Interface, or AWS SDKs.

Since the documentation clearly mentions this , all other options are invalid.
For more information on limits for AWS Lambda, please refer to the below URL

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

Ask our Experts

QUESTION 56 CORRECT

Your team is developing a series of Lambda functions. You need to ensure that you analyse the invocations of the functions during the testing phase. Which of the following tools can help you achieve this? Choose 2 answers from the options given below.

- [x] **A.** Amazon Cloudwatch ✔
- [ ] **B.** Amazon Inspector
- [x] **C.** Amazon X-Ray ✔
- [ ] **D.** Amazon Cloudtrail

Explanation :

Answer – A and C

The AWS Documentation mentions the following

Monitoring and Troubleshooting Lambda Applications

AWS Lambda will automatically track the behavior of your Lambda function invocations and provide feedback that you can monitor. In addition, it provides metrics that allows you to analyze the full function invocation spectrum, including event source integration and whether downstream resources perform as expected. The following sections provide guidance on the tools you can use to analyze your Lambda function invocation behavior:

Topics

- Using Amazon CloudWatch
- Using AWS X-Ray

Option B is incorrect since this is used to check EC2 Instances for vulnerabilities
Option D is incorrect since this is used to monitor API activity
For more information on troubleshooting AWS Lambda, please refer to the below URL

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

Ask our Experts

QUESTION 57 CORRECT

Your company needs to develop an application that needs to have a caching facility in place. The application cannot afford many cache failures and should be highly available. Which of the following would you choose for this purpose?

- A. Use Memcached on an EC2 Instance
- B. Use ElastiCache – Memcached
- C. Use ElastiCache – Redis in Cluster Mode ✔

○ **D.** Use Redis on an EC2 Instance

Explanation :

Answer – C
The AWS Documentation mentions the following
ElastiCache for Redis has multiple features to enhance reliability for critical production deployments:

- Automatic detection and recovery from cache node failures.
- Multi-AZ with automatic failover of a failed primary cluster to a read replica in Redis clusters that support replication.
- Redis (cluster mode enabled) supports partitioning your data across up to 15 shards.
- Redis version 3.2.6 supports in-transit and at-rest encryption with authentication so you can build HIPAA-compliant applications.
- Flexible Availability Zone placement of nodes and clusters for increased fault tolerance

Options A and D are incorrect since using just an EC2 Instance would be a single point of failure
Option B is incorrect since Redis would be better for high availability
For more information on Redis ElastiCache, please refer to the below URL

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

Ask our Experts

QUESTION 58 MARKED AS REVIEW CORRECT

Your team is developing a set of Lambda functions. They need to debug the Lambda functions using the X-Ray service. Which of the following are environment variables which are used by AWS Lambda to communicate with the X-Ray service? Choose 3 answers from the options given below

- [x] **A.** _X_AMZN_TRACE_ID ✔
- [x] **B.** AWS_XRAY_CONTEXT_MISSING ✔
- [x] **C.** AWS_XRAY_DAEMON_ADDRESS ✔
- [ ] **D.** AWS_LAMBDA_XRAY

Explanation :

Answer – A,B and C
The AWS Documentation mentions the following
AWS Lambda uses environment variables to facilitate communication with the X-Ray daemon and configure the X-Ray SDK.

- _X_AMZN_TRACE_ID: Contains the tracing header, which includes the sampling decision, trace ID, and parent segment ID. If Lambda receives a tracing header when your function is invoked, that header will be used to populate the _X_AMZN_TRACE_ID environment variable. If a tracing header was not received, Lambda will generate one for you.
- AWS_XRAY_CONTEXT_MISSING: The X-Ray SDK uses this variable to determine its behavior in the event that your function tries to record X-Ray data, but a tracing header is not available. Lambda sets this value to LOG_ERROR by default.
- AWS_XRAY_DAEMON_ADDRESS: This environment variable exposes the X-Ray daemon's address in the following format: IP_ADDRESS:PORT. You can use the X-Ray daemon's address to send trace data to the X-Ray daemon directly, without using the X-Ray SDK.

For more information on using Lambda with X-Ray, please refer to the below URL

- https://docs.aws.amazon.com/lambda/latest/dg/lambda-x-ray.html (https://docs.aws.amazon.com/lambda/latest/dg/lambda-x-

ray.html)

Ask our Experts

QUESTION 59 CORRECT

Your team is planning on deploying an application using the worker environment on AWS Elastic beanstalk. Which of the following is an additional requirement for a worker environment in AWS Elastic Beanstalk?

- A. Ensure that the application is uploaded as a zip file
- B. Ensure that the application size does not exceed 512 MB
- C. Ensure that the application does not include a parent level folder
- D. Ensure that the application contains a file called cron.yaml ✔

Explanation :

Answer - D
The AWS Documentation mentions the following
When you use the AWS Elastic Beanstalk console to deploy a new application or an application version, you'll need to upload a source bundle. Your source bundle must meet the following requirements:

- Consist of a single ZIP file or WAR file (you can include multiple WAR files inside your ZIP file)

- Not exceed 512 MB
- Not include a parent folder or top-level directory (subdirectories are fine)

If you want to deploy a worker application that processes periodic background tasks, your application source bundle must also include a cron.yaml file
Since this is clearly mentioned in the documentation all other options are incorrect.
For more information on application source bundles in Elastic beanstalk, please refer to the below URL

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

Ask our Experts

QUESTION 60 CORRECT

Your team is planning on using the AWS Code Build service to test out the build of the application. The application needs to connect to a database. How should you store the database password in a secure manner so that it is available during the build process?

- A. Store the password as an environment variable on the build server
- B. Store the password in AWS Systems Manager ✔
- C. Store the password in a config file on the build server
- D. Store the password in a config file in the application

Explanation :

Answer - B
The AWS Documentation mentions the following
We strongly discourage using environment variables to store sensitive values, especially AWS access key IDs and secret access keys.
Environment variables can be displayed in plain text using tools such as the AWS CodeBuild console and the AWS CLI.
For sensitive values, we recommend you store them in the Amazon EC2 Systems Manager Parameter Store and then retrieve them from your build spec.

All other options are invalid because they are all insecure ways to access passwords in applications from AWS CodeBuild.
For more information on referencing environment variables, please refer to the below URL

- https://docs.aws.amazon.com/codebuild/latest/userguide/build-env-ref-env-vars.html (https://docs.aws.amazon.com/codebuild/latest/userguide/build-env-ref-env-vars.html)

Ask our Experts

QUESTION 61 MARKED AS REVIEW CORRECT

Your team has just started using the API gateway service. Several AWS Lambda functions are used as the backend for the gateway service. You have deployed the API and made is available for test users. You have now made a change to the method response for the API gateway. What should you do next?

- A. Recreate the gateway service
- B. Redeploy the API ✔
- C. Redeploy the Lambda function
- D. Make a copy of the gateway API

Explanation :

Answer - B

The AWS Documentation mentions the following

To deploy an API, you create an API deployment (https://docs.aws.amazon.com/apigateway/api-reference/resource/deployment/) and associate it with a stage (https://docs.aws.amazon.com/apigateway/api-reference/resource/stage/). Each stage is a snapshot of the API and is made available for the client to call. Every time you update an API, which includes modification of methods, integrations, authorizers, and anything else other than stage settings, you must redeploy the API to an existing stage or to a new stage.

All other options are incorrect since the right way is to Redeploy the API

For more information on how to deploy an API, please refer to the below URL

- https://docs.aws.amazon.com/apigateway/latest/developerguide/how-to-deploy-api.html (https://docs.aws.amazon.com/apigateway/latest/developerguide/how-to-deploy-api.html)

Ask our Experts

QUESTION 62 CORRECT

Your team currently has a MySQL database on their on-premise data center. They now need to port the database onto AWS onto a suitable data store. Which of the following can be used for this purpose?

- A. AWS Config
- B. AWS Database Migration Service ✔
- C. AWS Trusted Advisor
- D. AWS EC2

Explanation :

Answer – B

The AWS Documentation mentions the following

AWS Database Migration Service (AWS DMS) is a cloud service that makes it easy to migrate relational databases, data warehouses, NoSQL databases, and other types of data stores. You can use AWS DMS to migrate your data into the AWS Cloud, between on-premises instances, or between combinations of cloud and on-premises setups.

Option A is invalid since this is a configuration service

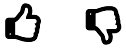
Option C is invalid since this is a recommendations service

Option D is invalid since this is a compute service

For more information on the Data Migration service, please refer to the below URL

- https://docs.aws.amazon.com/dms/latest/userguide/Welcome.html (https://docs.aws.amazon.com/dms/latest/userguide/Welcome.html)

Ask our Experts



QUESTION 63 CORRECT

A company has an application that is making use of a DynamoDB table. There is now a requirement to ensure that all changes to the items in the table are recorded and stored in a MySQL database. Which of the following would ideally be one of the implementation steps?

- A. Enable DynamoDB Accelerator
- B. Enable DynamoDB global tables

- C. Enable DynamoDB streams ✔
- D. Enable DynamoDB triggers

Explanation :

Answer – C
The AWS Documentation mentions the following
DynamoDB Streams enables solutions such as these, and many others. DynamoDB Streams captures a time-ordered sequence of item-level modifications in any DynamoDB table and stores this information in a log for up to 24 hours. Applications can access this log and view the data items as they appeared before and after they were modified, in near real time.
Option A is invalid since this is used to provide DynamoDB-compatible caching service that enables you to benefit from fast in-memory performance for demanding applications
Option B is invalid since this is used to provide a fully managed solution for deploying a multi-region, multi-master database, without having to build and maintain your own replication solution
Option D is invalid since there are no inbuilt triggers in DynamoDB
For more information on DynamoDB streams, please refer to the below URL

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

Ask our Experts

QUESTION 64 CORRECT

You have developed a Lambda function. This function needs to run on a scheduled basis. Which of the following

You have developed a Lambda function. This function needs to run on a scheduled basis. Which of the following can be done to accomplish this requirement in an ideal manner?

- A. Use the schedule service in AWS Lambda
- B. Use an EC2 Instance to schedule the Lambda invocation
- C. Use Cloudwatch events to schedule the Lambda function ✔
- D. Use Cloudtrail to schedule the Lambda function

Explanation :

Answer – C

The AWS Documentation mentions the following

Tutorial: Schedule AWS Lambda Functions Using CloudWatch Events

You can set up a rule to run an AWS Lambda function on a schedule. This tutorial shows how to use the AWS Management Console or the AWS CLI to create the rule. If you would like to use the AWS CLI but have not installed it, see the AWS Command Line Interface User Guide.

CloudWatch Events does not provide second-level precision in schedule expressions. The finest resolution using a cron expression is a minute. Due to the distributed nature of the CloudWatch Events and the target services, the delay between the time the scheduled rule is triggered and the time the target service honors the execution of the target resource might be several seconds. Your scheduled rule is triggered within that minute but not on the precise 0th second.

Option A is incorrect since there is no inbuilt scheduler in AWS Lambda

Option B is incorrect since this would add more maintenance overhead

Option D is incorrect since this service is an API monitoring service

For more information on running Lambda functions on schedules, please refer to the below URL

- https://docs.aws.amazon.com/AmazonCloudWatch/latest/events/RunLambdaSchedule.html (https://docs.aws.amazon.com/AmazonCloudWatch/latest/events/RunLambdaSchedule.html)

Ask our Experts

QUESTION 65 CORRECT

A Company has a web application. They want to deploy it to AWS. They don't want to manage the underlying infrastructure. Which of the following services can help to accomplish this?

- **A.** AWS Lambda and API Gateway ✔
- **B.** AWS EC2 and Cloudfront
- **C.** AWS Lambda and Cloudfront
- **D.** AWS Lambda and EC2

Explanation :

Answer – A
The AWS Documentation mentions the following

AWS Lambda is a compute service that lets you run code without provisioning or managing servers. AWS Lambda executes your code only

when needed and scales automatically, from a few requests per day to thousands per second. You pay only for the compute time you consume - there is no charge when your code is not running. With AWS Lambda, you can run code for virtually any type of application or backend service - all with zero administration
Amazon API Gateway is an AWS service that enables developers to create, publish, maintain, monitor, and secure APIs at any scale. You can create APIs that access AWS or other web services, as well as data stored in the AWS Cloud (https://aws.amazon.com/what-is-cloud-computing/).
Options B and D are incorrect since for EC2 you would need to manage the compute layer
Option C is incorrect since Cloudfront is not used along with AWS Lambda
For more information on AWS Lambda and the API gateway service, please refer to the below URL

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

Ask our Experts

Finish Review (https://www.whizlabs.com/learn/course/aws-cda-practice-tests/quiz/14839)

- PM Certification (https://www.whizlabs.com/project-management-certifications/)
- Big Data Certification (https://www.whizlabs.com/big-data-certifications/)

Mobile App

- Android Coming Soon
- iOS Coming Soon

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)