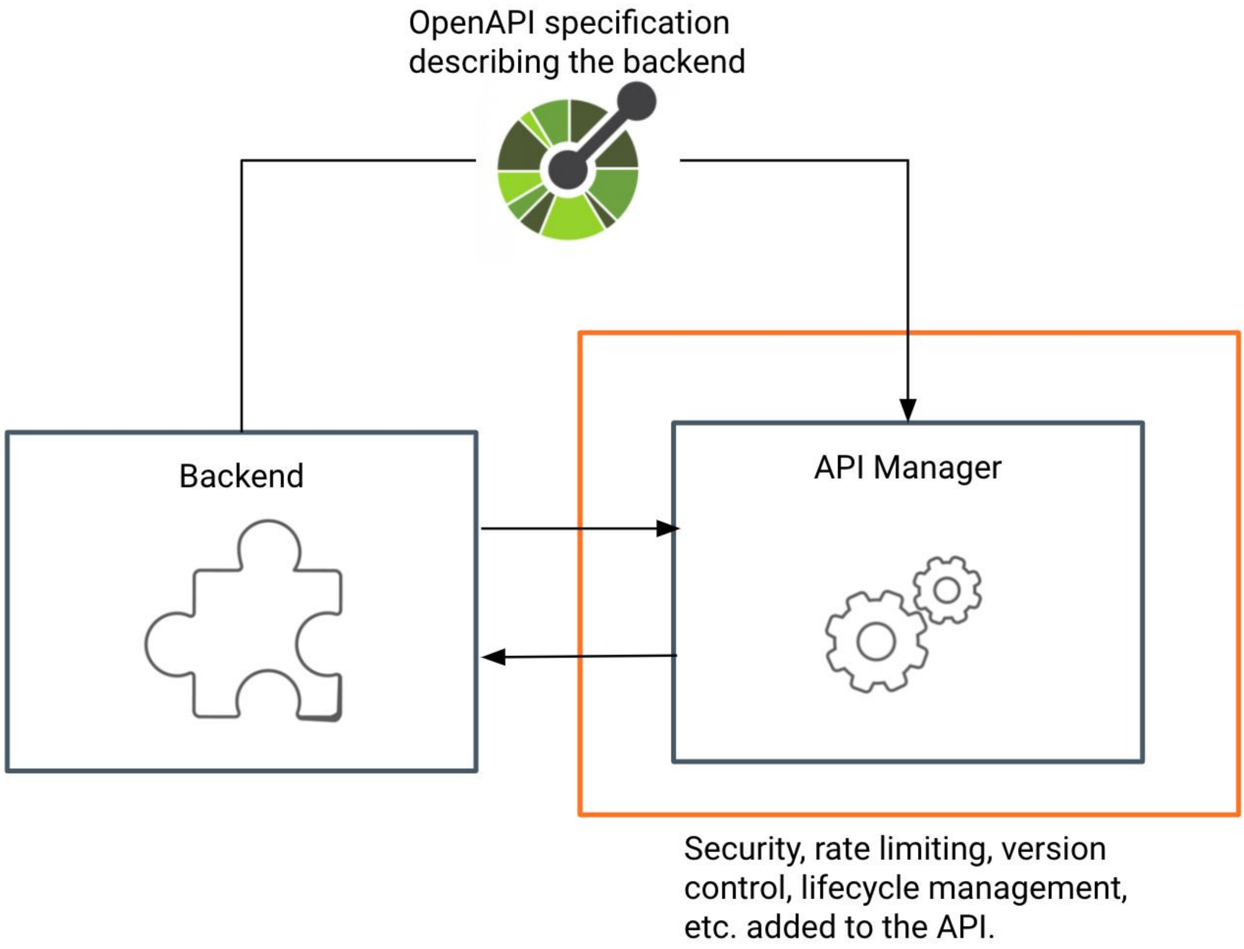
Create REST API

User story

Coltrain is one of the railway companies that is partnered up with GOGO Train to provide better service to their customers. Coltrain already has some internally managed APIs deployed in-house and these are managed by their internal development team. One of the APIs is a train schedule retrieval API, which is intended for the public community to get the Coltrain schedules. Currently, this API is exposed to the public and the Coltrain development team faces challenges in maintaining and handling the high load for the API.

By exposing this API through WSO2 API Manager, Coltrain expects to get the full benefits of an API Management solution such as API lifecycle management, security, rate limiting, etc. and decouple the maintenance overhead from the internal teams.

WSO2 API manager provides capability to import OAS definitions and create the API using that.

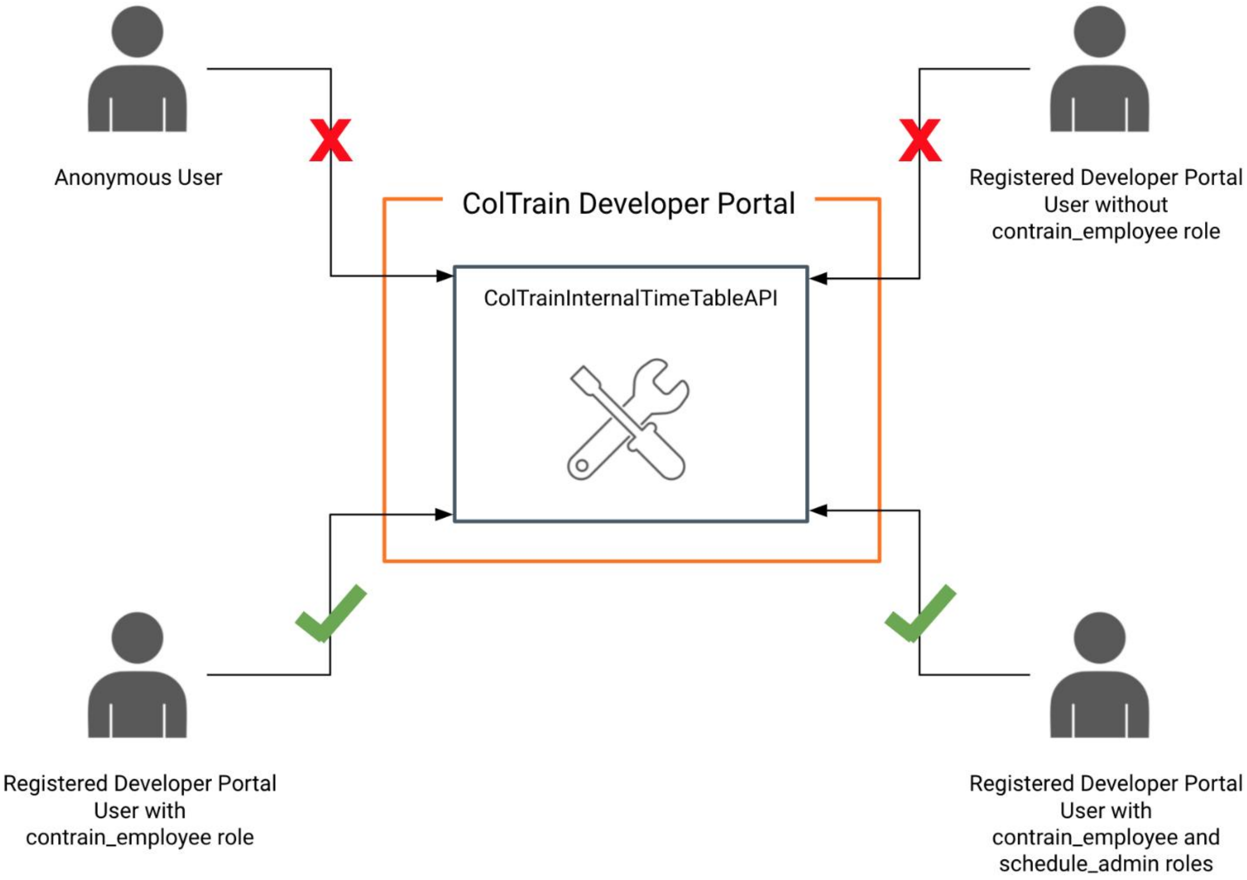


Engage Access Control to the API

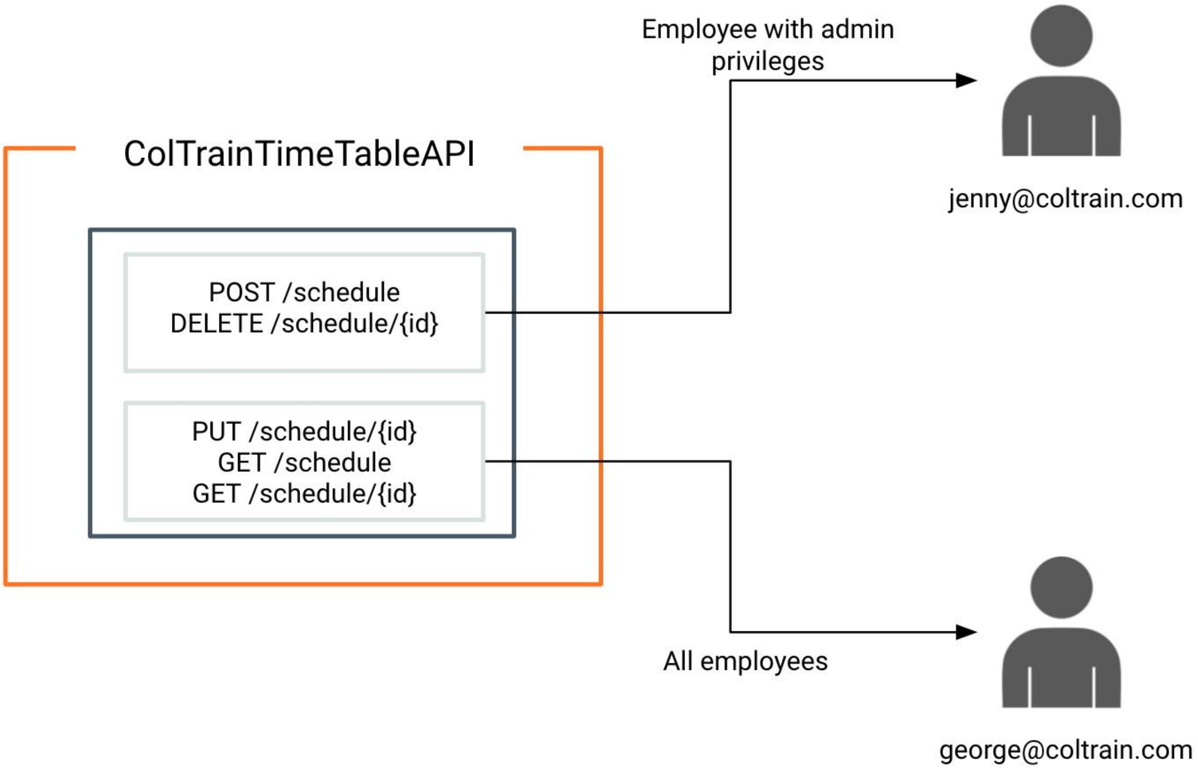
User Story

ColTrain has a separate API to manage schedules for their internal staff. This API needs to have more elevated permission levels to access than their public API. All the employees in the ColTrain company have access to the end-user application where they can view the train schedule details using this API. All the staff in the ColTrain should be able to check the available schedules whereas only the staff with admin privileges can add, edit or remove the existing schedule. Any other registered or public user should not be able to view this API since it is there for internal tasks. Coltrain wants to have a clear separation on who can view and access their APIs. They have identified that it would be a cumbersome task If they are to implement this from scratch to their backend APIs directly. Since now they are using an API Management platform, they wanted to move all these authentication and authorization tasks out of their internal APIs. This would be beneficial for their internal teams because they only have to pay attention to their APIs business logic only.

We could configure the API to be visible for a set of users. For example, this API should be visible for only Developer Portal users with **coltrain_employee** role only.


Anonymous User
Registered Developer Portal User without contrain_employee role
ColTrain Developer Portal
ColTrainInternalTimeTableAPI
Registered Developer Portal User with contrain_employee role
Registered Developer Portal User with contrain_employee and schedule_admin roles

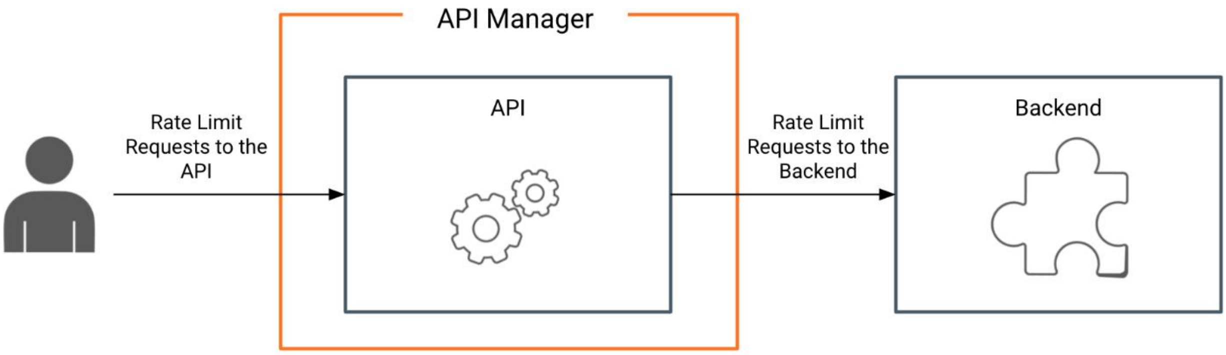
Also WSO2 API Manager provides capability to provide access control to the resources of the API by using OAuth2 scopes. Requests containing access tokens with the correct scope will be able to access these resources.



Rate Limiting

User story

While analyzing the traffic patterns and data, the GOGO DevOps team noticed that their backend is receiving a high number of requests and due to these high demand, their latency numbers also increased. The DevOps team did some performance tests on their user info backend and identified that their backend service can handle a maximum of 1000 TPS. So GOGO management decided to introduce rate limiting to manage their free users.


API Manager
Rate Limit Requests to the API
API
Rate Limit Requests to the Backend
Backend