1. What are the responsibilities of Management Plane and Control Plane?

The Management Plane is where API creation and API management takes place. It consists of portals (Publisher, Developer Portal, Admin Portal) for users to

- create and manage APIs
- implement rate limiting policies
- monitor, and monetization, etc.
- It also provides a set of APIs to interact with external tools like API Controller.
- It includes API Analytics dashboards, displaying various business insights.

The Control Plane is where

- · the API security validation
- · API key generation and
- rate limiting decisions are taken.

2. Which component is responsible for Generating the Access Token?

WSO2 API Manager's key manager component is responsible for handling token-related operations

3. Which components are involved in defining new Throttling Policies and applying them?

Traffic Manager component under Control Plane is involved in defining new Throttling Policies. WSO2 API Manager admins can add new throttling policies and define extra properties to the throttling policies.

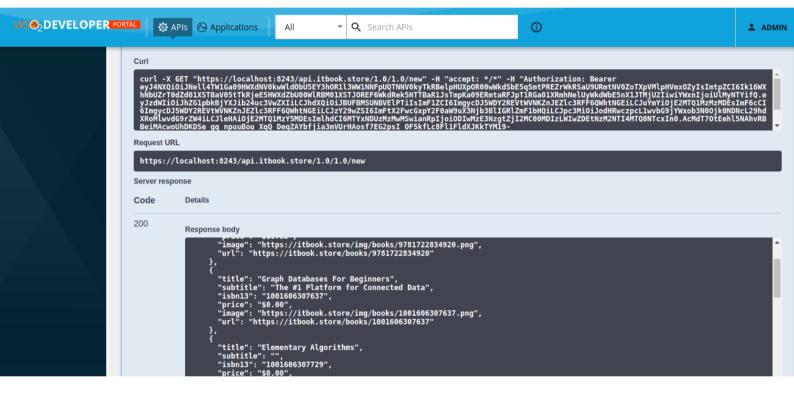
4. What is an "Application" in the Developer Portal? What is the use case of it?

An Application is the **logical representation** of a physical application such as a mobile app, web app, device, etc. For an application to use an API, the application should subscribe to the relevant APIs it intends to use. A

subscription to an API happens over a selected business plan, which determines the usage quota the application gets. An application has a consumer-key and a consumer-secret, which acts as the credentials of the application.

5. Work on Question 3 at here:

https://novigi.atlassian.net/wiki/spaces/TMI/pages/1754136738/WSO2
<a href="https://novigi.atlassian.net/wiki/spaces/TMI/pages/TMI/pages/TMI/pages/TMI/pa



Sample curl:-

curl --insecure -X GET "https://localhost:8243/api.itbook.store/1.0/1.0/new" -H "accept: */*" -H "Authorization: Bearer

eyJ4NXQiOiJNell4TW1Ga09HWXdNV0kwWldObU5EY3hOR1l3WW1NNFpUQTNNV0kyTkRBelpHUXpOR 00wWkdSbE5qSmtPREZrWkRSaU9URmtNV0ZoTXpVMlpHVmxOZyIsImtpZCI6Ik16WXhNbUZrT0dZd01 XSTBaV05tTkRjeE5HWXdZbU00WlRBM01XSTJOREF6WkdRek5HTTBaR1JsTmpKa09ERmtaRFJpT1RGa 01XRmhNelUyWkdWbE5nX1JTMjU2IiwiYWxnIjoiUlMyNTYifQ.eyJzdWliOiJhZG1pbkBjYXJib24uc3VwZXIi LCJhdXQiOiJBUFBMSUNBVElPTilsImF1ZCI6InJYemhwUk5ZUnBFVkh5ZlA5bjZXSlBmVmU3RWEiLCJuY mYiOjE2MTQ1MzcxNzksImF6cCI6InJYemhwUk5ZUnBFVkh5ZlA5bjZXSlBmVmU3RWEiLCJzY29wZSI6Im FtX2FwcGxpY2F0aW9uX3Njb3BlIGRlZmF1bHQiLCJpc3MiOiJodHRwczpcL1wvbG9jYWxob3N0Ojk0NDN cL29hdXRoMlwvdG9rZW4iLCJleHAiOjE2MTQ1NDA3NzksImlhdCI6MTYxNDUzNzE3OSwianRpIjoiYzJhM 2JhNjMtY2JlNy00YmE5LWE0NmYtNDRkOGJiMGVlYjMzIn0.CiOUHGumljQQj0h29lkUT_8BqLwTczrin0c Wxh0t2-cloIG1Ozs8D2hm4GqVpJCOtwXkFkVSYHCj9xwg4111pfsia1YWUXGap0k9m3v8cc0ig3TCLs-90vKqMUQqCPcPAOd80UPL3Z_4K80LoYbcFFeIk4LGUgVv1skRtxnVmxWExca_VnEob-HxkYwPrR-r9pHlTPJDyr83u2ugmei8R99I2PMKksgcAJAnaDuf-

6. What is an "API Product" in API Manager Publisher? What is the use-case of it?

API Product is a combination of resources from one or more available APIs. An API product allows API product managers to mix and match resources from the available APIs. Similar to using an API, an application that intends to use an API product needs to subscribe to the APIs under a selected business plan. An application that subscribes to an API product gets access to all of its resources, which belongs to one or more of the APIs that are used to create the API product.

7. In API Manager, at which levels you can apply throttling policies?

It is possible to throttle requests for each tier based on the request count per unit time or the amount of data (bandwidth) transferred through the Gateway per unit time

different levels of throttling are as follows:

- •Subscription-level throttling (API publisher))
 - **Burst Control**
- •Subscription-level throttling (API subscriber)
- Advanced throttling (API publisher)

API level throttling

Resource-level (Operation-level) Throttling

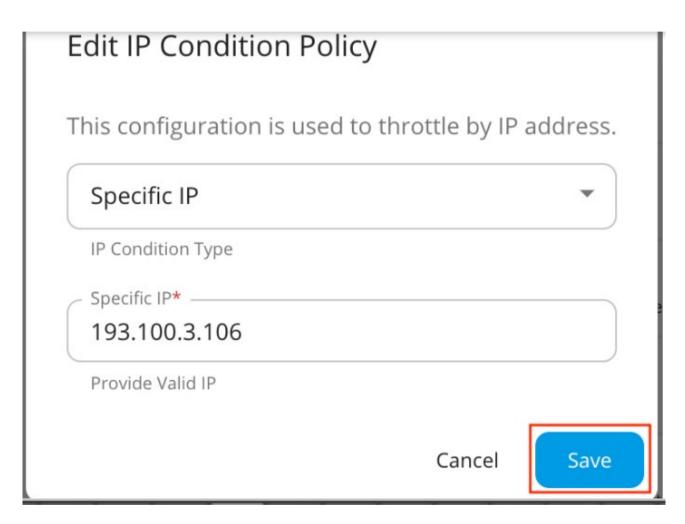
Advanced Throttling tiers

• Application-level throttling (application developer)

Application-level Throttling tiers

8. How can you apply a throttling policy to a range of IP addresses, on accessing an API?

we can control/restrict access to our API or its selected resources for a given IP address or address range. For example, if we need to grant permission for internal applications to consume a larger quota of our API resource than our external consumers, we can define an advanced policy with higher limits for our internal IP address range and lower limits for the rest.



9. How can you block API requests coming from an IP address?

By blacklisting requests, we can Block requests coming from a specific IP address.

To blacklist a request,

- 1.Log in to the Admin Portal using the URL https://localhost:9443/admin and our admin credentials.
- 2.Click Black List under the Throttle Policies section and click Add Item.
- 3. Select the item to black list, enter a value and click **Blacklist**.

10. What is an "API Handler"? How can you engage an new custom handler to an API (mention important steps)

An **API Handler** allows a message to be processed before passing it to the routing logic of the API Gateway. A handler allows the processing of both request and response messages.

Handlers can be used for

- security validation
- policy enforcement
- pushing out events to third party systems
- custom logging requirements, etc.

Engaging the custom handler

- 1.Build the custom authenticaor code created/downloaded previously, and copy the resulting jar to <APIM_HOME>/repository/components/lib directory
- 2.Engage the custom handler using the API template. To engage a custom handler to APIs, we need to add the custom handler with its logic in the <APIM_HOME>/repository/resources/api_templates/velocity_template.xm l file.
- 3. Restart the API Manager server.