|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  | Department of Health and Human Services, USA Logo |  |  |
|  |  |  |  |
|  |  | |  |
|  | **API Gateway PoC Security** | |  |
|  |  | |  |
|  | National Cancer Institute (NCI)  Center for Biomedical Informatics and Information Technology (CBIIT)  **Version 1.0**  **07/02/21** | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |
|  |  |  |  |
|  |  |  |  |

For Official Use Only

**Record of Changes**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version Number** | **Author** | **Section Number/ Paragraph Number** | **Summary of Changes** | **Date of Change** |
| 1.0 | Yakov Polonsky |  | Initial draft | 07/02/2021 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Table of contents**

[AWS Infrastructure SECURITY for API Gateway POC 1](#_Toc76139528)

[Background 1](#_Toc76139529)

[API Gateway endpoint type selection to meet the PoC requirements and security considerations 1](#_Toc76139530)

[Identity and Access management for AWS API Gateway 1](#_Toc76139531)

[API Gateway Authentication 2](#_Toc76139532)

[Cache encryption 3](#_Toc76139533)

[API Keys and Usage Plans 3](#_Toc76139534)

[Logging and monitoring 3](#_Toc76139535)

[Compliance validation for API Gateway 4](#_Toc76139536)

# AWS Infrastructure SECURITY for API Gateway POC

## Background

Security is a shared responsibility between AWS and AWS customer. The [shared responsibility model](http://aws.amazon.com/compliance/shared-responsibility-model/)

describes this as security of the cloud and security in the cloud:

* **Security of the cloud** – AWS is responsible for protecting the infrastructure that runs AWS services in the AWS Cloud. AWS also provides you with services that you can use securely. Third-party auditors regularly test and verify the effectiveness of our security as part of the [AWS Compliance Programs](http://aws.amazon.com/compliance/programs/). To learn about the compliance programs that apply to Amazon API Gateway, see [AWS services in scope by compliance program](http://aws.amazon.com/compliance/services-in-scope/).
* **Security in the cloud** – AWS customer responsibility is determined by the API Gateway AWS service. It includes the sensitivity of API Gateway data, identity and access management for API Gateway, logging and monitoring, compliance validation, resilience, and use of best security practices.

This document describes the API Gateway configuration to meet security and compliance objectives.

## API Gateway endpoint type selection to meet the PoC requirements and security considerations

An API endpoint type refers to the hostname of the API and depends on where the API traffic originates from. The table below lists endpoint types and the selection considerations for API Gateway PoC:

|  |  |  |
| --- | --- | --- |
| Edge-optimized | For geographically distributed clients. Includes CloudFront AWS service | Eliminated for security reasons.  Not required due to geographical distribution of our clients. |
| Regional | For clients in the same region. Includes AWS Route 53 service to perform routing | **Recommended**  Accessible by a variety of clients/customers with local geographical distribution  The URL can have access limit through ingress routing tables and resource policies |
| Private | For access from the given VPC. Includes VPC endpoint interface | Clients like ServiceNow are outside CBIIT managed VPCs  Requires advanced networking like DirectConnect to allow clients to reach API Gateway  Requires addition networking to reach the API from another VPC |

The Regional endpoint type has been recommended in API Gateway PoC although the different type can be chosen depending on requirements

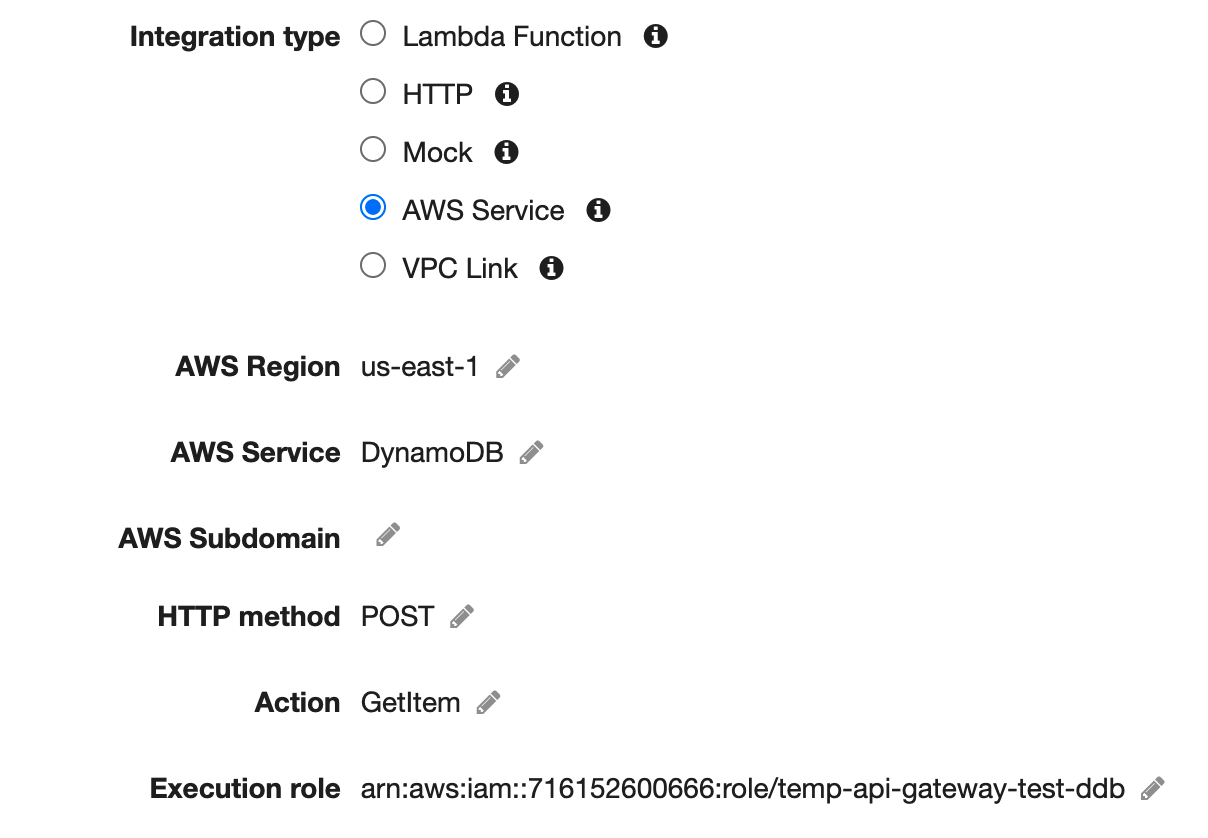
## Identity and Access management for AWS API Gateway

The access to API Gateway and from API Gateway to downstream services can be managed by Resource-based policies and Identity based policies.

The **resource-based policies** are JSON policy documents that can be attached to API gateway and use to control access to a specific API. The policy defines what actions can be performed by specified principle and under what conditions. For example, the policy below limits the access to API by a predetermined IP range. Only principals within the selected IP range 128.231.0.xxx can access API:



The **identity-based policies** are JSON permissions policy documents that can be attached to API Gateway endpoints as IAM role to access selected AWS resource. For example, the API endpoint “GetUserById” requires access to DynamoDB table. The execution role “temp-api-gateway-test-ddb” is attached to the endpoint:



The attached IAM role includes AWS-managed policy *AmazonDynamoDBFullAccess*. For more stricter policy, it can be replaced with the custom user-managed policy to limit access to read-only actions and to selected DynamoDB table.

The downstream AWS resources can also carry a policy restricting access from API Gateway only. Such policy can define a principal as API Gateway with assigned IAM role.

## API Gateway Authentication

API Gateway PoC uses a *Lambda authorizer*– an API Gateway feature that uses a Lambda Function to control access to API endpoints. The token type Lambda authorizer receives the caller’s identity in a bearer token, such as JWT or OAuth token.

Lambda authorizer provides OAuth2.0 authentication using CBIIT Okta identification server to verify a token sent by the client. Upon token validation, Lambda authorizer returns Allow / Deny policy back to API Gateway to control access to selected APIs.

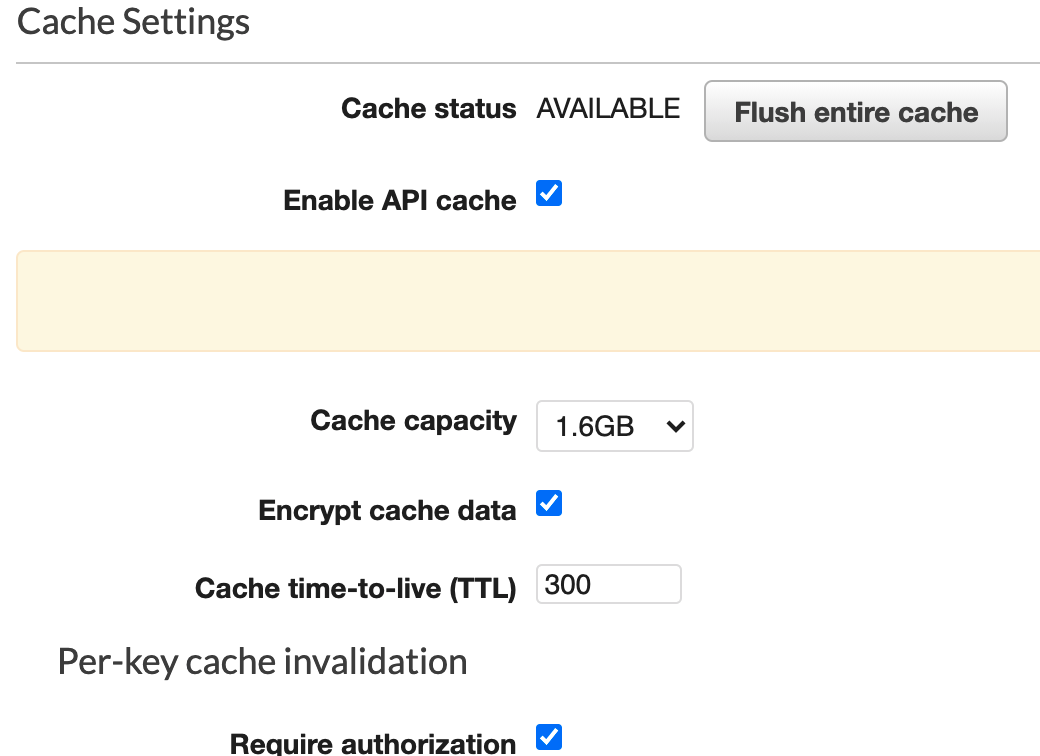
Lambda authorizer can also provide Basic authentication by decoding the client’s identity token and validating credentials against LDAP server.

The authorization can be applied on a method level by returning the appropriate access policy to API Gateway. For example, based on client’s identity the returned policy can allow only read-only methods and deny any methods that modify persistent data.

For other typed of authentication see [AWS Documentation](https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-use-lambda-authorizer.html).

## Cache encryption

API Gateway suggests encrypting cache data as one of the ways to protect data at rest. API Gateway settings allows to enable cache encryption when cache is enabled to enhance responsiveness. To further increase security of data at rest, the time-to-live(TTL) parameter allows you to limit the amount of time the data in cache is available. The picture below depicts the API Gateway cache settings:



## API Keys and Usage Plans

API Keys are used to add additional protection layer to API Gateway against direct access. By enabling this setting, API Gateway requires HTTP requests to include the origin custom header *x-api-key*, which value is set in API Gateway and given to the client. Each client is given a separate API Key value, so it can be used for monitoring and reporting in CloudWatch dashboards.

API Gateway allows to create Usage Plans associate with corresponding API Keys. Usage Plan protects backend from excess traffic by configuring standard or burst rate limits for each method in REST API.

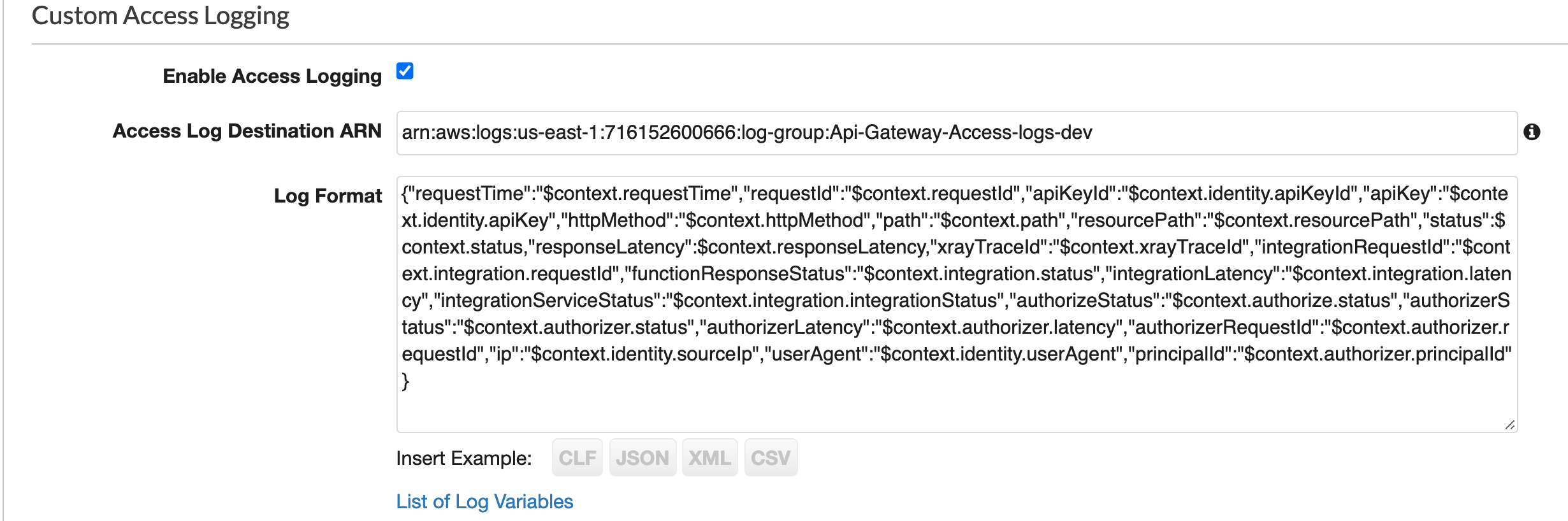
Usage Plans can set alarms to identify threats like DDoS attack. API Gateway can be protected from DDoS attacks by setting CloudFront distribution with AWS AWF.

API keys and usage plans can be used as an additional layer of authentication and authorization. AWS documentation does not recommend using it as the only means for access management. It recommends use it along with Lambda authorizer and IAM role.

## Logging and monitoring

Monitoring is important part of maintaining the reliability, availability, and performance of API Gateway. It allows to create custom format for access logs and CloudWatch alarms based on access log metrics exceeded given thresholds. Notifications are sent to SNS topics, support and security teams are notified immediately on possible issues.

The picture below depicts the custom format variables used in API Gateway PoC. This template produces the access log with JSON format entries containing values for selected variables:



## Compliance validation for API Gateway

Third-party auditors assess the security and compliance of Amazon API Gateway as part of multiple AWS compliance programs. These include SOC, PCI, FedRAMP, HIPAA, and others.

API Gateway integrates with other AWS services to provide the compliance validation:

* **API Config** records configuration changes made to API Gateway resources. AWS Config Rules feature defines configuration rules and automatically detects, tracks, and alerts violations to these rules. By tracking changes to these resource configuration properties, you can also author change-triggered AWS Config rules for your API Gateway resources and test your resource configurations against best practices.
* **Security Hub** provides with comprehensive view of your security state in AWS and helps to check API Gateway environment against security industry standards and best practices.

AWS Documentation includes security and compliance guides that discuss architectural considerations and provide steps for deploying security- and compliance-focused baseline environments on AWS.