Input Requirements for PubSub Terraform Module Development

[Summary](#_dx6cztegppuh)

[Prerequisites](#_u1vn4r9bnuo)

[Project](#_2do9osl4d0yu)

[PubSub API Enablement](#_pyfswduzt2pa)

[Requirements](#_lmhp63ygc8cg)

[Pubsub Topic](#_n2togmmey7hk)

[Pubsub Subscription](#_hb2q9tfl1uw5)

[Highlights from User Story](#_uxpqwmd9mjlb)

[Terraform Provisioning](#_aoa8kepl6u6t)

[Service Account](#_86yvw05y980u)

# Summary

The goal of this document is to define the necessary input parameters for enabling Pubsub service for each environment in AMEX’s Google Cloud Platform Setup.

# Prerequisites

### Project

A GCP project to host PubSub Topic and Subscription

### PubSub API Enablement

PubSub API to enabled as a pre-requisite for using the service

# 

# Requirements

Following are the parameters which are taken as inputs in the terraform code for provisioning the Pubsub resources. The parameters are divided as mandatory and optional. The optional parameters give us the levers for granular configurations.

### Pubsub Topic

Configurable parameters for creating a pub sub topic. The following arguments are supported:

Refer: <https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/pubsub_topic>

|  |  |  |  |
| --- | --- | --- | --- |
| Input | Description | Recommendation | Comments/Action Point |
| Name (mandatory) | Name of the topic | <App>-<Env>-<ID>-topic | To be shared by Amex |
| Labels (optional) | A set of key/value label pairs to assign to this Topic | App: Test1  Env: E1  Owner: John | Already shared by Amex |
| message\_storage\_policy(Enforced by Sentinel Policy) | Policy constraining the set of Google Cloud Platform regions where messages published to the topic may be stored. | A list of IDs of GCP regions where messages that are published to the topic may be persisted in storage  us-east4 | US-central1 has to be included ?  Open for clarification from Cloud Engg. |
| Schema (Enforced by Sentinel Policy) | Settings for validating messages published against a schema | Json format of the incoming messages | Open for clarification from App team  Keep it as optional. App teams are not planning to use it at this time |
| Message\_retention\_duration (Enforced by Sentinel Policy) | Indicates the minimum duration to retain a message after it is published to the topic. If this field is set, messages published to the topic in the last messageRetentionDuration are always available to subscribers. | For instance, it allows any attached subscription to seek a timestamp that is up to messageRetentionDuration in the past.  Cannot be more than 7 days or less than 10 minutes. | Open for clarification from App team  MessageRetention is required. It varies from app to app so it should be different value for each topic. Default of 7 days should be setup if not mentioned |
| encoding(Enforced by Sentinel Policy) | Schema Encoding | The encoding of messages validated against schema. Default value is ENCODING\_UNSPECIFIED. Possible values are ENCODING\_UNSPECIFIED, JSON, and BINARY. | Open for clarification from App team  Keep it configurable - ENCODING\_UNSPECIFIED can be a default option |

### Pubsub Subscription

Configurable parameters for creating a pub sub subscription. The following arguments are supported:

Refer: <https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/pubsub_subscription>

|  |  |  |  |
| --- | --- | --- | --- |
| Input | Description | Example | Comments |
| Name (Mandatory) | Name of the subscription | <App>-<Env>-<ID>-topic-<sub> | Nomenclature of topic name required  Already shared |
| Labels (optional) | A set of key/value label pairs to assign to this Subscription | App: Test1  Env: E1  Owner: John | Already shared |
| Topic (Mandatory) | A reference to a Topic resource | Topic ID |  |
| Expiration\_policy  (Optional) | A policy that specifies the conditions for this subscription's expiration. A subscription is considered active as long as any connected subscriber is successfully consuming messages from the subscription or is issuing operations on the subscription. | If expirationPolicy is not set, a default policy with ttl of 31 days will be used. If it is set but ttl is "", the resource never expires. The minimum allowed value for expirationPolicy.ttl is 1 day. | Open for clarification from App team  Keep it configurable – if there is no cost associated with keeping subscriptions, default it to never expire |
| Dead\_letter\_policy (Enforced by Sentinel Policy) | A policy that specifies the conditions for dead lettering messages in this subscription |  | No Action |
| Dead\_letter\_topic (Enforced by Sentinel Policy) | The name of the topic to which dead letter messages should be published |  | Naming Convention |
| Max\_delivery\_attempts (Optional) | The maximum number of delivery attempts for any message. | The value must be between 5 and 100. | Open for clarification from App team  5 should be fine for most of the usecases. |
| enable\_message\_ordering(optional) | If true, messages published with the same orderingKey in PubsubMessage will be delivered to the subscribers in the order in which they are received by the Pub/Sub system |  | Open for clarification from App team  Keep it configurable – keep default as False |
| Ack\_deadline\_seconds (optional) | This value is the maximum time after a subscriber receives a message before the subscriber should acknowledge the message | Default 10 seconds | Open for clarification from App team  Keep it configurable – Keep the default as 10 sec |

## 

## Highlights from User Story

Below are the high level needs and additional technical needs are scripted in comments section

1. Topics/messages must be limited to: us-east4 or us-central1
2. Topics must not be publicly accessible
3. Push Subscriptions are disallowed
4. All publishers and subscribers must only interact with topics within the same service perimeter – We need ability to have topics shared across projects
5. Dead-letter topics must reside within the same project as the subscriber
6. AXP-created schemas can only be used within the AXP organization it was created
7. Topic-level message encryption must use Google-managed keys
8. HTTP endpoints are disallowed
9. Pub/Sub Lite is disallowed

Note: The above mentioned highlights correspond to all environments (E1,E2,E3). To be confirmed by Amex.

Refer: <https://jira.aexp.com/jira/browse/CENGBD-584>

## Labeling Details

Labels marked as required are listed below:

1. aexp-app-env
2. aexp-data-classification
3. aexp-data-classification
4. aexp-app-carid
5. aexp-app-name
6. aexp-app-tier
7. aexp-ops-supportgroup
8. aexp-app-supportgroup
9. aexp-lifecycle-changenumber

# Access Management

Terraform Service Account: The service account to be used for provisioning the Pubsub code should have the following permissions

* roles/pubsub.admin

Roles to be used for publishing messages to the Topic

* roles/pubsub.publisher

Role to be used for consuming messages

* roles/pubsub.subscriber

Note: As per the definition of personas which will be used for Pubsub service

* Admin (roles/pubsub.admin): To be used by the Platform engineering team.
* User(roles/pubsub.publish & roles/pubsub.subscriber): to be used by users; developers, analytical users