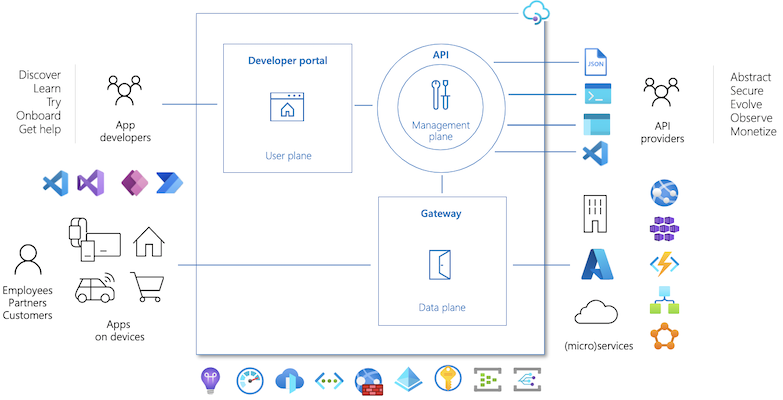
**Azure API Management**

**With Azure KeyVault**

# What is exactly API Management Service?

Azure API Management is made up of an API gateway, a management plane, and a developer portal. These components are Azure-hosted and fully managed by default. API Management is available in various tiers differing in capacity and features.  
[View different pricing tiers](https://azure.microsoft.com/en-us/pricing/details/api-management/)

****

## API Gateway component-

* All requests from client applications first reach the API gateway, which then forwards them to respective backend services.
* The gateway enables consistent configuration of routing, security, throttling, caching, and observability.
* Acts as a facade to backend services by accepting API calls and routing them to appropriate backends
* Optionally transforms requests and responses as specified in policy statements
* If configured, caches responses to improve response latency and minimize the load on backend services

[View Managed VS Self-hosted Gateway features](https://learn.microsoft.com/en-us/azure/api-management/api-management-gateways-overview#feature-comparison-managed-versus-self-hosted-gateways)

## 

## What are Policies in API Management? -

With policies, an API publisher can change the behavior of an API through configuration. Policies are a collection of statements that are executed sequentially on the request or response of an API.

Policies can be applied at different scopes, depending on your needs: global (all APIs), a product, a specific API, or an API operation.

[How to configure policies at different scopes?](https://learn.microsoft.com/en-us/azure/api-management/set-edit-policies?tabs=form#configure-policies-at-different-scopes)

# ACTUAL REQUIREMENT

When we have any backend api, which is not secured using SSL certificate, how can we secure it using Azure API Management service?

For e.g. our backend is running on- **http://example.org/**

here in this backend we have multiple api paths configured, for e.g.-

**/api/v1/getUser**

**/api/v1/getPost**

**….**

**….**

**/api/v1/putUser**

We want to map that to **https://api.example.org/** with all the multiple api paths and all **GET, PUT, POST, DELETE** methods.

# 

# STEPS-

**Step 1-** Create SSL certificate for the subdomain/wildcard in **.pfx** format, can also use **Azure KeyVault** for generating or importing the SSL certificate.

**Step 2-**  Create **Azure API Management** Instance in any one of the pricing tier (mostly preferred **consumption tier**).

# 

# 

# Once API Management is created add a CNAME record from api.example.com to somedomain.azure-api.net.

Here in below example API Gateway URL is api-management-sa.azire-api.net-

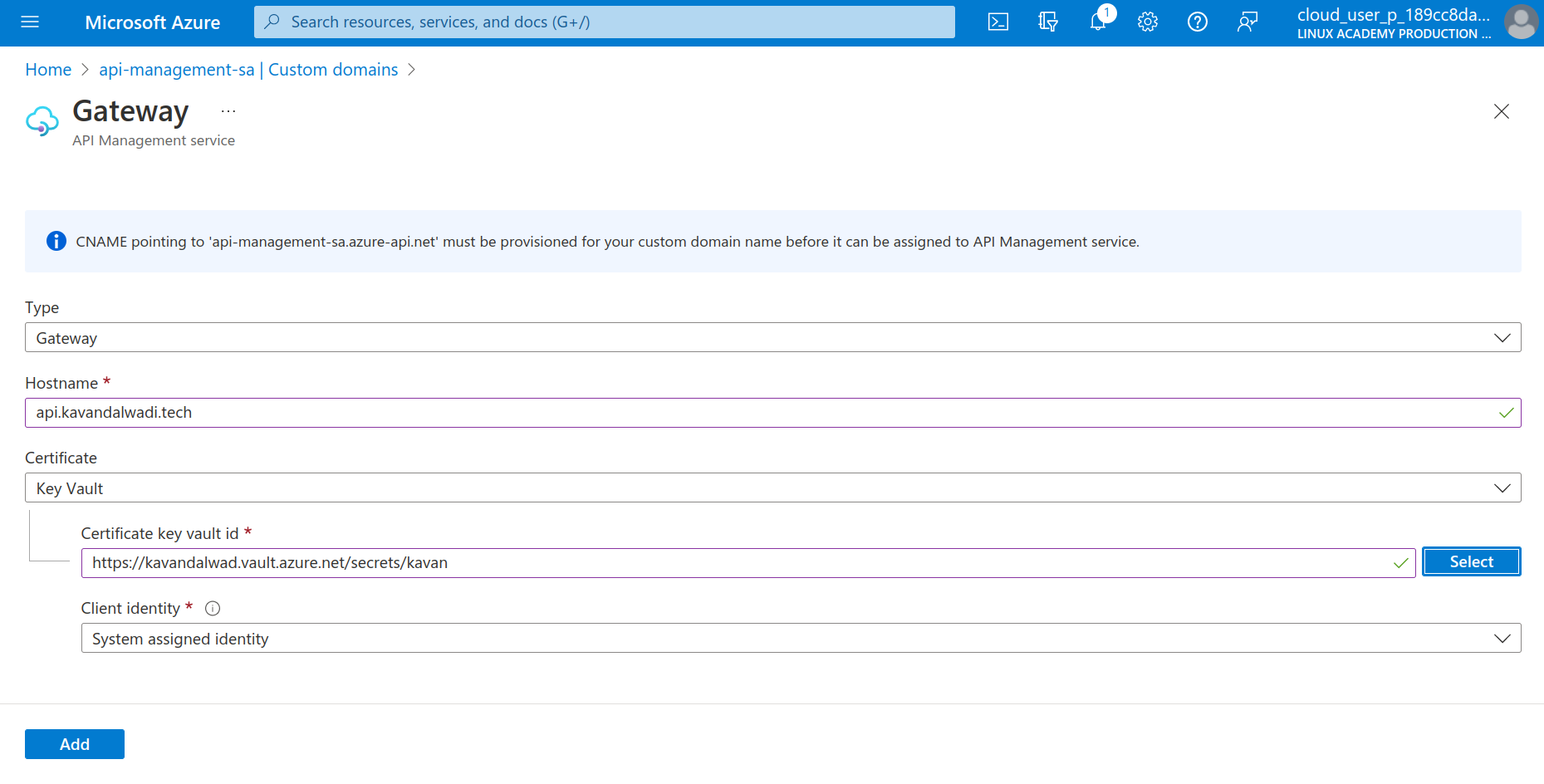
# 

# Step 3- Add custom domain in API Management from KeyVault.

# Go to Custom domains from left side panel, click on +Add.

# 

Add subdomain which we want to create and add SSL certificate from KeyVault

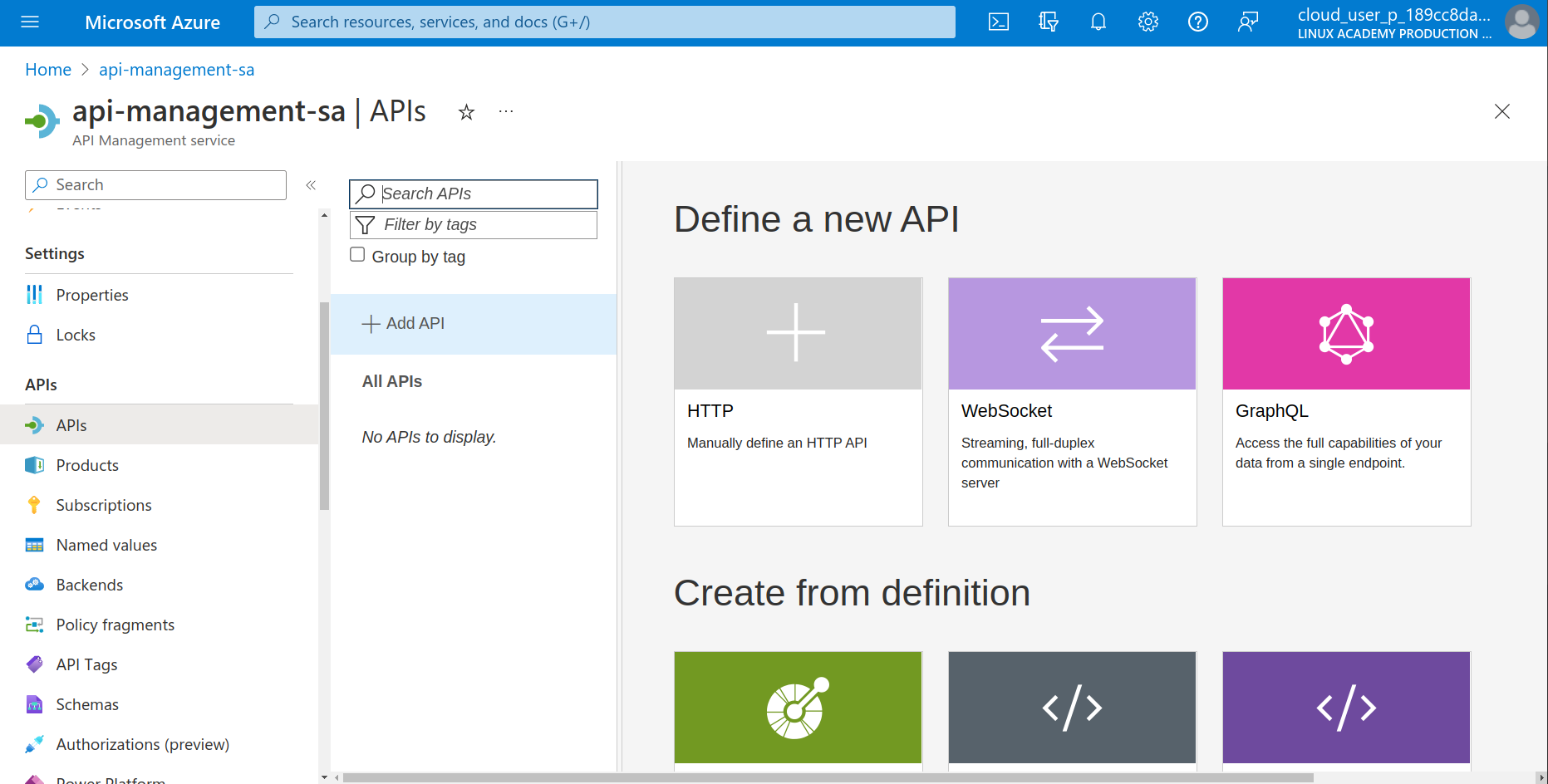


Click on Add, then Save the configuration.

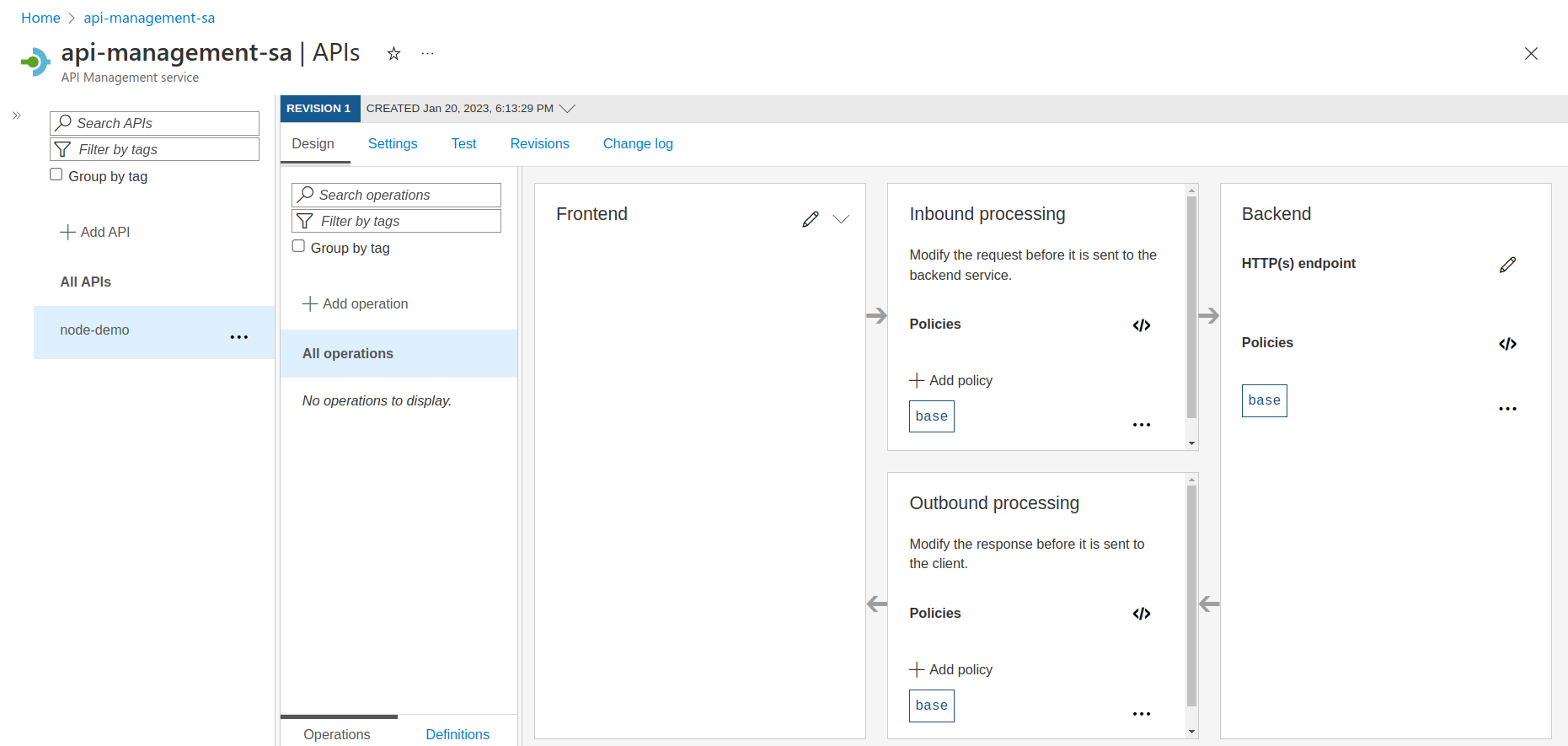
Once the custom domain is saved you can check the API Gateway endpoint it will be switched to your subdomain-

# 

# Create a HTTP api



Add the following policy in the All Operation-



<policies>

<inbound>

<set-backend-service base-url="http://api.example.org:8487/" />

<rewrite-uri template="/{path}/{path1}/{path2}" copy-unmatched-params="true" />

<base />

</inbound>

<backend>

<base />

</backend>

<outbound>

<base />

</outbound>

<on-error>

<base />

</on-error>

</policies>

Add all the required GET, PUT, POST, DELETE operation in the API as per requirements.