1. Explain the purpose and features on API Manager in Anypoint platform?

* It is used to implement non functional requirements
* The features f API manager are :
  + Unlock applications, data, and microservices with an API gateway
  + Apply prebuilt or custom security policies at runtime with no downtime
  + Proxy existing SOAP services or create new APIs from OAS and RAML definitions
  + Provision access across individual clients or entire teams with OAuth and SAML
  + Use a service mesh to secure and govern microservices — regardless of where they're hosted
  + Gain insight into the performance of APIs, track usage, and identify errors

1. Explain API Groups and what is the purpose of creating them?

API Groups is packaging a set of APIs

Purpose:

* enables you to bundle your APIs and resources to solve specific user needs.
* When you create an API Group, you can customize instances of that group with different SLAs and rate limit conditions based on the problem the instance must solve. You can then publish the API Group to Anypoint Exchange so that users can subscribe to the package.
* You can package different sets of APIs to target different consumers' requirements.
* API consumers can access a collection of related APIs instead of individual APIs, simplifying asset discovery for specific purpose example weather APIs.
* API Groups can enforce governance using SLA plans that can be modified with a single click.

Note:

You create an API Group for a specific organization and environment. API Groups are versioned, like the APIs contained within them, to more easily incorporate updates

<https://docs.mulesoft.com/api-manager/2.x/api-groups-landing-page#how-api-groups-works>

1. Name and explain available Policy Types in Mule?

The different types of policies available in Mule are default, custom, or automated policies, and each has its own scope, management, and usability

* **Default Policies**: MuleSoft provides several ready-to-use policies for areas such as authentication, security management, threat protection, and tokenization. Using the API Manager from Anypoint Platform, you can apply any of these policies to any of your API endpoints.
* **Custom Policies**: custom policy is used to meet your specific business needs. You can either customize an existing policy, or you can create an entirely new custom policy. These policies are categorized as either online or offline.
  + Online custom policy: Online Custom policies are applied and managed by API Manager, which is the default and recommended way to apply policies. Online policies enable you to manage the policy lifecycle by leveraging Anypoint Platform. This way, the applied policies are always in sync with API Manager, and are protected by the gatekeeper mechanism at startup.
  + Offline custom policy: Offline custom policies are applied directly to the runtime and managed manually. Because they can easily become out of sync with API Manager, using this type of policy is not recommended.

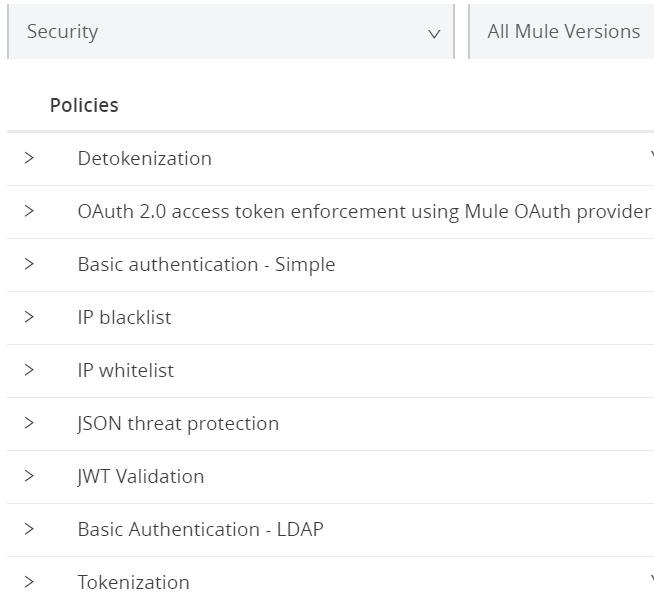
Offline custom policies are not protected by the Gatekeeper mechanism at startup. Additionally, client credentials validation is also not supported in offline policies.

* **Automated Policies**: You can apply any default or a custom policy to all the APIs in your environment, making that policy an automated policy. However, you require specific access, such as API Manager Environment Administrator, to create automated policies.

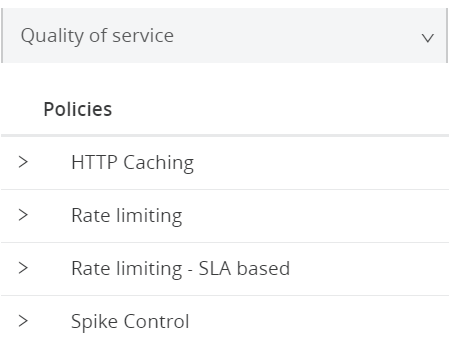
1. List the Policy categories with examples of policies belonging to each group?

There are different types of polies available in mule which are categorized as:

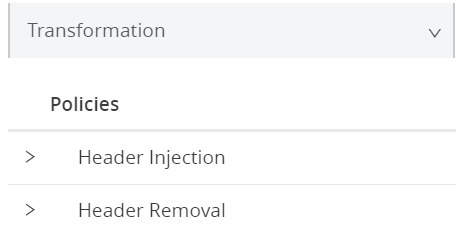
* Security



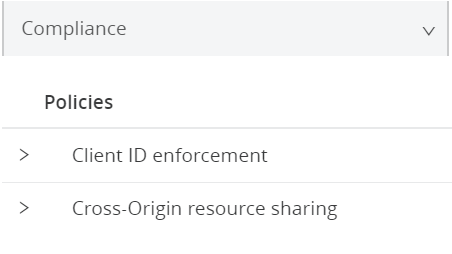
* QoS



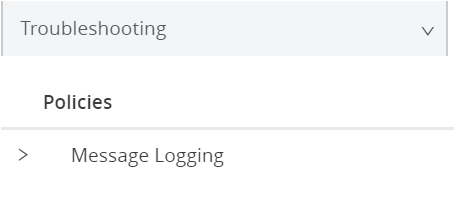
* Transformation



* Compliance



* Troubleshoot



1. Explain with examples Mule default and Custom policies?

Mule **default polices** are the out of box policy. Examples of such policy are IP Black List, IP White List, Oauth 2.0

**Custom Policies** are policies that anyone can develop and apply to their APIs, with the intention of extending existing functionality or defining new ones.

**Step to create a custome policy are:**

1. Develop the policy.
2. Package the policy.
3. Upload the resulting policy assets to Exchange.
4. Apply the policy to any API through API Manager.
5. Why should one add Rate Limiting to an API?

Rate Limiting Policy is used to impose limits on the number of requests that each application can make within a period of time

It improve the QoS by improving the availability of the API and avoid resource starvation

1. Explain Resource level policies?

Resource level policies are applied at a resource level which affects all HTTP methods (eg PUT, GET, POST), or selected HTTP methods, within the resource.

The uses for resource level policies are limited mainly by your imagination. Here are a few possibilities:

* Applying policies to specific resources
* Securing a subset of an API
* Setting different limits on resources

1. Difference between IP Whitelist and IP Blacklist? How can IP Whitelist be done in Mule API?

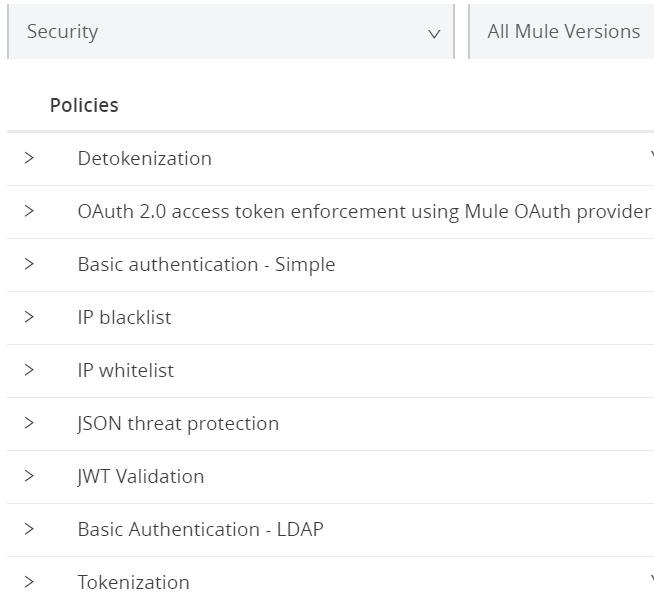
**IP Blacklist**

* The IP Blacklist policy controls access to a configured API endpoint from a single IP address or a range of IP addresses.
* The IP Blacklist policy restricts access to a protected resource when a match is found between a source IP (specified when configuring the policy) and a list of individual IPs or range of IPs.

**IP Whitelist policy**

* The IP Whitelist policy allows a list or a range of specified IP addresses to access a configured API endpoint.
* The IP Whitelist policy allows access to a protected resource when a match is found between a source IP (specified when configuring the policy) and a list of individual IPs or range of IPs.

1. What are the various methods of securing a MuleSoft API?



1. Explain Basic Authentication?

The Simple Authentication policy protects an API by forcing applications to provide a

username and password when making requests. This policy is available only in Mule 4 or

later.

1. Explain Detokenization policy?

Detokenization is the process of returning the previously masked sensitive data back into its original value to reduce the risk of compromising sensitive information.

1. What do you understand about the Environment in API manager?

Anypoint Platform enables you to create and manage separate deployment

environments for APIs and applications. These environments are independent from

each other and enable you to test your applications under the same conditions as

your production environment.

The API Manager Environment Administration permission allows you to do the

following things:

* + - * Create and modify your APIs as well as modifying those created by others
      * Apply policies
      * Define SLAs
      * Create alert

1. How to grant permission to a user?

To grant environment permissions to roles from API Manager:

1. **Click Access Management** > **Users** > **a user to give permissions** > **API Manager** > Permissions.
2. Select the permissions for the user and click blue plus icon to save the permissions:

https://docs.mulesoft.com/api-manager/2.x/environment-permission-task

1. Explain SLA Tier and how to enforce them on an API?

A Service Level Access (SLA) tier is a category of user access that you define for an API. The tier definition combined with an SLA-based policy determines whether access to the API at a certain level requires your approval. The tier definition also can limit the number of requests an application can make to the API. To enforce SLA tiers, you need to apply a rate-limiting or throttling policy that is SLA-based.

To define SLA tiers for an API version or to manage applications that request access to specific tiers, you need to set the API URL.

1. Explain features of API Analytics?

It is used to get real-time insights with prebuilt or custom dashboards and see how consumers are using your APIs, including the date, location, application, and platform type. Use the data to perform trend analysis and understand usage patterns

Features,

* Get real-time insights into API performance, usage, and errors
* Create and manage custom dashboards and charts
* Provide metrics to your API consumers
* Identify and analyze the root cause of errors

1. How to set up notifications for APIs in Anypoint platform? Explain the triggering points for Alerts to be generated?

An API alert is an alarm that flags one of the following problems:

* The API request violates a policy.
* Requests received by the API exceed a given number within a period of time.
* The API returns a specified HTTP error code.
* The API response time exceeds a certain amount.

To add an API alert:

* + - 1. Navigate to API Manager &gt; API Administration and click the API instance for which you

1. want to add an alert.
2. From the left navigation pane, select Alerts &gt; Add alert.
3. Specify the alert options:

* Name: Type an alert name, for example trial-alert.
* Enabled: Accept the default option: Enabled. You can delete an alert anytime if not required.
* Severity: Select a severity for the alert, for example, Info.
* Alert type: Select the type of alert to create, (for example, Request Count) and provide appropriate alert configuration values

1. Explain the oAuth and its working?

* OAuth 2.0 is a industry standard protocol for authorization.
* It allows sharing of resources stored on one site to another site without using their credentials.
* To secure an API in Anypoint Platform using OAuth, following policies are recommended:
* OpenAM OAuth Token Enforcement policy
* PingFederate OAuth Token Enforcement policy
* OpenID Connect Access Token Enforcement Policy
* None of these token enforcement policies allow access to the OAuth 2.0 protected resources if credentials from non-Mule client applications are used.

**Working**

* The user or application requests an access token using any valid grant type
* defined in the client application.
* The user or application sends a request with the access token.
* The federated policy validates the access token, provided as a well-formed
* query param or authorization header.

 The federated policy validates the token against the OAuth provider. To

improve performance, Mule caches the call to the authorization server,

which is only performed once during the lifetime of the token. When OpenId,

PingFederate, or OAuth 2.0 Access Token Enforcement Using External

Provider policies are in effect and your API is deployed under Mule 4, the

client ID returned by the OAuth provider is validated by the Client Id

Enforcement policy.

1. What is Autodiscovery? how to enable Autodiscovery?

* Autodiscovery is managing an instance within API manager to a corresponding Mule Runtime
* It is the process of associating Mule Runtime with API manager
* Two ways to implement auto discovery
  + **Manually** in basic endpoint: It is used to implement policy within the implementation
  + **Automatic** in end point with proxy

1. Differentiate between basic endpoint and endpoint with proxy?

**basic endpoint**

* In this we configure policies with implementation
* How it works
  + API manager is in control plane
  + Then configure policies with control plane
  + When mule runtime starts, the polices that are configured in API Manager gets downloaded to runtime where mule application is running

**endpoint with proxy**

* In the we create a separate proxy application
* Here we deploy the proxy application in gateway server [ i.e. Mule Runtime]
* The policies are configured to control plane
* When the gateway server starts it downloads that policies into the gateway server
* If the request is validated by the implemented policies, then the request is forwarded to the implementation. In this case the implementation can be mule app or non- mule app

**Difference**

* Extra worker node is required to deploy Endpoint with Proxy
* Autodiscovery is manual in basic endpoint whereas it is automatic in endpoint with Proxy

1. What is a proxy?

Proxy act as a gateway between the client and actual application. I t&#39;s an intermediary server

separating end users from the websites they browse. Proxy servers provide varying levels of

functionality, security, and privacy depending on your use case, needs, or company policy

1. Differentiate between Gateway and proxy and their benefits?

* **Both** a proxy server and a gateway **route traffic from inside a network** to the Internet.
* **A gateway**, however, is more like **a door to get to the Internet**, while a **proxy** **server acts like** a **wall** that bars the inside of the network from being exposed to the Internet.
* A **proxy server filters which connection is** allowed, while a gateway doesn’t do any filtering.
* API gateway is the runtime where proxy applications were deployed. It acts as a gateway or entry point where the proxy applications acts as a shield for backend application deployed in Mule runtime server .

The **advantage** of using a proxy is having a layer of separation to ensure that any attacks against our actual backend API are stopped well before anyone interacts with our main mule standalone servers.