PRACTICE TEST II - 2018 VERSION

Attempt	2	**Completed on**	Thursday , 06 December 2018 , 04:27 PM
Marks Obtained	42 / 65	**Time Taken**	00 H 28 M 37 S
Your score is	64.62%	**Result**	Fail

Domains / Topics wise Quiz Performance Report

S.No.	Topic	Total Questions	Correct	Incorrect	Unattempted
1	Deployment	17	9	8	0
2	Refactoring	10	7	3	0
3	Development with AWS Services	19	13	5	1
4	Security	10	7	3	0
5	Monitoring and Troubleshooting	2	0	2	0
6	Other	7	6	1	0

65 Questions	42 Correct	22 Incorrect	1 Unattempted

Show Answers: All

QUESTION 1 INCORRECT DEPLOYMENT

You're a developer at a company that needs to deploy an application using Elastic Beanstalk. There is a requirement to place a healthcheck.config file for the environment. In which of the following location should this config file be placed to ensure it is part of the elastic beanstalk environment?

- A. In the application root folder
- B. In the config folder ✖
- C. In the packages folder
- D. In the .ebextensions folder ✔

Explanation :

Answer – D
The AWS Documentation mentions the following
Elastic Beanstalk supports two methods of saving configuration option settings. Configuration files in YAML or JSON format can be included in your application's source code in a directory named .ebextensions and deployed as part of your application source bundle. You create and manage configuration files locally.
All other options are incorrect because the AWS documentation specifically mentions that you need to place custom configuration files in the .ebextensions folder
For more information on the environment configuration method , please refer to the below URL

- https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/environment-configuration-methods-before.html (https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/environment-configuration-methods-before.html)

Ask our Experts

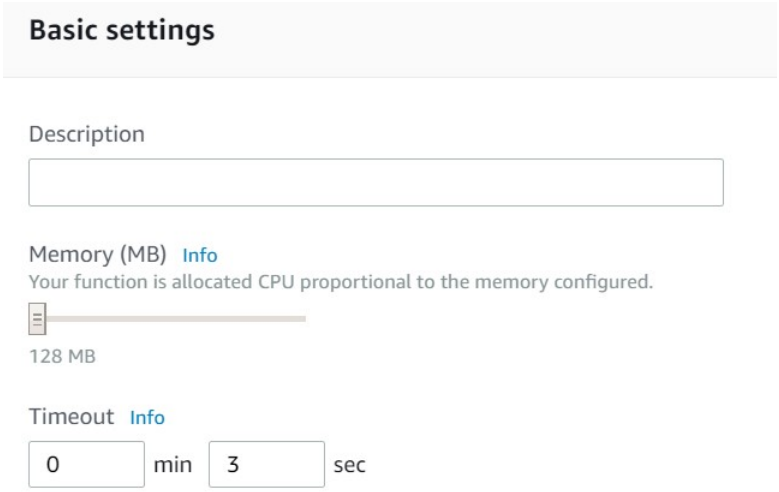
QUESTION 2 CORRECT REFACTORING

A Lambda function has been developed with the default settings and is using Node.js. The function makes calls to a DynamoDB table. The code was first tested and executed on an EC2 Instance in the same language and took 300 seconds to execute. When the lambda function is executed , it is not adding the required rows to the DynamoDB table. What needs to be changed in order to ensure that the Lambda function works as desired?

- A. Ensure that the underlying programming language is changed to python
- B. Change the timeout for the function ✔
- C. Change the memory assigned to the function to 1 GB
- D. Assignan IAM user to the Lambda function

Explanation :

Answer – B
If the lambda function was created with the default settings , it would have the default timeout of 3 seconds as shown below. Since the function executes in a timespan of 300 seconds on an EC2 instance , this value needs to be changed.



Option A is incorrect since the programming language is not an issue
Option C is incorrect since there is no mention on the amount of memory required in the question
Option D is incorrect since IAM roles should be assigned to the Lambda function
For more information on configuring Lambda functions , please refer to the below URL

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

Ask our Experts

QUESTION 3 INCORRECT DEVELOPMENT WITH AWS SERVICES

You need to setup a RESTful API service in AWS that would be serviced via the following url

https://democompany.com/customers (https://democompany.com/customers)

Which of the following combination of services can be used for development and hosting of the RESTful service? Choose 2 answers from the options below

- [x] **A.** AWS Lambda and AWS API gateway ✔
- [x] **B.** AWS S3 and Cloudfront ✖
- [ ] **C.** AWS EC2 and AWS Elastic Load Balancer ✔
- [ ] **D.** AWS SQS and Cloudfront

Explanation :

Answer – A and C
AWS Lambda can be used to host the code and the API gateway can be used to access the API's which point to AWS Lambda
Alternatively you can create your own API service , host it on an EC2 Instance and then use the AWS Application Load balancer to do path based routing.
Option B is incorrect since AWS S3 is normally is used to host static content
Option D is incorrect since AWS SQS is a queuing service
For more information on an example with RESTful API's , please refer to the below URL

- https://aws.amazon.com/getting-started/projects/build-serverless-web-app-lambda-apigateway-s3-dynamodb-cognito/module-4/ (https://aws.amazon.com/getting-started/projects/build-serverless-web-app-lambda-apigateway-s3-dynamodb-cognito/module-4/)

Ask our Experts

QUESTION 4 CORRECT SECURITY

You are developing a mobile based application that needs to make use of an authentication service. There are a set of videos files which need to be accessed via unauthenticated identities. How can you BEST achieve this using AWS?

- ○ **A.** Create an IAM user with public access
- ○ **B.** Create an IAM group with public access
- ○ **C.** Use AWS Cognito with unauthenticated identities enabled. ✔
- ○ **D.** Use AWS STS with SAML

Explanation :

Answer – C
This is also mentioned in the AWS Documentation
Using Identity Pools (Federated Identities)
Amazon Cognito identity pools provide temporary AWS credentials for users who are guests (unauthenticated) and for users who have been authenticated and received a token. An identity pool is a store of user identity data specific to your account.
To create a new identity pool in the console

1. Sign in to the Amazon Cognito console, choose Manage Federated Identities, and then choose Create new identity pool.
2. Type a name for your identity pool.
3. To enable unauthenticated identities select Enable access to unauthenticated identities from the Unauthenticated identities collapsible section.
4. If desired, configure an authentication provider in the Authentication providers section.

Options A and B are incorrect since it's not the right approach to use IAM users or groups for access for mobile based applications
Option D is incorrect since SAML is used for federated access.
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 5 INCORRECT REFACTORING

An application needs to make use of a messaging system. The messages need to be processed in the order they are received and also no duplicates should be allowed. Which of the following would you use for this purpose?

- A. Enable FIFO on an existing SQS Standard Queue. ✖
- B. Add the .fifo extension to the Standard SQS Queue
- C. Consider using SNS
- D. Use the FIFO SQS Queues ✔

Explanation :

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

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

options A and B are incorrect since an existing Standard queue can't be changed to FIFO.
Q: Can I convert my existing standard queue to a FIFO queue?

No. You must choose the queue type when you create it. However, it is possible to move to a FIFO queue
Option C is incorrect since this is a notification service and not a queuing service
For more information on SQS FIFO Queues, please refer to the below URL

- https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/FIFO-queues.html (https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/FIFO-queues.html)

Ask our Experts

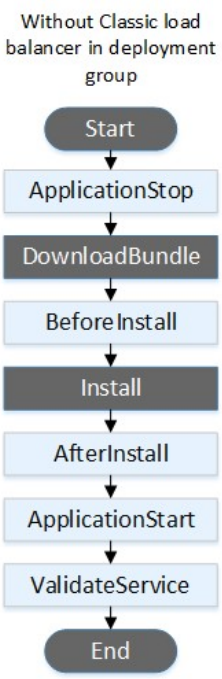
QUESTION 6 INCORRECT DEPLOYMENT

Which of the following is the right sequence of hooks that get called in AWS CodeDeploy?

- A. Application Stop->BeforeInstall->After Install->Application Start ✔
- B. BeforeInstall->After Install-> Application Stop-> Application Start
- C. BeforeInstall->After Install->Validate Service-> Application Start ✖
- D. BeforeInstall->Application Stop-> Validate Service-> Application Start

Explanation :

Answer - A
This is also mentioned in the AWS Documentation



Because of the order of events given in the AWS Documentation , all other options are invalid.

For more information on the hooks order , please refer to the below URL

- https://docs.aws.amazon.com/codedeploy/latest/userguide/reference-appspec-file-structure-hooks.html#reference-appspec-file-structure-hooks-run-order (https://docs.aws.amazon.com/codedeploy/latest/userguide/reference-appspec-file-structure-hooks.html#reference-appspec-file-structure-hooks-run-order)

Ask our Experts

QUESTION 7 CORRECT DEVELOPMENT WITH AWS SERVICES

As a developer you have created a Lambda function that is used to work with a bucket in Amazon S3. The Lambda function is not working as expected. You need to debug the issue and understand what's the underlying issue. How can you accomplish this?

- A. Use AWS Cloudwatch metrics
- B. Put logging statements in your code ✔
- C. Set the Lambda function debugging level to verbose
- D. Use AWS Cloudtrail logs

Explanation :

Answer – B
This is also mentioned in the AWS Documentation
You can insert logging statements into your code to help you validate that your code is working as expected. Lambda automatically integrates with Amazon CloudWatch Logs and pushes all logs from your code to a CloudWatch Logs group associated with a Lambda function (/aws/lambda/).
Option A is incorrect since the metrics will only give the rate at which the function is executing , but not help debug the actual error
Option C is incorrect since there is no such option
Option D is incorrect since this is only used for API monitoring
For more information on monitoring functions , please refer to the below URL

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

Ask our Experts

QUESTION 8 INCORRECT DEVELOPMENT WITH AWS SERVICES

You are developing a function that will be hosted in AWS Lambda. The function will be developed in .Net. There are a number of external libraries that are needed for the code to run. Which of the following is the best practise when it comes to working with external dependencies for AWS Lambda?

- A. Make sure that the dependencies are put in the root folder
- B. Selectively only include the libraries that are required ✔
- C. Make sure the libraries are installed in the beginning of the function
- D. Place the entire SDK dependencies in Amazon S3 ✖

Explanation :

Answer – B
This is also mentioned in the AWS Documentation
Minimize your deployment package size to its runtime necessities. This will reduce the amount of time that it takes for your deployment package to be downloaded and unpacked ahead of invocation. For functions authored in Java or .NET Core, avoid uploading the entire AWS SDK library as part of your deployment package. Instead, selectively depend on the modules which pick up components of the SDK you need
Option A is incorrect since dependencies don't need to be in the root folder
Option C is incorrect since they can run at runtime and don't need to be installed prior
Option D is incorrect since using the entire SDK sets is not advisable
For more information on best practises for AWS Lambda , 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 9 INCORRECT SECURITY

Your team has a Code Commit repository in your account. You need to give access to a set of developer's in another account access to your Code Commit repository. Which of the following is the most effective way to grant access?

- A. Create IAM users for each developer and provide access to the repository
- B. Create an IAM Group , add the IAM users and then provide access to the repository ✖
- C. Create a cross account role , give the role the privileges. Provide the role ARN to the developers. ✔
- D. Enable public access for the repository.

Explanation :

Answer – C
This is also mentioned in the AWS Documentation
Configure Cross-Account Access to an AWS CodeCommit Repository

You can configure access to AWS CodeCommit repositories for IAM users and groups in another AWS account. This is often referred to as cross-account access. This section provides examples and step-by-step instructions for configuring cross-account access for a repository named MySharedDemoRepo in the US East (Ohio) Region in an AWS account (referred to as AccountA) to IAM users who belong to an IAM group named DevelopersWithCrossAccountRepositoryAccess in another AWS account (referred to as AccountB).

All other options are incorrect because all of them are not recommended practises for giving access

For more information on an example for cross account role access , please refer to the below URL

- https://docs.aws.amazon.com/codecommit/latest/userguide/cross-account.html (https://docs.aws.amazon.com/codecommit/latest/userguide/cross-account.html)

Ask our Experts

QUESTION 10 INCORRECT MONITORING AND TROUBLESHOOTING

You have a lambda function that is processed asynchronously. You need a way to check and debug issues if the function fails? How could you accomplish this?

- A. Use AWS Cloudwatch metrics
- B. Assign a dead letter queue ✔
- C. Configure SNS notifications ✖
- D. Use AWS Cloudtrail logs

Explanation :

Answer – B
This is also mentioned in the AWS Documentation

Any Lambda function invoked asynchronously is retried twice before the event is discarded. If the retries fail and you're unsure why, use Dead Letter Queues (DLQ) to direct unprocessed events to an Amazon SQS (http://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/Welcome.html) queue or an Amazon SNS (https://docs.aws.amazon.com/lambda/latest/dg/lcome.html)topic to analyze the failure.

Option A is incorrect since the metrics will only give the rate at which the function is executing , but not help debug the actual error
Option C is incorrect since this will only provide notifications but not give the actual events which failed.
Option D is incorrect since this is only used for API monitoring

For more information on dead letter queues with AWS Lambda , please refer to the below URL

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

Ask our Experts

QUESTION 11 CORRECT DEVELOPMENT WITH AWS SERVICES

You are planning to use AWS Kinesis streams for an application being developed for a company. The company policy mandates that all data is encrypted at rest. How can you accomplish this in the easiest way possible for Kinesis streams?

- A. Use the SDK for Kinesis to encrypt the data before being stored at rest
- B. Enable server-side encryption for Kinesis streams ✔
- C. Enable client-side encryption for Kinesis streams
- D. Use the AWS CLI to encrypt the data

Explanation :

Answer – B
The easiest way is to use the in-built server-side encryption that is available with Kinesis streams
The AWS Documentation mentions the following
Server-side encryption is a feature in Amazon Kinesis Data Streams that automatically encrypts data before it's at rest by using an AWS KMS customer master key (CMK) you specify. Data is encrypted before it's written to the Kinesis stream storage layer, and decrypted after it's retrieved from storage. As a result, your data is encrypted at rest within the Kinesis Data Streams service. This allows you to meet strict regulatory requirements and enhance the security of your data.
Options A and C are invalid since this would involve too much of effort for encrypting and decrypting to the streams
Option D is invalid since this is the same as encrypting the data before it reaches the stream
For more information on server-side encryption with streams , please refer to the below URL

- https://docs.aws.amazon.com/streams/latest/dev/what-is-sse.html (https://docs.aws.amazon.com/streams/latest/dev/what-is-sse.html)

Ask our Experts

QUESTION 12 UNATTEMPTED DEVELOPMENT WITH AWS SERVICES

You are developing an application that is going to make use of Amazon Kinesis. Due to the high throughput , you decide to have multiple shards for the streams. Which of the following is TRUE when it comes to processing data across multiple shards?

- A. You cannot guarantee the order of data across multiple shards. Its possible only within a shard ✔
- B. Order of data is possible across all shards in a stream
- C. Order of data is not possible at all in Kinesis streams
- D. You need to use Kinesis firehose to guarantee the order of data

Explanation :

Answer – A

Kinesis Data Streams lets you order records and read and replay records in the same order to many Kinesis Data Streams applications. To enable write ordering, Kinesis Data Streams expects you to call the PutRecord API to write serially to a shard while using the ***sequenceNumberForOrdering*** parameter. Setting this parameter guarantees strictly increasing sequence numbers for puts from the same client and to the same partition key.

Option A is correct as it cannot guarantee the ordering of records across multiple shards.
Option B,C and D are incorrect because Kinesis Data Streams can order records on a single shard.
Each data record has a *sequence number* that is unique within its shard. Kinesis Data Streams assigns the sequence number after you write to the stream with ***putRecords*** or ***client.putRecord***.

For more information please refer:

- https://aws.amazon.com/blogs/database/how-to-perform-ordered-data-replication-between-applications-by-using-amazon-dynamodb-streams/ (https://aws.amazon.com/blogs/database/how-to-perform-ordered-data-replication-between-applications-by-using-amazon-dynamodb-streams/)
- https://docs.aws.amazon.com/streams/latest/dev/key-concepts.html (https://docs.aws.amazon.com/streams/latest/dev/key-concepts.html)

Ask our Experts

QUESTION 13 INCORRECT DEVELOPMENT WITH AWS SERVICES

A company is planning on developing an application that is going to make use of a DynamoDB table. The structure of the table is given below

Attribute Name	Type	Description
Product ID	Number	ID of product
Review ID	Number	Automatically generated GUID
Product Name	String	Name of the product
Product Description	String	Description of the product

Which of the following should be chosen as the partition key to ensure the MOST effective distribution of keys?

- A. Product ID ✖
- B. Review ID ✔
- C. Product Name
- D. Production Description

Explanation :

Answer – B
The most effective one will be the Review ID since you have a uniquely generated GUID for each record.
Option A is partially correct. It can be used as the partition key , but the question asks for the MOST effective distribution of keys and that would be the Review ID
Options C and D are incorrect since it would not be a best practise to keep these as the partition keys
For more information on 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 14 CORRECT REFACTORING

Your company is planning on using the Simple Storage service to host objects that will be accessed by users. There is a speculation that there would be roughly 6000 GET requests per second. Which of the following could be used to ensure optimal performance? Choose 2 answers from the options given below?

- [x] A. Use a Cloudfront distribution in front of the S3 bucket ✔
- [x] B. Use hash key prefixes for the object keys ✔
- [ ] C. Enable versioning for the objects
- [ ] D. Enable Cross Region Replication for the bucket

Explanation :

Answer – A and B
The AWS Documentation mentions the following on optimal performance for S3

Short Description

Amazon S3 maintains an index of object key names in each AWS Region. Object keys are stored in UTF-8 binary ordering across multiple partitions in the index. The key name determines which partition the key is stored in. Using a sequential prefix, such as a timestamp or an alphabetical sequence, increases the likelihood that Amazon S3 will target a specific partition for a large number of your keys, which can overwhelm the I/O capacity of the partition.

Resolution

If your workload is a mix of request types, introduce some randomness to key names by adding a hash string as a prefix to the key name. By introducing randomness to your key names, the I/O load is distributed across multiple index partitions. For example, you can compute an MD5 hash of the character sequence that you plan to assign as the key, and add three or four characters from the hash as a prefix to the key name. The following example shows key names with a four-character hexadecimal hash added as a prefix:

```
exampleawsbucket/232a-2019-14-03-15-00-00/cust1234234/photo1.jpg
exampleawsbucket/7b54-2019-14-03-15-00-00/cust3857422/photo2.jpg
exampleawsbucket/921c-2019-14-03-15-00-00/cust1248473/photo2.jpg
exampleawsbucket/ba65-2019-14-03-15-00-00/cust8474937/photo2.jpg
exampleawsbucket/8761-2019-14-03-15-00-00/cust1248473/photo3.jpg
exampleawsbucket/2e4f-2019-14-03-15-00-01/cust1248473/photo4.jpg
exampleawsbucket/9810-2019-14-03-15-00-01/cust1248473/photo5.jpg
exampleawsbucket/7e34-2019-14-03-15-00-01/cust1248473/photo6.jpg
exampleawsbucket/c34a-2019-14-03-15-00-01/cust1248473/photo7.jpg
...
```

Also you can use Cloudfront to give the objects to the user and cache them at the Edge locations , so that the requests on the bucket are reduced.

Option C is only used to prevent accidental deletion of objects
Option D is only used for disaster recovery scenarios
For more information on performance improvement , please refer to the below URL

https://aws.amazon.com/premiumsupport/knowledge-center/s3-bucket-performance-improve/
(https://aws.amazon.com/premiumsupport/knowledge-center/s3-bucket-performance-improve/)

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

For more details, please check below AWS Docs:
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 15 INCORRECT SECURITY

Your company currently stores its objects in S3. The current request rate is around 6000 GET requests per second. There is now a mandate for objects to be encrypted at rest. So you enable encryption using KMS. There are now performance issues being encountered. What could be the main reason behind this?

- A. Amazon S3 will now throttle the requests since they are now being encrypted using KMS ✖

- B. You need to also enable versioning to ensure optimal performance
- C. You are now exceeding the throttle limits for KMS API calls ✔
- D. You need to also enable CORS to ensure optimal performance

Explanation :

Answer – C
This is also mentioned in the AWS Documentation
You can make API requests directly or by using an integrated AWS service that makes API requests to AWS KMS on your behalf. The limit applies to both kinds of requests.
For example, you might store data in Amazon S3 using server-side encryption with AWS KMS (SSE-KMS). Each time you upload or download an S3 object that's encrypted with SSE-KMS, Amazon S3 makes a GenerateDataKey (for uploads) or Decrypt (for downloads) request to AWS KMS on your behalf. These requests count toward your limit, so AWS KMS throttles the requests if you exceed a combined total of 1200 uploads or downloads per second of S3 objects encrypted with SSE-KMS.
Option A is invalid since S3 will not throttle requests just because encryption is enabled.
Options B and D are invalid since these will not help increase performance
For more information on KMS limits improvement , please refer to the below URL

- https://docs.aws.amazon.com/kms/latest/developerguide/limits.html (https://docs.aws.amazon.com/kms/latest/developerguide/limits.html)

Ask our Experts

QUESTION 16 INCORRECT DEPLOYMENT

Your company is planning on using the Simple Storage service to host objects that will be accessed by users. There is a speculation that there would be roughly 6000 GET requests per second. Which of the following is the right way to use object keys for optimal performance?

- A. exampleawsbucket/2019-14-03-15-00-00/photo1.jpg
- B. exampleawsbucket/sample/232a-2019-14-03-15-00-00photo1.jpg
- C. exampleawsbucket/232a-2019-14-03-15-00-00/photo1.jpg ✔
- D. exampleawsbucket/sample/photo1.jpg ✖

Explanation :

Answer – C
The AWS Documentation mentions the following on optimal performance for S3

Short Description

Amazon S3 maintains an index of object key names in each AWS Region. Object keys are stored in UTF-8 binary ordering across multiple partitions in the index. The key name determines which partition the key is stored in. Using a sequential prefix, such as a timestamp or an alphabetical sequence, increases the likelihood that Amazon S3 will target a specific partition for a large number of your keys, which can overwhelm the I/O capacity of the partition.

Resolution

If your workload is a mix of request types, introduce some randomness to key names by adding a hash string as a prefix to the key name. By introducing randomness to your key names, the I/O load is distributed across multiple index partitions. For example, you can compute an MD5 hash of the character sequence that you plan to assign as the key, and add three or four characters from the hash as a prefix to the key name. The following example shows key names with a four-character hexadecimal hash added as a prefix:

```
exampleawsbucket/232a-2019-14-03-15-00-00/cust1234234/photo1.jpg
exampleawsbucket/7b54-2019-14-03-15-00-00/cust3857422/photo2.jpg
exampleawsbucket/921c-2019-14-03-15-00-00/cust1248473/photo2.jpg
exampleawsbucket/ba65-2019-14-03-15-00-00/cust8474937/photo2.jpg
exampleawsbucket/8761-2019-14-03-15-00-00/cust1248473/photo3.jpg
exampleawsbucket/2e4f-2019-14-03-15-00-01/cust1248473/photo4.jpg
exampleawsbucket/9810-2019-14-03-15-00-01/cust1248473/photo5.jpg
exampleawsbucket/7e34-2019-14-03-15-00-01/cust1248473/photo6.jpg
exampleawsbucket/c34a-2019-14-03-15-00-01/cust1248473/photo7.jpg
...
```

All other options are incorrect since they are not the right ways to store object keys for optimal performance
For more information on performance improvement , please refer to the below URL

- https://aws.amazon.com/premiumsupport/knowledge-center/s3-bucket-performance-improve/ (https://aws.amazon.com/premiumsupport/knowledge-center/s3-bucket-performance-improve/)

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

For more details, please check below AWS Docs:
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 17 CORRECT DEPLOYMENT

A company is planning on using DynamoDB as their data store. The tables in DynamoDB will be receiving millions of requests. Which of the following can be used to ensure the latency of requests to the DynamoDB table is kept at a minimal?

- A. Createa read replica of the DynamoDB table
- B. Enable Multi-AZ for the DynamoDB table
- C. Enable DynamoDB Accelerator ✔
- D. Enable Encryption for the DynamoDB table

Explanation :

Answer – C
The AWS Documentation mentions the following
Use Cases for DAX
DAX provides access to eventually consistent data from DynamoDB tables, with microsecond latency. A multi-AZ DAX cluster can serve millions of requests per second.

DAX is ideal for:
Applications that require the fastest possible response time for reads. Some examples include real-time bidding, social gaming, and trading applications. DAX delivers fast, in-memory read performance for these use cases.
Applications that read a small number of items more frequently than others. For example, consider an e-commerce system that has a one-day sale on a popular product. During the sale, demand for that product (and its data in DynamoDB) would sharply increase, compared to all of the other products. To mitigate the impacts of a "hot" key and a non-uniform data distribution, you could offload the read activity to a DAX cache until the one-day sale is over.

Applications that are read-intensive, but are also cost-sensitive. With DynamoDB, you provision the number of reads per second that your application requires. If read activity increases, you can increase your tables' provisioned read throughput (at an additional cost). Alternatively, you can offload the activity from your application to a DAX cluster, and reduce the amount of read capacity units you'd need to purchase otherwise.
Applications that require repeated reads against a large set of data. Such an application could potentially divert database resources from other applications. For example, a long-running analysis of regional weather data could temporarily consume all of the read capacity in a DynamoDB table, which would negatively impact other applications that need to access the same data. With DAX, the weather analysis could be performed against cached data instead.

Options A and B are incorrect since these are normally used for AWS RDS systems and not DynamoDB

Option D is incorrect since this will not help in increasing performance when you have numerous requests
For more information on DAX , please refer to the below URL

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

Ask our Experts

QUESTION 18 CORRECT DEVELOPMENT WITH AWS SERVICES

You've developed a Lambda function and are now in the process of debugging it. You add the necessary print statements in the code to assist in the debugging. You go to Cloudwatch logs , but you see no logs for the lambda function. Which of the following could be the underlying issue for this?

- A. You've not enabled versioning for the Lambda function
- B. The IAM Role assigned to the Lambda function does not have the necessary permission to create Logs ✔
- C. There is not enough memory assigned to the function
- D. There is not enough time assigned to the function

Explanation :

Answer – B
The AWS Documentation mentions the following
Note
"If your Lambda function code is executing, but you don't see any log data being generated after several minutes, this could mean your execution role for the Lambda function did not grant permissions to write log data to CloudWatch Logs. For information about how to make sure that you have set up the execution role correctly to grant these permissions, see Manage Permissions: Using an IAM Role (Execution Role)".

Option A is incorrect since versioning will not help in this case

Options C and D are incorrect since if these were the cases , then the function would not complete execution.
For more information on monitoring Lambda functions , please refer to the below URL

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

Ask our Experts

QUESTION 19 INCORRECT DEPLOYMENT

Your company has asked you to maintain an application using Elastic Beanstalk. They have mentioned that when updates are made to the application , that the infrastructure maintains its full capacity. Which of the following deployment methods should you use for this requirement?

- A. All at once
- B. Rolling ✖
- C. Immutable
- D. Rolling with additional batch ✔

Explanation :

Answer - D
The AWS Documentation mentions the following
"If you need to maintain full capacity during deployments, you can configure your environment to launch a new batch of instances prior to taking any instances out of service. This option is called a rolling deployment with an additional batch. When the deployment completes, Elastic Beanstalk terminates the additional batch of instances".

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

For more information on rolling version deployment in Elastic beanstalk , please refer to the below URL

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

Note:
"If the question says which method will deploy code ONLY to new instances". Then the answer would be Immutable deployment.

Ask our Experts

QUESTION 20 CORRECT DEPLOYMENT

Your company has asked you to maintain an application using Elastic Beanstalk. At times , you normally hit the application version limit when deploying new versions of the application. Which of the following is the most effective way to manage this issue?

- A. Create multiple environments and deploy the different versions to different environments
- B. Create an application lifecycle policy ✔
- C. Create multiple applications and deploy the different versions to different applications
- D. Delete the application versions manually

Explanation :

Answer – B
The AWS Documentation mentions the following

Each time you upload a new version of your application with the Elastic Beanstalk console or the EB CLI, Elastic Beanstalk creates an application version (https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/applications-versions.html). If you don't delete versions that you no longer use, you will eventually reach the application version limit (http://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html#limits_elastic_beanstalk) and be unable to create new versions of that application.
You can avoid hitting the limit by applying an *application version lifecycle policy* to your applications. A lifecycle policy tells Elastic Beanstalk to delete application versions that are old, or to delete application versions when the total number of versions for an application exceeds a specified number.
Options A and C are invalid because these are not the right approaches when managing deployment of application versions.
Option D even though possible , is not the most effective way.
For more information on application lifecycle , please refer to the below URL

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

Ask our Experts

QUESTION 21 CORRECT REFACTORING

A DynamoDB table is set with a Read Throughput capacity of 5 RCU. Which of the following read configuration will provide us the maximum number of read operations/sec?

- **A. Read capacity set to 5 for 4KB reads of data at strong consistency**
- **B. Read capacity set to 5 for 4KB reads of data at eventual consistency** ✔
- **C. Read capacity set to 15 for 1KB reads of data at strong consistency**
- **D. Read capacity set to 5 for 1KB reads of data at eventual consistency**

Explanation :

Answer – B
The calculation of throughput capacity for option B would be
Read capacity(5) * Amount of data(4) = 20.
Since its required at eventual consistency , we can double the read throughput to 20*2=40
For Option A
Read capacity(5) * Amount of data(4) = 20. Since we need strong consistency we have would get a read throughput of 20
For Option C
Read capacity(15) * Amount of data(1) = 15. Since we need strong consistency we have would get a read throughput of 15
For Option D
Read capacity(5) * Amount of data(1) = 5. Since we need eventual consistency we have would get a read throughput of 5*2=10
For more information on DynamoDB throughput , please refer to the below URL

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

Note:
One *read capacity unit* represents one strongly consistent read per second, or two eventually consistent reads per second, for an item up to 4 KB in size.
If you need to read an item that is larger than 4 KB, DynamoDB will need to consume additional read capacity units. The total number of read capacity units required depends on the item size, and whether you want an eventually consistent or strongly consistent read.

For example, with 5 read capacity units your application could:

- Perform strongly consistent reads of up to 20 KB per second (4 KB × 5 read capacity units).
- Perform eventually consistent reads of up to 40 KB per second (twice as much read throughput).

So with eventual consistency you can read up to 40KB/sec, hence the solution is B.

Ask our Experts

QUESTION 22 CORRECT DEVELOPMENT WITH AWS SERVICES

Your team is developing a solution that will make use of DynamoDB tables. Due to the nature of the application, the data is needed across a couple of regions across the world. Which of the following would help reduce the latency of requests to DynamoDB from different regions?

- A. Enable Multi-AZ for the DynamoDB table
- B. Enable global tables for DynamoDB ✔
- C. Enable Indexes for the table
- D. Increase the read and write throughput for the table

Explanation :

Answer - B
The AWS Documentation mentions the following
Amazon DynamoDB global tables provide a fully managed solution for deploying a multi-region, multi-master database, without having to build and maintain your own replication solution. When you create a global table, you specify the AWS regions where you want the table to be available. DynamoDB performs all of the necessary tasks to create identical tables in these regions, and propagate ongoing data changes to all of them.
For more information on Global tables , please refer to the below URL

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

Ask our Experts

QUESTION 23 INCORRECT DEVELOPMENT WITH AWS SERVICES

Your team is developing a solution that will make use of DynamoDB tables. Currently the application is designed to perform scan's on the entire table. Which of the following can be done to improve the performance of the application when it interacts with the DynamoDB table? Choose 2 answers from the options given below

- [x] A. Consider using parallel scans ✔
- [ ] B. Consider using large tables
- [x] C. Consider using string partition keys ✖
- [ ] D. Consider using queries ✔

Explanation :

Answer – A and D
The AWS Documentation mentions the following
Many applications can benefit from using parallel Scan operations rather than sequential scans. For example, an application that processes a large table of historical data can perform a parallel scan much faster than a sequential one. Multiple worker threads in a background "sweeper" process could scan a table at a low priority without affecting production traffic. In each of these examples, a parallel Scan is used in such a way that it does not starve other applications of provisioned throughput resources.
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
Option B is incorrect since having larger tables would just make the issue worse
Option C is incorrect since this would help in the issue.
For more information on scans and queries , 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 24 CORRECT

Your company has a large set of data sets that need to be streamed directly into Amazon S3. Which of the following would be perfect for such a requirement?

- A. Kinesis Streams
- B. Kinesis Data Firehose ✔
- C. AWS Redshift
- D. AWS DynamoDB

Explanation :

Answer – B
The AWS Documentation mentions the following
Amazon Kinesis Data Firehose is a fully managed service for delivering real-time streaming data (http://aws.amazon.com/streaming-data/) to destinations such as Amazon Simple Storage Service (Amazon S3), Amazon Redshift, Amazon Elasticsearch Service (Amazon ES), and Splunk.
Option A is partially valid , but since the stream of data needs to go directly into S3 , Firehose can be used instead of Kinesis streams
Option C is invalid because this is used as a petabyte warehouse system
Option D is invalid because this is an AWS fully managed NoSQL database.
For more information on Kinesis Firehose , please refer to the below URL

- https://docs.aws.amazon.com/firehose/latest/dev/what-is-this-service.html (https://docs.aws.amazon.com/firehose/latest/dev/what-is-this-service.html)

Ask our Experts

QUESTION 25 CORRECT DEVELOPMENT WITH AWS SERVICES

A company is planning on using Amazon Kinesis firehose to stream data into an S3 bucket. They need the data to be transformed first before it can be sent to the S3 bucket. Which of the following would be used for the transformation process?

- A. AWS SQS
- B. AWS Lambda ✔
- C. AWS EC2
- D. AWS API Gateway

Explanation :

Answer – B
The AWS Documentation mentions the following
Kinesis Data Firehose can invoke your Lambda function to transform incoming source data and deliver the transformed data to destinations. You can enable Kinesis Data Firehose data transformation when you create your delivery stream.
Because of what the AWS Documentation mentions , all other options are invalid
For more information on Kinesis Firehose , please refer to the below URL

- https://docs.aws.amazon.com/firehose/latest/dev/data-transformation.html (https://docs.aws.amazon.com/firehose/latest/dev/data-transformation.html)

Ask our Experts

QUESTION 26 INCORRECT DEPLOYMENT

Your company is hosting a static web site in S3. The code has recently been changed wherein Javascript calls are being made to the web pages in the same bucket via the FQDN. But the browser is blocking the requests. What should be done to alleviate the issue?

- A. Enable CORS on the bucket ✔
- B. Enable versioning on the bucket ✖
- C. Enable CRR on the bucket
- D. Enable encryption the bucket

Explanation :

Answer – A
Option B is incorrect because this is used to prevent accidental deletion of objects in S3
Option C is incorrect because this is used for Cross region replication of objects
Option D is incorrect because this is used to encrypt objects at rest

The AWS Documentation mentions the following
Cross-Origin Resource Sharing: Use-case Scenarios
The following are example scenarios for using CORS:

- Scenario 1: Suppose that you are hosting a website in an Amazon S3 bucket named website as described in Hosting a Static Website on Amazon S3. Your users load the website endpoint http://website.s3-website-us-east-1.amazonaws.com. Now you want to use JavaScript on the webpages that are stored in this bucket to be able to make authenticated GET and PUT requests against the same bucket by using the Amazon S3 API endpoint for the bucket, website.s3.amazonaws.com. A browser would normally block JavaScript from allowing those requests, but with CORS you can configure your bucket to explicitly enable cross-origin requests from website.s3-website-us-east-1.amazonaws.com.
- Scenario 2: Suppose that you want to host a web font from your S3 bucket. Again, browsers require a CORS check (also called a preflight check) for loading web fonts. You would configure the bucket that is hosting the web font to allow any origin to make these requests.

For more information on Cross Origin access , please refer to the below URL

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

Ask our Experts

QUESTION 27 CORRECT SECURITY

A company is storing sensitive data in their S3 bucket. The company policy states that all objects in the S3 bucket need to be encrypted at rest. Which of the following help ensure this policy is met?

- A. Deny permission to upload an object if the header does not includex-amz-server-side-encryption ✔
- B. Deny permission to upload an object if the header includesx-amz-server-side-encryption
- C. Deny permission to upload an object if the header does not includex-allow-encryption
- D. Deny permission to upload an object if the header includes x-allow-encryption

Explanation :

Answer - A

This is also given in the AWS Documentation

If you need server-side encryption for all of the objects that are stored in a bucket, use a bucket policy. For example, the following bucket policy denies permissions to upload an object unless the request includes the `x-amz-server-side-encryption` header to request server-side encryption:

```
{
  "Version": "2012-10-17",
  "Id": "PutObjPolicy",
  "Statement": [
    {
      "Sid": "DenyIncorrectEncryptionHeader",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::YourBucket/*",
      "Condition": {
        "StringNotEquals": {
          "s3:x-amz-server-side-encryption": "AES256"
        }
      }
    },
    {
      "Sid": "DenyUnEncryptedObjectUploads",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::YourBucket/*",
      "Condition": {
        "Null": {
          "s3:x-amz-server-side-encryption": "true"
        }
      }
    }
  ]
}
```

Since the documentation clearly mentions what is the requirement for encryption to upload objects , all other options are invalid.

For more information on Server-Side Encryption , please refer to the below URL

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

Ask our Experts

QUESTION 28 CORRECT

As a developer , you have enabled server logging on an S3 bucket. You have a simple static web page with CSS pages uploaded to the bucket which is 1 MB in total size. After a duration of 2 weeks , you come back and see that the size of the bucket has increased to 50MB. Which of the following could be a reason for this?

- A. You have enabled CRR on the bucket as well , that is why the space is being consumed
- B. You have enabled Encryption on the bucket as well , that is why the space is being consumed
- C. This is the normal behaviour since the logs are being delivered to the same bucket ✔
- D. Monitoring has been enabled for the bucket

Explanation :

Answer – C

An S3 bucket with server access logging enabled can accumulate many server log objects over time. Your application might need these access logs for a specific period after creation, and after that, you might want to delete them. You can use Amazon S3 lifecycle configuration to set rules so that Amazon S3 automatically queues these objects for deletion at the end of their life.

The correct answer is C. This is normal behaviour since the logs are being delivered to the same bucket.

For more information on deleting logs files , please refer to the below URL

- https://docs.aws.amazon.com/AmazonS3/latest/dev/deleting-log-files-lifecycle.html (https://docs.aws.amazon.com/AmazonS3/latest/dev/deleting-log-files-lifecycle.html)

Ask our Experts

QUESTION 29 CORRECT DEVELOPMENT WITH AWS SERVICES

Your application is developed to pick up metrics from several servers and push them off to Cloudwatch. At times , the application gets client 429 errors. Which of the following can be done from the programming side to resolve such errors?

- A. Use the AWS CLI instead of the SDK to push the metrics
- B. Ensure that all metrics have a timestamp before sending them across
- C. Use exponential backoff in your requests ✔
- D. Enable encryption for the requests

Explanation :

Answer – C
The main reason for such errors is that throttling is occurring when many requests are sent via API calls. The best way to mitigate this is to stagger the rate at which you make the API calls.
This is also given in the AWS Documentation
In addition to simple retries, each AWS SDK implements exponential backoff algorithm for better flow control. The idea behind exponential backoff is to use progressively longer waits between retries for consecutive error responses. You should implement a maximum delay interval, as well as a maximum number of retries. The maximum delay interval and maximum number of retries are not necessarily fixed values and should be set based on the operation being performed, as well as other local factors, such as network latency.
Option A is invalid , because this accounts to the same thing. It's basically the number of requests that is the issue.
Option B is invalid because anyway you have to add the timestamps when sending the requests
Option D is invalid because this would not help in the issue
For more information on API retries , please refer to the below URL

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

Ask our Experts

QUESTION 30 CORRECT

A company currently allows access to their API's to customers via the API gateway. Currently all clients have a 6-month period to move from using the older API's to newer versions of the API's. The code for the API is hosted in AWS Lambda. Which of the following is the ideal strategy to employ in such a situation?

- A. Create another AWS Lambda version and give the link to that version to the customers.
- B. Create another AWS Lambda ALIAS and give the link to that version to the customers.
- C. Create another stage in the API gateway ✔
- D. Create a deployment package that would automatically change the link to the new Lambda version

Explanation :

Answer – C
The best way is to create a separate stage in the API gateway as maybe 'v2' and then customers could use both API versions. They can still slowly change their usage onto the new version in this duration.
Below is the concept of the API stage in the AWS Documentation

API stage
"A logical reference to a lifecycle state of your API (for example, 'dev', 'prod', 'beta', 'v2'). API stages are identified by API ID and stage name".

Options A and B are incorrect since access needs to be provided via the gateway
Option D is incorrect since you need to keep both versions running side by side
For more information on the API gateway , please refer to the below URL

- https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-basic-concept.html (https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-basic-concept.html)

Ask our Experts

QUESTION 31 CORRECT SECURITY

Your company is developing an application that will primarily be used by users on their mobile devices. The users need to have the ability to authenticate themselves via identity providers such as Facebook. Which of the following service should be used for user management?

- A. AWS STS with IAM
- B. AWS Cognito ✔
- C. AWS SAML
- D. AWS Federation

Explanation :

Answer – B
This is also given in the AWS Documentation
Amazon Cognito provides authentication, authorization, and user management for your web and mobile apps. Your users can sign in directly with a user name and password, or through a third party such as Facebook, Amazon, or Google.
All other options are invalid since you need to use AWS Cognito which offers integration with external identity providers
For more information on AWS Cognito , please refer to the below URL

- https://docs.aws.amazon.com/cognito/latest/developerguide/what-is-amazon-cognito.html (https://docs.aws.amazon.com/cognito/latest/developerguide/what-is-amazon-cognito.html)

Ask our Experts

QUESTION 32 INCORRECT DEPLOYMENT

A company has a cloudformation template that is used to create a huge list of resources. It creates a VPC, subnets , EC2 Instances , Autoscaling Groups , Load Balancers etc. Which of the following should be considered when designing such Cloudformation templates?

- A. Ensure to create one entire stack from the template
- B. Look towards breaking the templates into smaller manageable templates ✔
- C. Package the templates together and use the cloudformation deploy command
- D. Package the templates together and use the cloudformation package command ✖

Explanation :

Answer - B
This recommendation is also given in the AWS Documentation

As your infrastructure grows, common patterns can emerge in which you declare the same components in each of your templates. You can separate out these common components and create dedicated templates for them. That way, you can mix and match different templates but use nested stacks to create a single, unified stack. Nested stacks are stacks that create other stacks. To create nested stacks, use the AWS::CloudFormation::Stack (https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-properties-stack.html) resource in your template to reference other templates.
Option A is incorrect since this is not the recommended design practise.
Options C and D are incorrect because these are used for packaging and deployment and not for the design stages
For more information on best practises for Cloudformation , please refer to the below URL

- https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/best-practices.html (https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/best-practices.html)

Ask our Experts

QUESTION 33 CORRECT DEPLOYMENT

You have the following YAML file given to you which is required to deploy a Lambda function using serverless deployment.

```
AWSTemplateFormatVersion: '2010-09-09'
Transform: AWS::Serverless-2016-10-31
Resources:
 TestFunction:
  Type: AWS::Serverless::Function
  Properties:
   Handler: index.handler
   Runtime: nodejs6.10
   Environment:
    Variables:
     S3_BUCKET: demobucket
```

Which of the following is required to ensure the deployment can take place?

- A. Use the cloudformation package command to package the deployment
- B. Use the cloudformation package command to deploy the template
- C. Place the function code at the root level of the working directory along with the YAML file ✔
- D. Place the function code in the .eb extensions folder

Explanation :

Answer – C
The above snippet is used to create a serverless application that is deployed using the serverless deployment language. You need to ensure that the Lambda function is present as part of the deployment package
Options A and B are incorrect since these are not cloudformation specific templates
Option D is incorrect since this is normally used for Elastic beanstalk deployments
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 34 CORRECT DEVELOPMENT WITH AWS SERVICES

Your developing a common lambda function that will be used across several environments such as staging , development etc. The lambda function needs to interact with a database in each of these environments. What is the best way to develop the Lambda function?

- A. Create a Lambda function for each environment so that each function can point to its respective database
- B. Create one Lambda function and use environment variables for each database connection(s) ✔
- C. Create one Lambda function and create several versions for each database
- D. Create one Lambda function and create several ALIAS for each database

Explanation :

Answer – B
This is also mentioned in the AWS Documentation
Environment variables for Lambda functions enable you to dynamically pass settings to your function code and libraries, without making changes to your code. Environment variables are key-value pairs that you create and modify as part of your function configuration, using either the AWS Lambda Console, the AWS Lambda CLI or the AWS Lambda SDK. AWS Lambda then makes these key value pairs available to your Lambda function code using standard APIs supported by the language, like process.env for Node.js functions.
Option A is incorrect since this would result in unnecessary code functions and more maintenance requirement for the functions
Options C and D are incorrect since these are not the right way to design the functions for this use case
For more information on Lambda environment variables , please refer to the below URL

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

Ask our Experts

QUESTION 35 CORRECT DEVELOPMENT WITH AWS SERVICES

As a developer you have been told to create an API gateway stage that will directly interact with DynamoDB tables. Which of the following feature of the API Gateway must be used to fulfill this requirement?

- A. Ensure to create an Integration request ✔
- B. Ensure to enable CORS
- C. Ensure to enable DAX
- D. Enable Binary payloads

Explanation :

Answer – A
This is also mentioned in the AWS Documentation
For example, with DynamoDB as the backend, the API developer sets up the integration request to forward the incoming method request to the chosen backend. The setup includes specifications of an appropriate DynamoDB action, required IAM role and policies, and required input data transformation. The backend returns the result to API Gateway as an integration response. To route the integration response to an appropriate method response (of a given HTTP status code) to the client, you can configure the integration response to map required response parameters from integration to method
Option B is incorrect since this is only required for cross domain requests.
Option C is incorrect since this is only required for low latency to DynamoDB tables
Option D is incorrect since this is only required is the request is not a text-based request
For more information on the developer experience for the API gateway , please refer to the below URL

- https://docs.aws.amazon.com/apigateway/latest/developerguide/welcome.html#api-gateway-overview-developer-experience (https://docs.aws.amazon.com/apigateway/latest/developerguide/welcome.html#api-gateway-overview-developer-experience)

Ask our Experts

QUESTION 36 CORRECT DEPLOYMENT

You have recently developed an AWS Lambda function to be used as a backend technology for an API gateway instance. You need to give the API gateway URL to a set of users for testing. What must be done before the users can test the API?

- A. Ensure that a deployment is created in the API gateway ✔
- B. Ensure that CORS is enabled for the API gateway
- C. Generate the SDK for the API
- D. Enable support for binary payloads

Explanation :

Answer – A
This is also mentioned in the AWS Documentation
In API Gateway, a deployment is represented by a Deployment (http://docs.aws.amazon.com/apigateway/api-reference/resource/deployment/) resource. It is like an executable of an API represented by a RestApi (http://docs.aws.amazon.com/apigateway/api-reference/resource/rest-api/) resource. For the client to call your API, you must create a deployment and associate a stage to it. A stage is represented by a Stage (http://docs.aws.amazon.com/apigateway/api-reference/resource/stage/) resource and represents a snapshot of the API, including methods, integrations, models, mapping templates, Lambda authorizers (formerly known as custom authorizers), etc
Option B is incorrect since this is only required for cross domain requests.
Option C is incorrect since this is only required when you want to use your code to call the API gateway and there is no mention of that requirement in the question
Option D is incorrect since this is only required is the request is not a text-based request and there is no mention of the type of payload in the question
For more information on setting up deployments , please refer to the below URL

- https://docs.aws.amazon.com/apigateway/latest/developerguide/set-up-deployments.html (https://docs.aws.amazon.com/apigateway/latest/developerguide/set-up-deployments.html)

Ask our Experts

QUESTION 37 CORRECT REFACTORING

You just developed code in AWS Lambda that makes use of recursive functions. After several invocations, you are beginning to see throttling errors in the metrics. Which of the following should be done to resolve this issue?

- A. Place the recursive function in a separate package
- B. Use versioning for the recursive function
- C. Avoid using recursive code altogether ✔
- D. Use the API gateway to call the recursive code.

Explanation :

Answer - C
This is also clearly mentioned in the AWS Documentation

- **Avoid using recursive code** in your Lambda function, wherein the function automatically calls itself until some arbitrary criteria is met. This could lead to unintended volume of function invocations and escalated costs. If you do accidentally do so, set the function concurrent execution limit to 0 immediately to throttle all invocations to the function, while you update the code..

Because of the recommendations that is mentioned in the AWS Documentation , all other options are incorrect.
For more information on the best practises for AWS Lambda , 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 38 CORRECT

An application is making a request to AWS STS for temporary access credentials. Below is the response being received

AQoDYXdzEPT//////////wEXAMPLEtc764bNrC9SAPBSM22wDOk4x4HIZ8j4FZTwdQW
LWsKWHGBuFqwAeMicRXmxfpSPfIeoIYRqTflfKD8YUuwthAx7mSEI/qkPpKPi/kMcGd
QrmGdeehM4IC1NtBmUpp2wUE8phUZampKsburEDy0KPkyQDYwT7WZ0wq5VSXDvp75YU
9HFvlRd8Tx6q6fE8YQcHNVXAkiY9q6d+xo0rKwT38xVqr7ZD0u0iPPkUL64lIZbqBAz
+scqKmlzm8FDrypNC9Yjc8fPOLn9FX9KSYvKTr4rvx3iSIlTJabIQwj2ICCR/oLxBA==

wJalrXUtnFEMI/K7MDENG/bPxRfiCYzEXAMPLEKEY

2011-07-15T23:28:33.359Z
AKIAIOSFODNN7EXAMPLE

arn:aws:sts::123456789012:assumed-role/demo/lambda
ARO123EXAMPLE123:lambda

6

c6104cbe-af31-11e0-8154-cbc7ccf896c7

Which of the following is TRUE with regards to the above response?

- A. The SecretAccessKey can be used like Access keys to make request to resources
- B. The user will assume the role of arn:aws:sts::123456789012:assumed-role/demo/lambda ✔
- C. The session token will be valid for the lifetime of the application
- D. The Request ID can be used to make requests to access other AWS resources

Explanation :

Answer – B
Some of the aspects that get incorporated in the call to STS are

- The Amazon Resource Name (ARN) of the role that the app should assume.
- The duration, which specifies the duration of the temporary security credentials.
- A role session name, which is a string value that you can use to identify the session. This value can be captured and logged by CloudTrail to help you distinguish between your role users during an audit.

Options A and D are invalid because you need the session token to make requests to access other AWS resources
Option C is invalid because these tokens are short lived tokens
For more information on temporary access credentials , please refer to the below URL

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

Ask our Experts

QUESTION 39 CORRECT DEPLOYMENT

You have an application that is hosted on an EC2 Instance. This application is part of a custom domain www.demo.com (http://www.demo.com). The application has been changed to make calls to the API gateway. But the browser is not rendering the responses and Javascript errors are being seen in the developer console. What must be done to ensure that this issue can be resolved.

- A. Make the application call a Lambda function instead.
- B. There is an issue with the stage defined on the API gateway, hence define a new stage
- C. Make use of Cognito user pools
- D. Enable CORS for the API gateway ✔

Explanation :

Answer – D
This is given in the AWS Documentation
When your API's resources receive requests from a domain other than the API's own domain, you must enable cross-origin resource sharing (CORS) for selected methods on the resource. This amounts to having your API respond to the OPTIONS preflight request with at least the following CORS-required response headers:

- Access-Control-Allow-Methods
- Access-Control-Allow-Headers
- Access-Control-Allow-Origin

Option A is invalid because you should not make the architecture change , since this is not the underlying issue.
Option B is invalid because this is the problem with CORS and not the stage itself
Option C is invalid because using Cognito user pools would just add one more unnecessary layer of authentication which is not part of the question requirement.

For more information on CORS for API gateway , please refer to the below URL

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

Ask our Experts

QUESTION 40 CORRECT REFACTORING

You've define a DynamoDB table with a read capacity of 5 and a write capacity of 5. Which of the following statements are TRUE? Choose 3 answers from the options given below

- [x] **A. Strong consistent reads of a maximum of 20 KB per second** ✔
- [ ] **B. Eventual consistent reads of a maximum of 20 KB per second**
- [ ] **C. Strong consistent reads of a maximum of 40 KB per second**
- [x] **D. Eventual consistent reads of a maximum of 40 KB per second** ✔
- [x] **E. Maximum writes of 5KB per second** ✔

Explanation :

Answer – A,D and E
This is also given in the AWS Documentation
For example, suppose that you create a table with 5 read capacity units and 5 write capacity units. With these settings, your application could:

- Perform strongly consistent reads of up to 20 KB per second (4 KB × 5 read capacity units).
- Perform eventually consistent reads of up to 40 KB per second (twice as much read throughput).
- Write up to 5 KB per second (1 KB × 5 write capacity units).

Based on the documentation , all other options are incorrect
For more information on provisioned throughput , please refer to the below URL

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

Ask our Experts

QUESTION 41 CORRECT DEVELOPMENT WITH AWS SERVICES

An application is currently in production that makes calls to an AWS RDS Instance. The application consists of a reporting module and a transactional system. Due high load times , the response time for the application used to get very high. This was being attributed to the number of queries being fired against the database system. Which of the following can be used to resolve the response time for the application?

- ○ **A. Place a cloudfront distribution in front of the database**
- ◉ **B. Enable Read Replica's for the database** ✔
- ○ **C. Move the database to DynamoDB**
- ○ **D. Enable Multi-AZ for the database**

Explanation :

Answer – B

The AWS Documentation mentions the following
You can reduce the load on your source DB instance by routing read queries from your applications to the read replica. Read replicas allow you to elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads.
Option A is incorrect since normally cloudfront distribution are placed in front of the front tier of the application
Option C is incorrect since changing the entire architecture is not the ideal approach
Option D is incorrect since this is used for fault tolerant scenarios for the database
For more information on Read Replica's , please refer to the below URL

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

Ask our Experts

QUESTION 42 CORRECT DEVELOPMENT WITH AWS SERVICES

An application is currently in production that makes calls to an AWS RDS Instance. The database has recently been facing performance problems. It has been noticed that the same queries are putting a strain on the database. Which of the following can be used to resolve the issue?

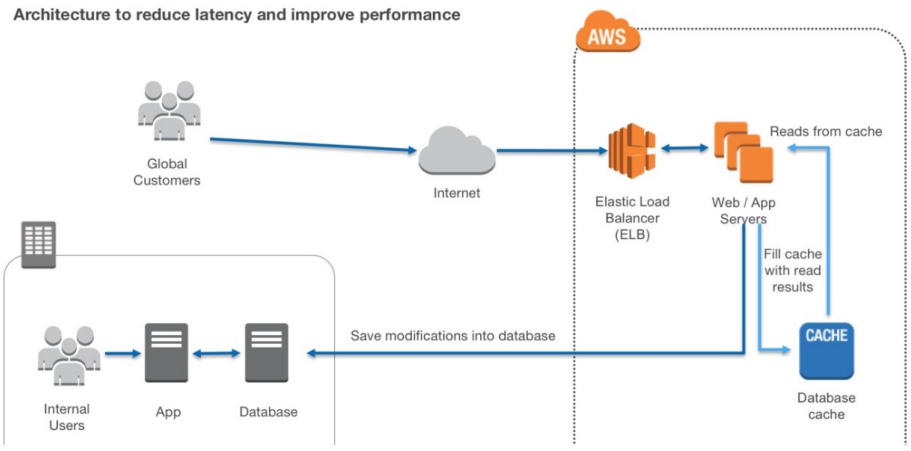
- A. Placea cloudfront distribution in front of the database
- B. EnableMulti-AZ for the database
- C. Placean SQS queue in front of the database
- D. Placean ElastiCache in front of the database ✔

Explanation :

Answer – D
The AWS Documentation mentions the following
Proposed solution: an in-memory cache based on Amazon ElastiCache
Because the issue involves latency to the backend database, we propose an in-memory cache based on Amazon ElastiCache to reduce network latency and to offload the database pressure. This solution dramatically reduces the data retrieval latency. It also scales request volume considerably, because Amazon ElastiCache can deliver extremely high request rates, measured at over 20 million per second.
The following diagram shows the proposed architecture.

Proposed solution: an in-memory cache based on Amazon ElastiCache

Because the issue involves latency to the backend database, we propose an in-memory cache based on Amazon ElastiCache to reduce network latency and to offload the database pressure. This solution dramatically reduces the data retrieval latency. It also scales request volume considerably, because Amazon ElastiCache can deliver extremely high request rates, measured at over 20 million per second. The following diagram shows the proposed architecture.



Option A is incorrect since normally cloudfront distribution are placed in front of the front tier of the application
Option B is incorrect since this is used for fault tolerant scenarios for the database
Option C is incorrect since this is used for queuing of messages
For more information on reducing latency's for hybrid architectures , please refer to the below URL

- https://aws.amazon.com/blogs/database/latency-reduction-of-hybrid-architectures-with-amazon-elasticache/ (https://aws.amazon.com/blogs/database/latency-reduction-of-hybrid-architectures-with-amazon-elasticache/)

Ask our Experts

QUESTION 43 CORRECT SECURITY

A company is planning on using a cache service for their application. An important requirement is that trying to recover data lost in cache is an expensive affair for the company , which they would want to avoid. Which of the following should be used for this purpose?

- A. Amazon SQS queues
- B. Amazon ElastiCache – Memcached
- C. Amazon ElastiCache – Redis ✔
- D. Amazon Lambda

Explanation :

Answer – C
Choose Redis if you want high availability. The below table gives the comparison

	Memcached	Redis (cluster mode disabled)	Redis (cluster mode enabled)
Engine versions	1.4.x	2.8.x and 3.2.x	3.2.x
Data types	Simple ‡	2.8.x - Complex *	Complex †
		3.2.x - Complex †	
Data partitioning	Yes	No	Yes
Cluster is modifiable	Yes	Yes	No
Online resharding	No	No	3.2.10
Encryption	No	3.2.6	3.2.6
HIPAA Compliance	No	3.2.6	3.2.6
Multi-threaded	Yes	No	No
Node type upgrade	No	Yes	No
Engine upgrading	Yes	Yes	No
High availability (replication)	No	Yes	Yes
Automatic failover	No	Optional	Required
Pub/Sub capabilities	No	Yes	Yes

Option A is incorrect since this is a queuing service available from AWS
Option B is incorrect since this does not offer high availability
Option D is incorrect since this is a serverless computing service available from AWS
For more information on the comparison for the Cache engines , please refer to the below URL

- https://docs.aws.amazon.com/AmazonElastiCache/latest/mem-ug/SelectEngine.html (https://docs.aws.amazon.com/AmazonElastiCache/latest/mem-ug/SelectEngine.html)

Ask our Experts

QUESTION 44 CORRECT DEPLOYMENT

You have docker containers which are going to be deployed in the AWS Elastic Container Service. You need to ensure that instances of containers cannot access each other since these different instances are going to be used by individual customers. How can you accomplish this?

- A. Place IAM Roles for the underlying EC2 Instances
- B. Place the access keys in the Docker containers
- C. Place the access keys in the EC2 Instances
- D. Configure the Security Groups of the instances to allow only required traffic. ✔

Explanation :

Answer – D
Q: How does Amazon ECS isolate containers belonging to different customers?
Amazon ECS schedules containers for execution on customer-controlled Amazon EC2 instances or with AWS Fargate and builds on the same isolation controls and compliance that are available for EC2 customers. Your compute instances are located in a Virtual Private Cloud (VPC) with an IP range that you specify. You decide which instances are exposed to the Internet and which remain private.
Your EC2 instances use an IAM role to access the ECS service.

- Your ECS tasks use an IAM role to access services and resources.
- Security Groups and networks ACLs allow you to control inbound and outbound network access to and from your instances.
- You can connect your existing IT infrastructure to resources in your VPC using industry-standard encrypted IPsec VPN connections.
- You can provision your EC2 resources as Dedicated Instances. Dedicated Instances are Amazon EC2 Instances that run on hardware dedicated to a single customer for additional isolation.

For more information, please check below AWS Docs:

- https://aws.amazon.com/ecs/faqs/ (https://aws.amazon.com/ecs/faqs/)

Option A is incorrect since the Roles need to be assigned on the task level
Options B and C are incorrect since access keys is not the ideal security practise.
For more information on Task IAM Roles , 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 SECURITY

An application needs to use an authentication in AWS. Users need to have MFA enabled when trying to log into the application. Which of the following can be used for this purpose?

- A. Create an IAM user with public access
- B. Create an IAM group with public access
- C. Use AWS Cognito with MFA ✔
- D. Use AWS STS with SAML

Explanation :

Answer – C
This is mentioned in the AWS Documentation
Adding Multi-Factor Authentication (MFA) to a User Pool

Multi-factor authentication (MFA) increases security for your app by adding another authentication method, and not relying solely on user name and password. You can choose to use SMS text messages, or time-based one-time (TOTP) passwords as second factors in signing in your users.
With adaptive authentication, you can configure your user pool to require second factor authentication in response to an increased risk level. To add adaptive authentication to your user pool, see Adding Advanced Security to a User Pool.
Options A and B are incorrect since it's not the right approach to use IAM users or groups for access for mobile based applications
Option D is incorrect since SAML is used for federated access.
For more information on Cognito with MFA , please refer to the below URL

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

Ask our Experts

QUESTION 46 CORRECT REFACTORING

When calling an API operation on an EC2 Instance , the following error message was returned

A client error (UnauthorizedOperation) occurred when calling the RunInstances operation:

You are not authorized to perform this operation. Encoded authorization failure message:

oGsbAaIV7wlfj8zUqebHUANHzFbmkzILlxyj__y9xwhIHk99U_cUq1FIeZnskWDjQ1wSHStVfdCEyZILGoccGpCiCIhORceWF9 Jvowq6mNim0

Which of the following can be used to get a human readable error message?

- A. Use the command aws sts decode-authorization-message ✔
- B. Use the command aws get authorization-message
- C. Use the IAM Policy simulator , enter the error message to get the human readble format
- D. Use the command aws set authorization-message

Explanation :

Answer – A
This is mentioned in the AWS Documentation
Decodes additional information about the authorization status of a request from an encoded message returned in response to an AWS request.
For example, if a user is not authorized to perform an action that he or she has requested, the request returns a Client.UnauthorizedOperation response (an HTTP 403 response). Some AWS actions additionally return an encoded message that can provide details about this authorization failure
Because of the right command used in the documentation, all other options are incorrect
For more information on the command , please refer to the below URL

- https://docs.aws.amazon.com/cli/latest/reference/sts/decode-authorization-message.html (https://docs.aws.amazon.com/cli/latest/reference/sts/decode-authorization-message.html)

Ask our Experts

QUESTION 47 INCORRECT SECURITY

You have defined some custom policies in AWS. You need to test out the permissions assigned to those policies.

Which of the following can be used for this purpose via the CLI? Choose 2 answers from the options given below

- [ ] **A. Get the context keys first** ✔
- [x] **B. Use the aws iam simulate-custom-policy command** ✔
- [x] **C. Get the AWS IAM Access keys first** ✖
- [ ] **D. Use the aws iam get-custom-policy command**

Explanation :

Answer – A and B
This is mentioned in the AWS Documentation
Policy simulator commands typically require calling API operations to do two things:

1. Evaluate the policies and return the list of context keys that they reference. You need to know what context keys are referenced so that you can supply values for them in the next step.
2. Simulate the policies, providing a list of actions, resources, and context keys that are used during the simulation.

Because of the right command used in the documentation, all other options are incorrect
For more information on policy simulation , please refer to the below URL

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

Ask our Experts

QUESTION 48 INCORRECT DEPLOYMENT

You have been instructed to use the CodePipeline service for the CI/CD automation in your company. Due to security reasons , the resources that would be part of the deployment are placed in another account. Which of the following steps need to be carried out to accomplish this deployment? Choose 2 answers from the options given below

- [ ] **A. Define a customer master key in KMS** ✔
- [ ] **B. Create a reference Code Pipeline instance in the other account**
- [x] **C. Add a cross account role** ✔
- [x] **D. Embed the access keys in the codepipeline process** ✖

Explanation :

Answer – A and C
Option B is invalid since this would go against the security policy
Option D is invalid since this is not a recommended security practice.
This is mentioned in the AWS Documentation
You might want to create a pipeline that uses resources created or managed by another AWS account. For example, you might want to use one account for your pipeline and another for your AWS CodeDeploy resources. To do so, you must create a AWS Key Management Service (AWS KMS) key to use, add the key to the pipeline, and set up account policies and roles to enable cross-account access.
For more information on pipelines used to access resources in another account , please refer to the below URL

- https://docs.aws.amazon.com/codepipeline/latest/userguide/pipelines-create-cross-account.html (https://docs.aws.amazon.com/codepipeline/latest/userguide/pipelines-create-cross-account.html)

Ask our Experts

QUESTION 49 CORRECT DEPLOYMENT

You have deployed an application an EC2 Instance. This application makes calls to a DynamoDB service. There are numerous performance issues present in the application. You decide to use the XRay service to debug the performance issues. You are not able to see the trails in the XRay service. Which of the following could be the underlying issue? Choose 2 answers from the options given below

- [x] **A. The X-Ray daemon is not installed on the EC2 Instance** ✔
- [ ] **B. The right AMI is not chosen for the EC2 Instance**
- [x] **C. Ensure that the IAM Role attached to the Instance has permission to upload data ontoX-Ray** ✔
- [ ] **D. Ensure that the IAM Role attached to the Instance has permission to upload data onto Cloudwatch**

Explanation :

Answer – A and C
You need to have the daemon service running on the EC2 Instance. And a role needs to be attached to the EC2 Instance
Running the X-Ray Daemon on Amazon EC2
You can run the X-Ray daemon on the following operating systems on Amazon EC2:

- Amazon Linux
- Ubuntu
- Windows Server (2012 R2 and newer)

Use an instance profile to grant the daemon permission to upload trace data to X-Ray. For more information, see Giving the Daemon Permission to Send Data to X-Ray.
Option B is incorrect since the agent can be installed on different types of instances
Option D is incorrect since the traces need to be sent to the X-Ray service
For more information on the X-Ray daemon service , please refer to the below URL

- https://docs.aws.amazon.com/xray/latest/devguide/xray-daemon-ec2.html (https://docs.aws.amazon.com/xray/latest/devguide/xray-daemon-ec2.html)

Ask our Experts

QUESTION 50 INCORRECT MONITORING AND TROUBLESHOOTING

Your company is hosting a set of resources on the AWS Cloud. There is now a security requirement that states that all requests to the STS service be monitored. How can you accomplish this requirement?

- ○ **A. Monitor the Cloudwatch logs service**
- ○ **B. Create a CloudTrail** ✔
- ○ **C. Use the STS logging service** ✖
- ○ **D. Use Cloudwatch metrics**

Explanation :

Answer – B
The AWS Documentation mentions the following
CloudTrail logs all authenticated API requests (made with credentials) to IAM and AWS STS APIs, with the exception of DecodeAuthorizationMessage. CloudTrail also logs nonauthenticated requests to the AWS STS actions, AssumeRoleWithSAML and AssumeRoleWithWebIdentity and logs information provided by the identity provider. You can use this information to map calls made by a federated user with an assumed role back to the originating external federated caller.
Option A is incorrect since the log service will not have the trail of the API calls
Option C is incorrect since STS does not have the logging service
Option D is incorrect since Cloudwatch metrics will not have the trail of the API calls
For more information on cloudtrail integrations , please refer to the below URL

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

Ask our Experts

QUESTION 51 CORRECT DEVELOPMENT WITH AWS SERVICES

Your team has developed an application that makes use of AWS resources. In order to provide frequent releases to the customer, you are required to automate the CI/CD process. Which of the following can be used for this purpose?

- A. Create a Pipeline using AWS CodePipeline. Configure a stage for Unit testing as wellin the Pipeline.
- B. Use AWS CodeCommit to host your code repository. Use the build tool in AWS CodeCommit to build your pipeline
- C. Create a Pipeline in the AWS CodeBuild Service
- D. Create a Pipeline in the AWS CodeStar service ✔

Explanation :

Answer – D

Automated continuous delivery pipeline
AWS CodeStar accelerates software release with the help of AWS CodePipeline (https://aws.amazon.com/codepipeline/details/), a continuous integration and continuous delivery (CI/CD) service. Each project comes pre-configured with an automated pipeline that continuously builds, tests, and deploys your code with each commit.

Task	Available approaches	Approaches described in this topic
Create a continuous delivery (CD) pipeline with AWS CodePipeline that automates builds with AWS CodeBuild	• AWS CodePipeline console • AWS CLI • AWS SDKs	• Using the AWS CodePipeline console • Using the AWS CLI • You can adapt the information in this topic to use the AWS SDKs. For more information, reference the create pipeline action documentation for your programming language through the SDKs section of *Tools for Amazon Web Services* or see `CreatePipeline` in the *AWS CodePipeline API Reference*.
Add test and build automation with AWS CodeBuild to an existing pipeline in AWS CodePipeline	• AWS CodePipeline console • AWS CLI • AWS SDKs	• Add build automation by using the AWS CodePipeline console • Add test automation by using the AWS CodePipeline console • For the AWS CLI, you can adapt the information in this topic to create a pipeline that contains an AWS CodeBuild build action or test action. For more information, see Edit a Pipeline (AWS CLI) and the AWS CodePipeline Pipeline Structure Reference in the *AWS CodePipeline User Guide*. • You can adapt the information in this topic to use the AWS SDKspipeline. For more information, reference the update pipeline action documentation for your programming language through the SDKs section of *Tools for Amazon Web Services* or see `UpdatePipeline` in the *AWS CodePipeline API Reference*.

Option B is incorrect since AWS CodeCommit does not have the facility in itself to carry out the build
Options C is incorrect since the CodePipeline service is used for building build pipelines.
For more information, please refer to the below URL

- https://aws.amazon.com/codestar/features/ (https://aws.amazon.com/codestar/features/)

Ask our Experts

QUESTION 52 CORRECT SECURITY

Your using the AWS CodeDeploy service to deploy an application onto AWS. The application uses secure parameters which are stored in the AWS Systems Manager Parameter store. Which of the following must be done , so that the deployment can be automated via CodeDeploy? Choose 2 answers from the options given below.

- [x] **A.** Use the aws ssm get-parameters with the --with-decryption option ✔
- [ ] **B.** Use the aws ssm get-parameters with the --with-no-decryption option
- [ ] **C.** Give permissions to the AWS Code Deploy service via AWS Access Keys
- [x] **D.** Give permissions to the AWS Code Deploy service via an IAM Role ✔

Explanation :

Answer - A and D
You need to specify the --with-decryption option, this allows the CodeDeploy service to decrypt the password so that it can be used in the application. Also use IAM Roles to ensure the CodeDeploy service can access the KMS service
Option B is incorrect since you need to specify the --with-decryption option
Option C is incorrect since this is not a secure way to access AWS services
For more information on an example on this , please refer to the below URL

- https://aws.amazon.com/blogs/mt/use-parameter-store-to-securely-access-secrets-and-config-data-in-aws-codedeploy/ (https://aws.amazon.com/blogs/mt/use-parameter-store-to-securely-access-secrets-and-config-data-in-aws-codedeploy/)

Ask our Experts

QUESTION 53 INCORRECT REFACTORING

An application is currently accessing a DynamoDB table. Currently the tables queries are performing well. Changes have been made to the application and now the performance of the application is starting to degrade. After looking at the changes , you see that the queries are making use of an attribute which is not the partition key? Which of the following would be the adequate change to make to resolve the issue?

- ○ **A.** Add an index for the DynamoDB table ✔
- ○ **B.** Change all the queries to ensure they use the partition key ✖
- ○ **C.** Enable global tables for DynamoDB
- ○ **D.** Change the read capacity on the table

Explanation :

Answer – A
The AWS Documentation mentions the following
Amazon DynamoDB provides fast access to items in a table by specifying primary key values. However, many applications might benefit from having one or more secondary (or alternate) keys available, to allow efficient access to data with attributes other than the primary key. To address this, you can create one or more secondary indexes on a table, and issue Query or Scan requests against these indexes.
A secondary index is a data structure that contains a subset of attributes from a table, along with an alternate key to support Query operations. You can retrieve data from the index using a Query, in much the same way as you use Query with a table. A table can have multiple secondary indexes, which gives your applications access to many different query patterns.
Option B , although possible , is not the ideal approach to change the application code.
Option C is used to disaster recovery scenarios
Option D is not right , because we don't know if this would solve the issue in the long run
For more information on Secondary Indexes , please refer to the below URL

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

Ask our Experts

QUESTION 54 CORRECT DEPLOYMENT

Your team developed and deployed an application on an EC2 Instance. To test the application, you were given access credentials which also included the rights to write to an S3 bucket. Once the testing was confirmed , an IAM Role was assigned to the Instance. This role only has permissions to read from the bucket. But you notice that the application still has access to write to the S3 bucket. Why is this the case?

- A. You need to restart the instance for the Role settings to take effect
- B. The Environment variables which were set for CLI access are taking priority ✔
- C. The CLI is corrupted , hence the credentials are not being revoked
- D. The EBS Volume needs to be reattached again for the Instance profile to take effect

Explanation :

Answer – B
Below is an excerpt from the documentation on how the credentials are evaluated when it comes to access. So when using the CLI , if the environment variables were set with the Access Keys , they would take preference over the IAM Role.
Using the Default Credential Provider Chain
When you initialize a new service client without supplying any arguments, the AWS SDK for Java attempts to find AWS credentials by using the default credential provider chain implemented by the DefaultAWSCredentialsProviderChain class. The default credential provider chain looks for credentials in this order:

1. Environment variables–AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY. The AWS SDK for Java uses the EnvironmentVariableCredentialsProvider class to load these credentials.
2. Java system properties–aws.accessKeyId and aws.secretKey. The AWS SDK for Java uses the SystemPropertiesCredentialsProvider to load these credentials.
3. The default credential profiles file– typically located at ~/.aws/credentials (location can vary per platform), and shared by many of the AWS SDKs and by the AWS CLI. The AWS SDK for Java uses the ProfileCredentialsProvider to load these credentials.
4. You can create a credentials file by using the aws configure command provided by the AWS CLI, or you can create it by editing the file with a text editor. For information about the credentials file format, see AWS Credentials File Format.
5. Amazon ECS container credentials– loaded from the Amazon ECS if the environment variable AWS_CONTAINER_CREDENTIALS_RELATIVE_URI is set. The AWS SDK for Java uses the ContainerCredentialsProvider to load these credentials.

Instance profile credentials– used on EC2 instances, and delivered through the Amazon EC2 metadata service. The AWS SDK for Java uses the InstanceProfileCredentialsProvider to load these credentials.
Option A and D are incorrect since the IAM Role is instantly applied to the EC2 Instance
Option C is incorrect because even if the CLI is corrupted , still this would not be the cause of the underlying issue
For more information on an example on how credentials are evaluated , please refer to the below URL

- https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/credentials.html (https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/credentials.html)

Ask our Experts

QUESTION 55 INCORRECT DEPLOYMENT

You are planning on deploying an application to the worker role in Elastic Beanstalk. Which of the following is a must have as part of the deployment?

- A. An appspec.yaml file ✖
- B. A cron.yaml file ✔
- C. A cron.config file
- D. An appspec.json file

Explanation :

Answer – B
This is also given in the AWS Documentation

Create an Application Source Bundle
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. For more information, see Periodic Tasks.

Because of the exact requirement given in the AWS Documentation, all other options are invalid.

For more information on creating an application source bundle for 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 56 INCORRECT DEVELOPMENT WITH AWS SERVICES

You are developing a Java based application that needs to make use of the AWS KMS service for encryption. Which of the following must be done for the encryption and decryption process? Choose 2 answers from the options given below.

- [x] **A. Use the Customer master key to encrypt the data** ✖
- [ ] **B. Use the Customer master key to generate a data key for the encryption process** ✔
- [x] **C. Use the Customer master key to decrypt the data** ✖
- [ ] **D. Use the generated data key to decrypt the data** ✔

Explanation :

Answer – B and D
The AWS Documentation mentions the following
The AWS Encryption SDK is a client-side encryption library that makes it easier for you to implement cryptography best practices in your application. It includes secure default behaviour for developers who are not encryption experts, while being flexible enough to work for the most experienced users.
Options A and C are incorrect because you should never use the Customer master keys directly for the encryption of decryption process.
In the AWS Encryption SDK, by default, you generate a new data key for each encryption operation
For more information on the Encryption SDK , please refer to the below URL

- https://docs.aws.amazon.com/kms/latest/developerguide/programming-top.html (https://docs.aws.amazon.com/kms/latest/developerguide/programming-top.html)

Note:
AWS Docs Says
"When you encrypt your data, your data is protected, but you have to protect your encryption key. One strategy is to encrypt it. *Envelope encryption* is the practice of encrypting plaintext data with a data key, and then encrypting the data key under another key.
You can even encrypt the data encryption key under another encryption key, and encrypt that encryption key another encryption key.
But, eventually, one key must remain in plaintext so you can decrypt the keys and your data. This top-level plaintext key encryption key is known as the *master key*."
For more information on the enveloping, please refer to the below URL

- https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#enveloping (https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#enveloping)

Ask our Experts

QUESTION 57 CORRECT DEVELOPMENT WITH AWS SERVICES

You are developing an application for your company. They need to ensure that the JSON data generated by the application is stored in a backend store. Which of the following is the ideal data store for this scenario?

- A. AWS DynamoDB ✔
- B. AWS RedShift
- C. AWS RDS MySQL
- D. AWS Aurora

Explanation :

Answer – A
The below example from the AWS Documentation shows how data is stored in DynamoDB

People

```
{
    "PersonID": 101,
    "LastName": "Smith",
    "FirstName": "Fred",
    "Phone": "555-4321"
}
```

```
{
    "PersonID": 102,
    "LastName": "Jones",
    "FirstName": "Mary",
    "Address": {
        "Street": "123 Main",
        "City": "Anytown",
        "State": "OH",
        "ZIPCode": 12345
    }
}
```

```
{
    "PersonID": 103,
    "LastName": "Stephens",
    "FirstName": "Howard",
    "Address": {
        "Street": "123 Main",
        "City": "London",
        "PostalCode": "ER3 5K8"
    },
    "FavoriteColor": "Blue"
}
```

Hence this is the perfect store for storing JSON related data.

Option B is incorrect since this is used to store data warehousing data
Options C and D are incorrect since these are not the ideal store for JSON related data
For more information on how DynamoDB works , please refer to the below URL

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

Ask our Experts

QUESTION 58 CORRECT

You have a legacy application that works via XML messages. You need to place the application behind the API gateway in order for customers to make API calls. Which of the following would you need to configure?

- A. Enable Payload compression

- B. You will need to work with the Request and Response Data mapping ✔
- C. Enable CORS
- D. Enable multiple stages

Explanation :

Answer - B
This is also mentioned in the AWS Documentation
For example, suppose that an API has a application/json template defined for a request payload and has a application/xml template defined for the response payload. If the client sets the "Content-Type : application/json", and "Accept : application/xml" headers in the request, both the request and response payloads will be processed with the corresponding mapping templates. If the Accept:application/xml header is absent, the application/xml mapping template will be used to map the response payload. To return the response payload unmapped instead, you must set up an empty template for application/json.
Since the documentation clearly mentions what should be the way to handle such requests , all other options are incorrect
For more information on request-response data mappings , please refer to the below URL

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

Ask our Experts

QUESTION 59 CORRECT DEPLOYMENT

You are planning on using the Serverless Application model which will be used to deploy a serverless application consisting of a Node.js function. Which of the following steps need to be carried out? Choose 2 answers from the options given below.

- [ ] A. Usethe cloudformation package command
- [x] B. Use the sam package command ✔
- [ ] C. Use the cloudformation deploy command
- [x] D. Use the sam deploy command ✔

Explanation :

Answer – B and D
The AWS Documentation gives an example on this

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

The package command returns an AWS SAM template, in this case `serverless-output.yaml` that contains the `CodeUri` that points to the deployment zip in the Amazon S3 bucket that you specified. This template represents your serverless application. You are now ready to deploy it.

Deployment

To deploy the application, run the following command:

```
sam deploy \
   --template-file serverless-output.yaml \
   --stack-name new-stack-name \
   --capabilities CAPABILITY_IAM
```

Here you need to use the sam commands and not the cloudformation commands

For more information on serverless deploy , 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 60 INCORRECT REFACTORING

Your application currently points to several Lambda functions in AWS. A change is being made to one of the Lambda functions. You need to ensure that application traffic is shifted slowly from one Lambda function to the other. Which of the following steps would you carry out?

Select 2 Options:

- [ ] **A. Create an ALIAS with the –routing-config parameter** ✔
- [x] **B. Update the ALIAS with the –routing-config parameter** ✔
- [ ] **C. Create a version with the –routing-config parameter**
- [ ] **D. Update the version with the –routing-config parameter**
- [x] **E. Update the function with the - config parameter** ✖

Explanation :

Answer – A and B
This is mentioned in the AWS Documentation
By default, an alias points to a single Lambda function version. When the alias is updated to point to a different function version, incoming request traffic in turn instantly points to the updated version. This exposes that alias to any potential instabilities introduced by the new version. To minimize this impact, you can implement the routing-config parameter of the Lambda alias that allows you to point to two different versions of the Lambda function and dictate what percentage of incoming traffic is sent to each version.
Options C and D are incorrect since you need to use ALIAS for this purpose.
Option E is incorrect. Because A & B are the correct ways to achieve the requirement.
For more information on shifting traffic using ALIAS , please refer to the below URL

- https://docs.aws.amazon.com/lambda/latest/dg/lambda-traffic-shifting-using-aliases.html (https://docs.aws.amazon.com/lambda/latest/dg/lambda-traffic-shifting-using-aliases.html)

Ask our Experts

QUESTION 61 CORRECT REFACTORING

An application needs to make use of an SQS queue for working with messages. An SQS queue has been created with the default settings. The application needs 60 seconds to process each message. Which of the following step need to be carried out by the application.

- ( ) **A. Change the VisibilityTimeout for each message and then delete the message after processing is completed.** ✔
- ( ) **B. Delete the message and change the visibility timeout.**
- ( ) **C. Process the message , change the visibility timeout. Delete the message**
- ( ) **D. Process the message and delete the message**

Explanation :

Answer – A
If the SQS queue is created with the default settings , then the default visibility timeout is 30 seconds. And since the application needs more time for processing , you first need to change the timeout and delete the message after it is processed.
Option B is incorrect since you need to process the message first
Options C and D are incorrect since you need to change the visibility timeout for each message first
For more information on SQS visibility timeout , please refer to the below URL

- https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-visibility-timeout.html (https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-visibility-timeout.html)

Ask our Experts

QUESTION 62 CORRECT

An application currently makes use of DynamoDB tables. There are thousand requests made per second on the DynamoDB table. Another application takes the changes to the items in the DynamoDB table , for further analytics processing. Which of the following can be affectively used to manage this requirement?

- A. Enable a scan on the entire table to check for changes
- B. Create a query to check for changes
- C. Enableg lobal tables for DynamoDB
- D. Enable streams for DynamoDB ✔

Explanation :

Answer – D
The below information from the AWS Documentation helps to supplement this requirement
Capturing Table Activity with DynamoDB Streams
Many applications can benefit from the ability to capture changes to items stored in a DynamoDB table, at the point in time when such changes occur. Here are some example use cases:

- An application in one AWS region modifies the data in a DynamoDB table. A second application in another AWS region reads these data modifications and writes the data to another table, creating a replica that stays in sync with the original table.
- A popular mobile app modifies data in a DynamoDB table, at the rate of thousands of updates per second. Another application captures and stores data about these updates, providing near real time usage metrics for the mobile app.
- A global multi-player game has a multi-master topology, storing data in multiple AWS regions. Each master stays in sync by consuming and replaying the changes that occur in the remote regions.
- An application automatically sends notifications to the mobile devices of all friends in a group as soon as one friend uploads a new picture.
- A new customer adds data to a DynamoDB table. This event invokes another application that sends a welcome email to the new customer.

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.
Options A and B are incorrect since these would result in a lot of throughput requirement for the table
Option C is incorrect since this is used for replication of data
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 63 INCORRECT

An application currently makes use of DynamoDB tables. There is a requirement that a user can only view certain

items in the table. How can this be accomplished?

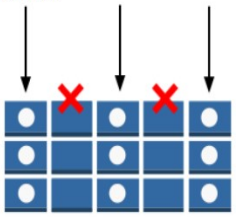
- ○ **A.** Make use of queries based on the partition key ✖
- ○ **B.** Make use of queries based on the sort key
- ○ **C.** Create a separate index on the table
- ○ **D.** Use IAM polices with specific conditions ✔

Explanation :

Answer – D
The AWS Documentation mentions this specific use case

- Hide information so that only a subset of attributes are visible to the user. An example might be an app that displays flight data for nearby airports, based on the user's location. Airline names, arrival and departure times, and flight numbers are all displayed. However, attributes such as pilot names or the number of passengers are hidden, as shown in the following illustration:

- Hide information so that only a subset of attributes are visible to the user. An example might be an app that displays flight data for nearby airports, based on the user's location. Airline names, arrival and departure times, and flight numbers are all displayed. However, attributes such as pilot names or the number of passengers are hidden, as shown in the following illustration:



To implement this kind of fine-grained access control, you write an IAM permissions policy that specifies conditions for accessing security credentials and the associated permissions. You then apply the policy to IAM users, groups, or roles that you create using the IAM console. Your IAM policy can restrict access to individual items in a table, access to the attributes in those items, or both at the same time.

To implement this kind of fine-grained access control, you write an IAM permissions policy that specifies conditions for accessing security credentials and the associated permissions. You then apply the policy to IAM users, groups, or roles that you create using the IAM console. Your IAM policy can restrict access to individual items in a table, access to the attributes in those items, or both at the same time.

All other options are invalid since the right approach is to use IAM polices with specific conditions
For more information on specifying conditions , please refer to the below URL

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

Ask our Experts

QUESTION 64 CORRECT DEVELOPMENT WITH AWS SERVICES

You are developing an application that would be used to upload images from users. You need to effectively store the images and also the name of the user who uploaded the image. How would you accomplish this? Choose 2 answers from the options given below.

- ☐ **A.** Store the images in DynamoDB
- ☑ **B.** Store the images in S3 ✔
- ☐ **C.** Store the name of the user in S3
- ☑ **D.** Store the name of the user in DynamoDB ✔

Explanation :

Answer – B 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.
Options A and C are incorrect since it should be the other way around in terms of the storage
For more information on this use case , please refer to the below URL

- https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/bp-use-s3-too.html (https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/bp-use-s3-too.html)

Ask our Experts

QUESTION 65 CORRECT SECURITY

Your application must write to an SQS queue. Your corporate security policies require that AWS credentials are always encrypted and are rotated at least once a week. How can you securely provide credentials that allow your application to write to the queue?

- **A. Have the application fetch an access key from an Amazon S3 bucket at run time.**
- **B. Launch the application's Amazon EC2 instance with an IAM role.** ✔
- **C. Embed the Access keys in the application**
- **D. Create environment variables in the EC2 Instance with the Access Keys**

Explanation :

Answer – B
This is clearly mentioned in the AWS Documentation
IAM Roles for Amazon EC2
Applications must sign their API requests with AWS credentials. Therefore, if you are an application developer, you need a strategy for managing credentials for your applications that run on EC2 instances. For example, you can securely distribute your AWS credentials to the instances, enabling the applications on those instances to use your credentials to sign requests, while protecting your credentials from other users. However, it's challenging to securely distribute credentials to each instance, especially those that AWS creates on your behalf, such as Spot Instances or instances in Auto Scaling groups. You must also be able to update the credentials on each instance when you rotate your AWS credentials.
We designed IAM roles so that your applications can securely make API requests from your instances, without requiring you to manage the security credentials that the applications use. Instead of creating and distributing your AWS credentials, you can delegate permission to make API requests using IAM roles as follows:

1. Create an IAM role.
2. Define which accounts or AWS services can assume the role.
3. Define which API actions and resources the application can use after assuming the role.
4. Specify the role when you launch your instance, or attach the role to a running or stopped instance.
5. Have the application retrieve a set of temporary credentials and use them.

All other options are invalid because you should not use Access Keys , this is the recommended best practise.
For more information on IAM Roles , please refer to the below URL

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

Ask our Experts

Certification

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

Company

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

Mobile App

- Android Coming Soon
- iOS Coming Soon

Follow us

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

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

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

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