OBJECTIVE : API GATEWAY

Attempt	1
Marks Obtained	1 / 15
Your score is	6.67%
Completed on	Monday , 28 January 2019 , 07:02 PM
Time Taken	00 H 01 M 44 S
Result	Fail

Domains / Topics wise Quiz Performance Report

S.No.	Topic	Total Questions	Correct	Incorrect	Unattempted
1	Other	15	1	2	12

15	**1**	**2**	**12**
Questions	Correct	Incorrect	Unattempted

Show Answers

All ▼

QUESTION 1 CORRECT

Topic : Designing highly available, cost-efficient, fault-tolerant, scalable systems

Which of the following services are automatically integrated with the API gateway service in the background to ensure better response to calls made to the API Gateway?

○ **A.** AWS Cloudwatch

○ **B.** AWS Cloudfront

○ **C.** AWS Volume gateway

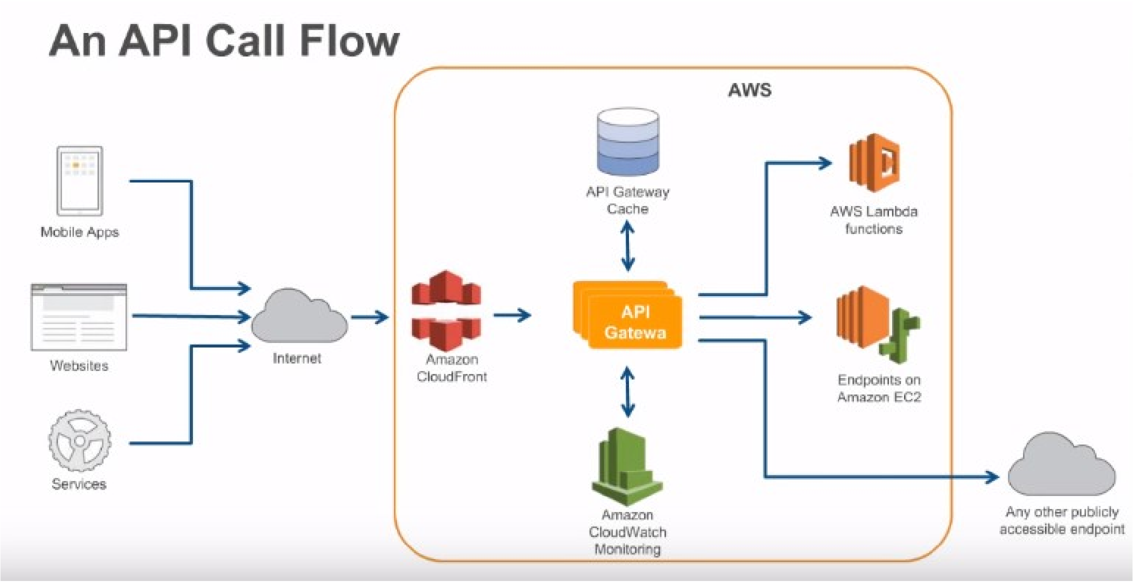
○ **D.** AWS Lambda ✔

Explanation :

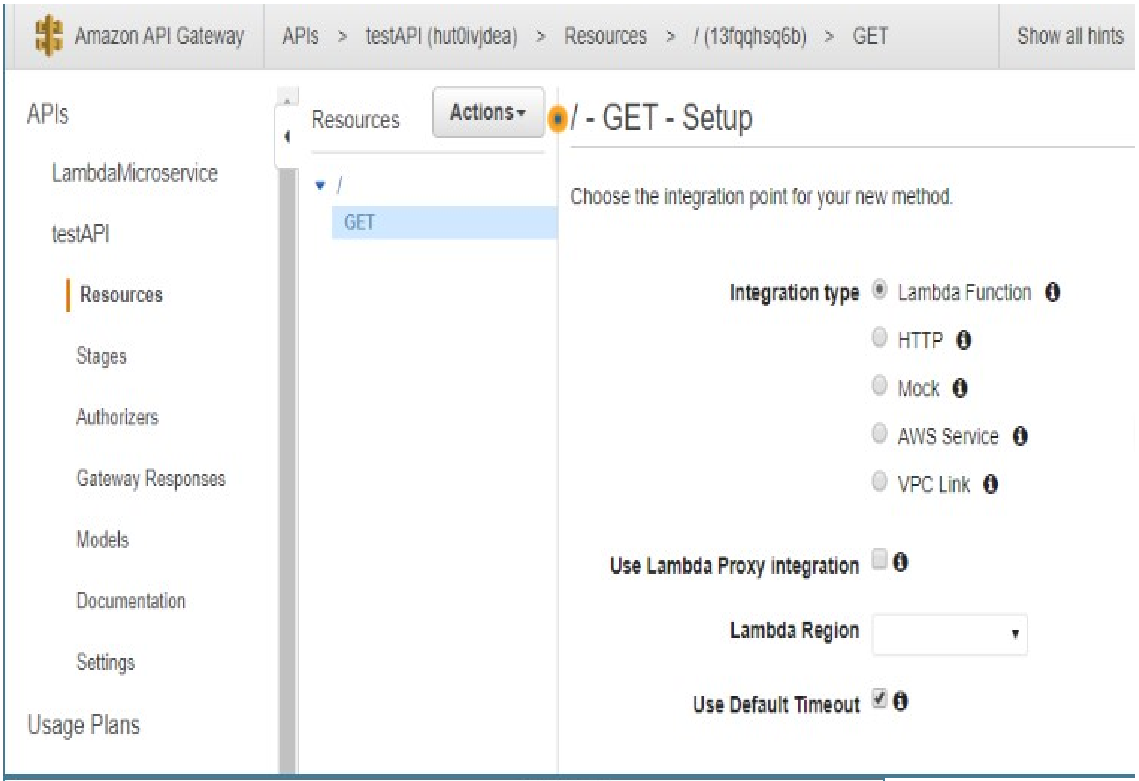
Answer – D

API Gateway is designed for web and mobile developers who want to provide secure, reliable access to back-end APIs for access from mobile apps, web apps,etc.

The business logic behind the APIs can be provided by a publicly accessible endpoint that API Gateway proxies call, or it can be entirely run as a Lambda function.



For example, an application can call an API in API Gateway to upload a user's annual income and expense data to Amazon S3 or Amazon DynamoDB, process the data in AWS Lambda to compute tax owed, and file a tax return.



/ - GET - Setup

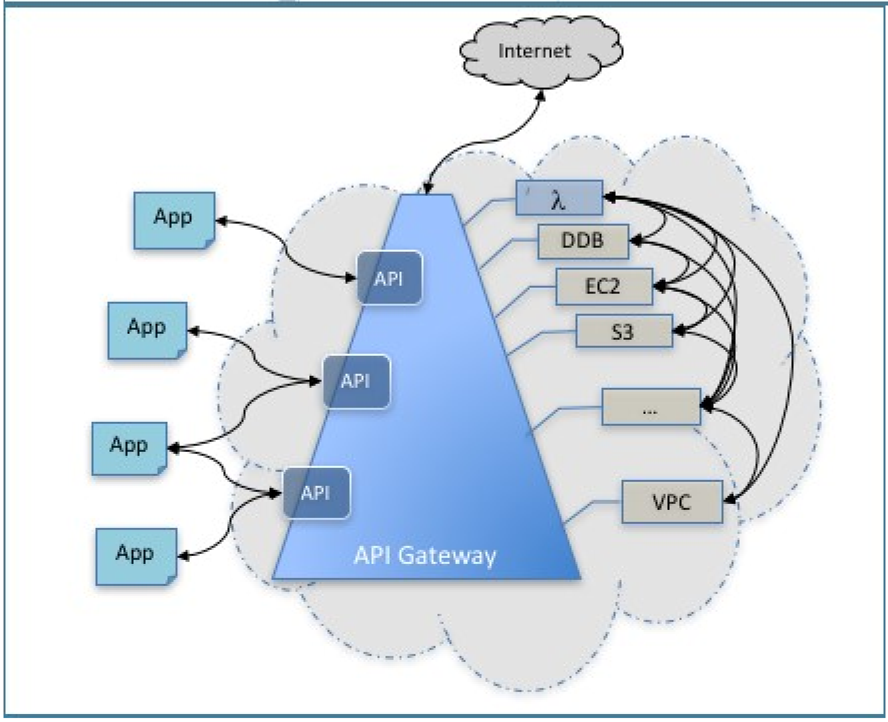
Choose the integration point for your new method.

Integration type ● Lambda Function
○ HTTP
○ Mock
○ AWS Service
○ VPC Link

Use Lambda Proxy integration □

Lambda Region

Use Default Timeout ☑



Option A is incorrect. Cloud Watch offers Cloud Monitoring services for the resources being used.

Option B is incorrect. AWS CloudFront is a web service that speeds up distribution of your static and dynamic web content, through a worldwide network of edge locations where the contents are cached for 24 hours by default.

Option C is incorrect. AWS Storage Gateway service is used to store data in the AWS Cloud. It offers a scalable and cost effective storage that maintains data security too.

For more information on the features of the API gateway , please refer to the below URL:

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

Ask our Experts

👍 👎

QUESTION 2 INCORRECT

Topic : Designing highly available, cost-efficient, fault-tolerant, scalable systems

There is a requirement in your organization to use the API gateway. But there is a specific requirement to have separate API's versions for staging , testing and production environments. Which feature of the API gateway can be used to fulfil this requirement.

○ **A.** API Domain Name ✖

○ **B.** Swagger extensions

○ **C.** Using AWS Cloudfront

○ **D.** Using Stages ✔

Explanation :

Answer – D

A stage prescribes a unique base URL: (of the https://{restapi-id}.execute-api.{region} amazonaws.com/{stageName} format) for your users to call the associated API snapshot. Using different stage-deployment combinations, you can enable smooth and robust version control for the API.

For more information on the API gateway deployments and stages, please refer to the below URL:

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

Ask our Experts

👍 👎

QUESTION 3 INCORRECT

Topic : Implementation and Deployment

1. You have the following IAM policy attached to a user.

```
"Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "execute-api:Invoke"
   ],
   "Resource": [
    "arn:aws:execute-api:us-east-1:123456:demoapi/*/GET/person"
   ]
}
```

What specific permission does this policy provide

○ **A.** It would provide the user to invoke and manage all the API's under demoapi ✖

○ **B.** It would allow the user to get the list of person's exposed by the demoapi ✔

○ **C.** It would allow the user to delete the list of person's exposed by the demoapi

○ **D.** It would allow the user to get ,list and delete of person's exposed by the demoapi

Explanation :

Answer - B
The Invoke permission allows the user to invoke the relevant API. Since the method specified is only the GET method , hence the user would only have access to get the list of Person's exposed by demoapi.
For more information on controlling access to API's, please refer to the below URL:

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

Ask our Experts

👍 👎

QUESTION 4 UNATTEMPTED

Topic : Implementation and Deployment

If you want to provide a user the permission to just list the resources, methods, models, and stages in the API with the identifier of a123456789 in the AWS region of us-east-1, which one of the below IAM policies could be used for this

○ **A.** { "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["apigateway:GET"], "Resource": ["arn:aws:apigateway:us-east-1::/restapis/a123456789/*"] }]} ✓

○ **B.** { "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["apigateway:*"], "Resource": ["arn:aws:apigateway:us-east-1::/restapis/a123456789/*"] }]}

○ **C.** { "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["apigateway:*"], "Resource": ["*"] }]}

○ **D.** { "Version": "2012-10-17", "Statement": [{ "Effect": "Deny", "Action": ["apigateway:GET"], "Resource": ["arn:aws:apigateway:us-east-1::/restapis/a123456789/*"] }]}

Explanation :

Answer - A

Option B is invalid because this would also allow the user to perform all available API Gateway actions for the API

Option C is invalid because it grants the full access to any of the API Gateway resource of the AWS account.

Option D is invalid because this becomes the Deny permission

For more information on controlling access to API's, please refer to the below URL:

- http://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-iam-policy-examples.html (http://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-iam-policy-examples.html)

Ask our Experts

👍 👎

QUESTION 5 UNATTEMPTED

Topic : Data Security

Which of the below security features of the API gateway can be used to ensure that API's resources can receive requests from a domain other than the API's own domain

○ **A.** API Stages

○ **B.** API Deployment

○ **C.** API CORS ✓

○ **D.** API Access

Explanation :

Answer – C
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 and B are invalid because these are used to ensure users can call API's.
Option D is invalid because there is no such thing as API Access.
For more information on enabling CORS, please refer to the below URL:

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

Ask our Experts

👍 👎

QUESTION 6 UNATTEMPTED

Topic : Implementation and Deployment

You have an EC2 Instance located in your AWS VPC. This EC2 Instance hosts an application that is going to make use of the API Application gateway. Which of the following features can assist to ensure that the EC2 Instances only accepts request from the API Gateway.

○ **A.** Use the CORS feature in the API Gateway

○ **B.** Use SSL Certificates ✓

○ **C.** Use Swagger Extensions

○ **D.** Use Stages

Explanation :

Answer – B
You can use API Gateway to generate an SSL certificate and use its public key in the backend to verify that HTTP requests to your backend system are from API Gateway. This allows your HTTP backend to control and accept only requests originating from Amazon API Gateway, even if the back end is publicly accessible.
Option A is invalid because this is used to provide cross domain access to API's
Option C is invalid because this is an additional extension plugin to the API gateway.
Option D is invalid because this is used to deploy your API's
For more information on using SSL Certificates, please refer to the below URL:

- http://docs.aws.amazon.com/apigateway/latest/developerguide/getting-started-client-side-ssl-authentication.html (http://docs.aws.amazon.com/apigateway/latest/developerguide/getting-started-client-side-ssl-authentication.html)

Ask our Experts

👍 👎

QUESTION 7 UNATTEMPTED

Topic : Implementation and Deployment

When integrating AWS Lambda or calling an AWS Lambda function from the API gateway ,which of the following is a must pre-requisite action that must be performed first

○ **A.** Grant access to the IAM role to have the required access with to lambda.
✓

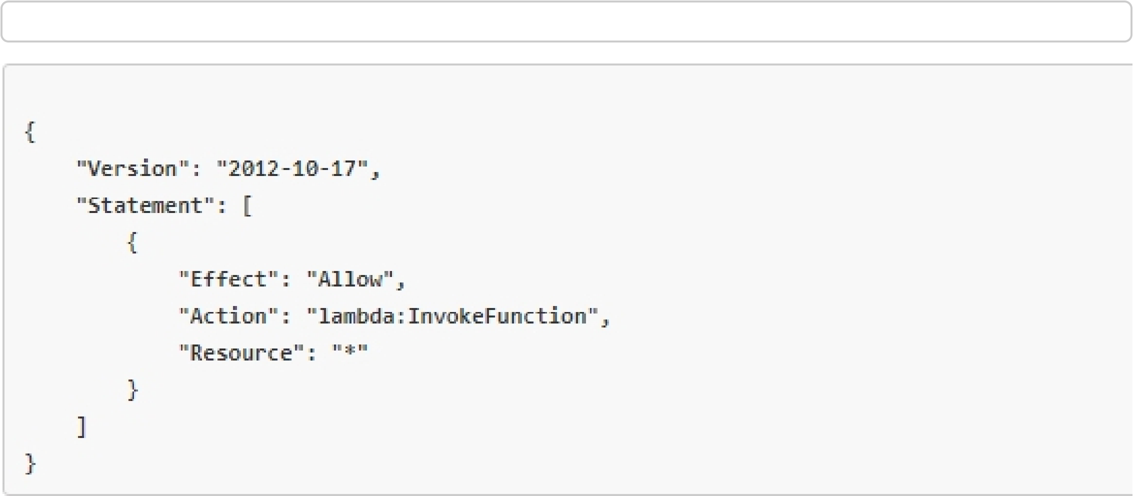
○ **B.** Grant access to the IAM user to have the required access level with Cloudwatch

○ **C.** Grant access to the IAM user to have the required access level with API Gateway

○ **D.** Grant access to the IAM group to have the required access level for API Gateway

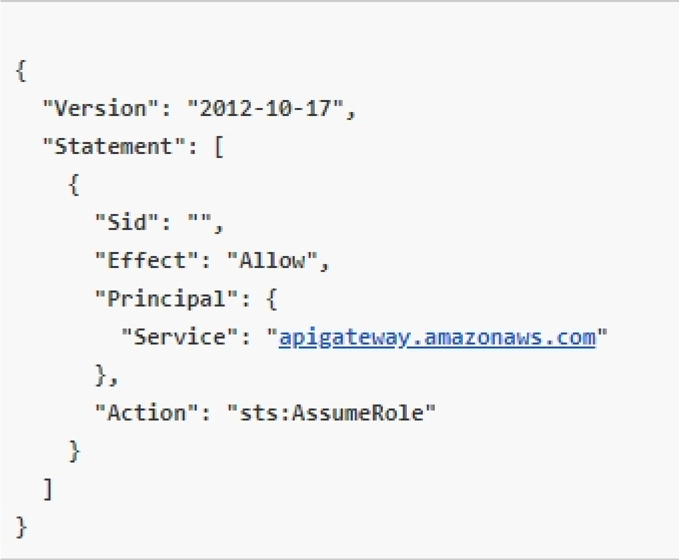
Explanation :

Answer - A When API Gateway is integrated with AWS Lambda or another AWS service, such as Amazon Simple Storage Service or Amazon Kinesis, you must also enable API Gateway as a trusted entity to invoke an AWS service in the backend. To do so, create an IAM role and attach a service-specific access policy to the role. This is demonstrated in the following example for invoking a Lambda function:



```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "lambda:InvokeFunction",
            "Resource": "*"
        }
    ]
}
```

Next, add the following trust policy to allow API Gateway to call the backend Lambda function on behalf of the attached user who is assigned the IAM role.



```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "apigateway.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Without specifying this trust relationship, API Gateway is denied the right to call the backend on behalf of the user, even when the user has been granted permissions to access the backend directly.
When an API Gateway API is set up with IAM roles and policies to control client access, the client must sign API requests with Signature Version 4 (http://docs.aws.amazon.com/general/latest/gr/sigv4_signing.html). Alternatively, you can use the AWS CLI or one of the AWS SDKs to handle request signing for you. For more information, see Invoking an API in Amazon API Gateway (https://docs.aws.amazon.com/apigateway/latest/developerguide/how-to-call-api.html).

You may visit

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

for more info.

Ask our Experts

QUESTION 8 UNATTEMPTED

Topic : Implementation and Deployment

You are currently architecting a solution for your company that will make use of API gateways. You want to ensure that you design the API gateway in such a way that latency to requests to the API gateway is reduced. Which of the following things can you ensure is carried out to fulfil this requirement.

○ **A.** Use AWS API Gateway with Cloudfront

○ **B.** Enable API Caching ✓

○ **C.** Enable API Stages

○ **D.** Enable CORS configuration for the API Gateway

Explanation :

Answer – B
Option A is invalid because Cloudfront is already used along with the API gateway
Option C is invalid because this is used to deploy API's
Option D is invalid because this is used for cross domain access of API's
You can enable API caching in Amazon API Gateway to cache your endpoint's response. With caching, you can reduce the number of calls made to your endpoint and also improve the latency of the requests to your API. When you enable caching for a stage, API Gateway caches responses from your endpoint for a specified time-to-live (TTL) period, in seconds. API Gateway then responds to the request by looking up the endpoint response from the cache instead of making a request to your endpoint. The default TTL value for API caching is 300 seconds. The maximum TTL value is 3600 seconds. TTL=0 means caching is disabled.
For more information on the API Gateway cache feature please refer to the below URL:

- http://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-caching.html (http://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-caching.html)

Ask our Experts

👍 👎

QUESTION 9 UNATTEMPTED

Topic : Troubleshooting

You are encountering a "429" Error code from your API Gateway. What can you do to resolve this error

○ **A.** Consider using Cloudfront to cache the request

○ **B.** Consider changing the throttling limits for your account ✓

○ **C.** Consider enabling CORS configuration for your API

○ **D.** Consider using stage variables for your API

Explanation :

Answer - B
When request submissions exceed the steady-state request rate and burst limits, API Gateway fails the limit-exceeding requests and returns 429 Too Many Requests error responses to the client.
As an API owner, you can set the default method throttling to override the account-level request throttling limits for a specific stage or for individual methods in an API. The Default method throttling limits are bounded by the account-level rate limits, even if you set the default method throttling limits higher than the account-level limits.
For more information on the API Gateway request throttling please refer to the below URL:

- http://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-request-throttling.html (http://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-request-throttling.html)

Ask our Experts

👍 👎

QUESTION 10 UNATTEMPTED

Topic : Implementation and Deployment

You are trying to enable the API Caching for your API Gateway by using AWS free tier Account. But you charged by AWS. Which of the following reason for this?

○ **A.** The API Resource is not defined properly

○ **B.** The Method Resource is not defined properly

○ **C.** You are using the AWS Free Tier Account ✓

○ **D.** The Swagger extensions are not enabled

Explanation :

Answer - C
The following lists the exceptions of the general pricing scheme:

- API caching in Amazon API Gateway is not eligible for the AWS Free Tier.
- Calling methods with the authorization type (http://docs.aws.amazon.com/apigateway/api-reference/resource/method/#authorizationType) of AWS_IAM, CUSTOM, andCOGNITO_USER_POOLS are not charged for authorization and authentication failures.
- Calling methods requiring API keys are not charged when API keys are missing or invalid.
- API Gateway-throttled requests are not charged when the request rate or burst exceed the pre-configured limits.
- Usage plan-throttled requests are not charged when rate limits or quota exceed the pre-configured limits.

For more information on the API Gateway limits please refer to the below URL:

- http://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-pricing.html (http://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-pricing.html)

Ask our Experts

👍 👎

QUESTION 11 UNATTEMPTED

Topic : Implementation and Deployment

You have defined an api path /sping in the API gateway, but are getting unexpected results when calling the relevant API. Why is this the case

○ **A.** You have not enable API Cache

○ **B.** The /sping is reserved by AWS ✓

○ **C.** You have to increase the throttling for your account

○ **D.** You need to enable cross account access

Explanation :

Answer - B
Some of the known issues when using the API gateway is given below

- The plain text pipe character (|) is not supported for any request URL query string and must be URL-encoded.
- Paths of /ping and /sping are reserved for the service health check. Use of these for API root-level resources with custom domains will fail to produce the expected result.
- Cross-account authentication is not currently supported in API Gateway. An API caller must be an IAM user of the same AWS account of the API owner.

For more information on the known issues please refer to the below URL:

- http://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-known-issues.html (http://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-known-issues.html)

Ask our Experts

👍 👎

QUESTION 12 UNATTEMPTED

Topic : Implementation and Deployment

You need to pass configuration parameters from your API Gateway to the Lambda function. Which of the following can be used for this purpose

○ **A.** Swagger extensions

○ **B.** Stage Variables ✓

○ **C.** API Gateway variables

○ **D.** Deployment variables

Explanation :

Answer - B
Stage variables are name-value pairs that you can define as configuration attributes associated with a deployment stage of an API. They act like environment variables and can be used in your API setup and mapping templates.
You can also use stage variables to pass configuration parameters to a Lambda function through your mapping templates.
For more information on stage variables please refer to the below URL:

- http://docs.aws.amazon.com/apigateway/latest/developerguide/stage-variables.html (http://docs.aws.amazon.com/apigateway/latest/developerguide/stage-variables.html)

Ask our Experts

👍 👎

QUESTION 13 UNATTEMPTED

Topic : Implementation and Deployment

You want to use the API Gateway to make calls to Amazon S3. Which of the following can assist in this?

○ **A.** Using Stage variables

○ **B.** Using the AWS Service proxy ✓

○ **C.** Using REST API

○ **D.** Using Cloudfront along with the API Gateway

Explanation :

Answer - B
In addition to exposing Lambda functions or HTTP endpoints, you can also create an API Gateway API as a proxy to an AWS service, such as Amazon SNS, Amazon S3, Kinesis, enabling your client to access the backend AWS services through your APIs.
For more information on AWS Proxy service please refer to the below URL:

- http://docs.aws.amazon.com/apigateway/latest/developerguide/getting-started-aws-proxy.html (http://docs.aws.amazon.com/apigateway/latest/developerguide/getting-started-aws-proxy.html)

Ask our Experts

QUESTION 14 **UNATTEMPTED**

Topic : Data Security

Apart from IAM Roles and policies which of the below services can be used to control access to your API gateway

○ **A.** Amazon Cloudfront

○ **B.** Amazon Cloudwatch

○ **C.** Amazon Cognito ✓

○ **D.** Web Identity Federation

Explanation :

Answer - C

In addition to using IAM roles and policies or custom authorizers, you can also use a user pool in Amazon Cognito to control who can access your API in API Gateway. A user pool serves as your own identity provider to maintain a user directory. It supports user registration and sign-in, as well as provisioning identity tokens for signed-in users.

For more information on the integration please refer to the below URL:

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

Ask our Experts

👍 👎

QUESTION 15 UNATTEMPTED

Topic : Implementation and Deployment

After creating an API , what must be done so that users can call the relevant API

○ **A.** Deploy the API ✓

○ **B.** Copy the API

○ **C.** Build the API

○ **D.** Assign an SSL Certificate

Explanation :

Answer - A

After creating your API, you must deploy it to make the API callable for your users. An API deployment represents an API snapshot and becomes callable by the API users when it is associated with a stage. Deploying an API involves creating a deployment and stage and associating the deployment with the stage.
For more information on deploying the API please refer to the below URL:

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

Ask our Experts

👍 👎

Finish Review (https://www.whizlabs.com/learn/course/aws-csaa-practice-tests/quiz/14568)

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)