Preparing to deliver the workshop

Instructor requirements:

- Being very comfortable with 3scale both in terms of configuration and of operations. Knowing the basics of the Developer Portal
- Being comfortable with RH SSO and especially around OpenID Connect protocol
- Being able to use Postman (or similar REST client) to build REST request and REST authentication
- Having a basic knowledge of OpenShift

Attendees requirements:

- To use the GUI of OpenShift: https://docs.openshift.com/container-platform/3.11/architecture/infrastructure_components/web_console.html#browser-requirements
- Basic knowledge of REST protocol
- Basic knowledge of containers
- Basic understanding of OAuth social applications

Environment:
Environment reachable here:
https://tutorial-web-app-webapp.apps.openbanking-4f6a.openshiftworkshop.com/

End Users credentials:
user[1..100] / openshift

3scale dedicated instances here:
https://userX-admin.apps.openbanking-4f6a.openshiftworkshop.com
access using username and password
dedicated gateway
https://userX.amp.apps.openbanking-4f6a.openshiftworkshop.com

Duration and format

This is a workshop designed for approximately 2 hours delivery. The focus is on the adoption of the products to build a comprehensive financial solution. This is not an introduction to the different products used in the open banking solution portal, but it is focused on the modules and functionalities relevant for the FSI industry. Typically, instructors would talk through the introduction slides, and then for each hands-on lab, explain the steps needed to achieve the

objective of the lab calling on the main functionalities of the products. At the end of each activity there will be a checkpoint with the attendees.

Timeline

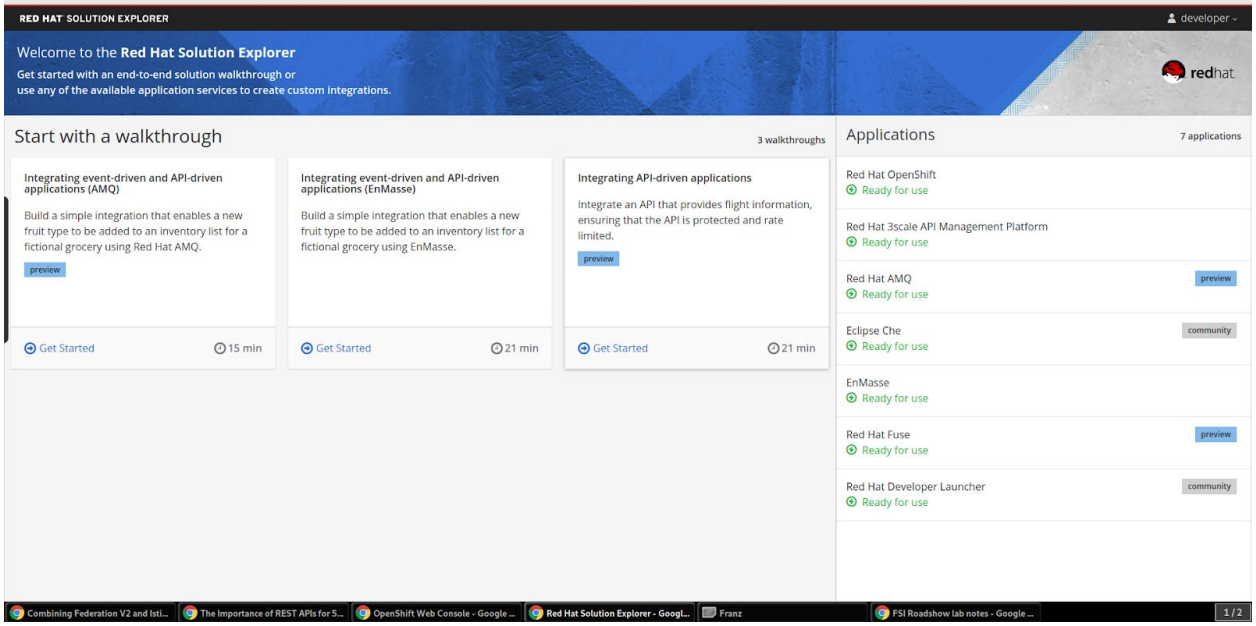
30 minutes	Architecture and key features
30 minutes	*Start of Practical Part 1* Financial Backend service demo and building blocks on Fuse Online [hands-on of the attendees in parallel]
25 minutes	Basics of Service Configuration and Integration in 3scale. Basics of Developer portal content publishing [hands-on of the attendees in parallel]
5 minutes	**CHECKPOINT**
15 minutes	**BREAK**
10 minutes	*Start of Practical Part 2* Introducing OIDC & OAuth [slides]
30 minutes	Basics of RH SSO and 3scale OIDC API authentication [hands-on of the attendees in parallel]
5 minutes	**CHECKPOINT**
10 minutes	(optional according to schedule) OpenShift high level walkthrough [simple demo]
5 minutes	**Q&A and closing**

Practical Part 1

Integr8ly

Login into the integr8ly environment main page

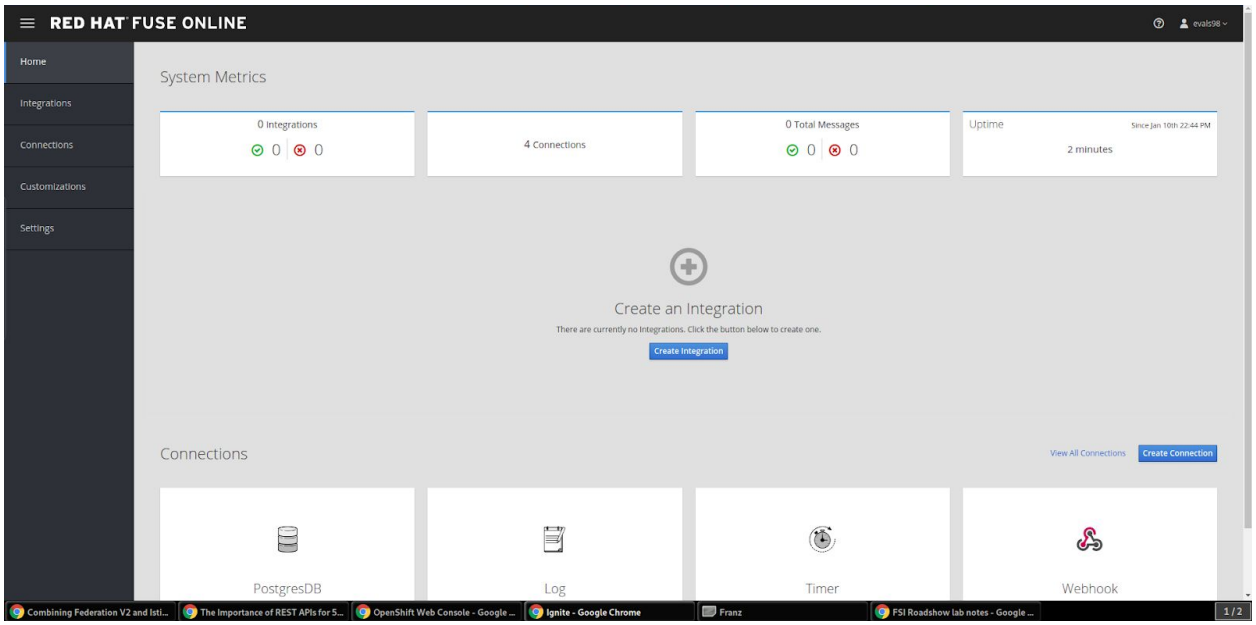
https://tutorial-web-app-webapp.apps.openbanking-4f6a.openshiftworkshop.com/



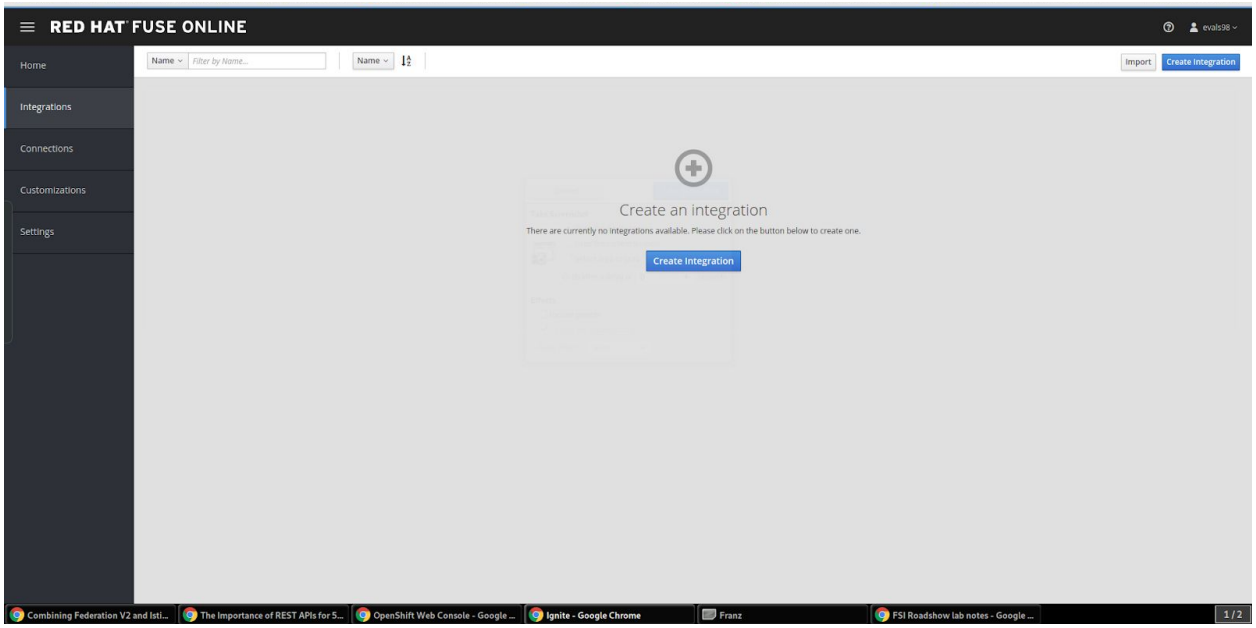
We will see how integr8ly environment works and what you get. It provides out of the box integration between products but it doesn't change the base product. You can still install this type of environment starting from a clean or empty OpenShift installation.

Fuse Online

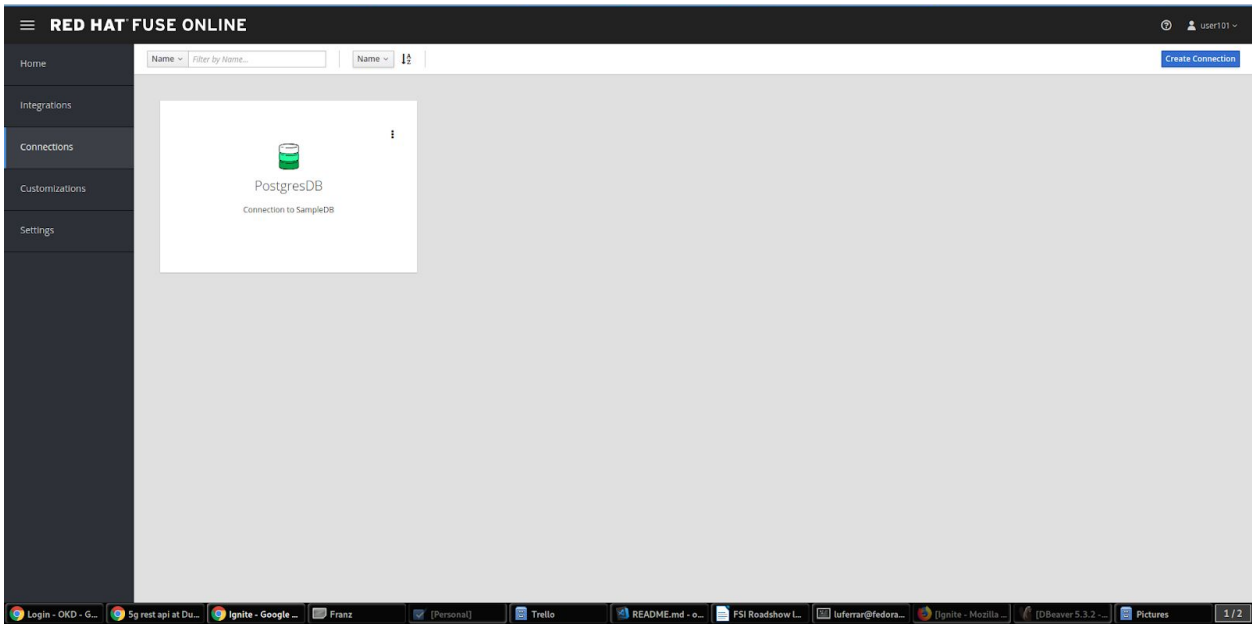
Let's start our first lab session, by opening Red Hat Fuse Online. We will see the main functionalities of it and then use it.



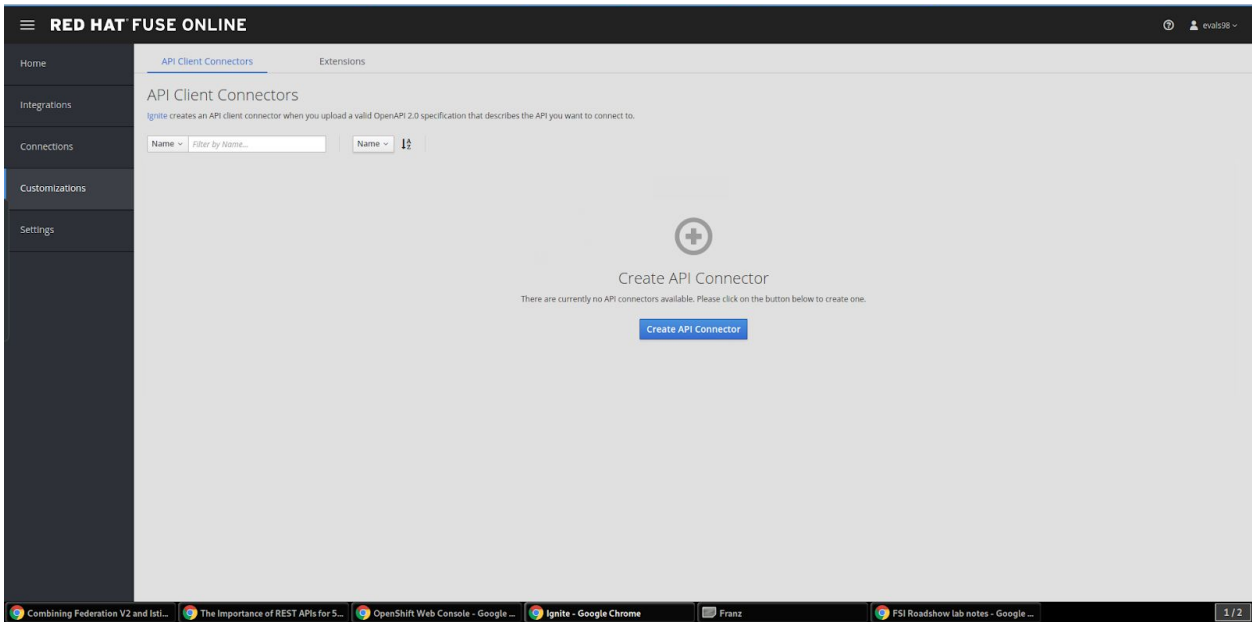
Explain the main dashboard, especially important when you then show messages coming from the request being sent.



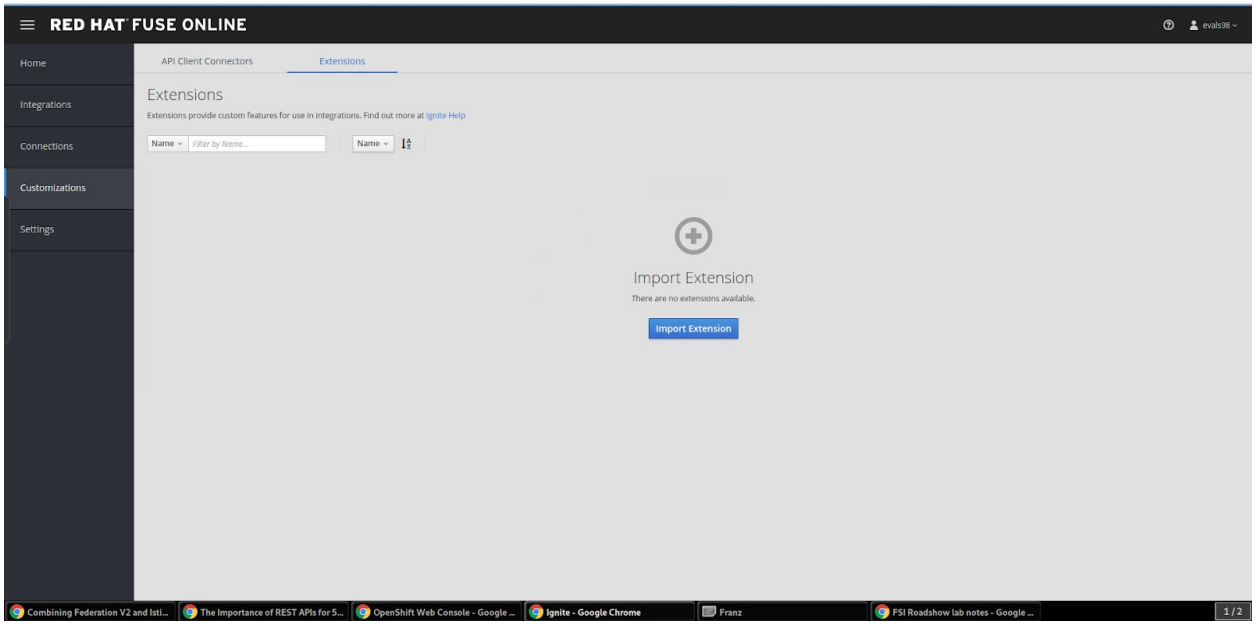
Explain the role of the integration window (seeing graphically the mediation/transformation) and the relevance for citizen developers. Little detour on what's behind the curtains (Camel) to reassure people that's not new technology but a well tested one and with 100s of possible connectors.



Connections section. Explain that you can start or end (or sometimes interpose) connections which are completely configured connectors. We will be showing the configuration of one connector during today's lab.
Various connectors are available and new connectors are coming in the future and will be ported onto Fuse Online. Make a couple of examples about possible integrations or mashups.



Customizations view. Explain the two panes available here, the first one dedicated to API connections, which we will be using afterwards as Connection in the Integration.



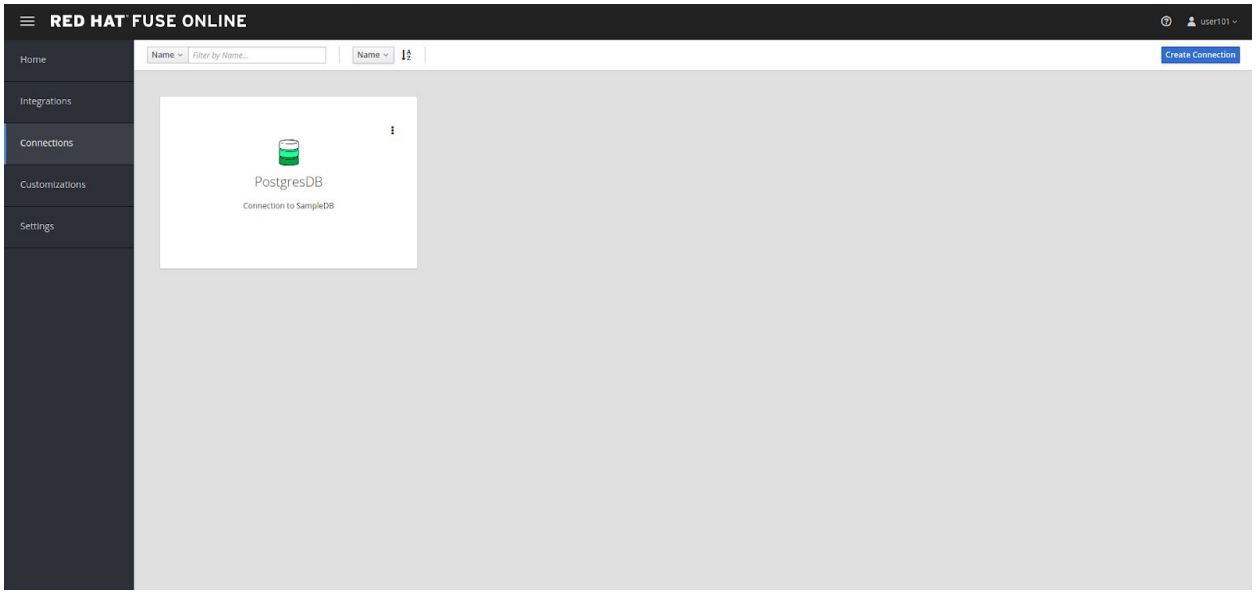
Extensions pane: this is the part where you can extend the functionalities of the platform. Ideally you would have prepared one compiled extension and you can import it to see how easy it is to add transformation functionalities to the product.

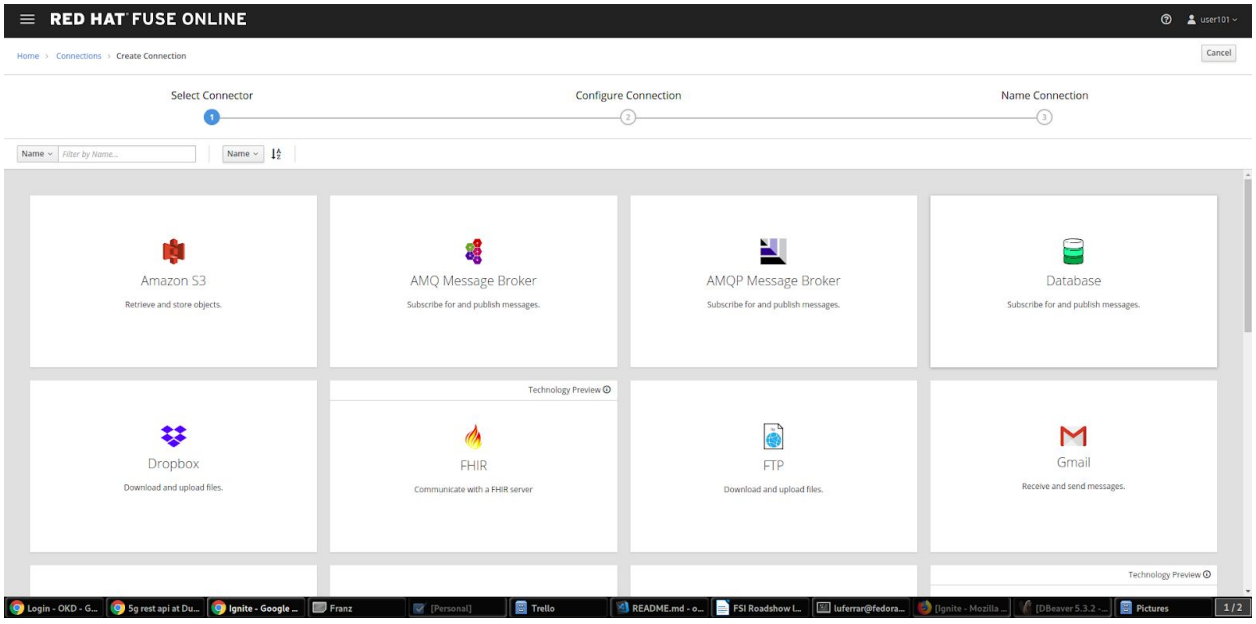
Let's start INTEGRATING now!

This first session will take us to the creation of a simple REST service from a database source. This is quite a common scenario and one that goes well for quick prototyping service scenarios. Let's start by creating the connection to an existing DB that I previously created. It is a DBaaS built on PostgreSQL and hosted on ElephantSQL. You could be running this anywhere else, as

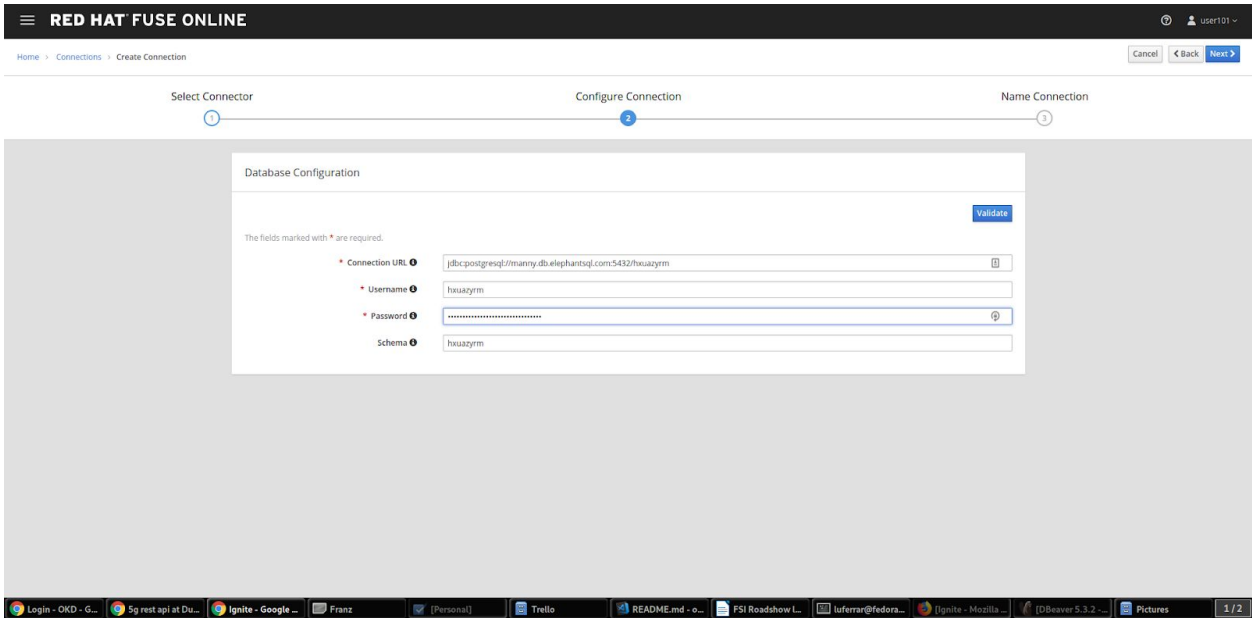
long as you have a public direct connection to the DB to use.

Create connection



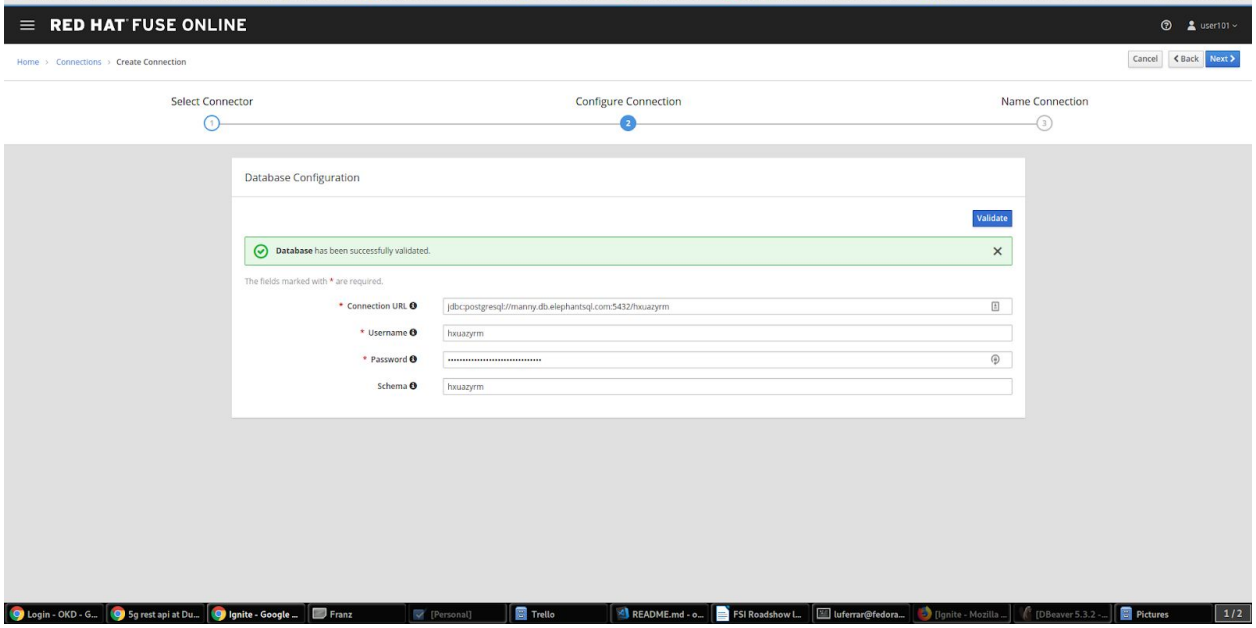


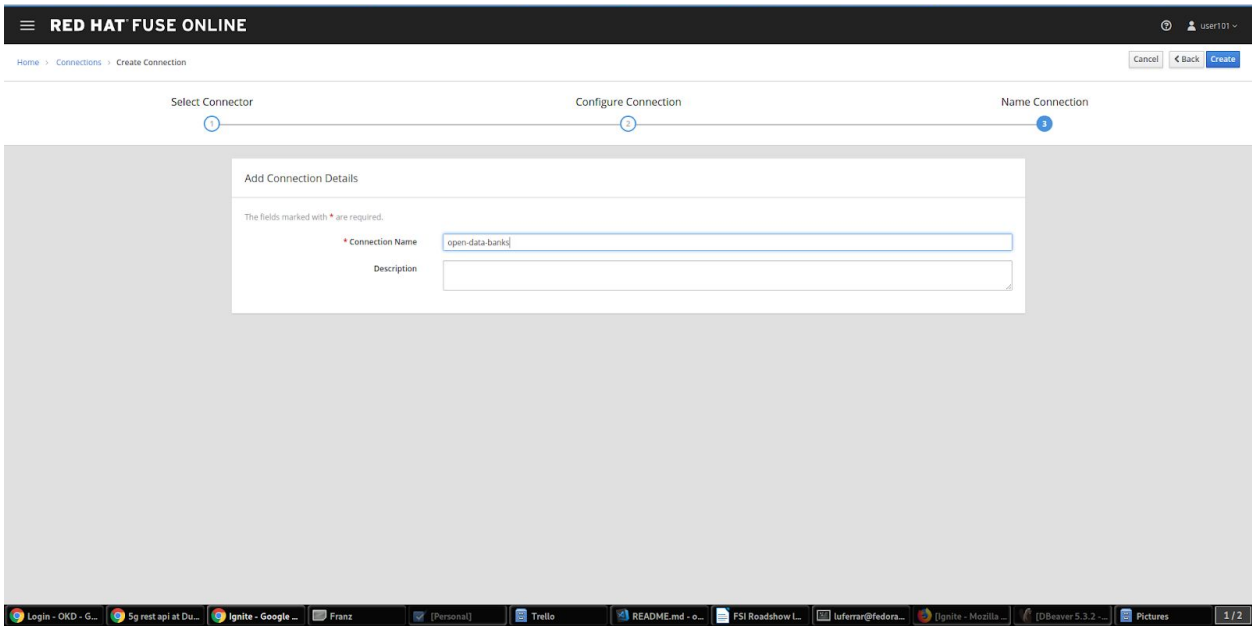
Select a Database connector

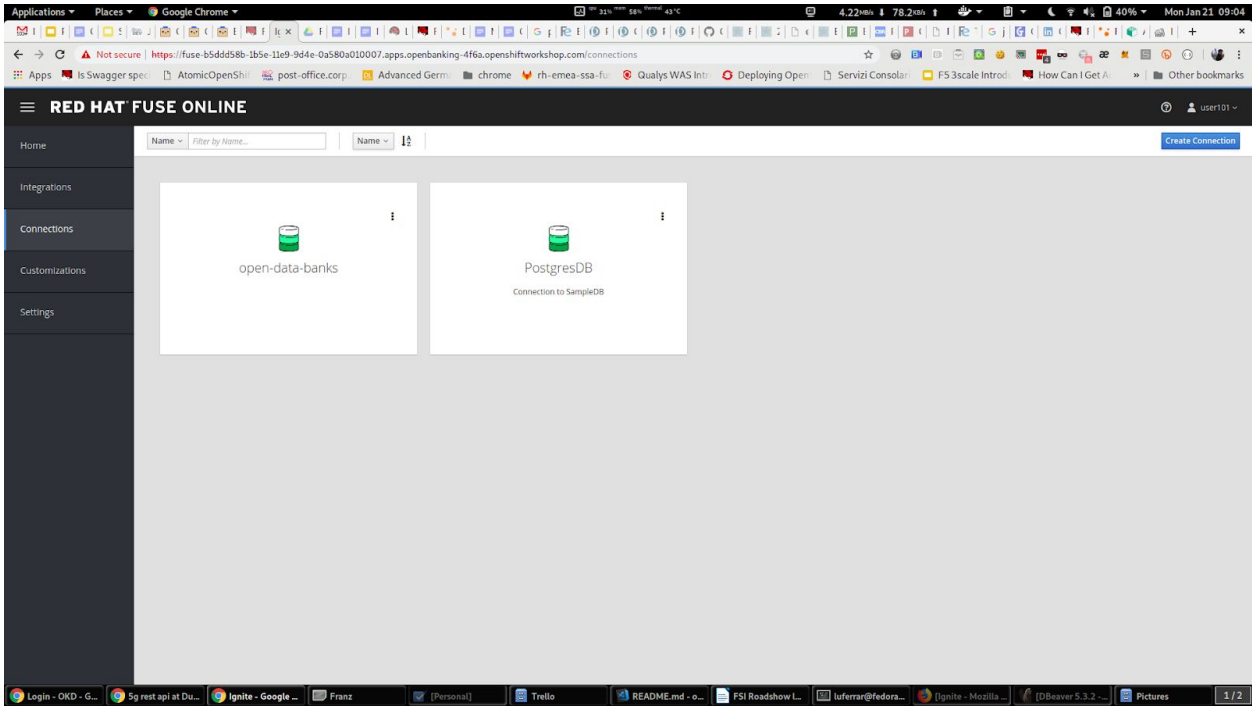


Use the following connection details and validate them:
Connection details: jdbc:postgresql://manny.db.elephantsql.com:5432/hxuazyrm
username: hxuazyrm
password: eiHvH6xbZ2_DRdeoAu_tLbNe3des_NUf
schema: hxuazyrm

Let's name the connection and finalize it.

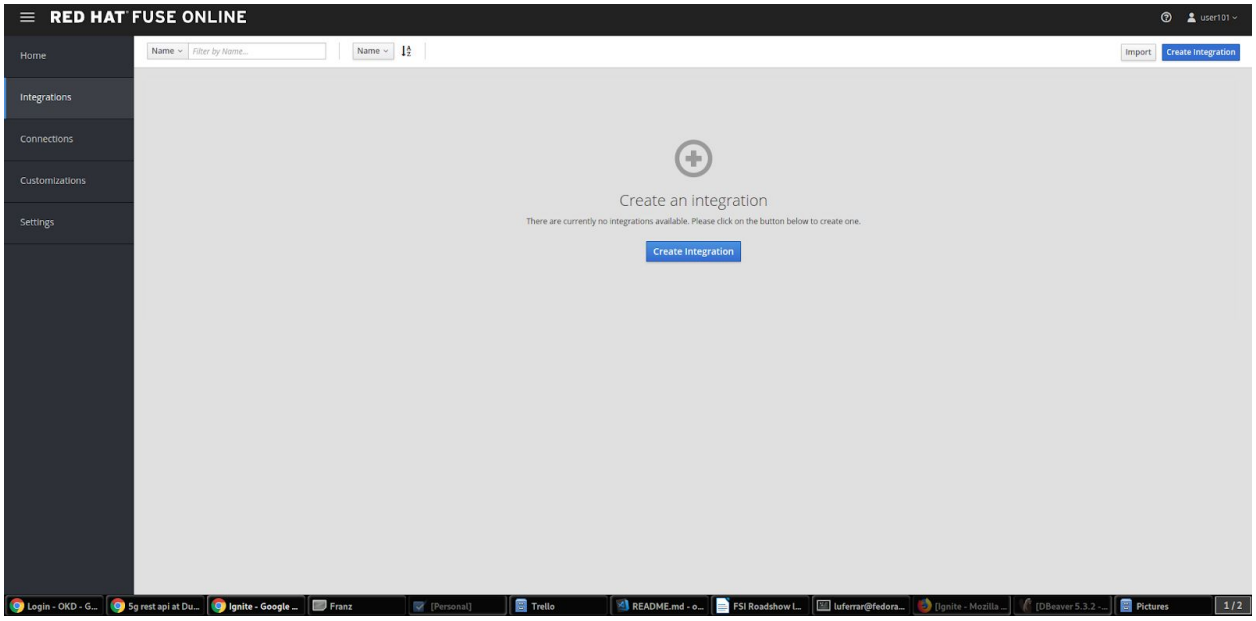




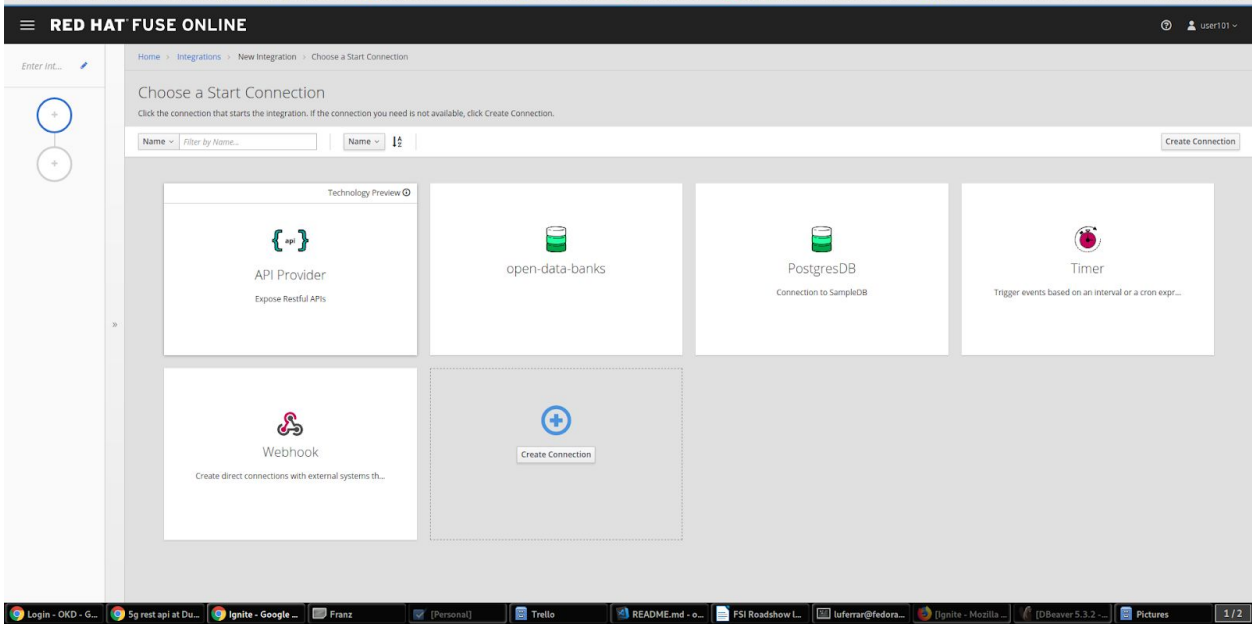


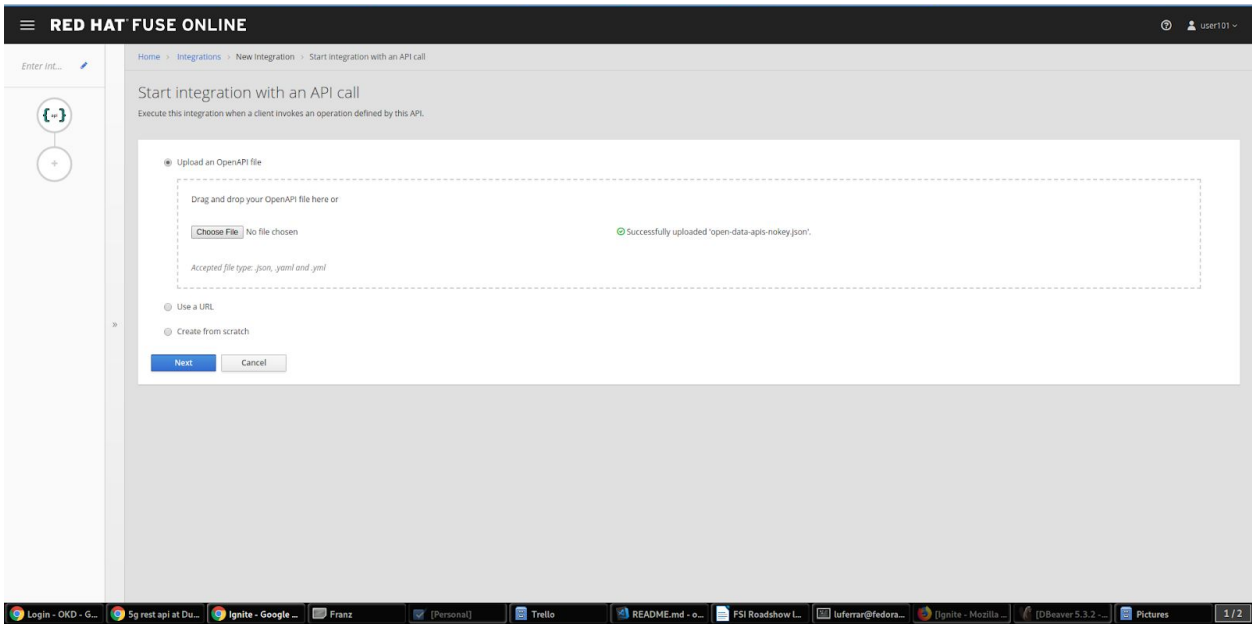
We can now use this connection as an integration starting, middle or finishing point.

Now that we have configured the end of the integration transformation and seen where to find the start we will put the two pieces together. **Integrations -> create**

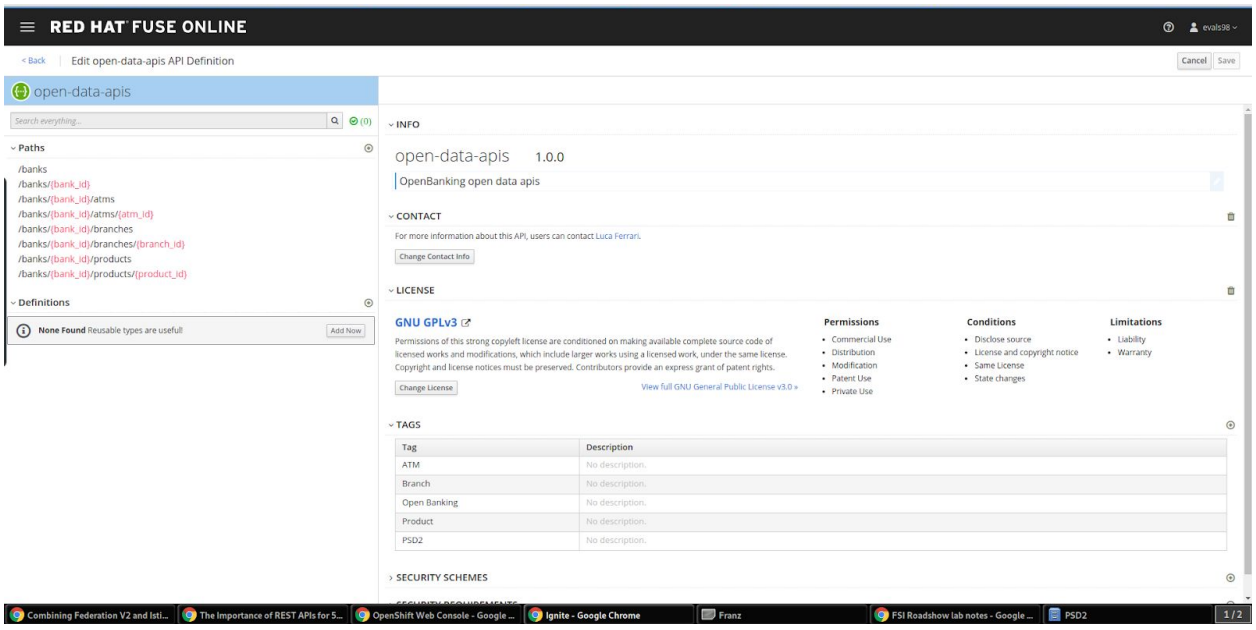


We will start by exposing a REST endpoint that will then get linked to the backend datasource. Use the API Provider connector with the following OpenAPI file: https://raw.githubusercontent.com/lucamaf/open-banking-roadshow/master/open-data-apis-nokey.json



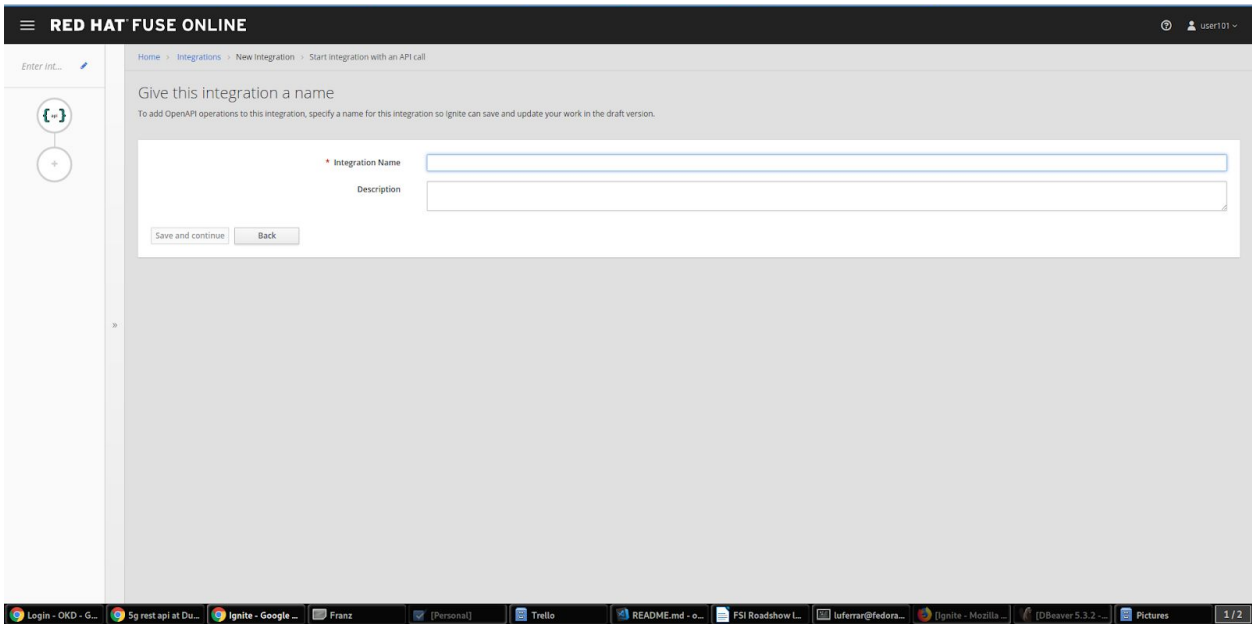


The definition is the same one used on the Open Banking solution portal for Open Data APIs as seen before.
There is a validation happening on the API definition, but no error was identified so we can proceed with the configuration of the connector.
To show how easy it is to correct definitions, **-> review/edit**

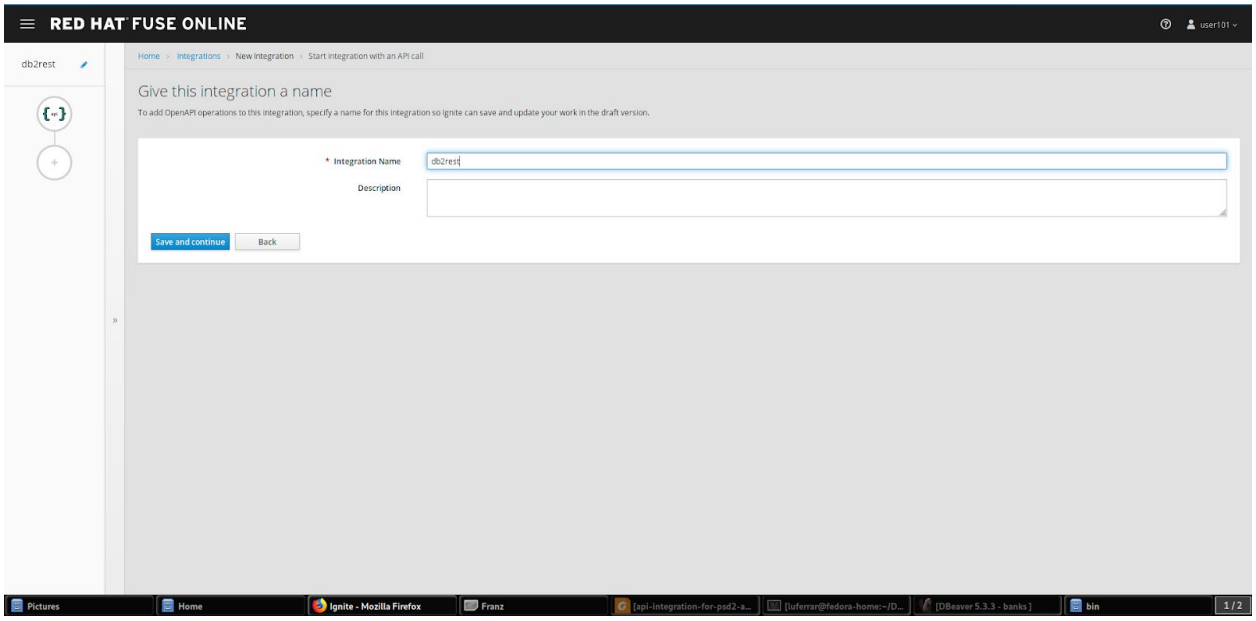


This opens a window on Apicurito which is a scaled down version of Apicurio, our API Design platform. It is fairly easy to change elements graphically and also with the help of this tool an API team can start with a Design First approach when configuring the API. Also the same team doesn't need to know about the rules around OpenAPI specifications thanks to this tool.
The service is exposed without any protection (that's one of the reasons we are going to be using 3scale later on) since the API definition is not adding any authentication on top of it.

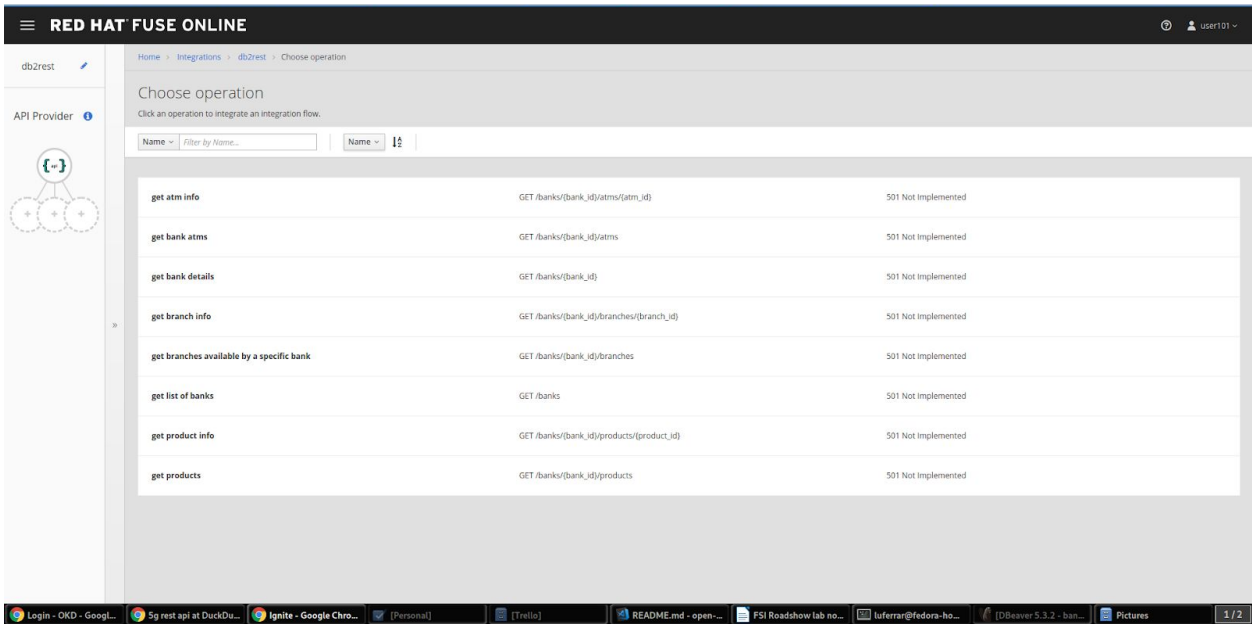
Name the integration.



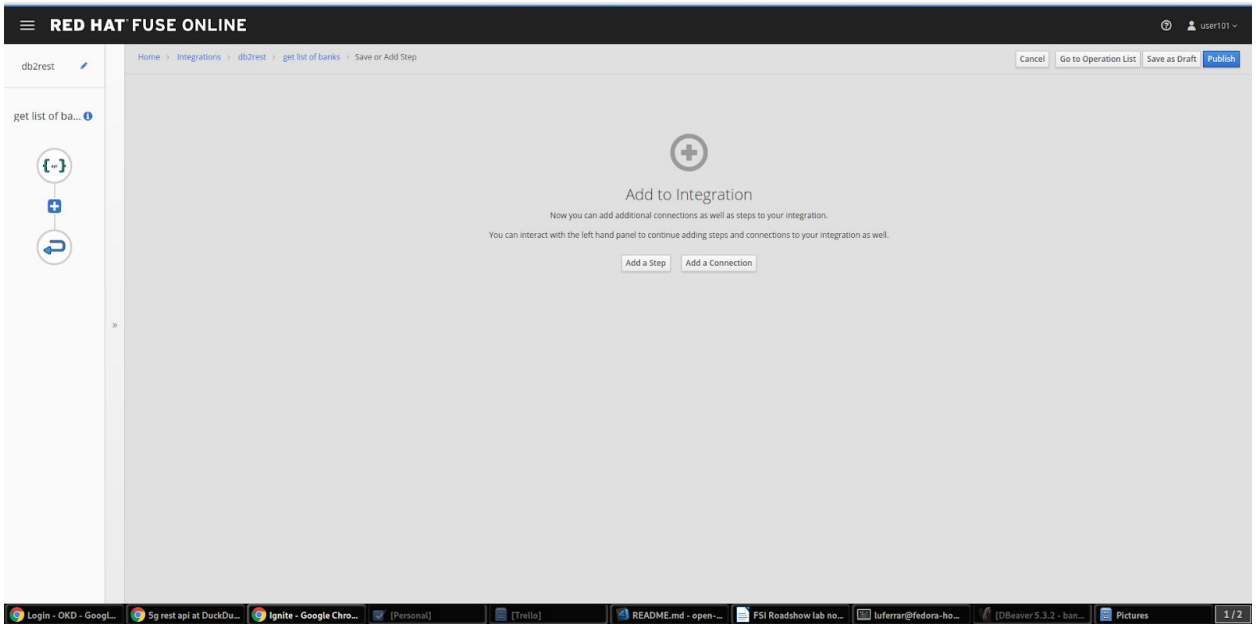
And save and continue



We are going to implement just one of the endpoint exposed, in particular the *get banks* (/banks) one.



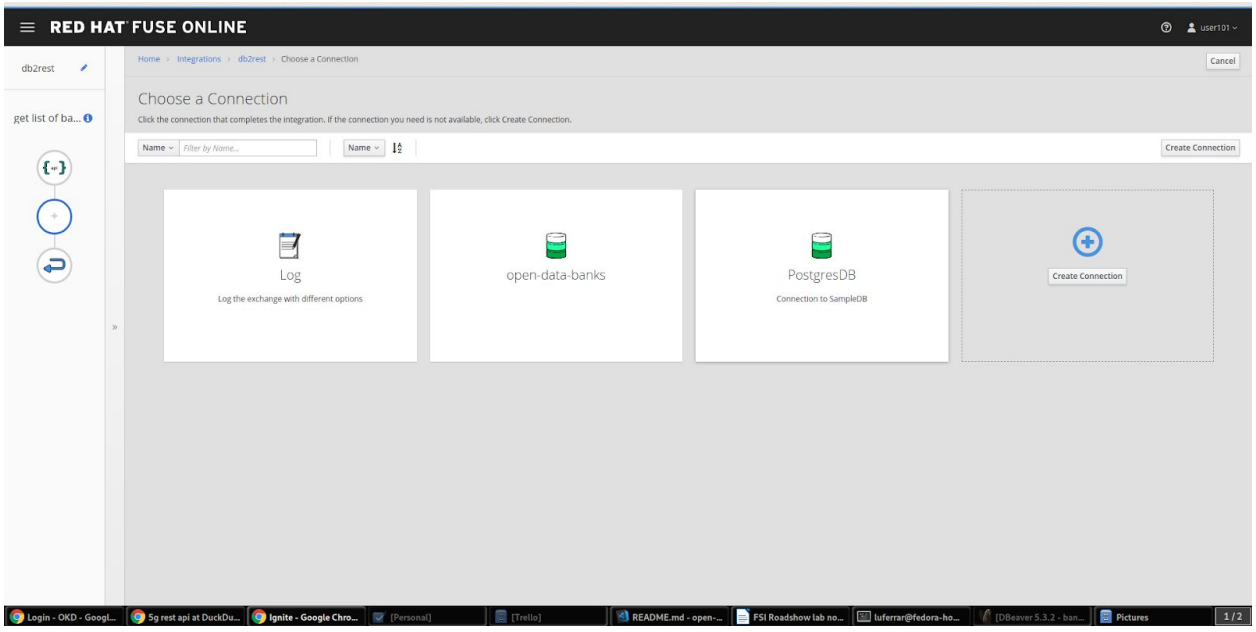
Click on *get list of banks*



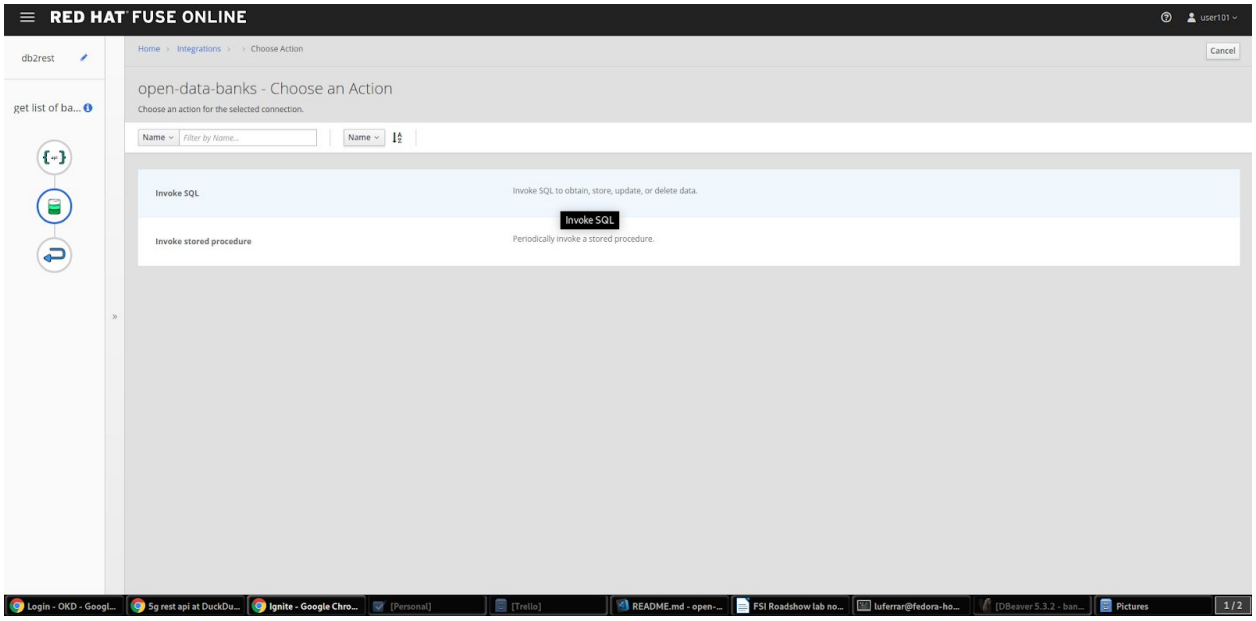
We now have a dumb pipe which connects an endpoint to receive user requests and return always 200 (all OK) - the return blue arrow symbol.

Let's connect this front end to the database we previously configured as a terminating connection.

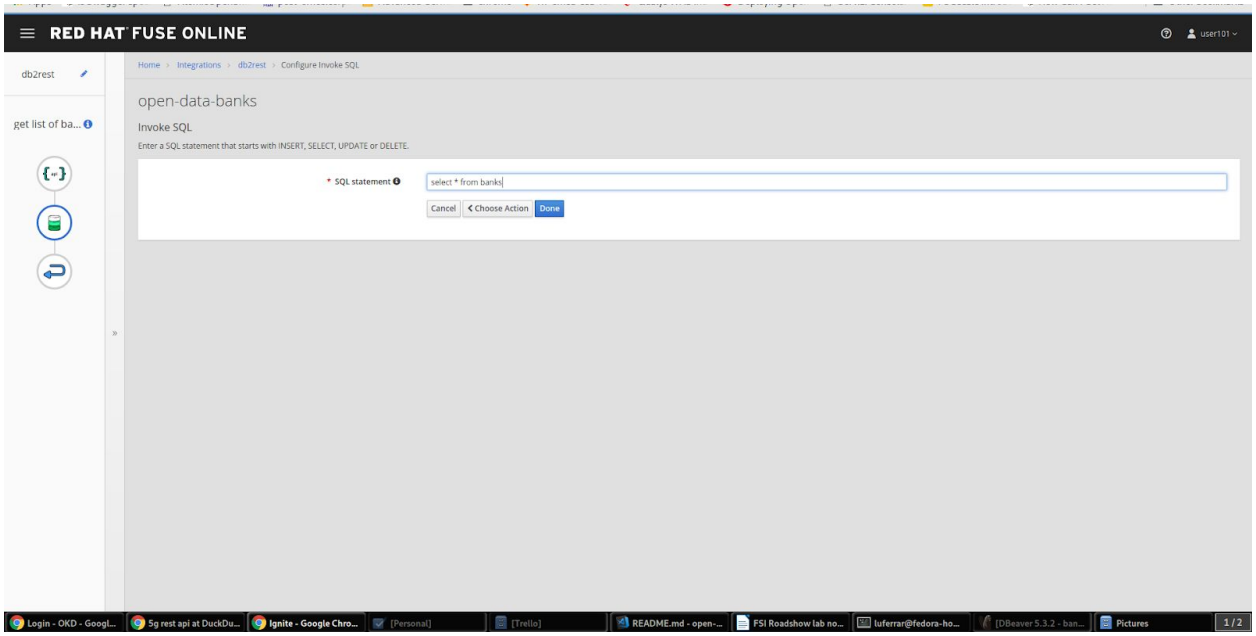
Add a connection



Click on the previously configured data source.

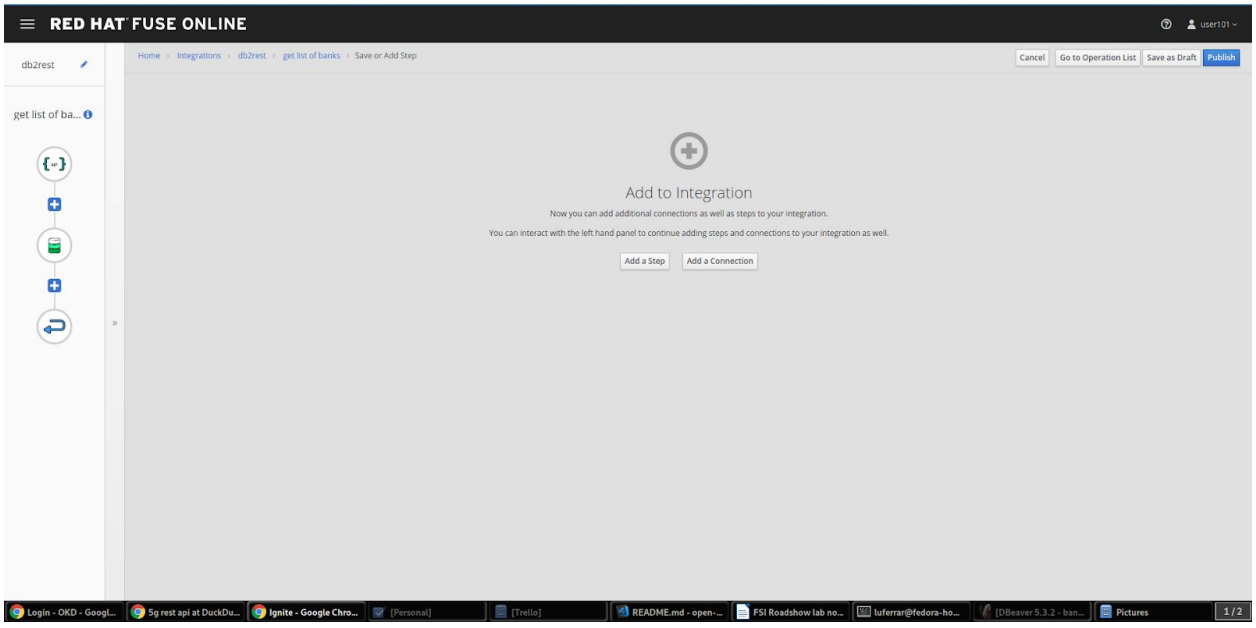


And we will invoke a simple SQL statement to return the data from a single table.

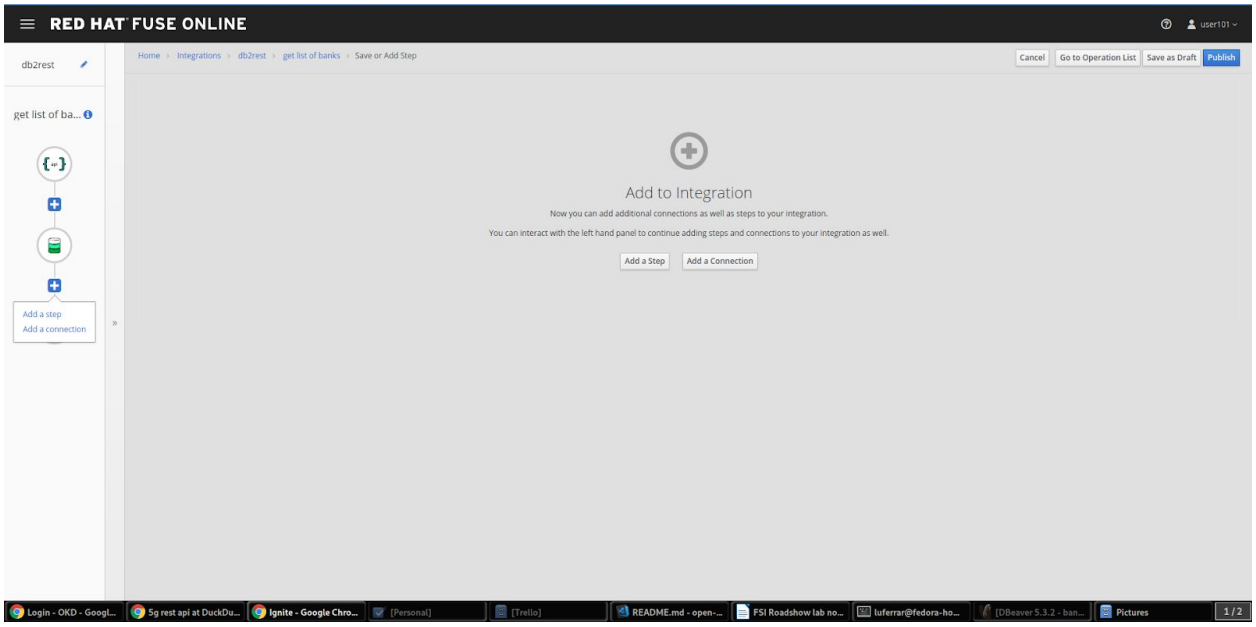


The simple statement to introduce is:
*select * from banks*

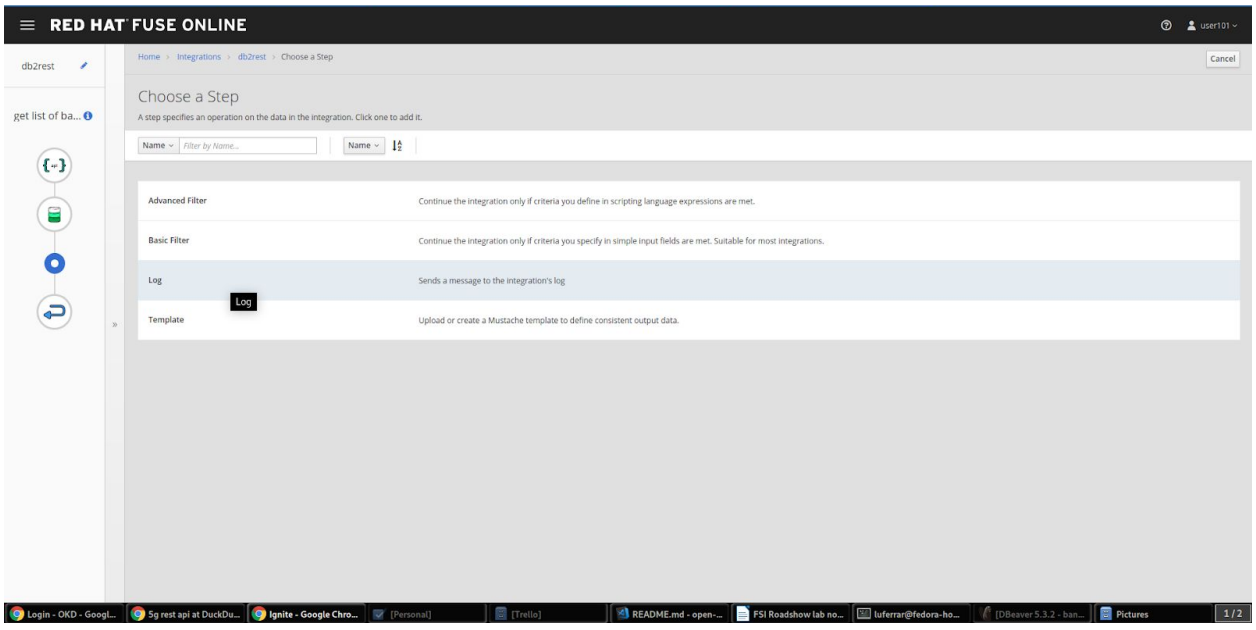
When you click done the statement will validate and you should be able to proceed with the configuration of the integration.



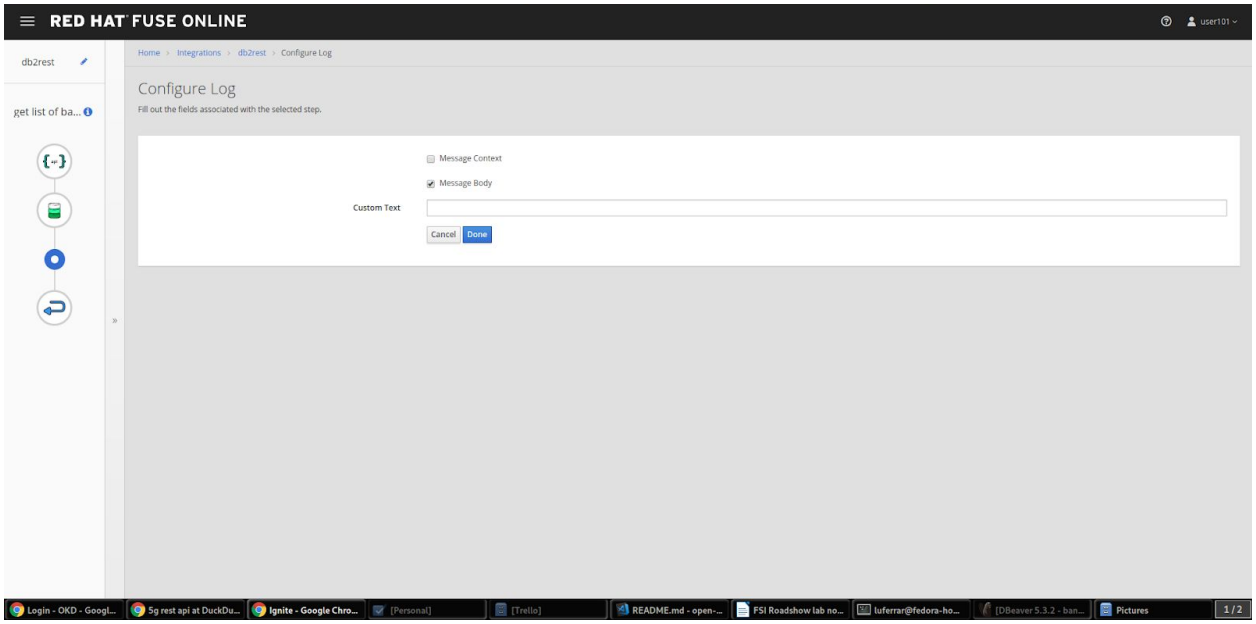
And now let's add a simple log of the requests coming through. Add a step.



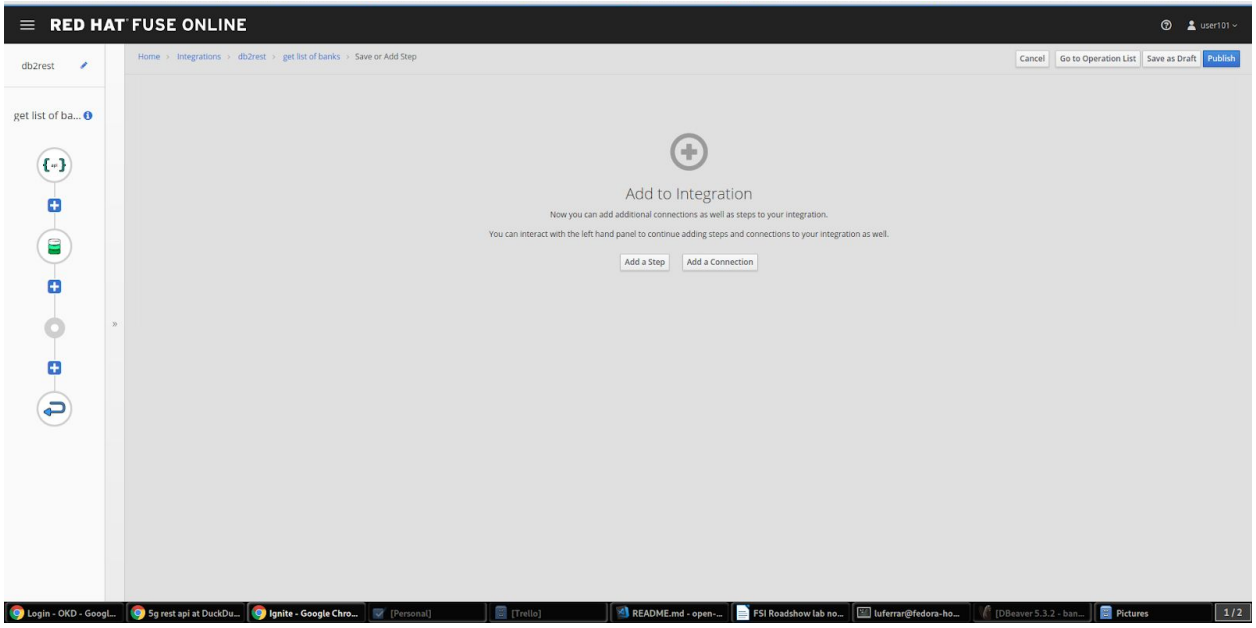
Select the log step.



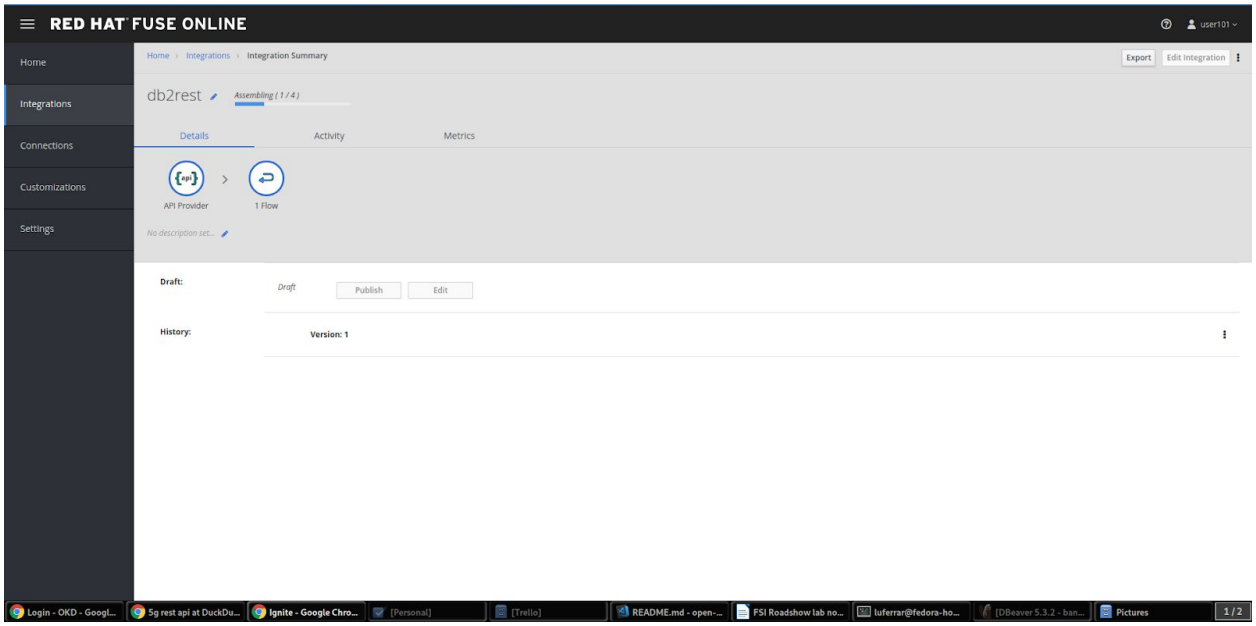
We are going to be sending a copy of the responses coming through to the integration log.



We are going to log just the message body.



We are now ready to deploy and expose this integration in our platform, to use it. Hit **Publish**

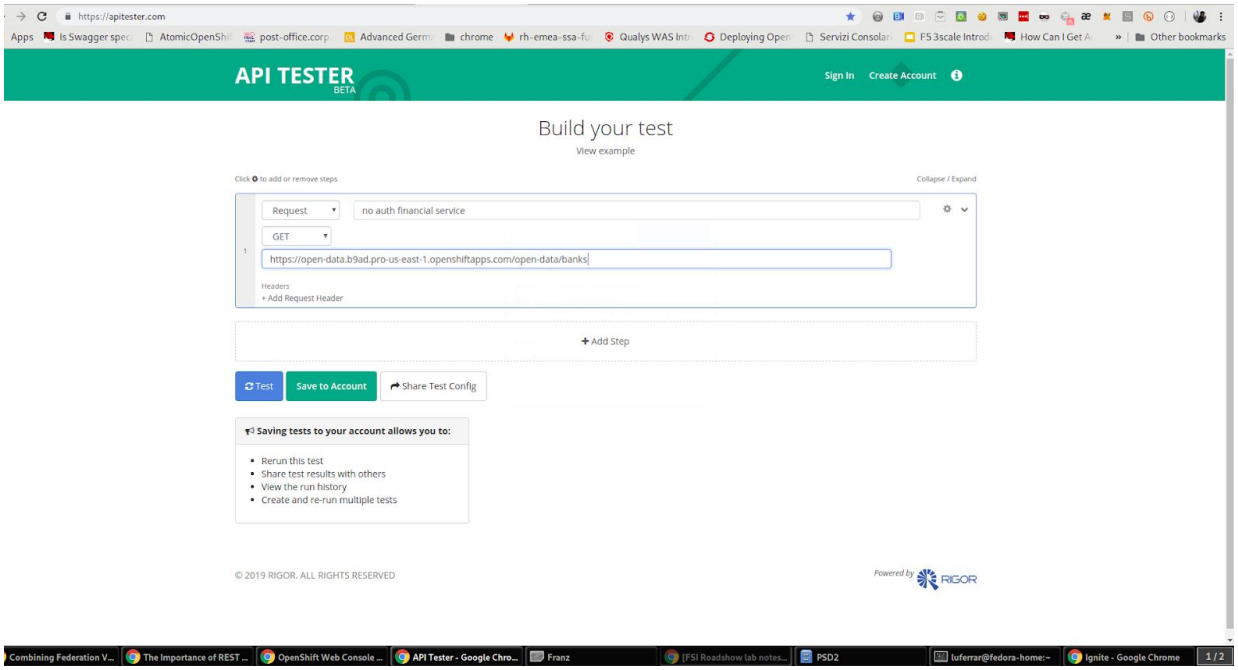


You can check the progress in building the integration changing through phases.
We can notice the platform is getting the required components and constructing the block.
When the building is completed we can test the Integration block.

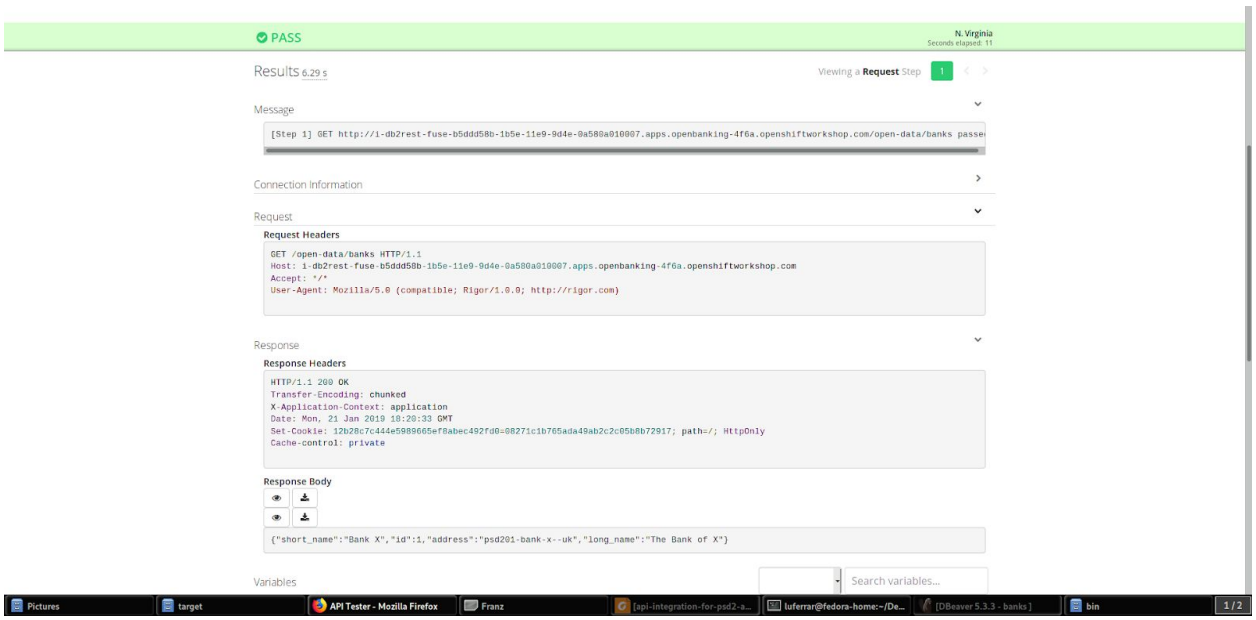
SINCE AUTO DISCOVERY FEATURE IS ACTIVE WE WILL NOT GET AUTOMATICALLY A URL WITH THE INTEGRATION BUILDING PROCESS, BUT API MANAGEMENT WILL BE ABLE TO SEE IT AND PROTECT IT ANYWAY.

Now that you have shown the attendees how to build the full integration block you can test the integration just built, using this online tool https://apitester.com/ . For the attendees to also test you can share the following URL for them to use http://i-db2rest-fuse-b5ddd58b-1b5e-11e9-9d4e-0a580a010007.apps.openbanking-4f6a.openshiftworkshop.com

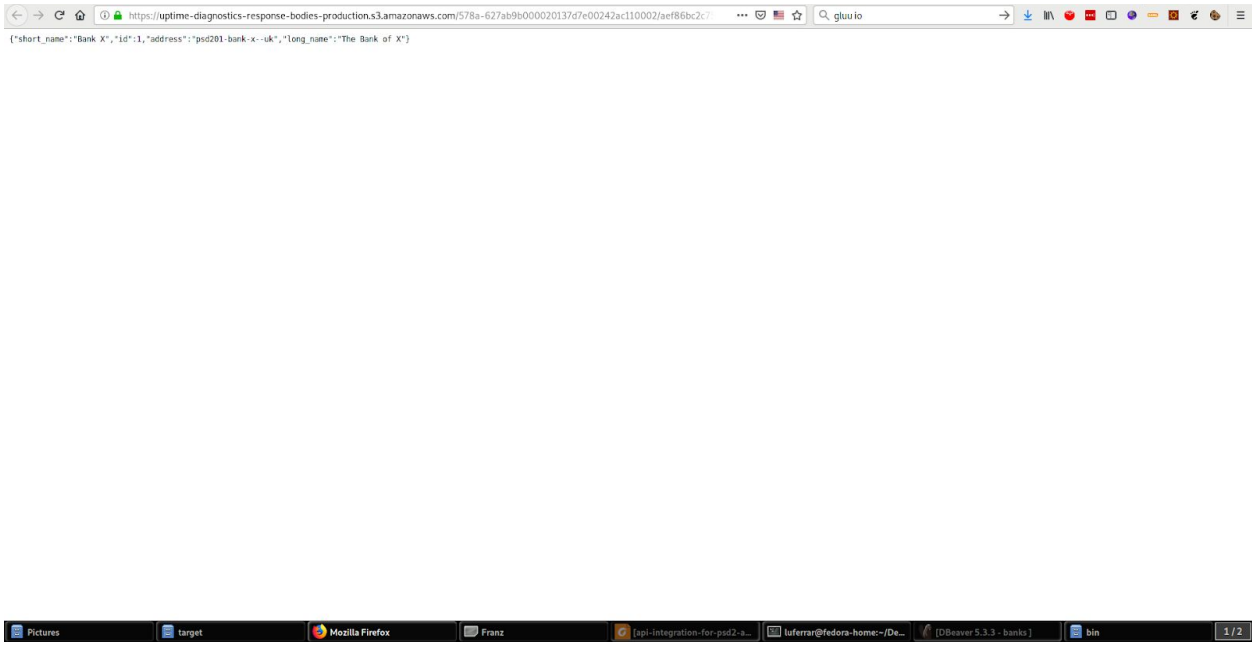
Explain the role of the API tester as mimicking a full Web or Mobile application but stripped down of the GUI.



Populate the fields with the following URL
http://i-db2rest-fuse-b5ddd58b-1b5e-11e9-9d4e-0a580a010007.apps.openbanking-4f6a.openshiftworkshop.com/open-data/banks
and hit **Test**



Show that everything went 200 fine and open the Response Body (eye icon)



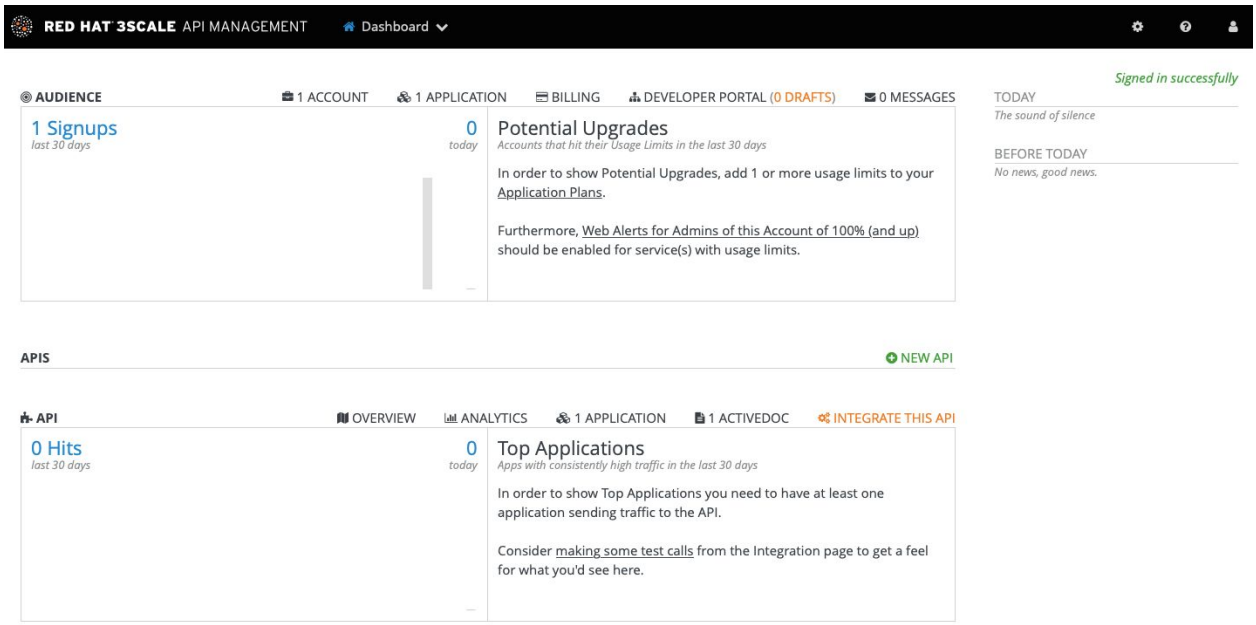
Show the structure of the JSON response, with basic information given around banks (dummy data).

3scale

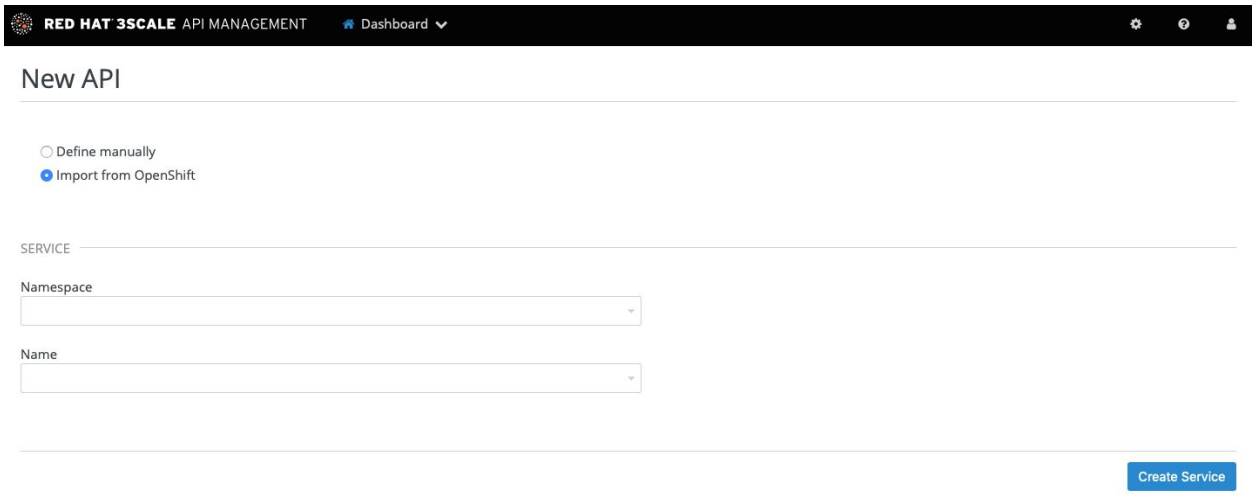
To reach 3scale as a user you can just go back to the main integr8ly dashboard and click on 3scale

Introducing now 3scale, for the purpose of managing these exposed APIs, securing them and tracking their usage. **Dashboard**

Explain that you are now logged in as an administrator or API provider. The dashboard will show a summary of the trends in usage of the platform, in terms of developers signups, usage of APIs and message sent and received.

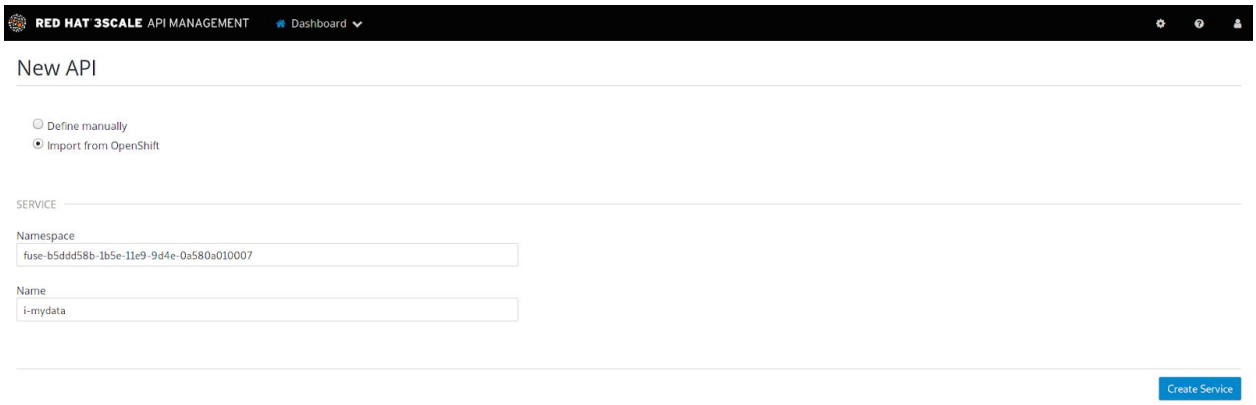


Let's start managing and protecting the API we just created on Fuse Online.
Click on the green button **New API** and select **Import from OpenShift**. We are going to be using the auto-discovery feature we saw before. We would be helped by this feature and would save time configuring the service.

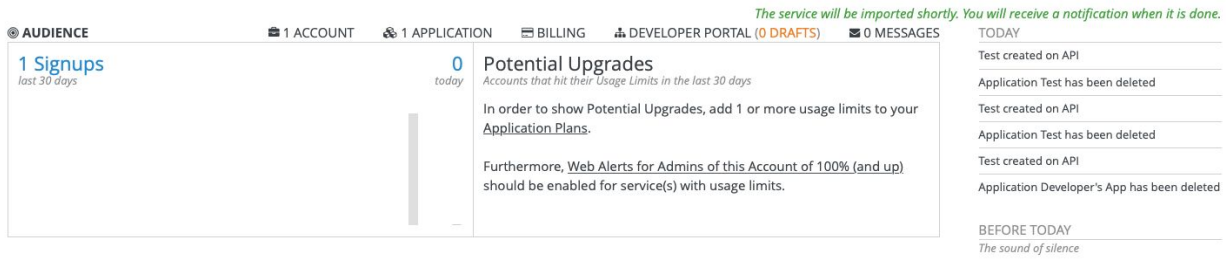


You are now presented with the permissions screen and you should click the *Allow selected permissions* button to proceed. This is to allow API management to go and look for services in our container platform.

You will now see the auto-discovered Fuse service appear in the *Namespace* field. Click the blue **Create Service** button and proceed in starting the service configuration.



You will be redirected to the Dashboard view where a success message should appear as shown in the following screenshot.

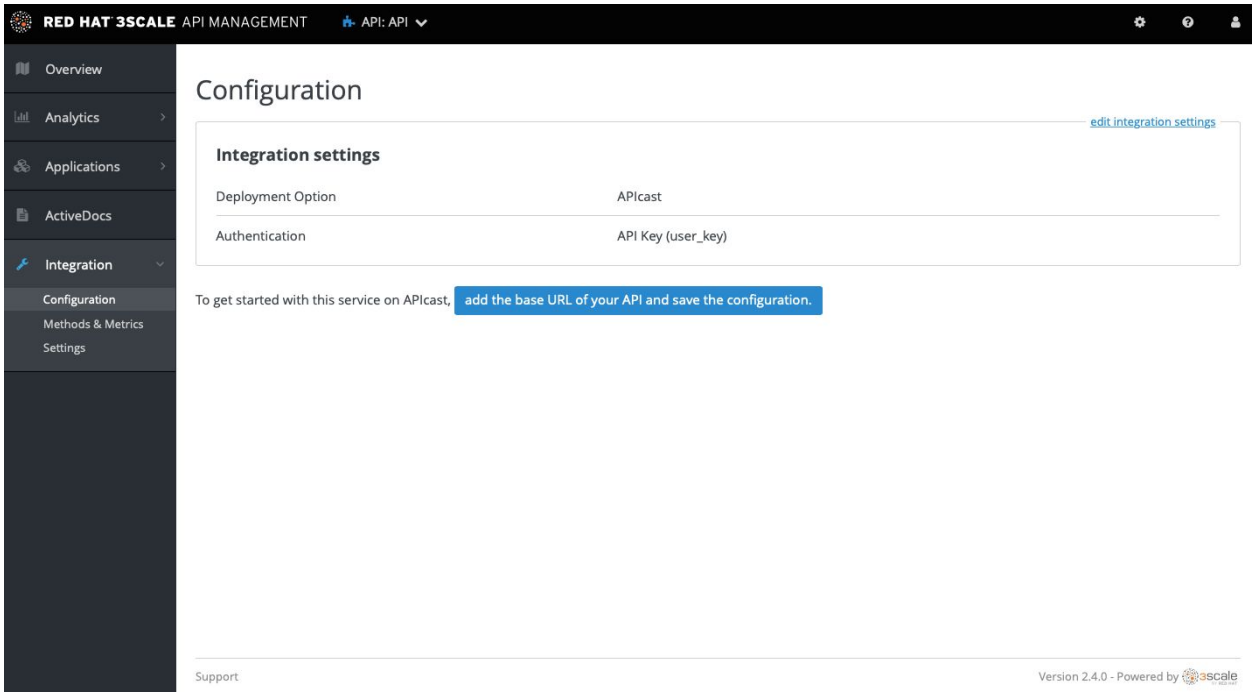


Once the service is created you will see that in the dropdown menu where you can also see **Audience.**

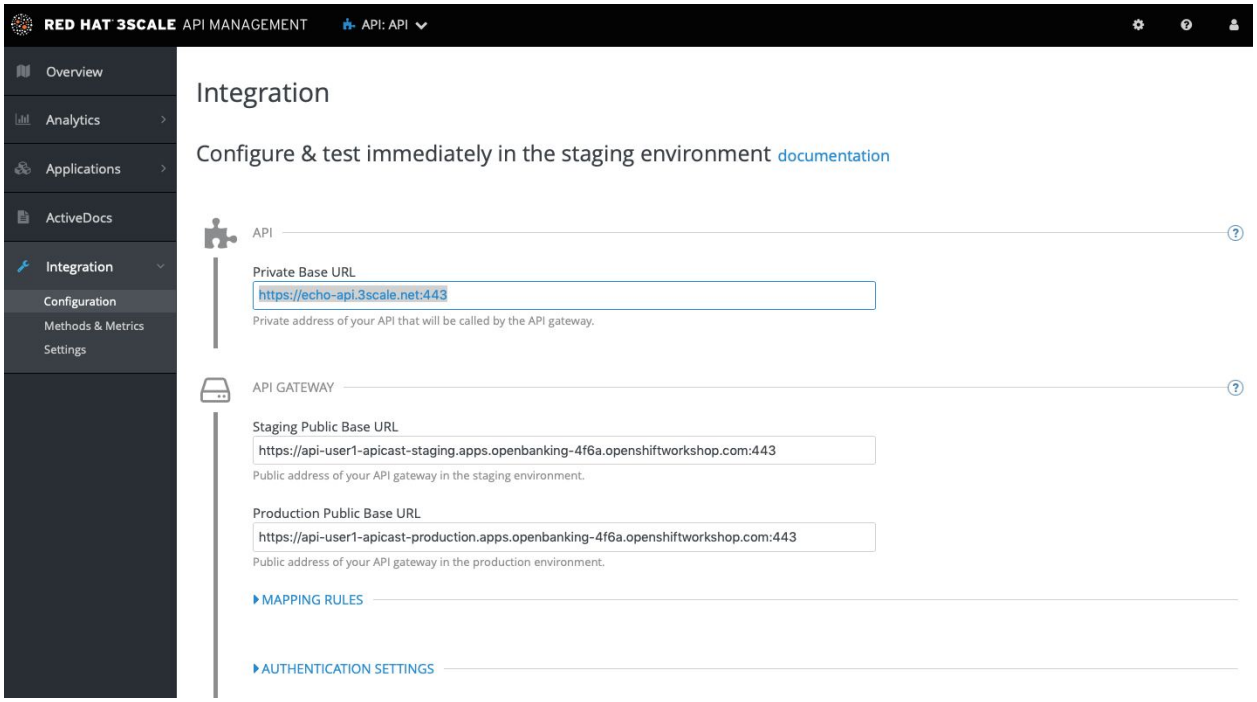
We can now proceed on changing the details of the configuration of the API and publish the update on the Developer Portal so that the public Developers can sign up for the open financial

API.

API-> Integration

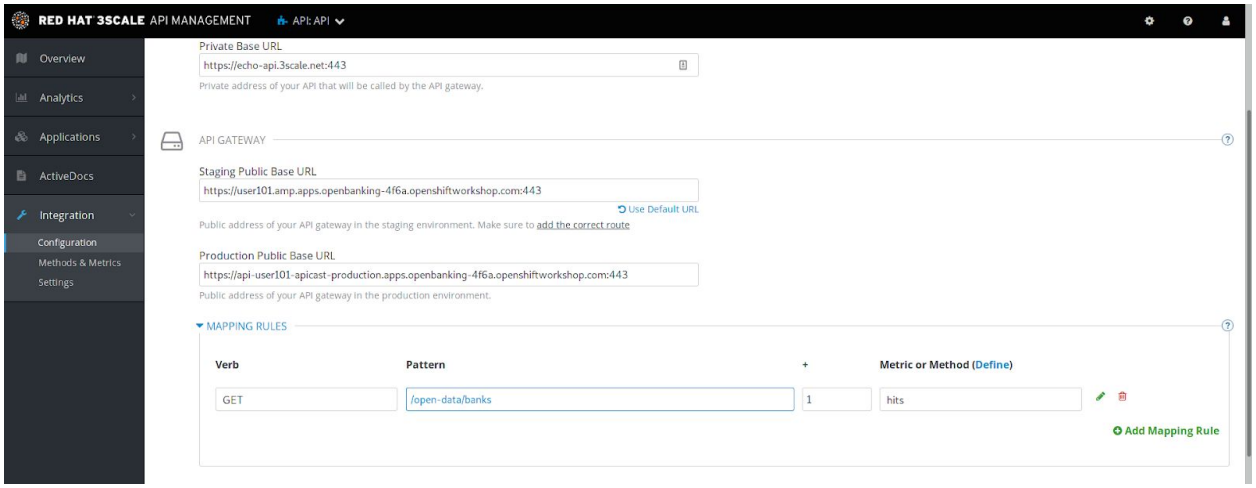


This is where you configure the rest of the details of the mapped Service. The private base URL should already be filled with the details coming from the auto-discovery feature.



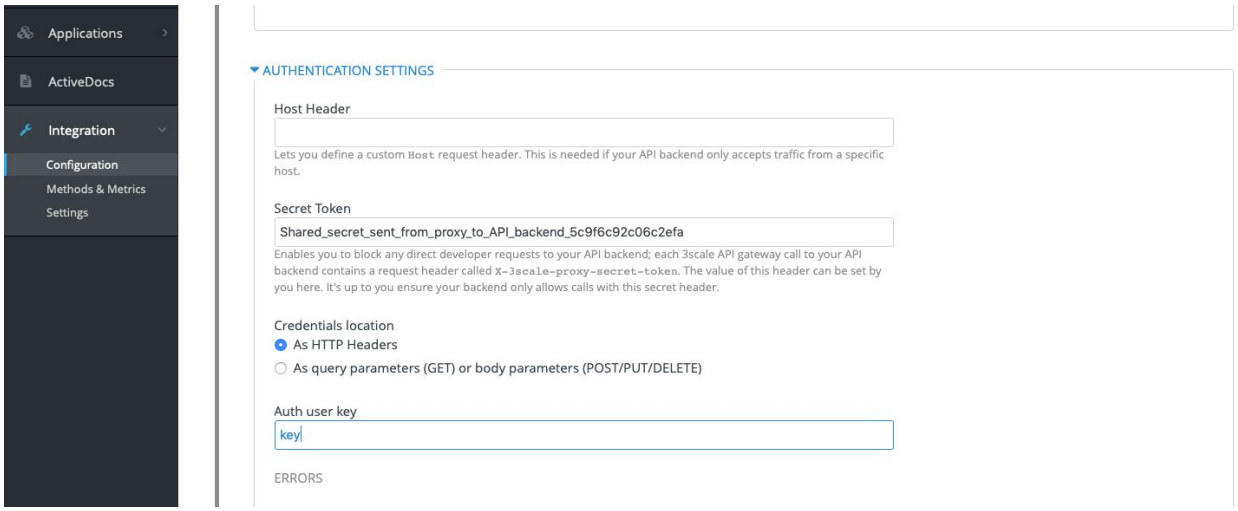
We have the section where we map the Backend API and then 2 URLs where we expose the managed API on the staging first and production gateways or infrastructure. We will be changing the Staging and Public address of the gateway. In this case we are not going to use

separate staging or public infrastructure so it can be the same address. (please notice the format of the staging and public base url for the gateways https://userX.amp.apps.openbanking-4f6a.openshiftworkshop.com)

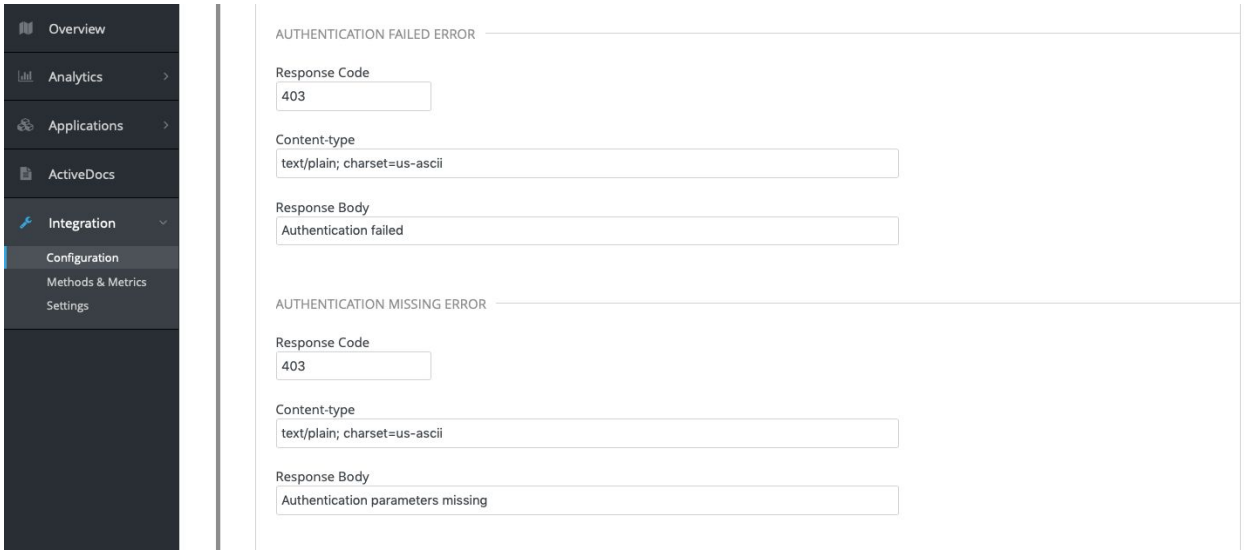


We will now make sure we map a single endpoint or resource in 3scale and disallow any other endpoint (i.e. the other endpoints have not been implemented yet).

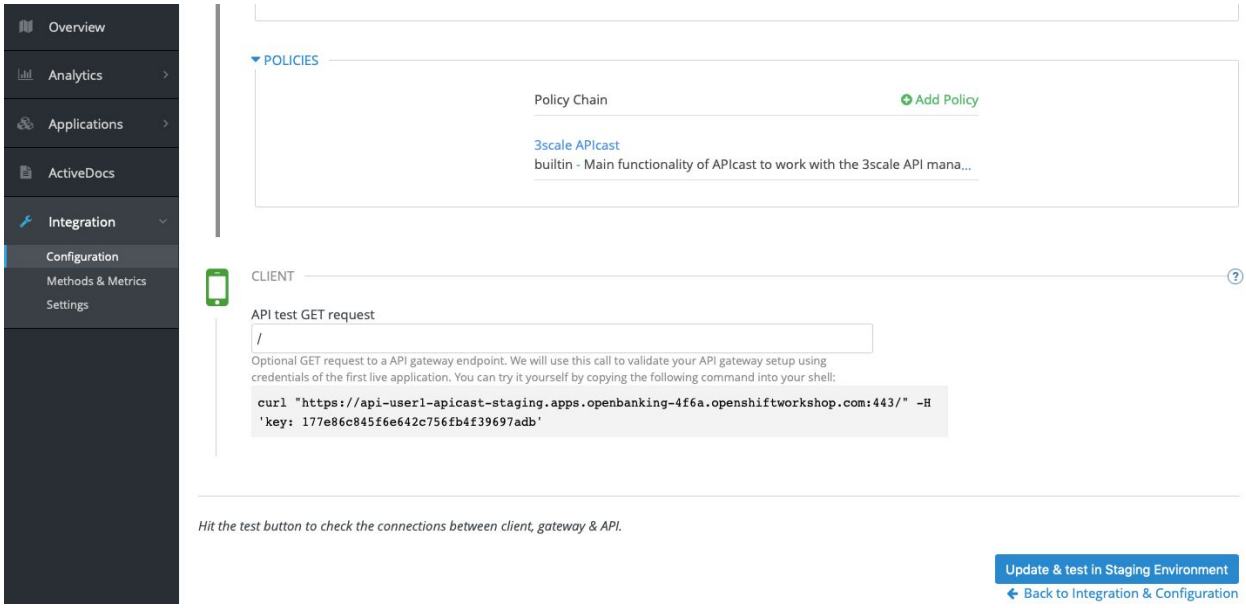
The endpoint you want to map is /open-data/banks$ (notice the $ at the end of the path that will allow us to make sure users cannot improperly access any other resource). We can now check the configuration of authentication settings.



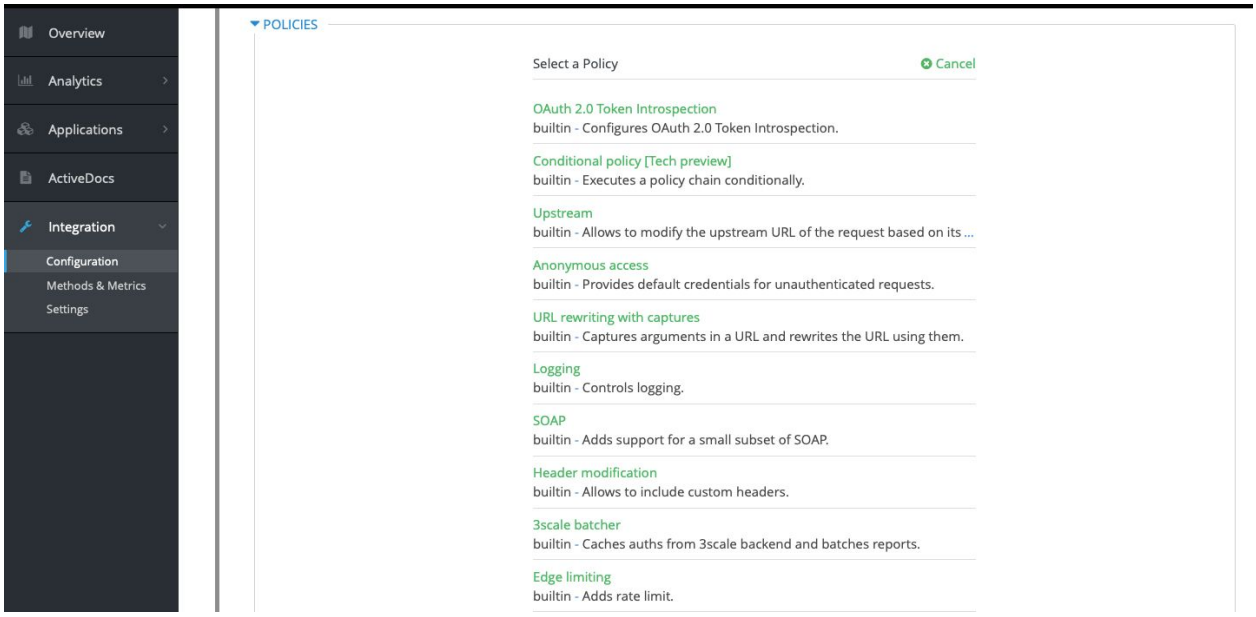
We see that we have already api key protection enabled, but we might want to pass this information as HTTP Header instead of HTTP parameter. We will also change the header name to ‘key’



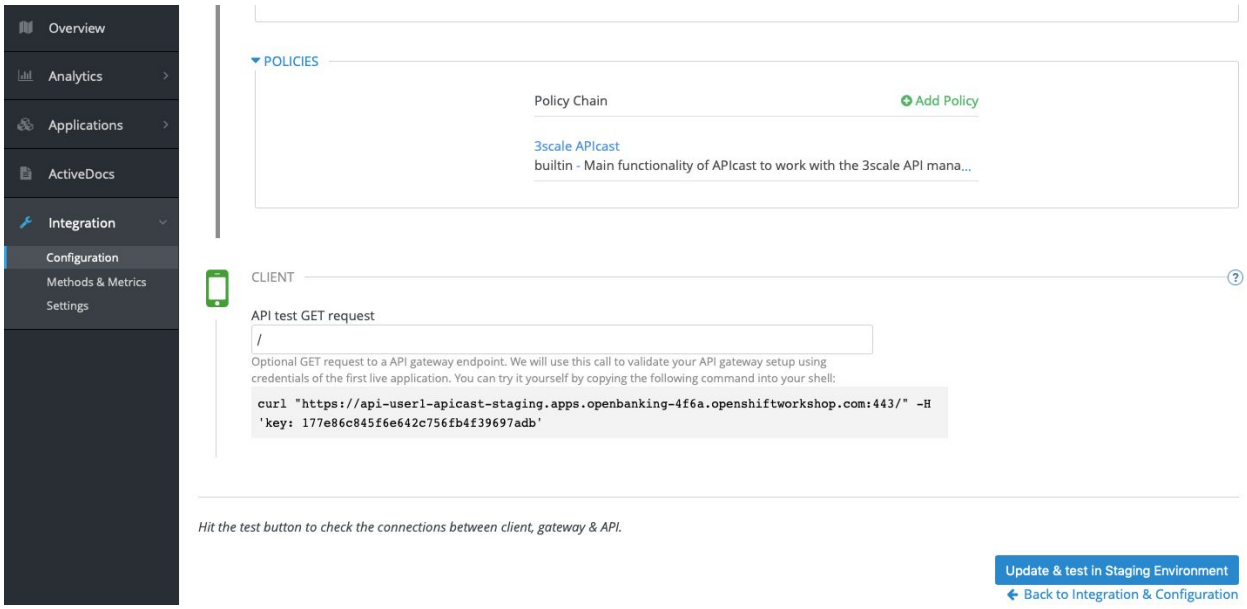
Explain that you can also customize the error returned to the end user. **Policies**



These are like additional plugin that you can configure to adapt the service to your own preference. **Add Policy**



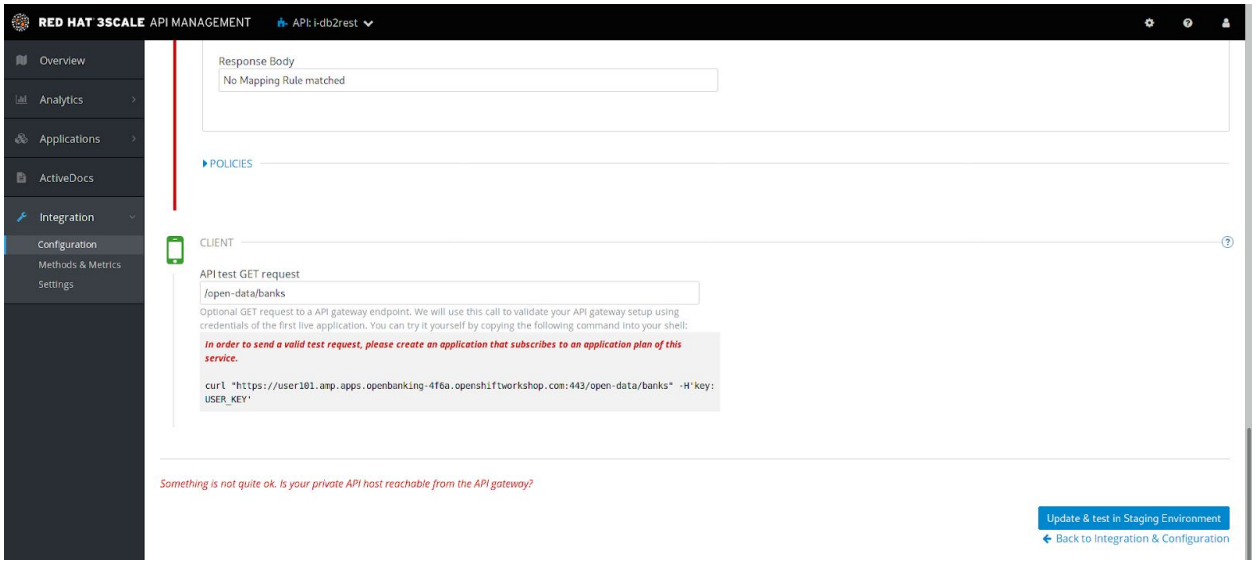
Several policies are available and the list is always increasing. Highlight the presence of SOAP policy to map SOAP services and advanced rate limit functionalities, rate limit policy. Update the API test GET request field with the same pattern you are mapping above (excluding the $).



Hitting the big blue button will allow you to two things at once:

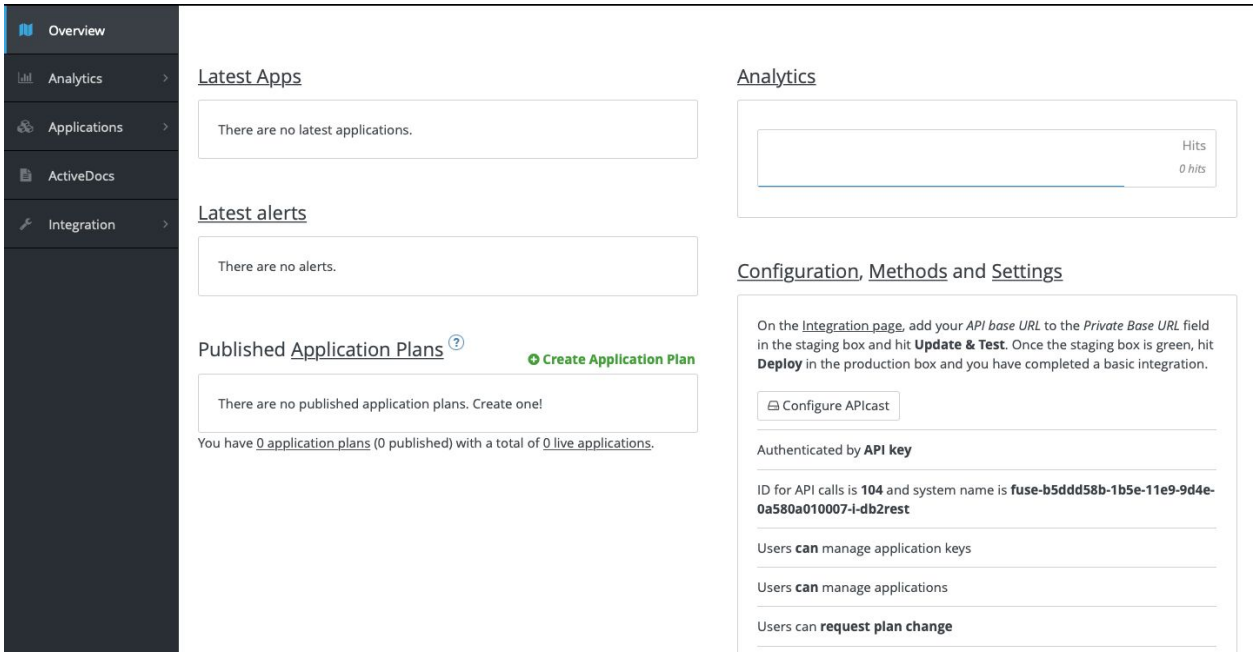
- Update the service configuration
- Test the configuration just uploaded to the gateway.

The second one will fail since we are not providing any valid key, so we will get unauthorized request but the gateway will receive the updated configuration in any case.

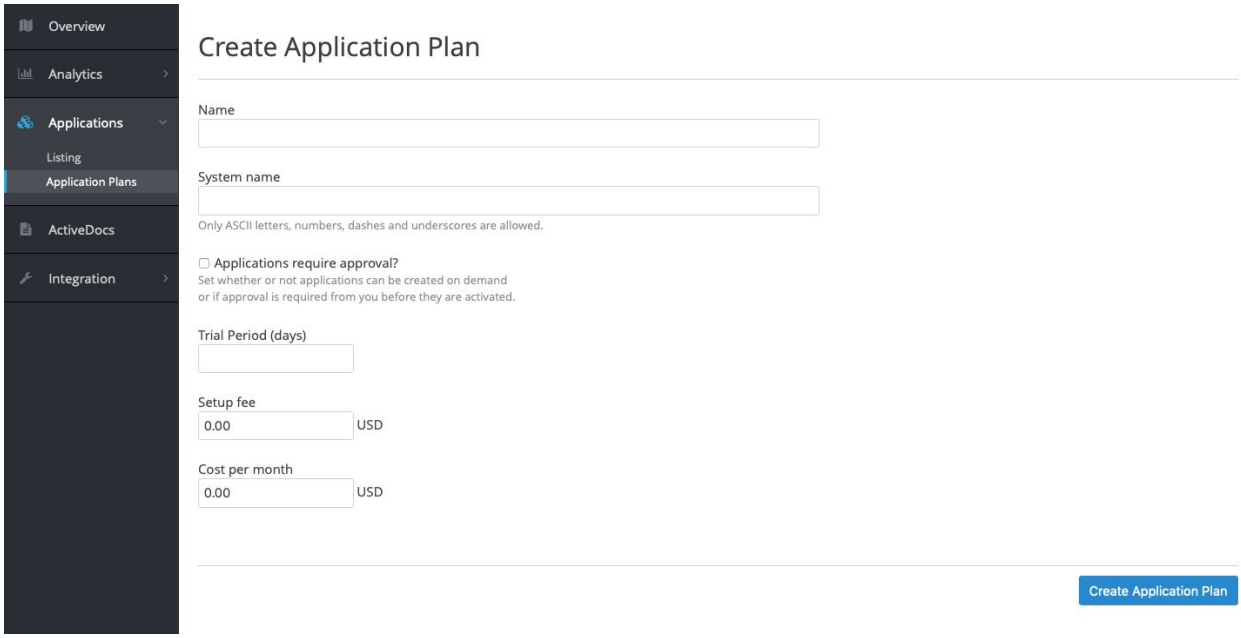


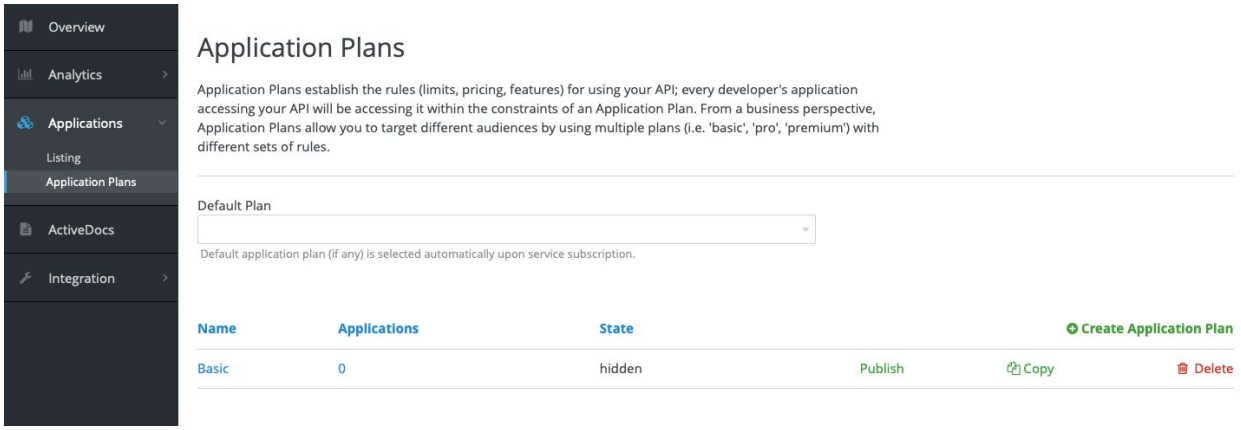
We will now fix the test request error as advised by the warning message.
Let's switch to explaining the role of API contracts of Application Plans.

Now from the Service overview page click the green link *Create application plan*. Since we are creating a Service we will need to offer a way for Developers to subscribe to it and use it. Application plan are the way to do that (also called API Contracts).

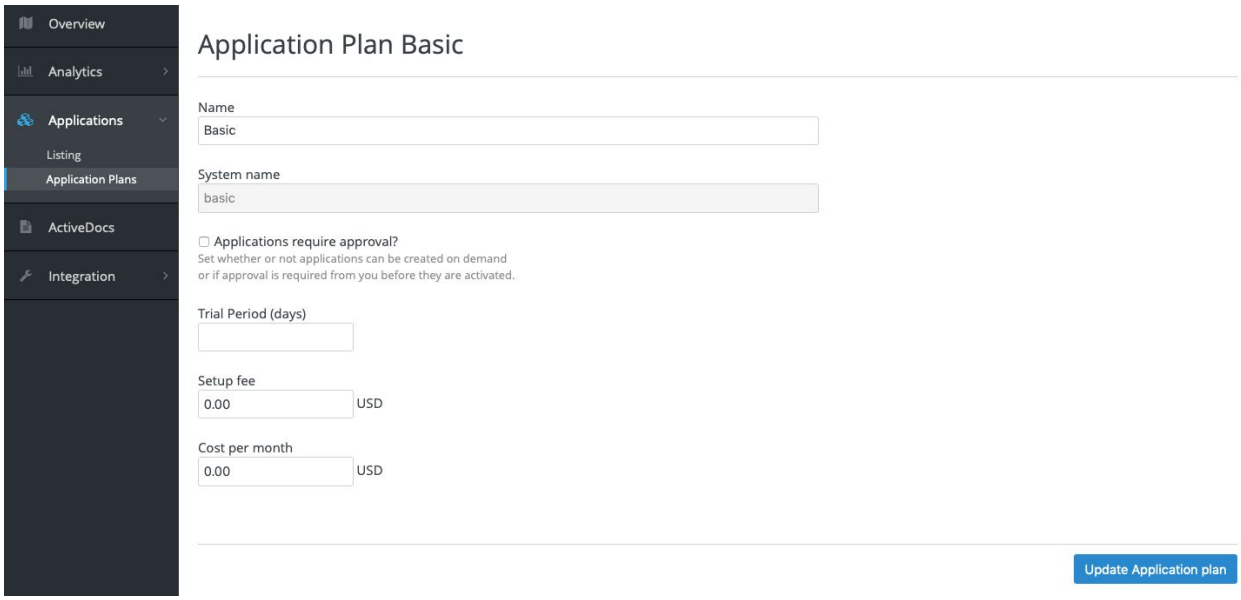


Fill out the fields on the *create application plan* form and click the blue button to submit the form.
You can safely ignore for now the monetization options and use whichever name you prefer.



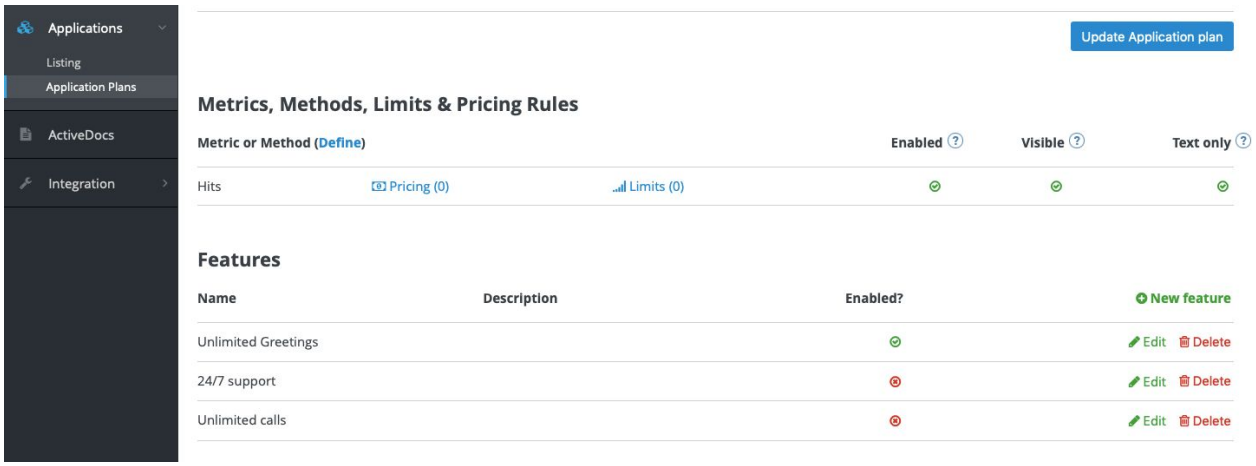


We see that we have 1 API contract (or Application Plan), but no application associated to it. The application plans are in **hidden** state by default, so let's publish this one so that it is usable and visible on the Developer portal. Let's open the application plan.

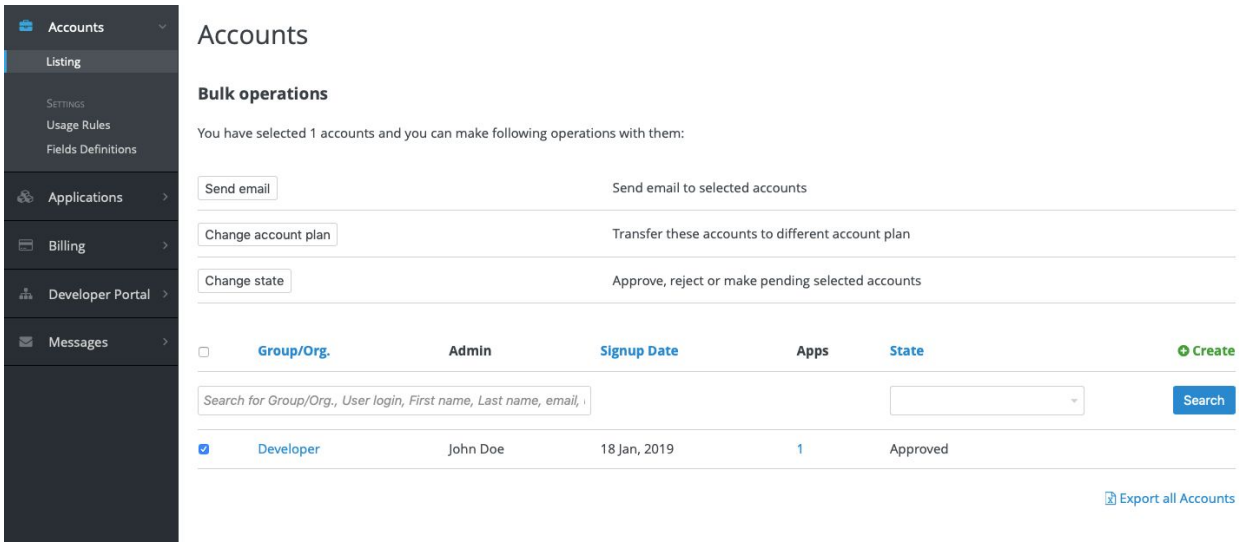


Main elements:

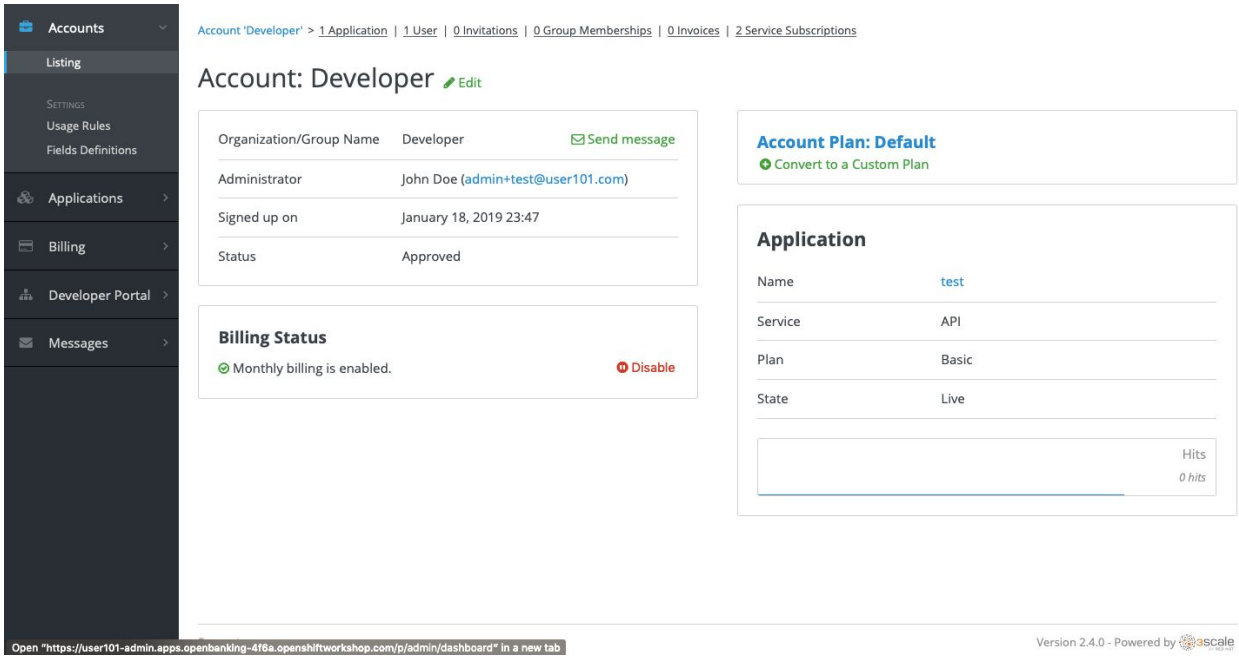
- Monetization settings (trial, setup, cost per month)
- Endpoint mapped (in this case generic Hits) and relative monetization and rate limiting settings



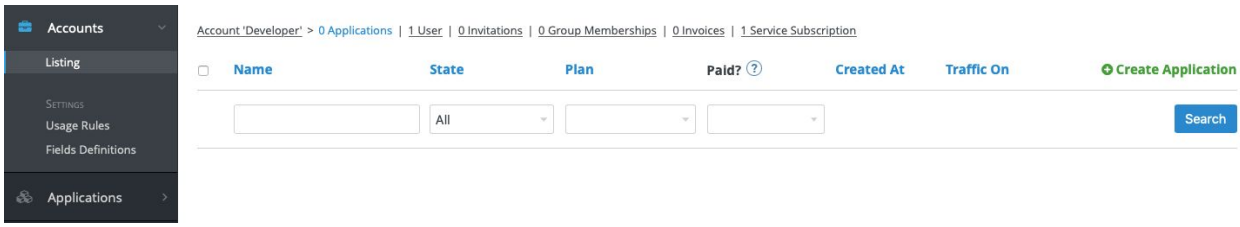
We can now switch to the Audience tab to create an Application to test the Configuration.

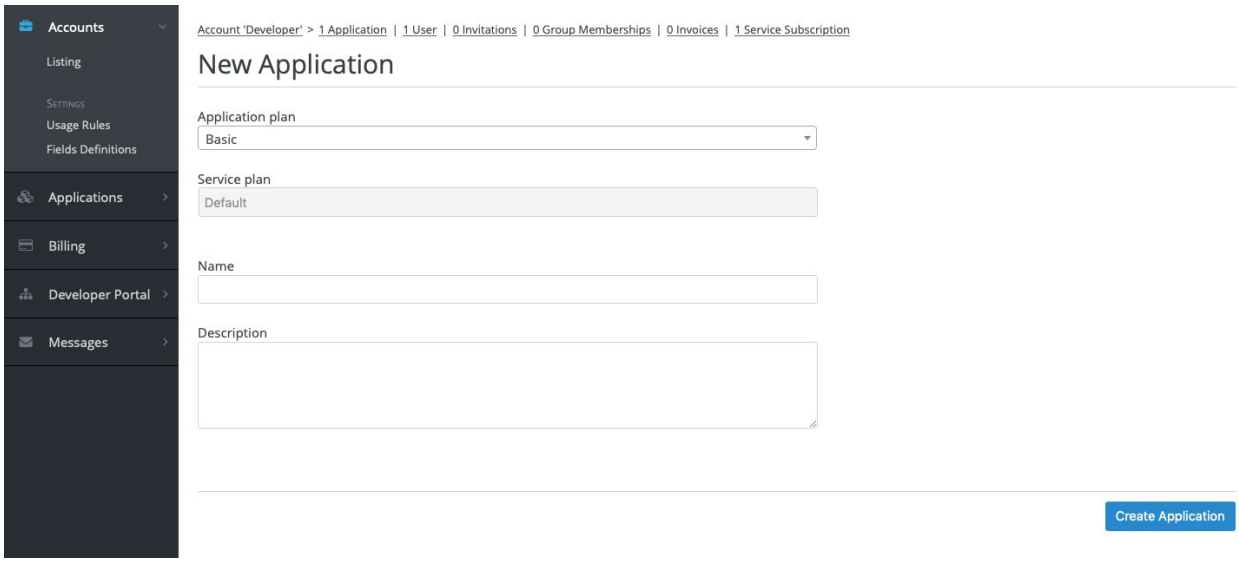


From here we can see how we can, as Provider, approve or deny Developers' Accounts registrations. Let's click on the default **Developer**



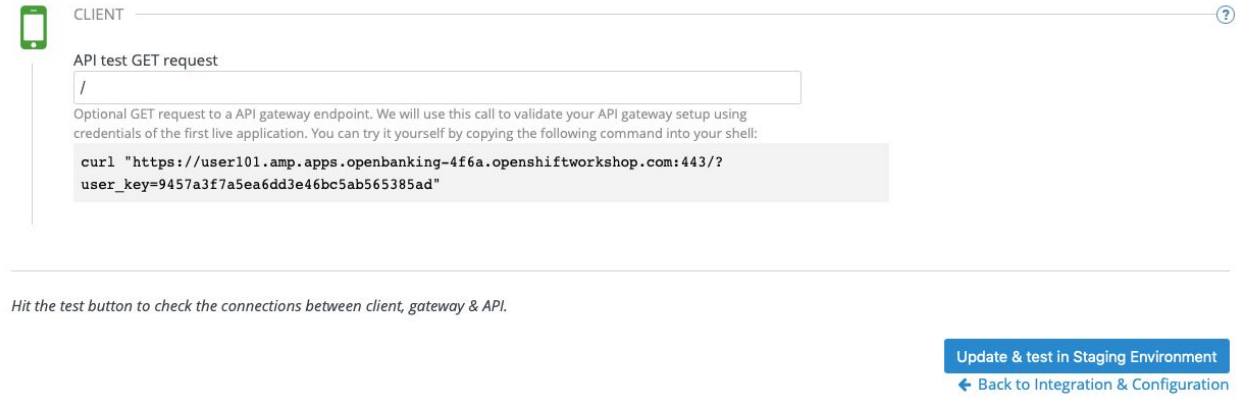
We can see that the Developer has the default application associated, but it's subscribed to the default Service. We can also see the Developer user details.
Let's click on **0 Applications** and **Create application**



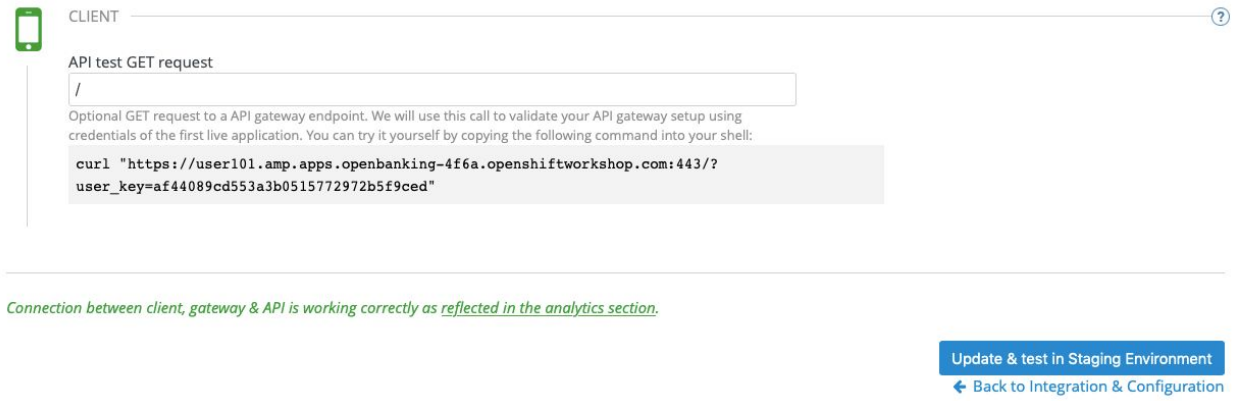


Here we can now subscribe the application to the **Application plan** we created on our new Service from the drop down field available. Let's fill in the rest of the fields with some basic details and click the big blue button: *Create Application.*

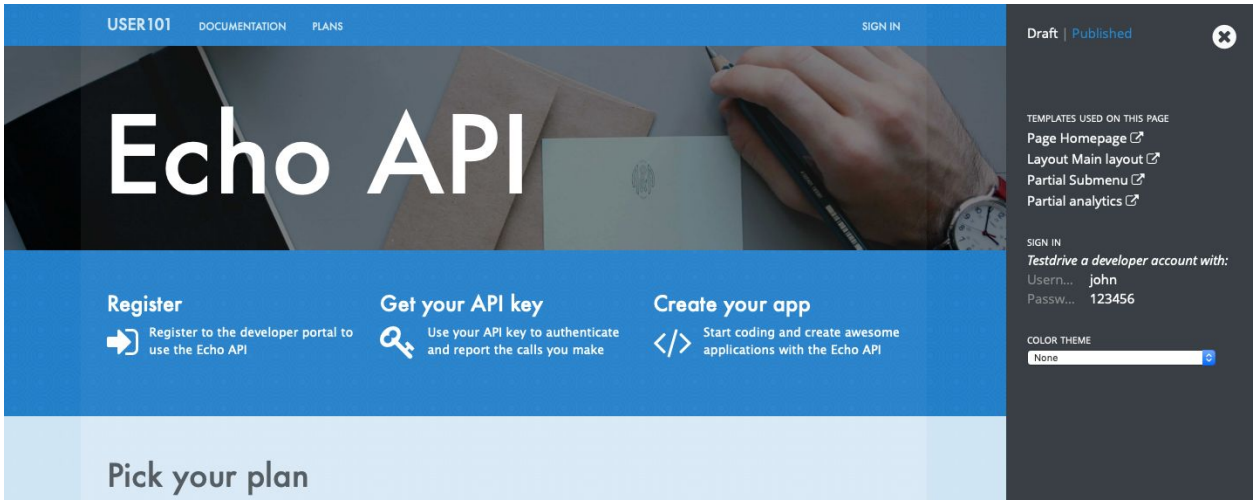
We now have an assigned key so we can go back to the Configuration window of the API service and make a successful test call. **API -> Integration -> edit Apicast configuration**



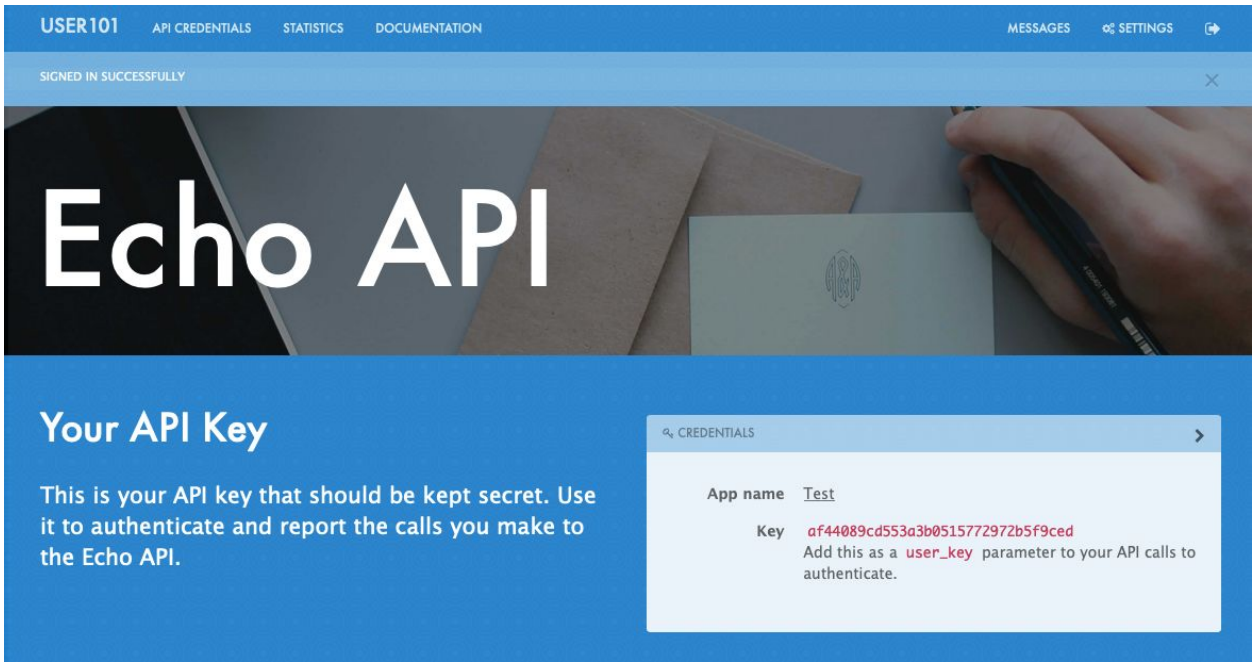
We now have a pre-populated key in the example curl statement, let's try again testing the deployed configuration.



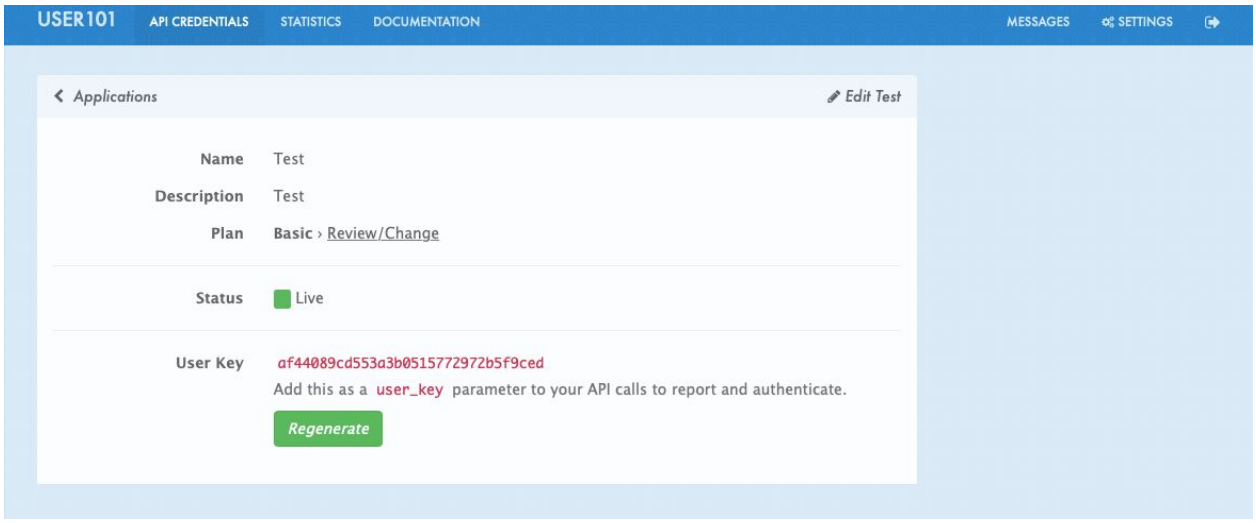
As we can see we turned the testing into a success.
Let's switch to the developers' point of view by accessing the Developer portal. **Developer portal -> Visit Developer Portal**
The sidebar allows us to edit pages of the Developer Portal live, but we are not interested in it so we can close it.



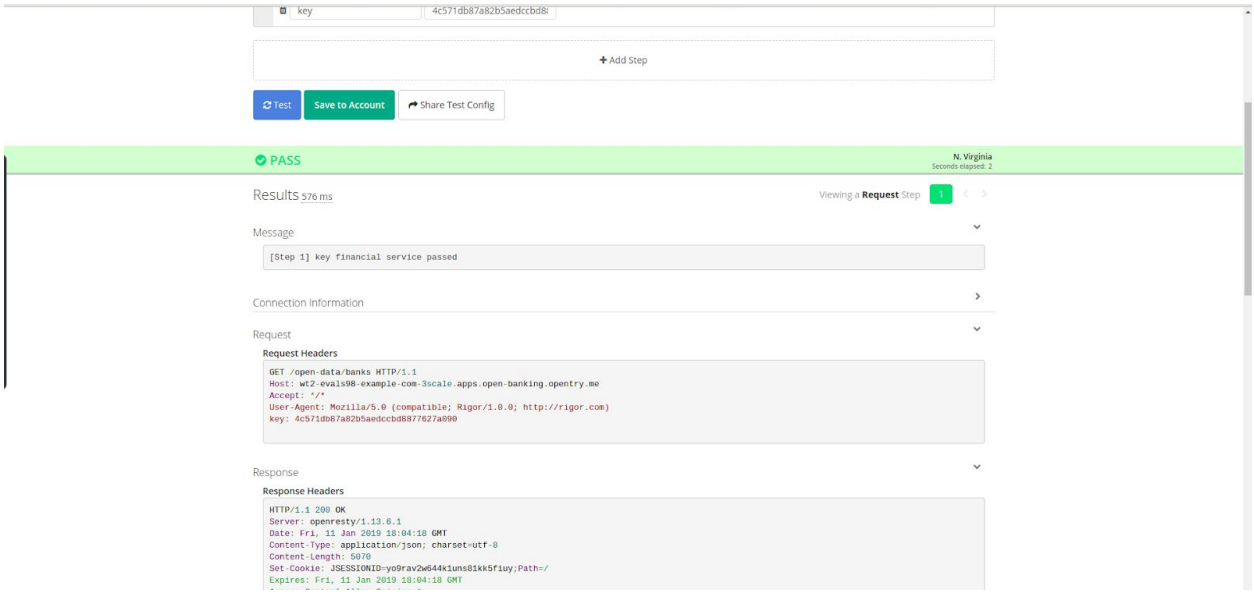
Let's sign in with the default user credentials provided in the sidebar. john / 123456



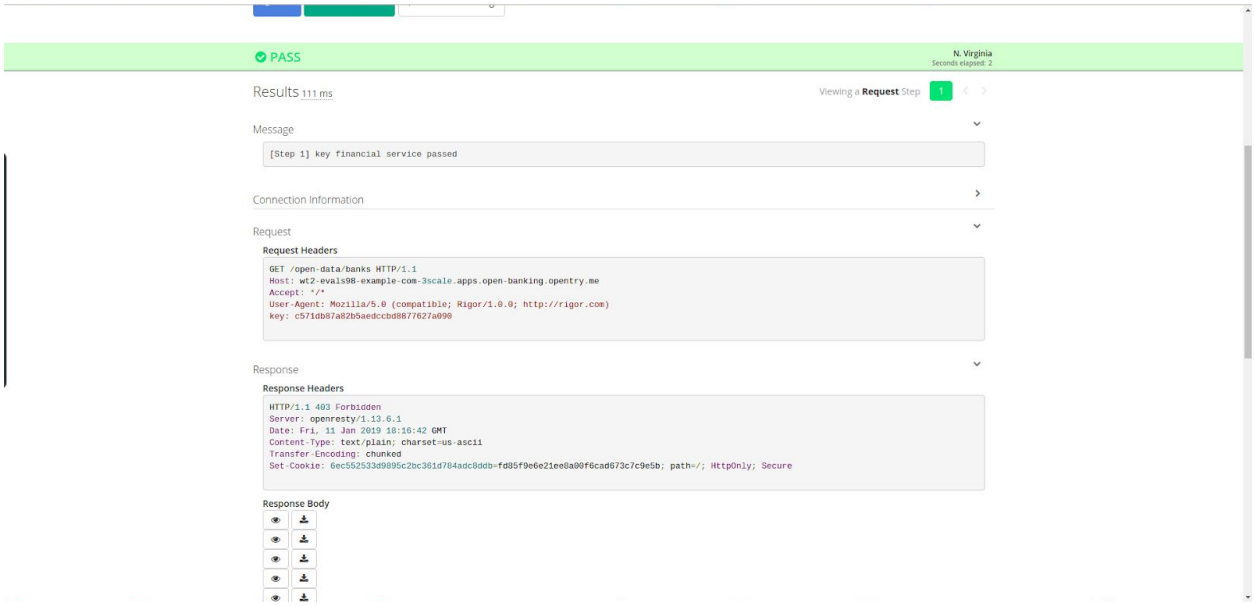
We are now logged in the developer's dashboard. Let's see the Applications I have



I can now use the credential that I have associated with the application and test the protected service. Let's move to an online API testing tool, https://apitester.com/



Use the URL for your API gateway, the following format should be configured in your service already: https://userX.amp.apps.openbanking-4f6a.openshiftworkshop.com the key Header and related value. As we can see we succeed with 200 OK!
Let's now just test with a wrong key or path then to confirm the role of API Management.



As expected we receive a Forbidden error.

Checkpoint

Break

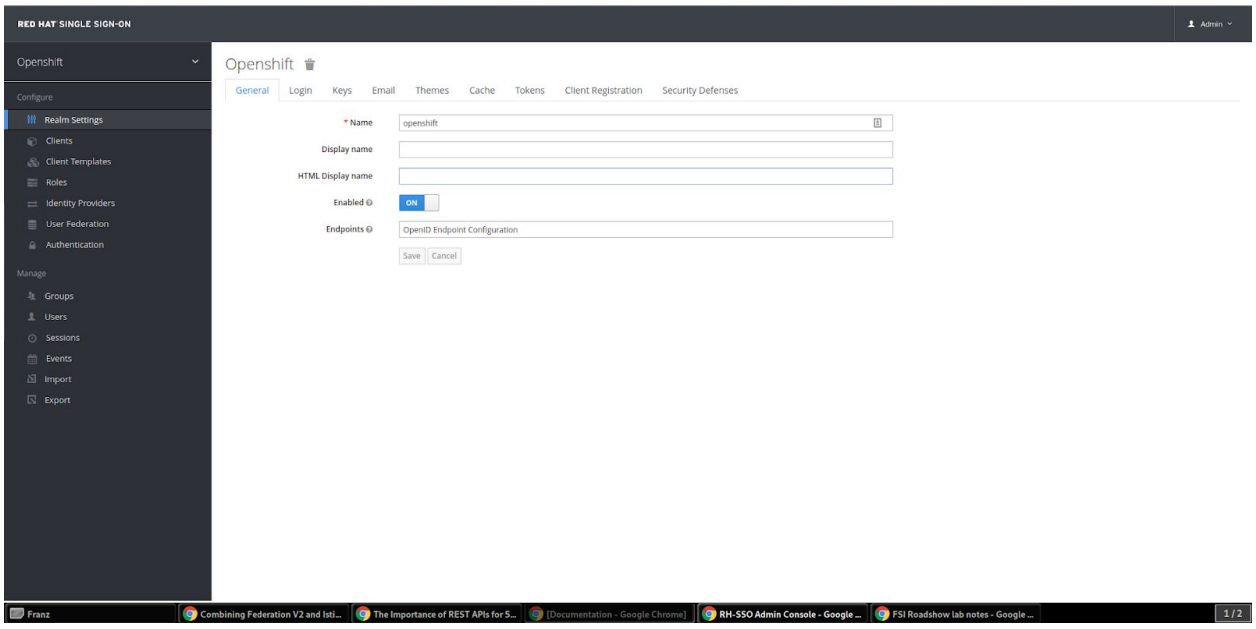
Practical Part 2

RH SSO and 3SCALE OIDC

Let's now improve the security of the controlled service with OIDC. API key is not considered a safe method anymore and is vulnerable to many attacks.
After introducing content around OAuth and OIDC, let's see the main elements of RH SSO itself.

SINCE AS INTEGR8LY USERS YOU DON'T HAVE ACCESS TO THE RELATED RH SSO REALM, YOU ARE GOING TO SEE HOW TO CONFIGURE A RH SSO CLIENT THAT WILL THEN BE USED BY EVERYBODY IN THEIR 3SCALE CONFIGURATION. AS ADMIN YOU WILL NEED TO GET THE USER AND PASSWORD FROM THE ENVIRONMENT VARIABLES OF SSO TO ACCESS THE ADMIN CONSOLE OF RH SSO. YOU WILL NEED TO LOGIN TO OPENSHIFT AS ADMIN.

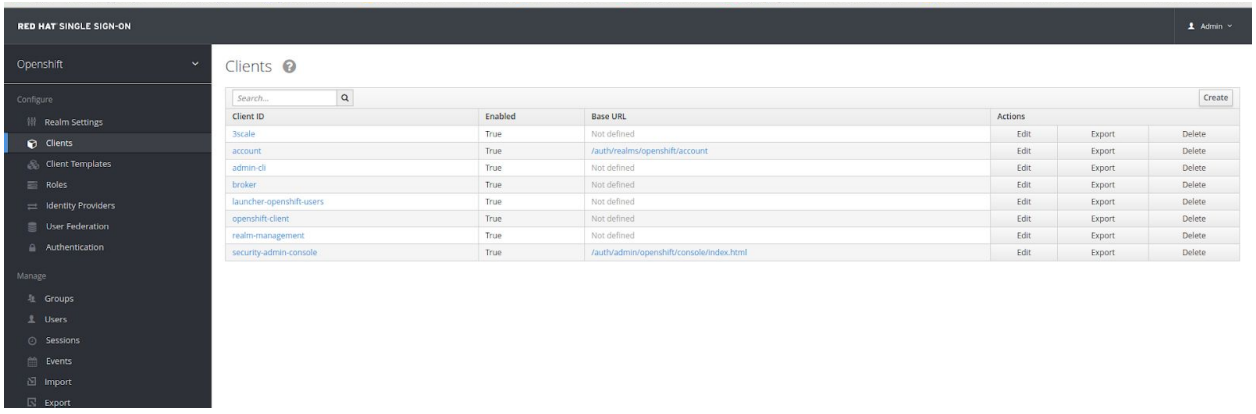
Let's start with RH SSO main dashboard
https://sso-test.apps.openbanking-4f6a.openshiftworkshop.com
Alternatively
http://sso-rhsso.apps.openshift.es



The realms are like separate instances of the platform, dedicated to separating users and applications. As we can see we can customize several aspects of the realm like the theme of the login page or the the tokens' default parameters. **Endpoints -> OpenID Endpoint Configuration**

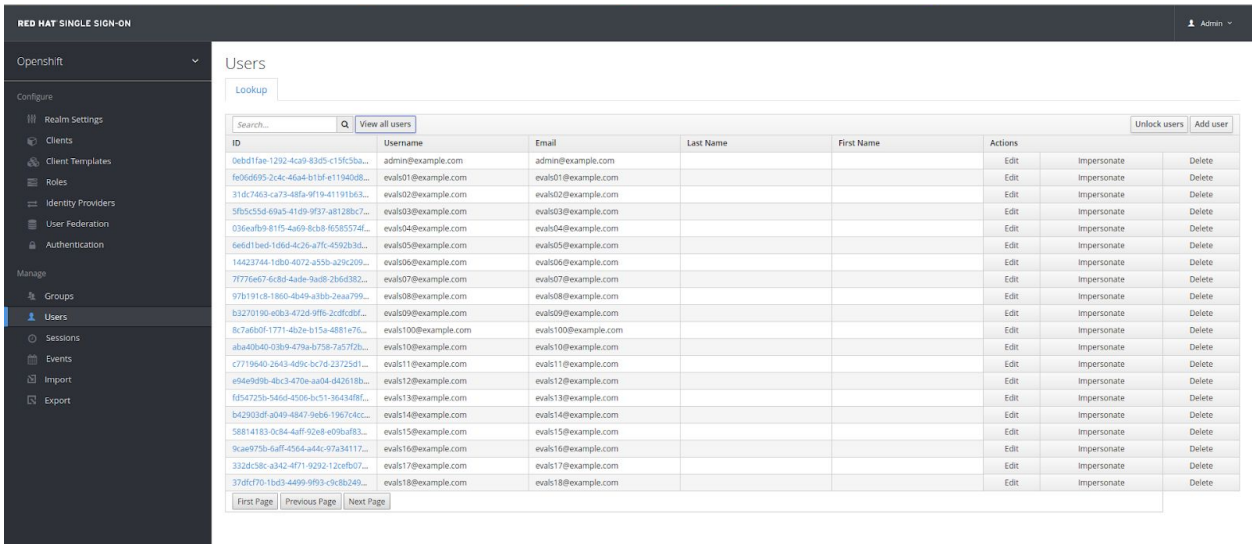
```
{
  "issuer": "https://secure-sso-sso.apps.open-banking.opentry.me/auth/realms/openshift",
  "authorization_endpoint": "https://secure-sso-sso.apps.open-banking.opentry.me/auth/realms/openshift/protocol/openid-connect/auth",
  "token_endpoint": "https://secure-sso-sso.apps.open-banking.opentry.me/auth/realms/openshift/protocol/openid-connect/token",
  "token_introspection_endpoint": "https://secure-sso-sso.apps.open-banking.opentry.me/auth/realms/openshift/protocol/openid-connect/token/introspect",
  "userinfo_endpoint": "https://secure-sso-sso.apps.open-banking.opentry.me/auth/realms/openshift/protocol/openid-connect/userinfo",
  "end_session_endpoint": "https://secure-sso-sso.apps.open-banking.opentry.me/auth/realms/openshift/protocol/openid-connect/logout",
  "jwks_uri": "https://secure-sso-sso.apps.open-banking.opentry.me/auth/realms/openshift/protocol/openid-connect/certs",
  "check_session_iframe": "https://secure-sso-sso.apps.open-banking.opentry.me/auth/realms/openshift/protocol/openid-connect/login-status-iframe.html",
  "grant_types_supported": [
    "authorization_code",
    "implicit",
    "refresh_token",
    "password",
    "client_credentials"
  ],
  "response_types_supported": [
    "code",
    "none",
    "id_token",
    "token",
    "id_token token",
    "code id_token",
    "code token",
    "code id_token token"
  ],
  "subject_types_supported": [
    "public",
    "pairwise"
  ],
  "id_token_signing_alg_values_supported": [
    "RS256"
  ],
  "userinfo_signing_alg_values_supported": [
    "RS256"
  ],
  "request_object_signing_alg_values_supported": [
    "none",
    "RS256"
  ],
  "response_modes_supported": [
    "query",
    "fragment",
    "form_post"
  ],
  "registration_endpoint": "https://secure-sso-sso.apps.open-banking.opentry.me/auth/realms/openshift/clients-registrations/openid-connect",
  "token_endpoint_auth_methods_supported": [
    "private_key_jwt",
    "client_secret_basic",
```


This is where we can find the public endpoints of the Realm exposed by RH SSO (we are going to be using this later).
Let's now take a look at the Clients section.

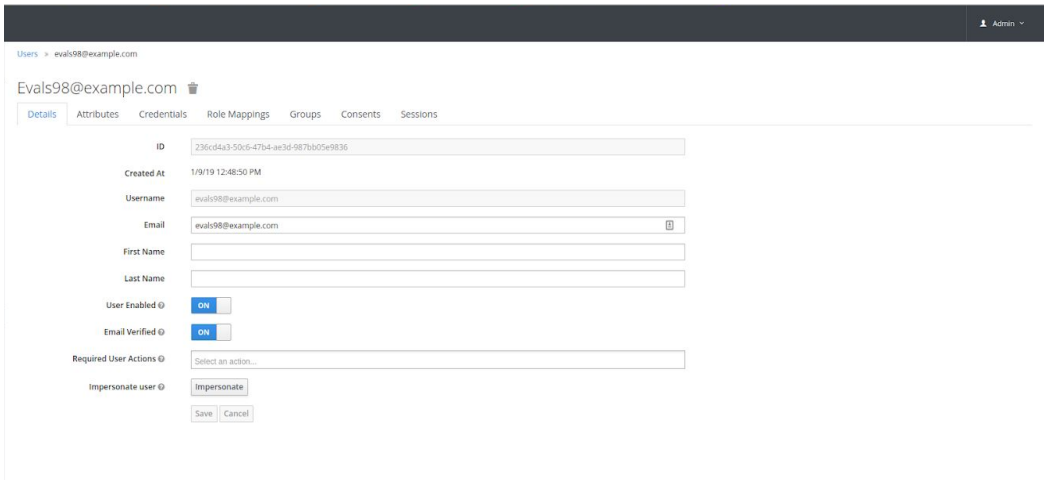


Here we can configure the applications that will authenticate using RH SSO as an IDP. As we can see there are some default clients dedicated to authentication in the integr8ly environment.

Users -> View all users

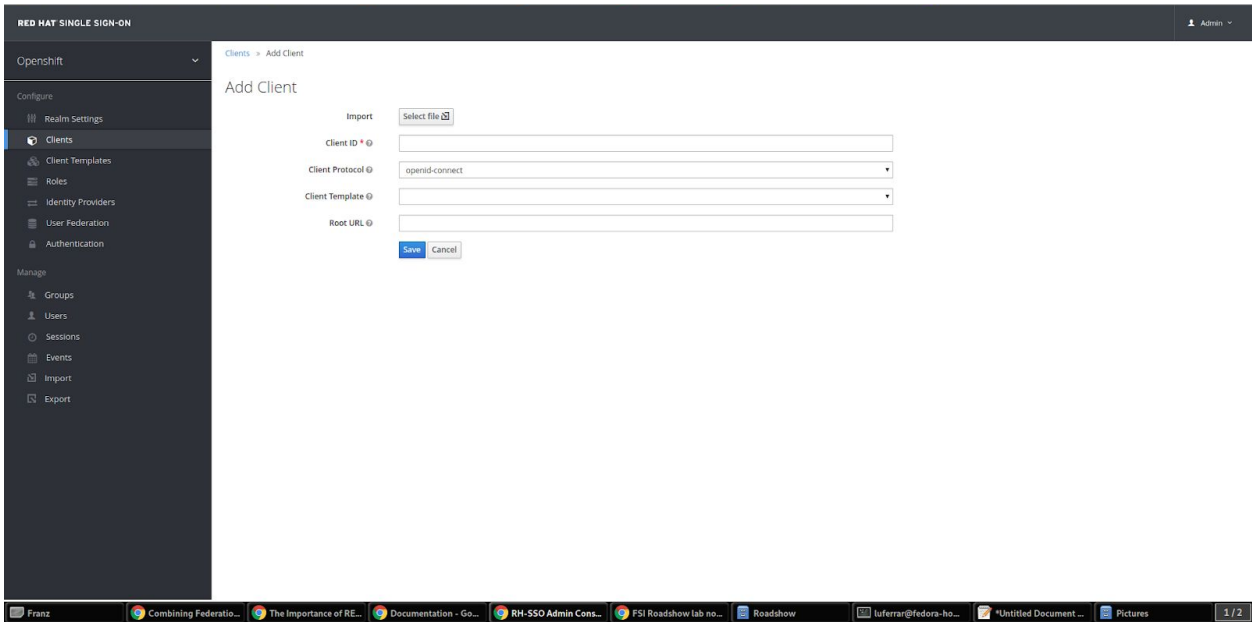


Here we can see all the users that are stored inside RH SSO, making it act as an IDM as well. These are the end users of the applications created in Clients. Let's explore one of these users.

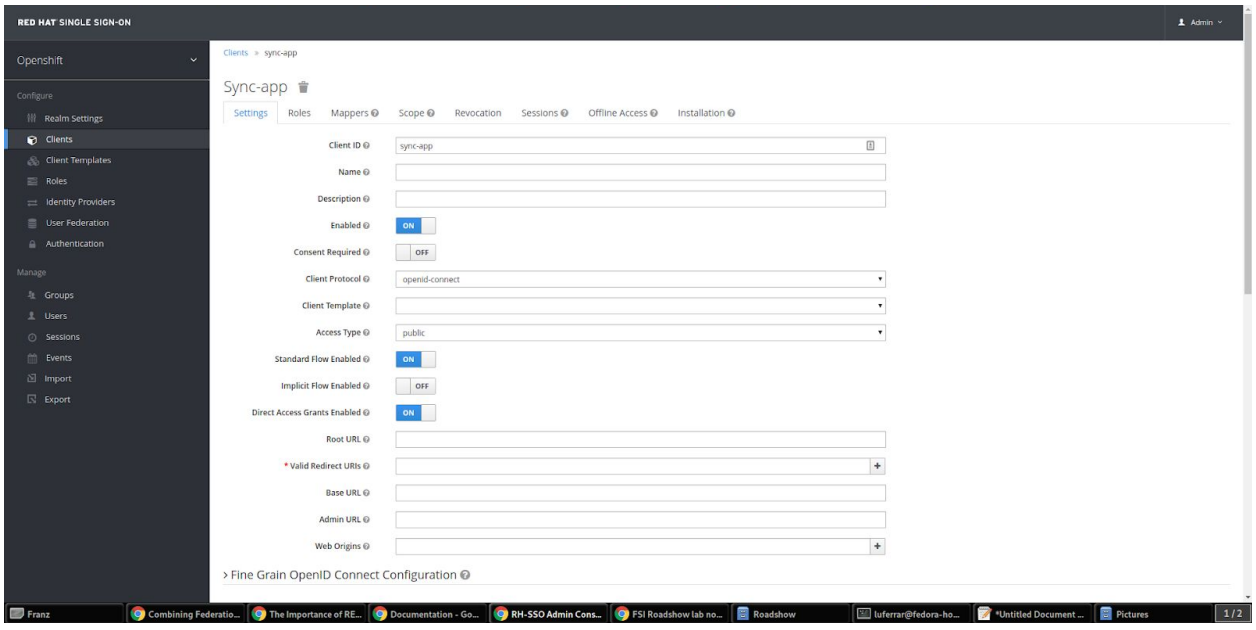


We can see here the type of information stored along with basic user details. The user profile can be customized with additional attributes as well.

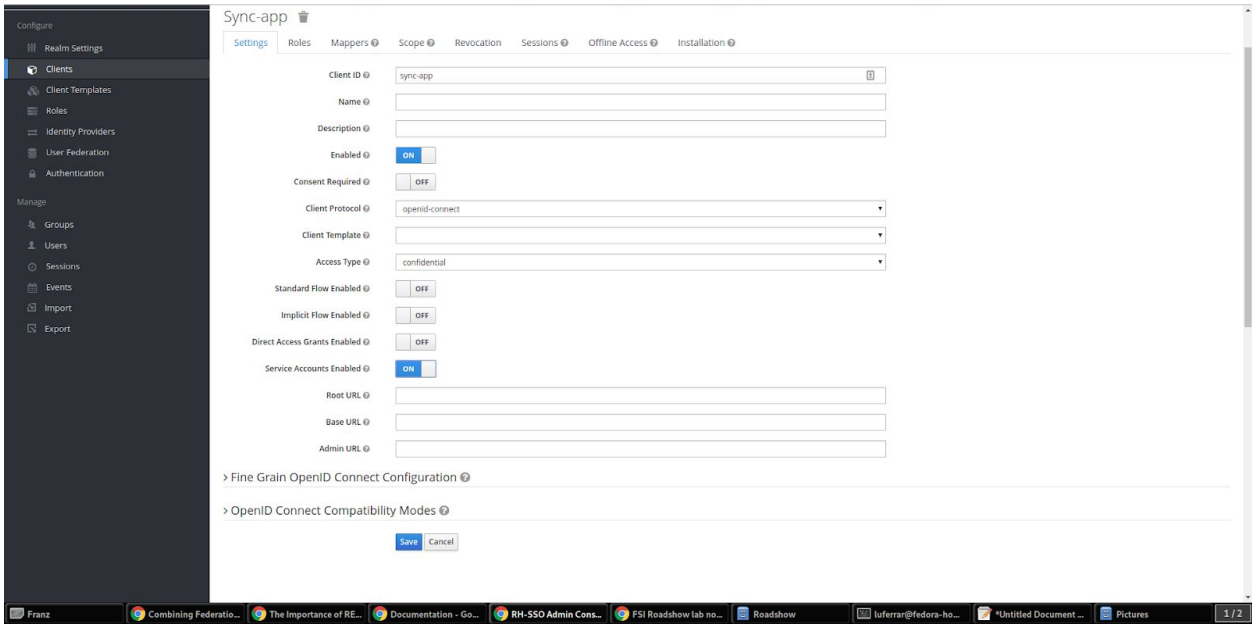
We will take advantage of one of the features available in OIDC and not in OAUTH which is dynamic client registration.
Normally to make sure an API application authenticates with RH SSO, we would need to manually create the application on both platforms. With this feature, we let 3scale sync the applications to RH SSO, as well as obviously authenticating our API calls. Let's create a special type of such Client in RH SSO. **Clients -> Create**



Let's call it sync-app and configure the other details required to let it communicate with 3scale.

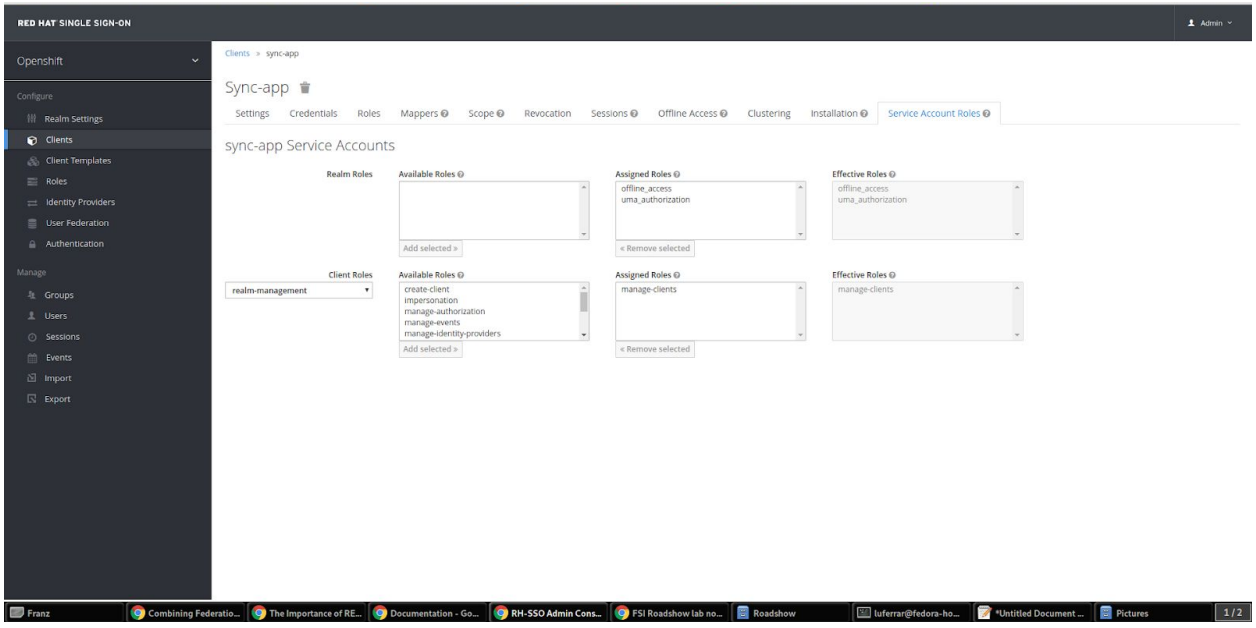


We are going to give it the rights to create applications on behalf of 3scale (*service accounts enabled*).



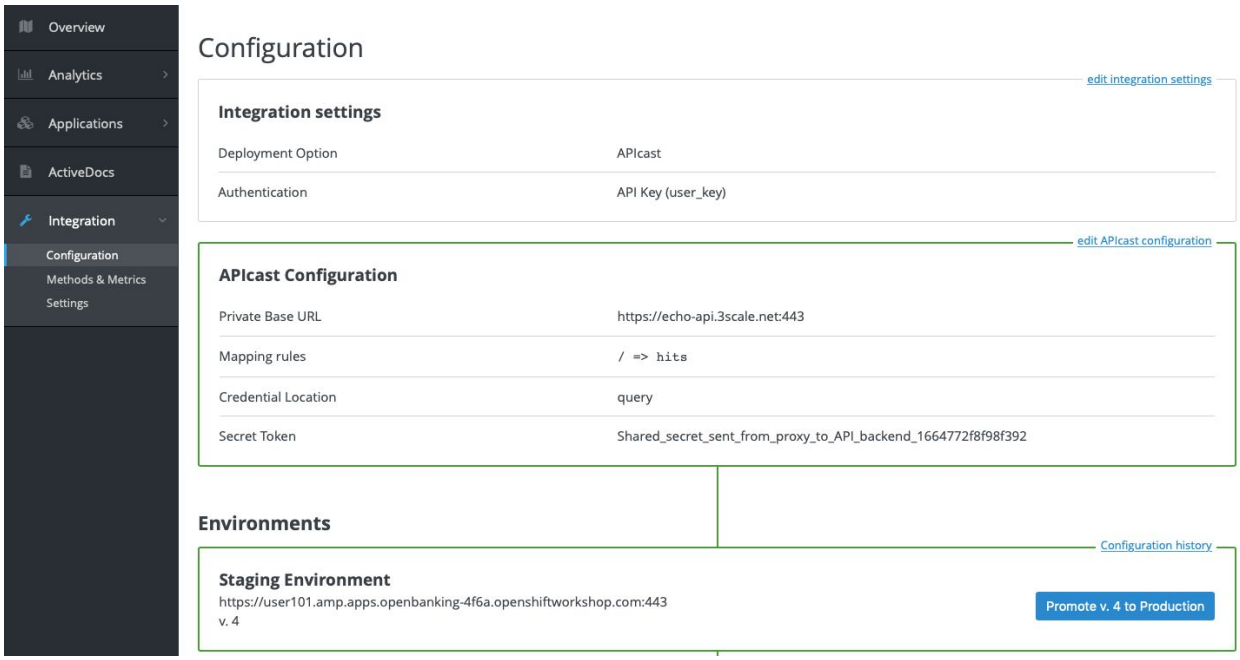
Save -> Service account roles

Add manage-clients to the allowed this special client to create application on behalf of API management

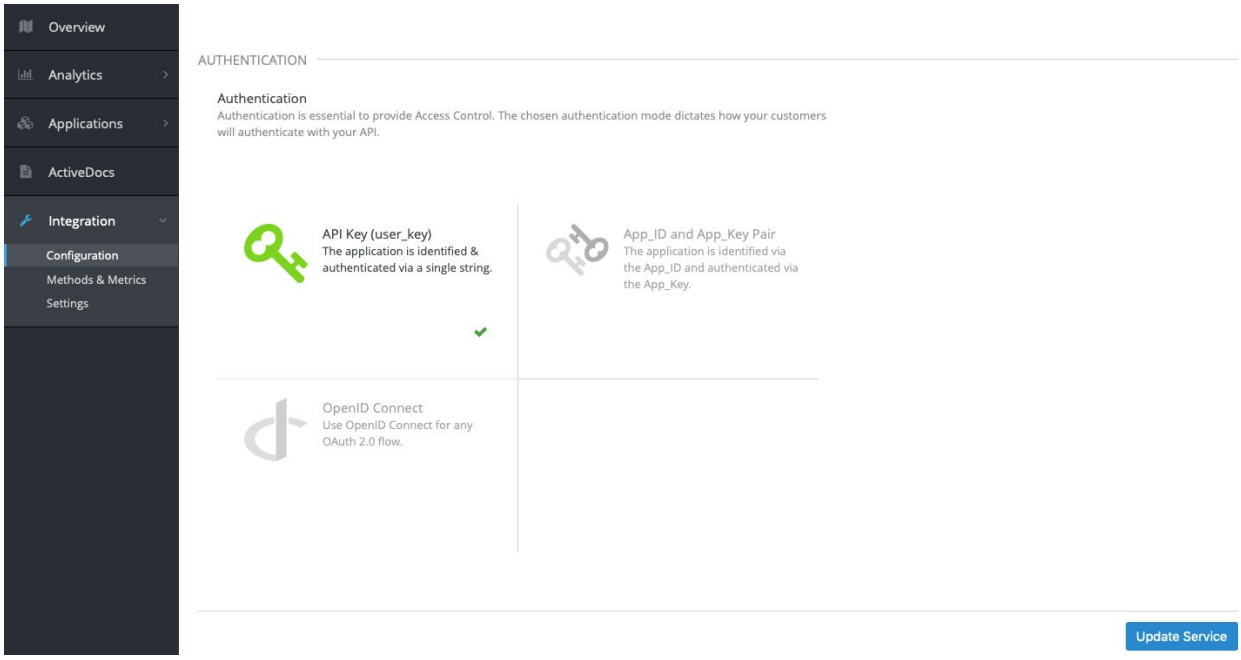


And now we are ready to use these application credentials inside 3scale OIDC configuration section.

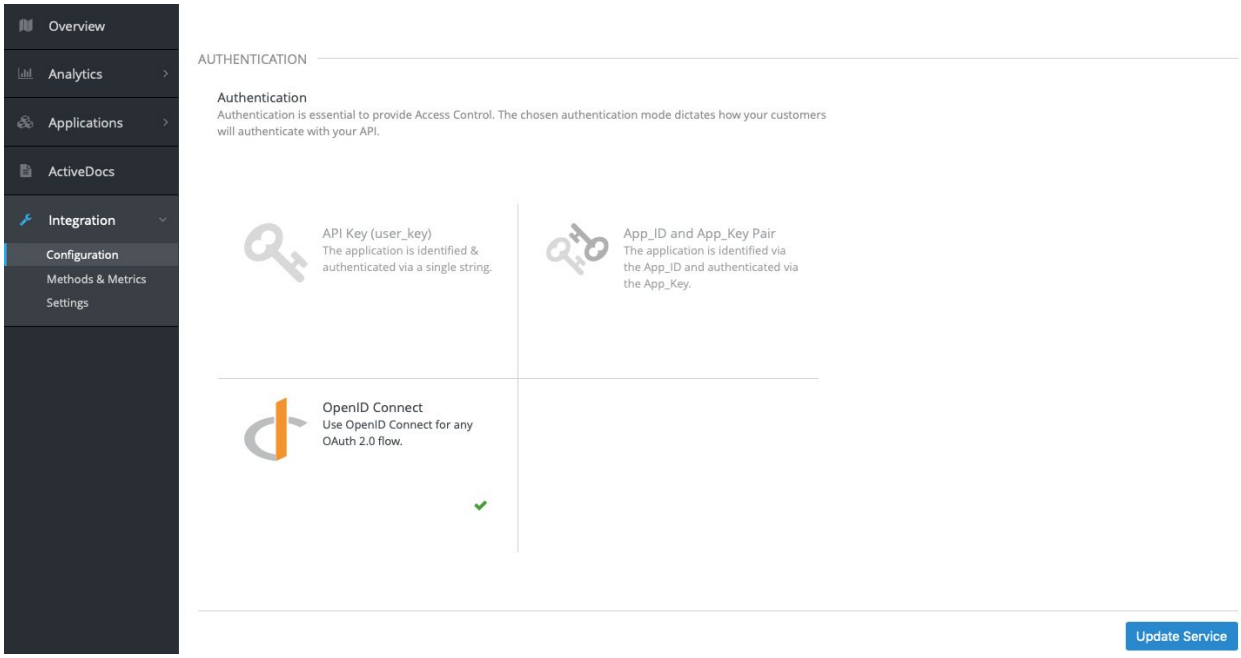
Let's now switch back to 3scale to configure the API management side of OIDC authentication.



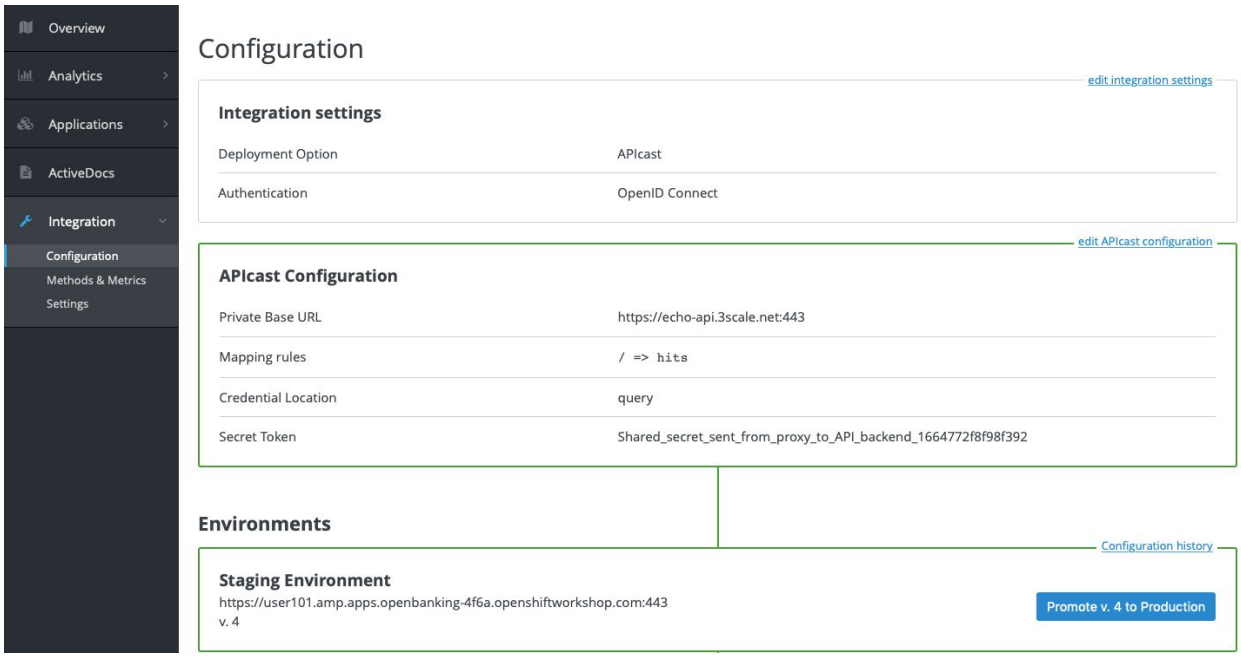
We can see that we have a fully configured API with API key as the Authentication method. We are going to change it to the more secure OpenID Connect, to ensure our financial data are protected from attacks performed when a key is compromised. **Edit integration settings**



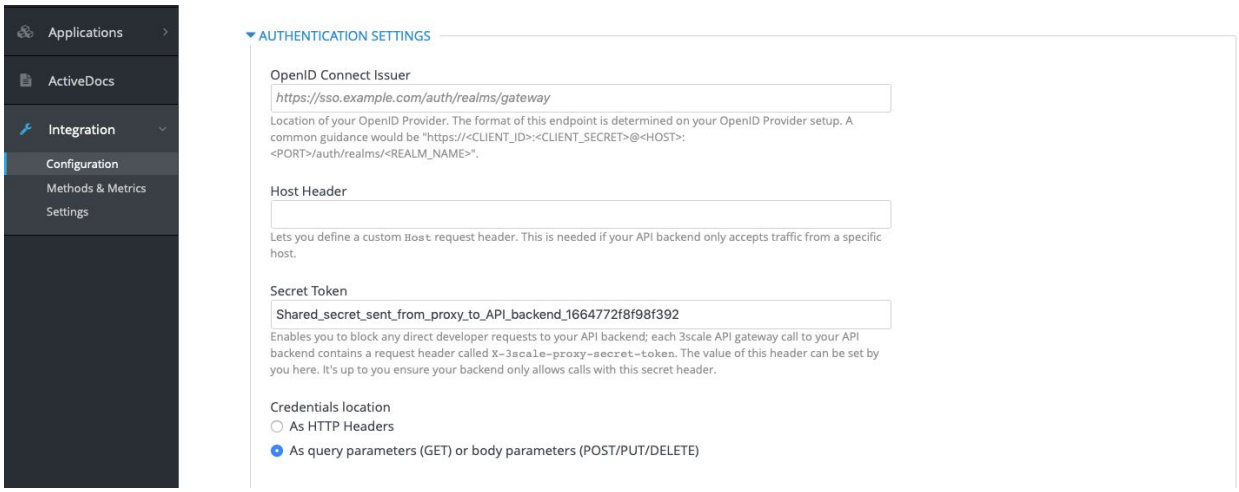
We are going to change it to OpenID Connect. **Update service**



Clearly the platform is warning us that we have customers using this API and it might break their application, changing the authentication method. In a real world case, we would inform the developer in advance by using the messaging and notification functionality available within the platform.



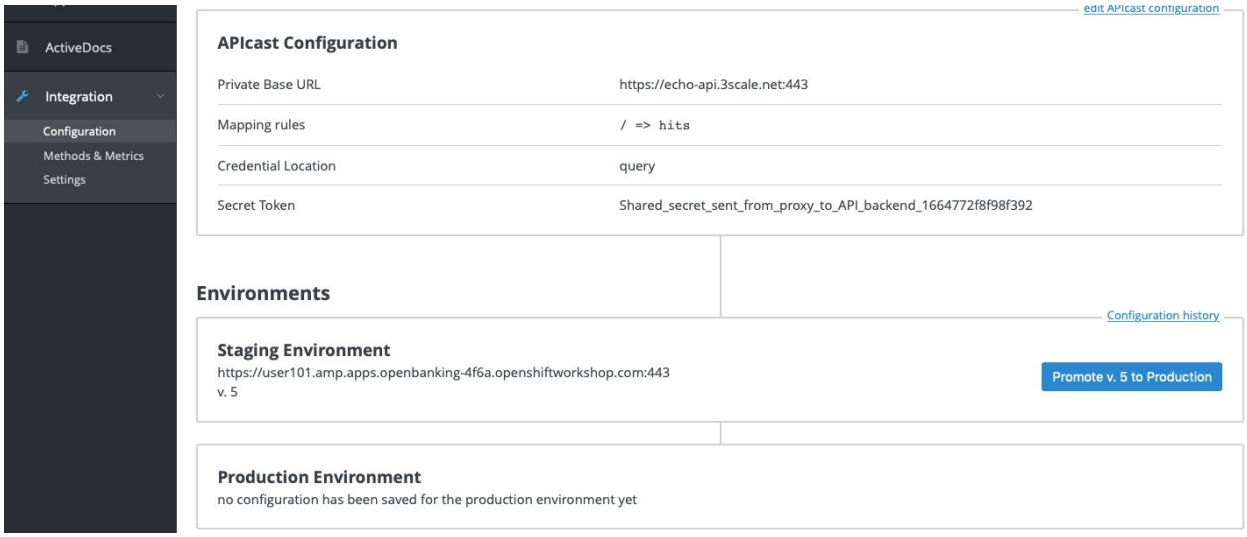
We have now changed the authentication method, we are just left with configuring the correct IdP inside 3scale to make sure it is authenticating the requests with RH SSO. **edit apicast configuration**



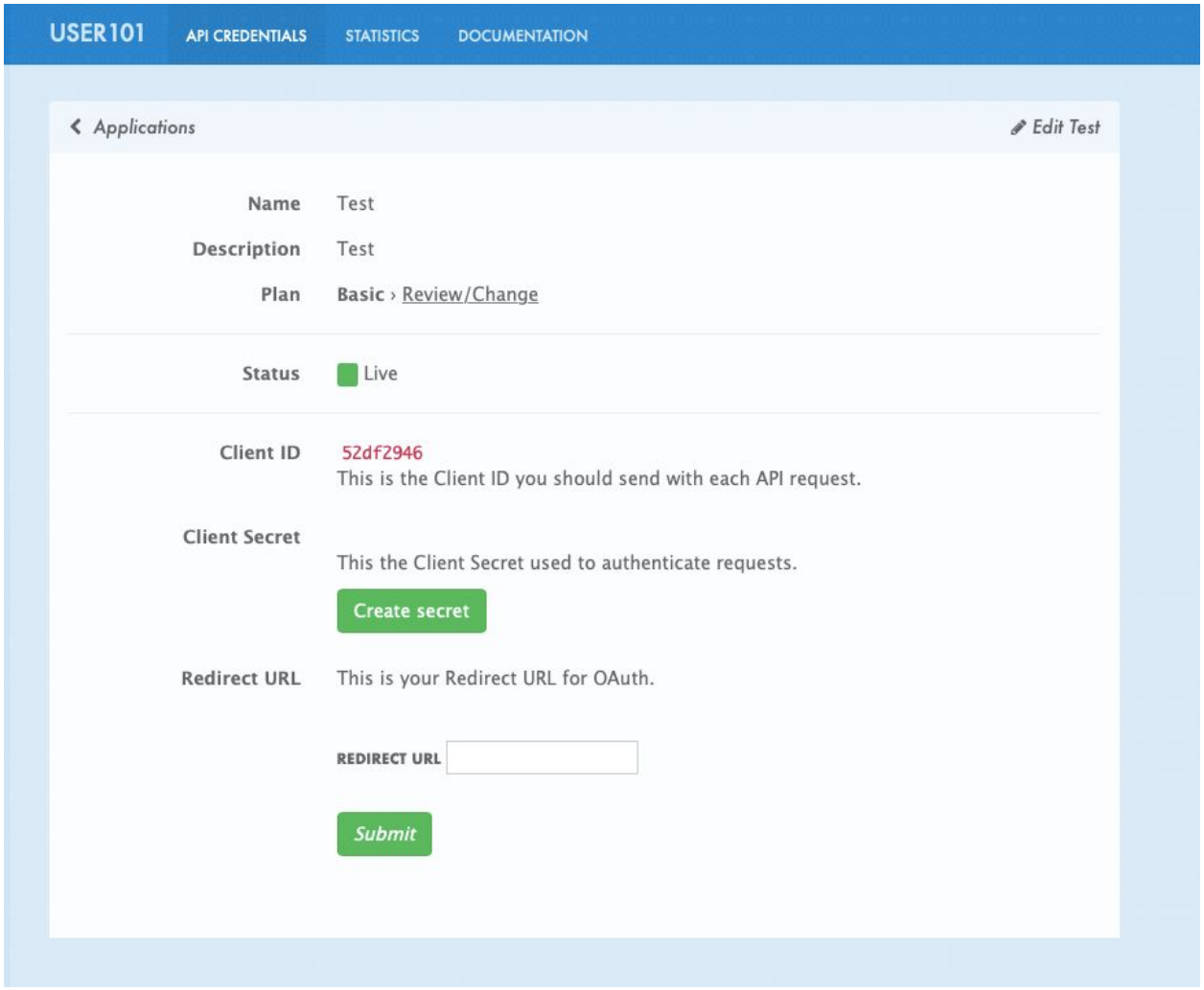
As we see we have a dedicated field for this purpose now: **OpenID Connect Issuer**

Let's build a url of this format to use it:
http://client-id:client-secret@<rh-sso-public-endpoint>
where client-id: sync-app
client secret: 1b6886b5-db99-4343-a6ca-73ef8fd25b95
rh-sso-public-endpoint: http://sso-rhsso.apps.openshift.es/auth/realms/3scale-auth

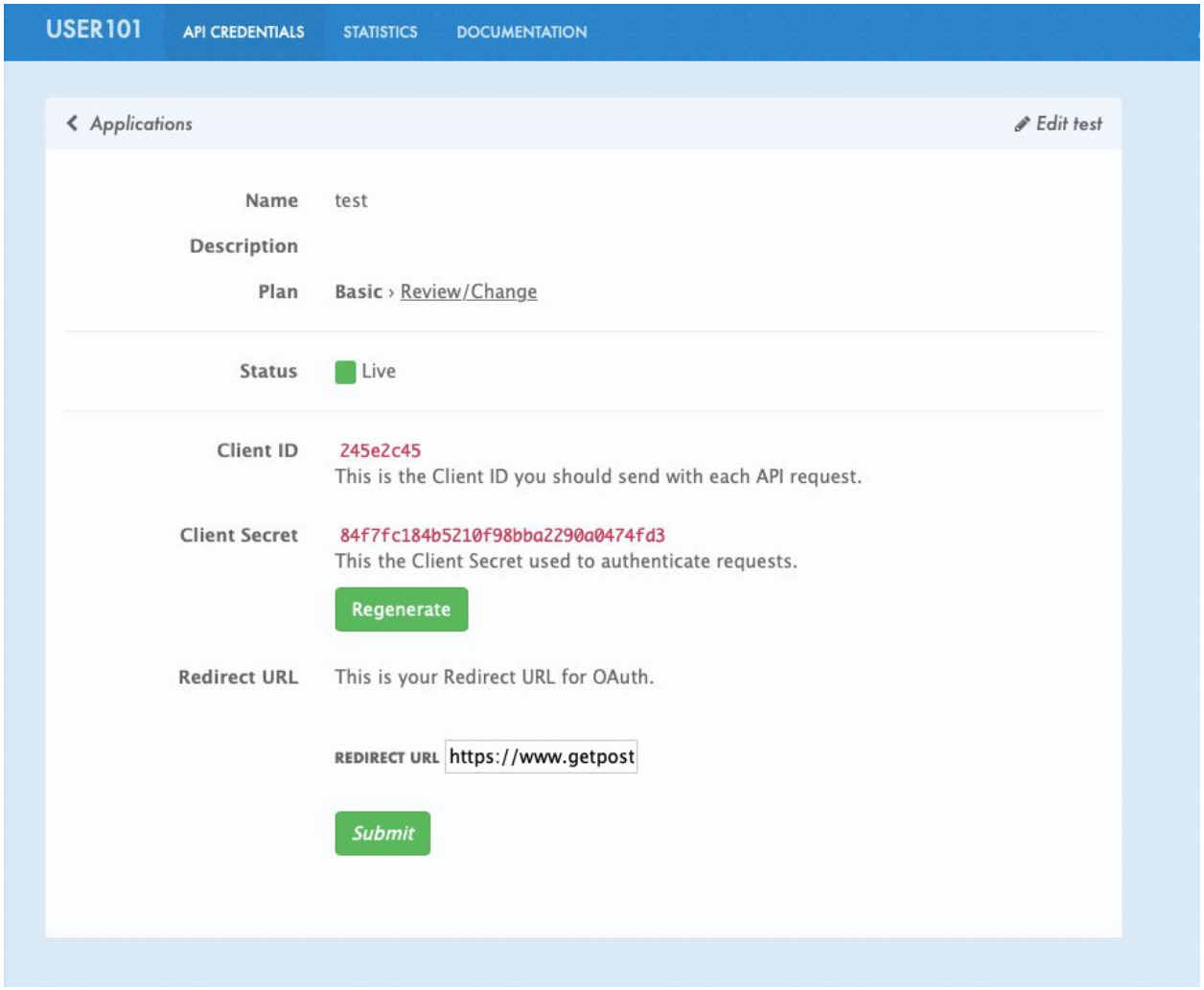
And update the staging environment and promote the configuration to production by clicking the blue button *Promote to production.*



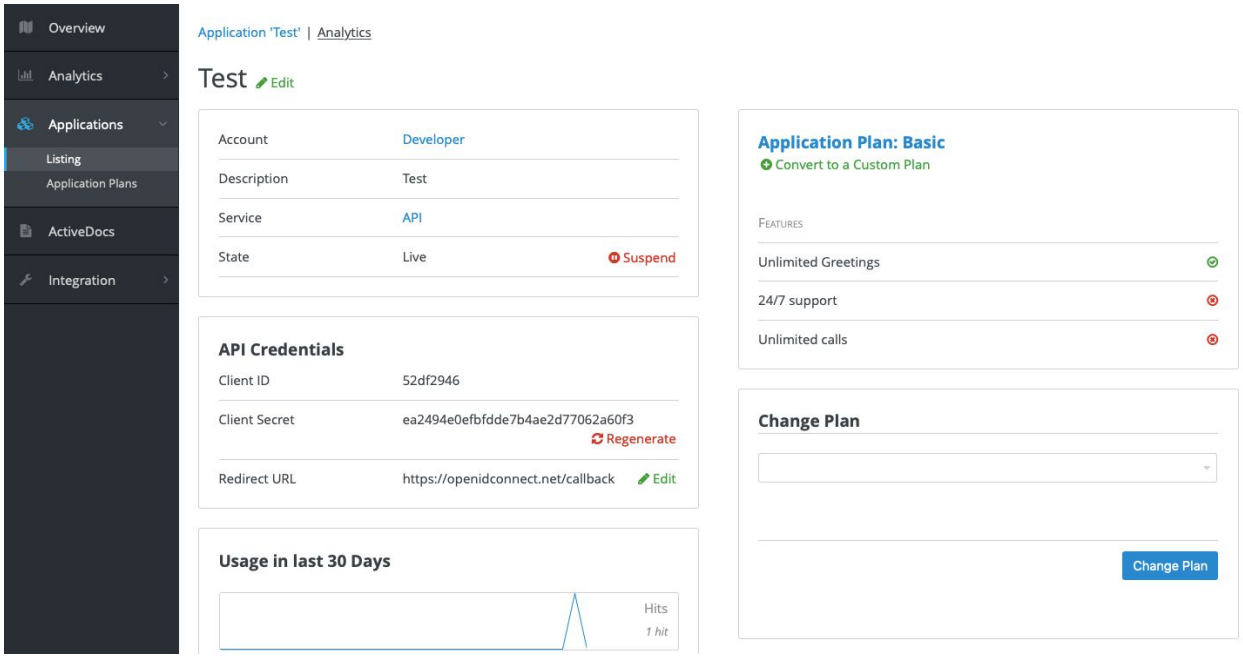
Let's now switch perspective and get in the shoes of the developer and open their Applications section.

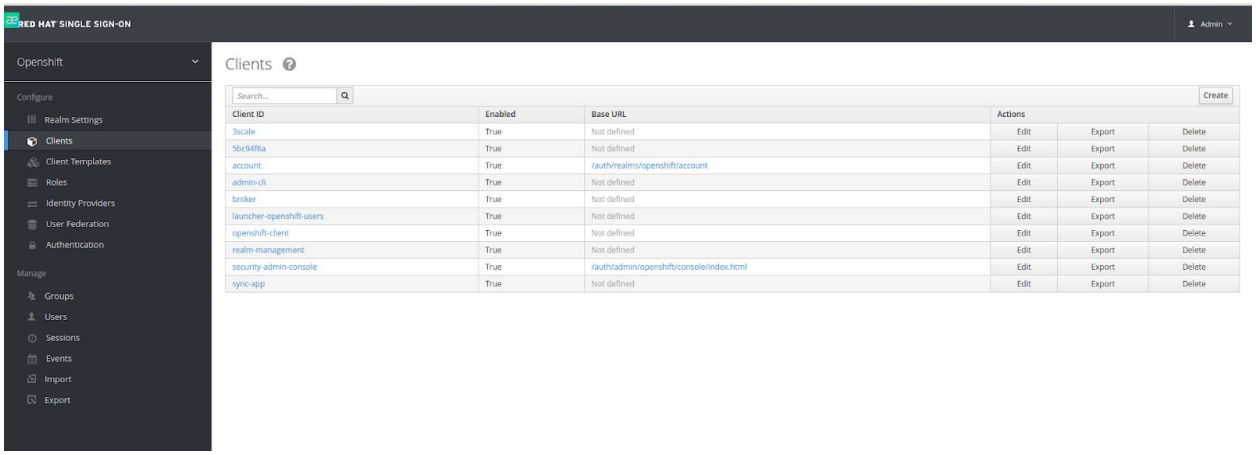


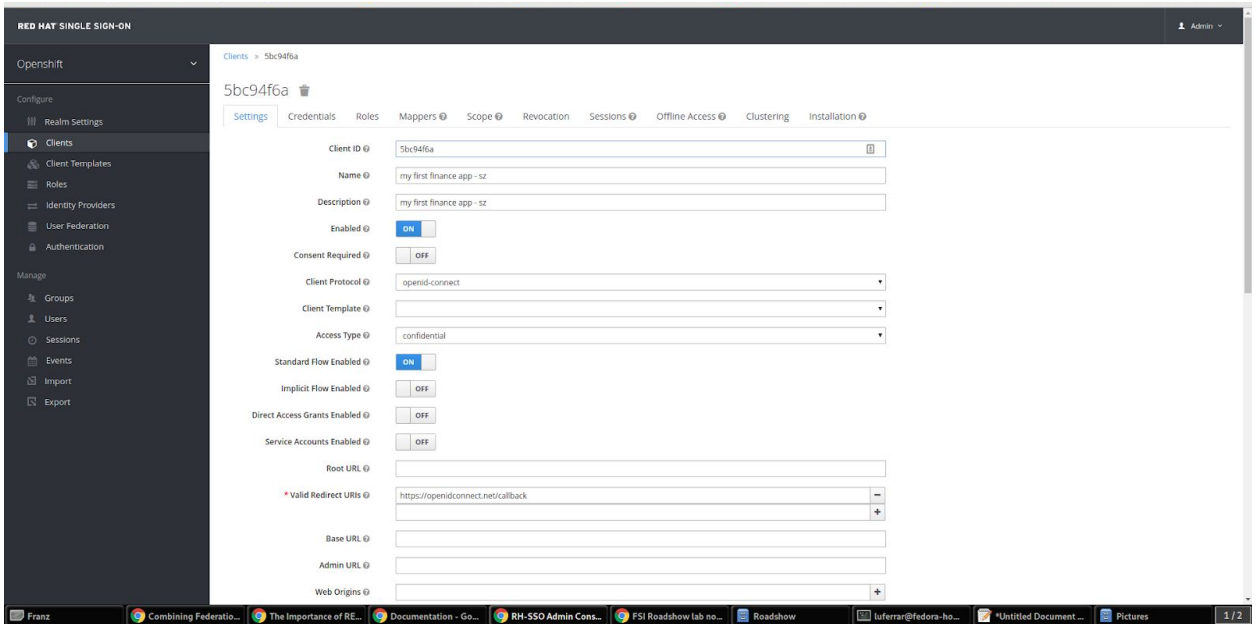
We can see the secret of their application is absent as is the redirect URL. We are going to generate the first and add as redirect url the following https://openidconnect.net/callback (we are going to explain why in a moment).



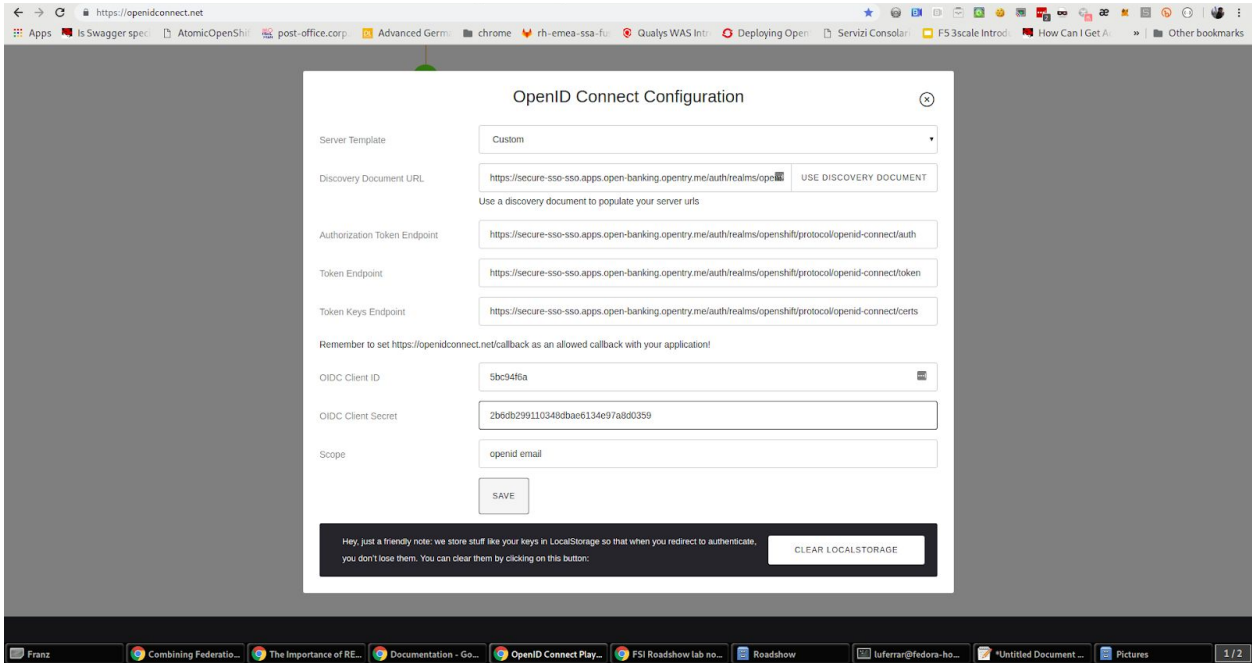
Let's make sure that the application is now aligned in terms of credentials both in 3scale and RH SSO.


Overview
Analytics
Applications
Listing
Application Plans
ActiveDocs
Integration
Application 'Test' | Analytics
Test Edit
Account Developer
Description Test
Service API
State Live Suspend
API Credentials
Client ID 52df2946
Client Secret ea2494e0efbfdde7b4ae2d77062a60f3
Regenerate
Redirect URL https://openidconnect.net/callback Edit
Usage in last 30 Days
Hits
1 hit
Application Plan: Basic
Convert to a Custom Plan
Features
Unlimited Greetings
24/7 support
Unlimited calls
Change Plan
Change Plan

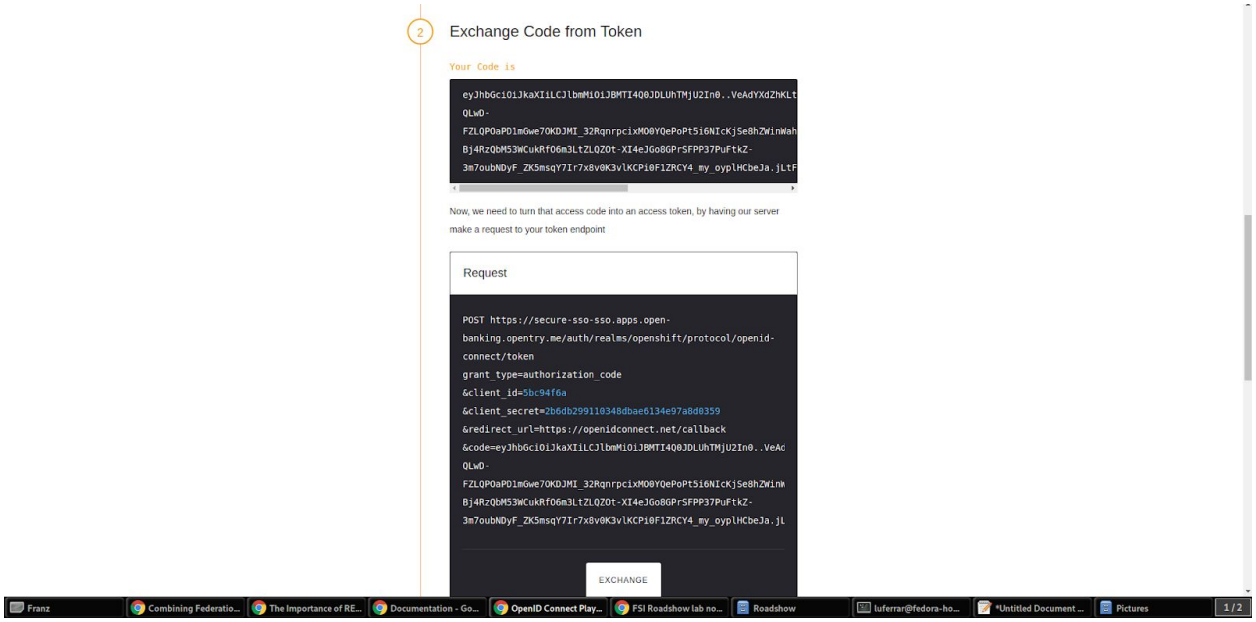

RED HAT SINGLE SIGN-ON
Admin
Openshift
Configure
Realm Settings
Clients
Client Templates
Roles
Identity Providers
User Federation
Authentication
Manage
Groups
Users
Sessions
Events
Import
Export
Clients
Search...
Create
Client ID
Enabled
Base URL
Actions
3scale True Not defined Edit Export Delete
5bc94f6a True Not defined Edit Export Delete
account True /auth/realms/openshift/account Edit Export Delete
admin-cli True Not defined Edit Export Delete
broker True Not defined Edit Export Delete
launcher-openshift-users True Not defined Edit Export Delete
openshift-client True Not defined Edit Export Delete
realm-management True Not defined Edit Export Delete
security-admin-console True /auth/admin/openshift/console/index.html Edit Export Delete
sync-app True Not defined Edit Export Delete



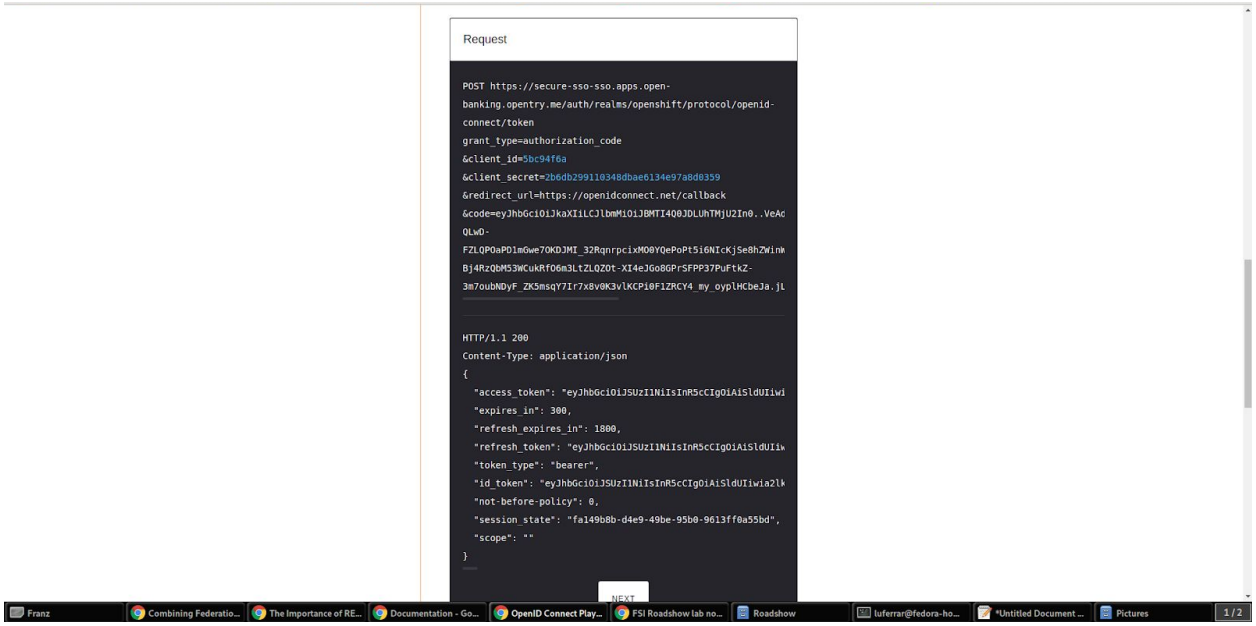
All seems good! Let's now try to authenticate the end user, using OpenID Connect.
We are going to need a special web client, a little bit more intelligent than just the API tester: https://openidconnect.net/
Let's configure it with the correct parameters from the previous steps. **Configuration**
Let's change the server template to custom and input in the discovery URL the one we opened before in our RH SSO realm
http://sso-rhsso.apps.openshift.es/auth/realms/3scale-auth/.well-known/openid-configuration
We are going to use the client id and secret as from the application in the developer portal.
And lastly as scope we are going to add **openid** and **email**. **SAVE**



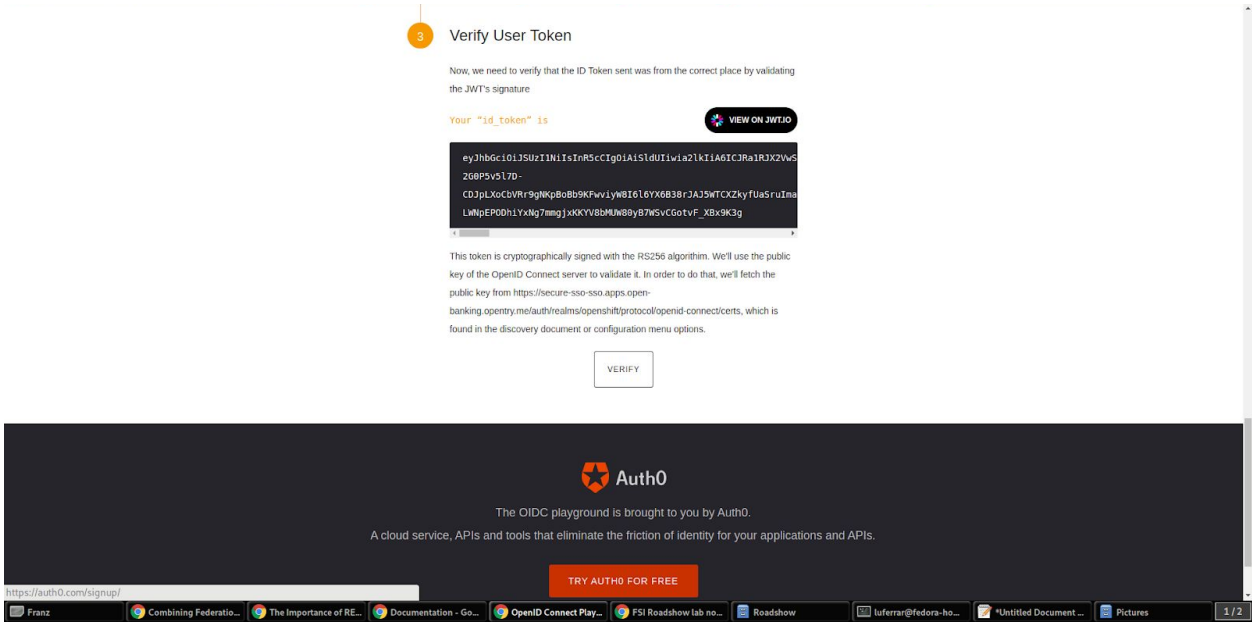
Start the authentication flow by hitting start. You are going to be redirected to the RH SSO login interface where you can use a default user details and password (luca / password). Once you login you will receive a temporary code to be exchanged for the final credentials or access token.



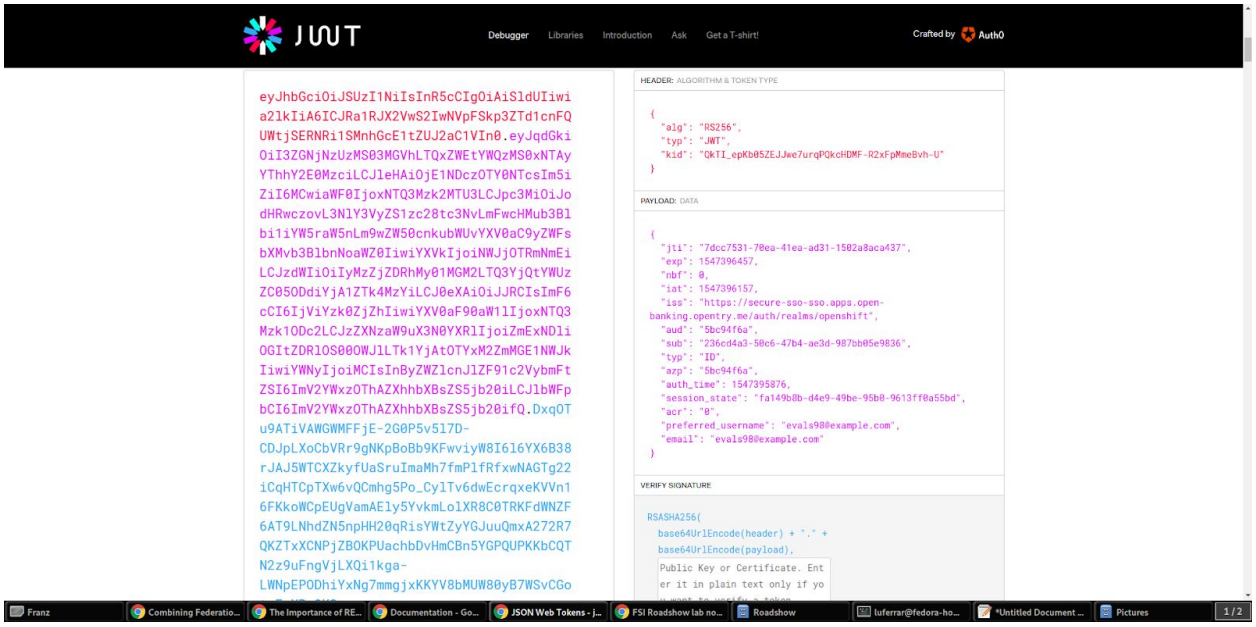
Hit **Exchange**



You will receive the “access_token” which is an expiring credential that we will be using to authenticate with 3scale to get access to the configured API. We can see that another important piece of information is shown there regarding when this credential will expire.
We can hit **NEXT** and id_token will also be shown, which contains the more user related details.



We can decode the information on JWT.io and found our user details once again as passed to the Backend service.

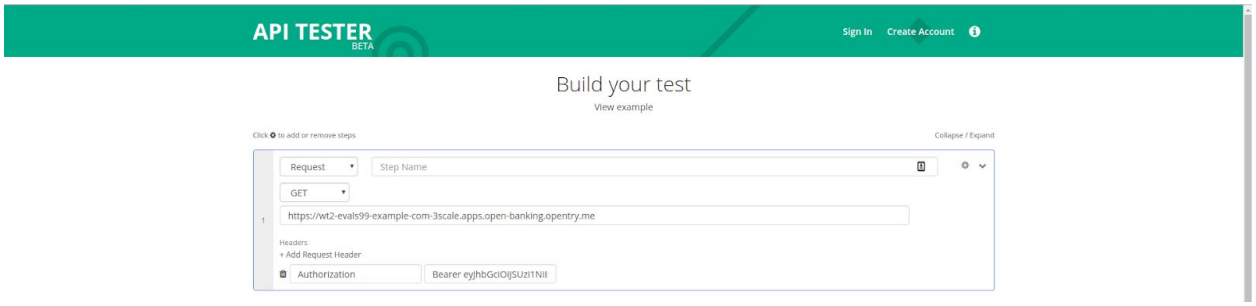


Let's now go back to our OpenID client and copy the access token long string.
It should look something like this:

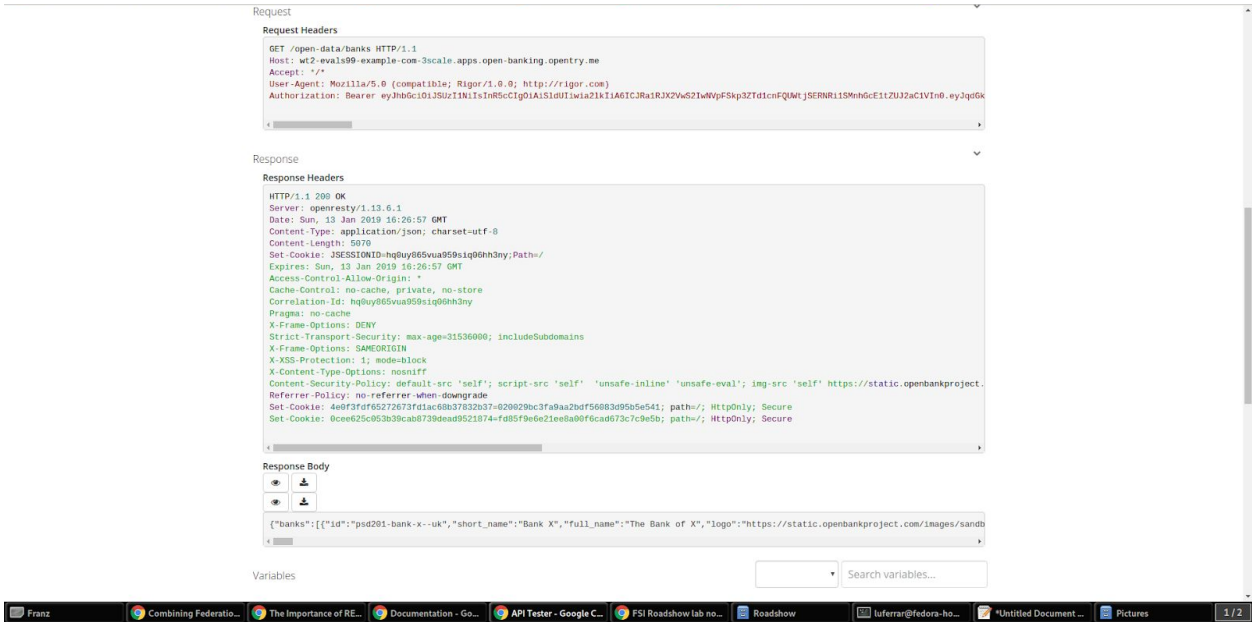
eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldUIiwia2lkIiA6ICJRa1RJX2VwS2IwNVpFSkp3ZTd1cnFQUWtjSERNRi1SMnhGcE1tZUJ2aC1VIn0.eyJqdGkiOiIyYzJmZjQ5ZS01MDY4LTQ0MjQtYTRiNS05MWU3OTk3MTM0YTMiLCJleHAiOjE1NDczOTc1NTIsIm5iZiI6MCwiaWF0IjoxNTQ3Mzk2NjUyLCJpc3MiOiJodHRwczovL3NlY3VyZS1zc28tc3NvLmFwcHMub3Blbi1iYW5raW5nLm9wZW50cnkubWUvYXV0aC9yZWFsbXMvb3BlbnNoaWZ0IiwiYXVkIjoiNWJjOTRmNmEiLCJzdWIiOiIyMzZjZDRhMy01MGM2LTQ3YjQtYWUzZC05ODdiYjA1ZTk4MzYiLCJ0eXAiOiJCZWFyZXIiLCJhenAiOiI1YmM5NGY2YSIsImF1dGhfdGltZSI6MTU0NzM5NTg3Niwic2Vzc2lvbl9zdGF0ZSI6ImZhMTQ5YjhiLWQ0ZTktNDliZS05NWIwLTk2MTNmZjBhNTViZCIsImFjciI6IjAiLCJhbGxvd2VkLW9yaWdpbnMiOltdLCJyZWFsbV9hY2Nlc3MiOnsicm9sZXMiOlsidW1hX2F1dGhvcml6YXRpb24iXX0sInJlc291cmNlX2FjY2Vzcyl6eyJhY2NvdW50Ijp7InJvbGVzIjpbIm1hbmFnZS1hY2NvdW50IiwibWFuYWdlLWFjY291bnQtbGlua3MiLCJ2aWV3LXByb2ZpbGUiXX19LCJwcmVmZXJyZWRfdXNlcm5hbWUiOiJldmFsczk4QGV4YW1wbGUuY29tIiwiZW1haWwiOiJldmFsczk4QGV4YW1wbGUuY29tIn0.O7y6GDFq5CajAT0DkywEuQqEuD5H7_YMqrVC4AMPthZ-m_xZ_DAPBEqj3mmzp1o1JOo0_4pMxNgKpyyqCQiFY79GRS5IJE6aVrZK53rQkud5dlaZAE1-ryiD8CtP_MrQtsTS7bVKbaFyCXNyFfxy3c-TER8GnGG90OlYPXpy5M954slcp4CWXxA7ZwVEuQNRRs5w2G2TCjrFyQjCzsINFwDRtADjbMiY7kq1cwRB5qM9ipdEEligDnH8dietiOZgY24sK10vtowjz_CHuWr5W3474dAZVFC7utwStI_bNcoj1gENRcz5cP7fH7Nim8e4itWoSVPRVYcfDHyYb9zixQ

We are going to use this as a Header in our call towards the OpenID protected service.
Let's go back to our api tester and add this as an Authorization header. The format is

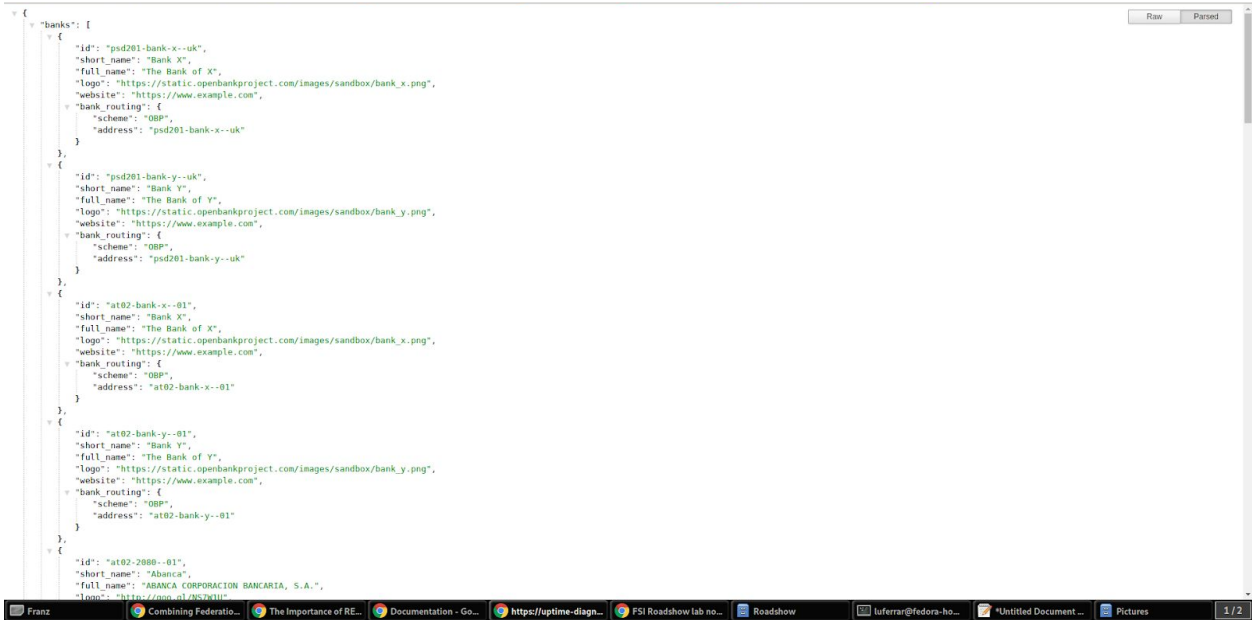
Authorization Bearer <access_token_value_here>



Let's hit **Test**



And success!



The work done by the API management behind the curtain is quite impressive:

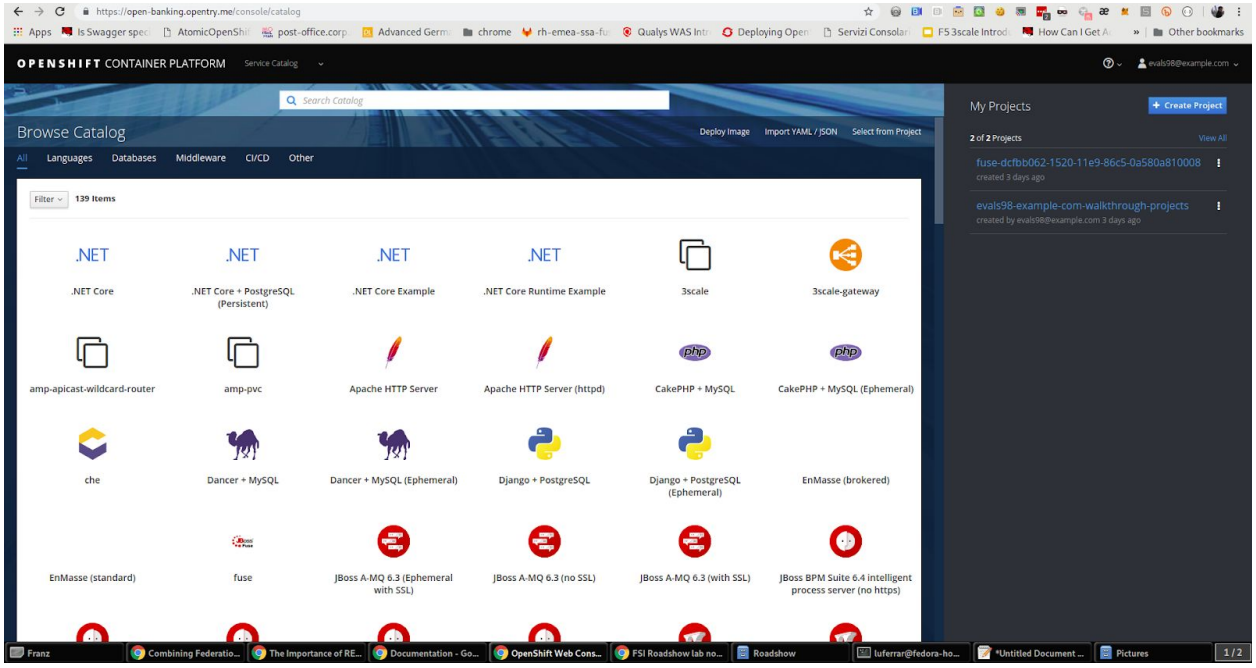
- Check for the validity of the access token credentials (not expired, legit and associated to the correct application)
- Check for rate limits on the application triggering the call
- Apply monetization rules to the call
- Apply any additional policy that might modify the call in real time

Checkpoint

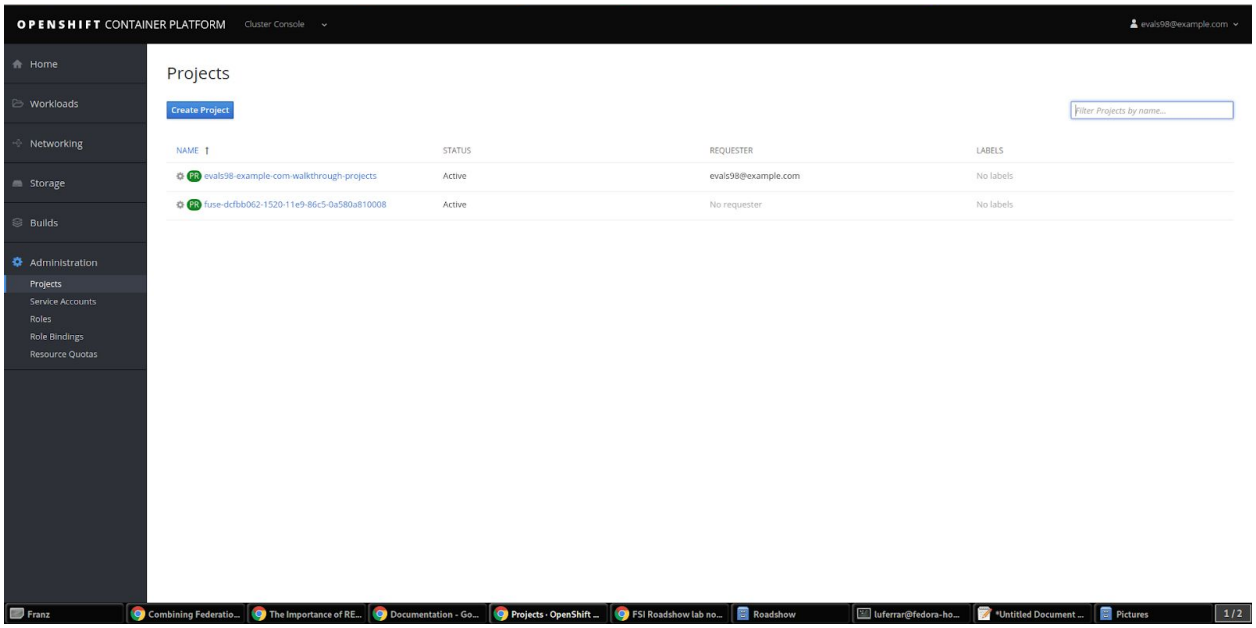
Improved security to the highest grade possible while using standards.

OpenShift (optional)

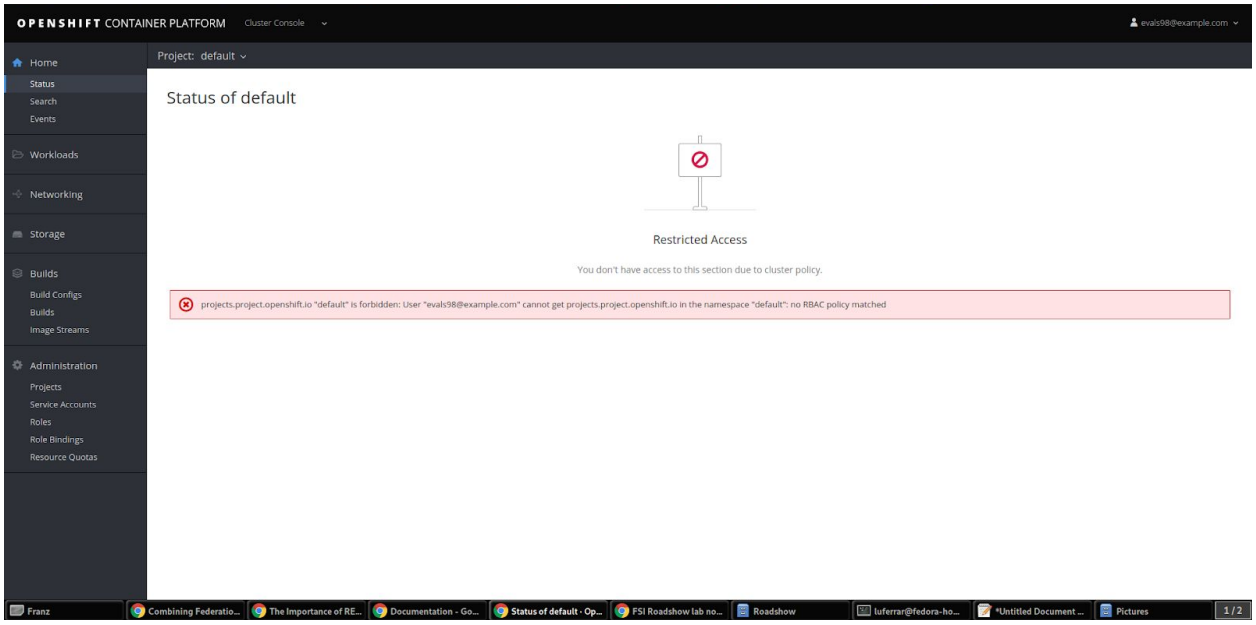
As user you will login into openshift and it already looks evident that the end user has been profiled as developer on OpenShift and it has access only to Objects and Projects he created or he has the right to see given his role.



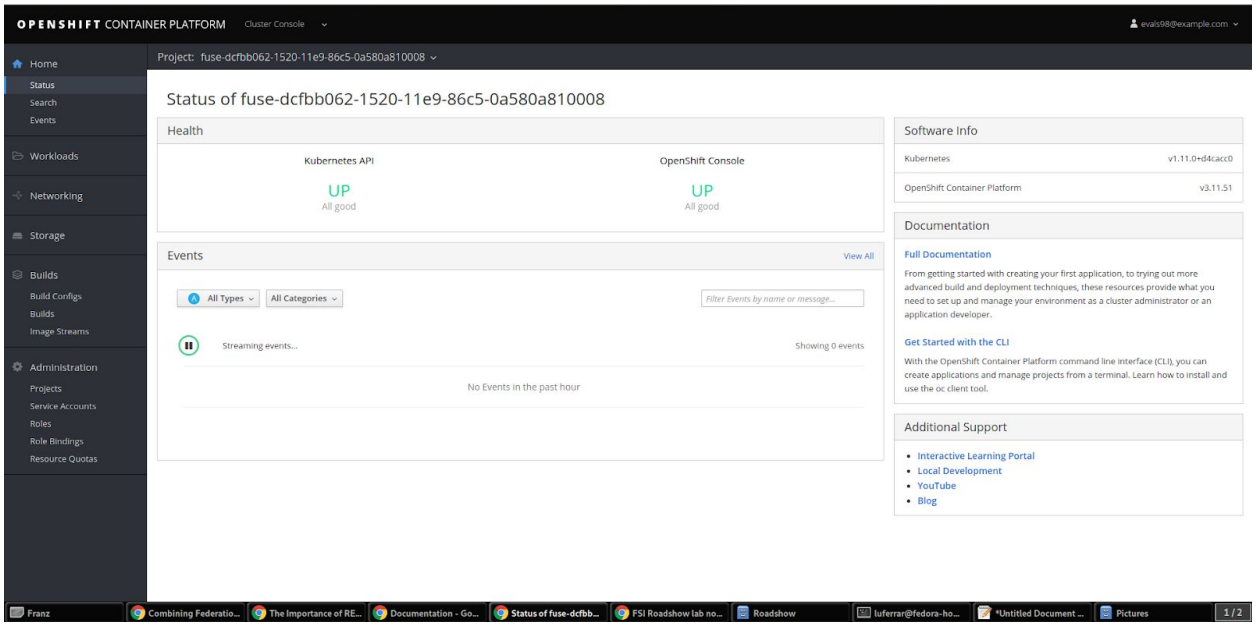
If we click on the fuse project we will be able to access to the Fuse Online installation dedicated to the user. We would also be able to see any integration project running alongside Fuse installation.
If we switch to the cluster console, this will give us some Operations details on the project created or assigned to our user.



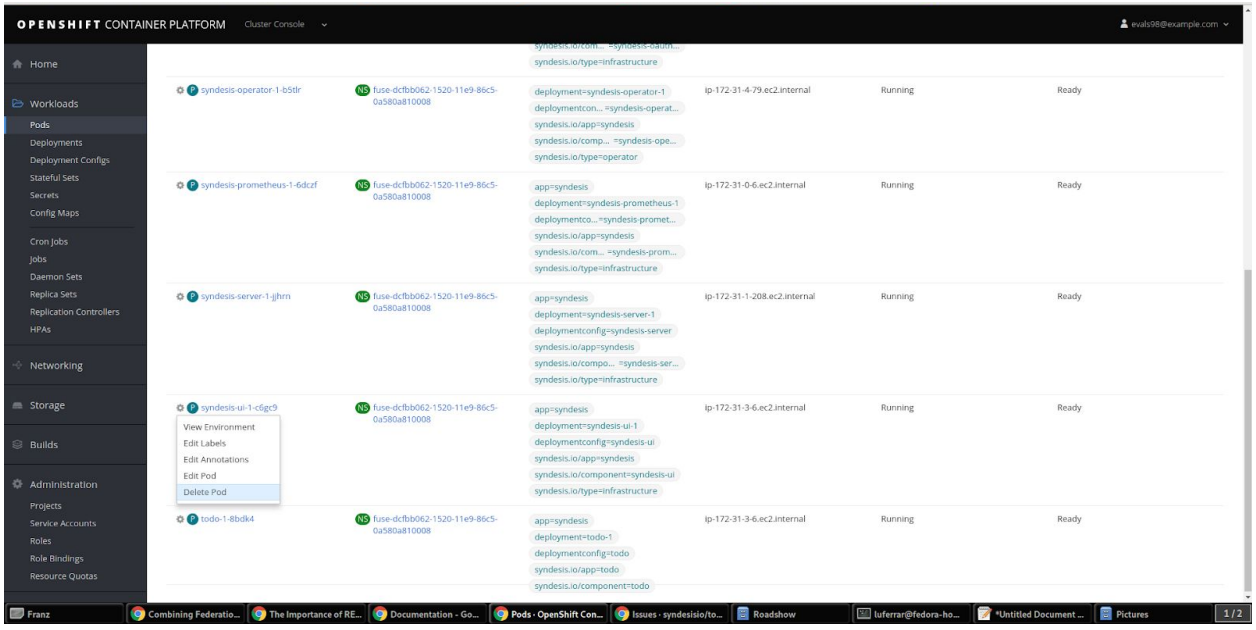
This type of console is also used by Operations administrators to check the health of OpenShift.
We can see the RBAC in action if we click on **Home -> Status**

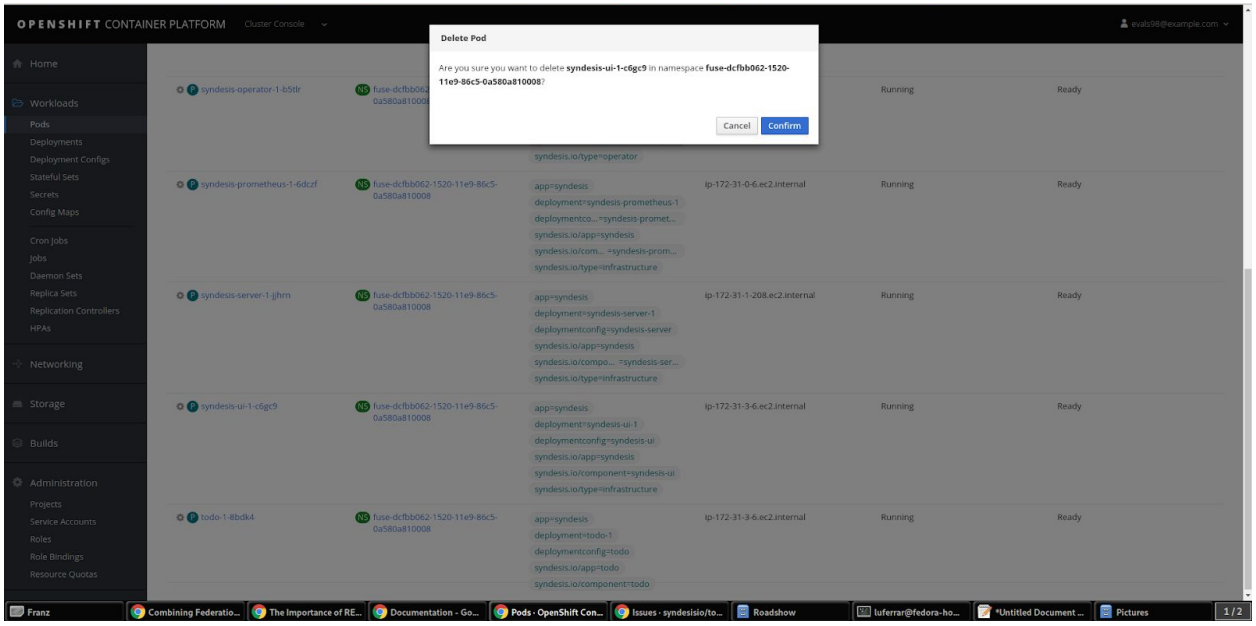


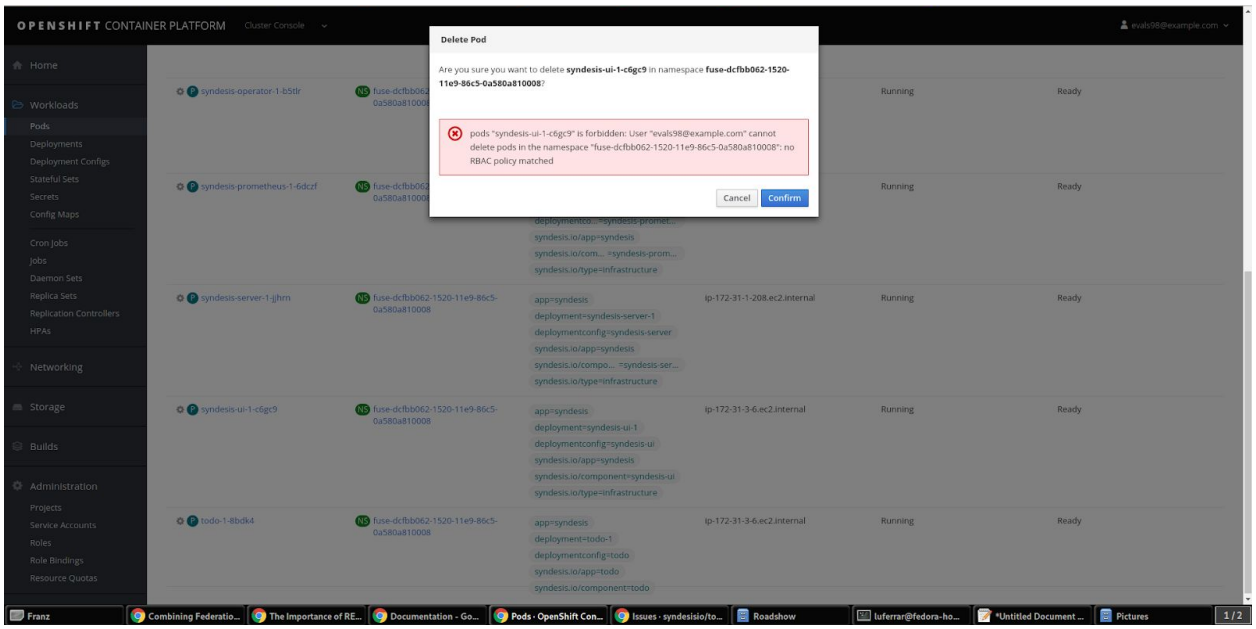
The Project default is excluded from the scope of any evals users, since it can contain system components.
We can just switch to the Fuse project to see if there anything wrong with it in the cluster.



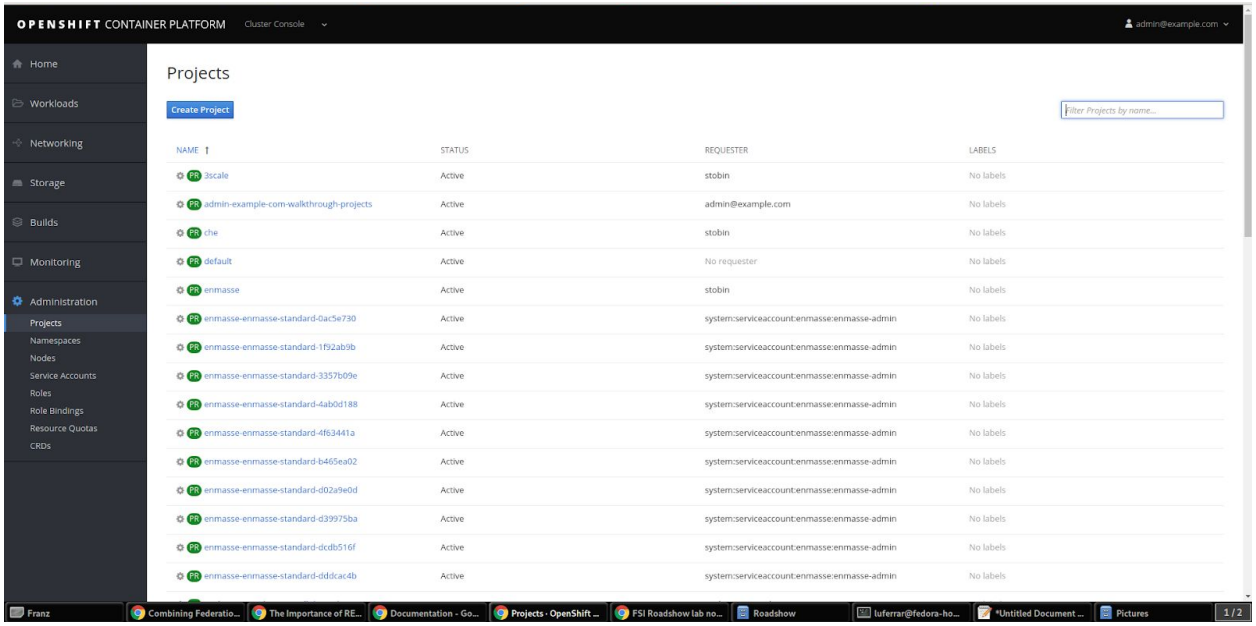
We will now try as bad intentioned user to change some parameters around the installed products.



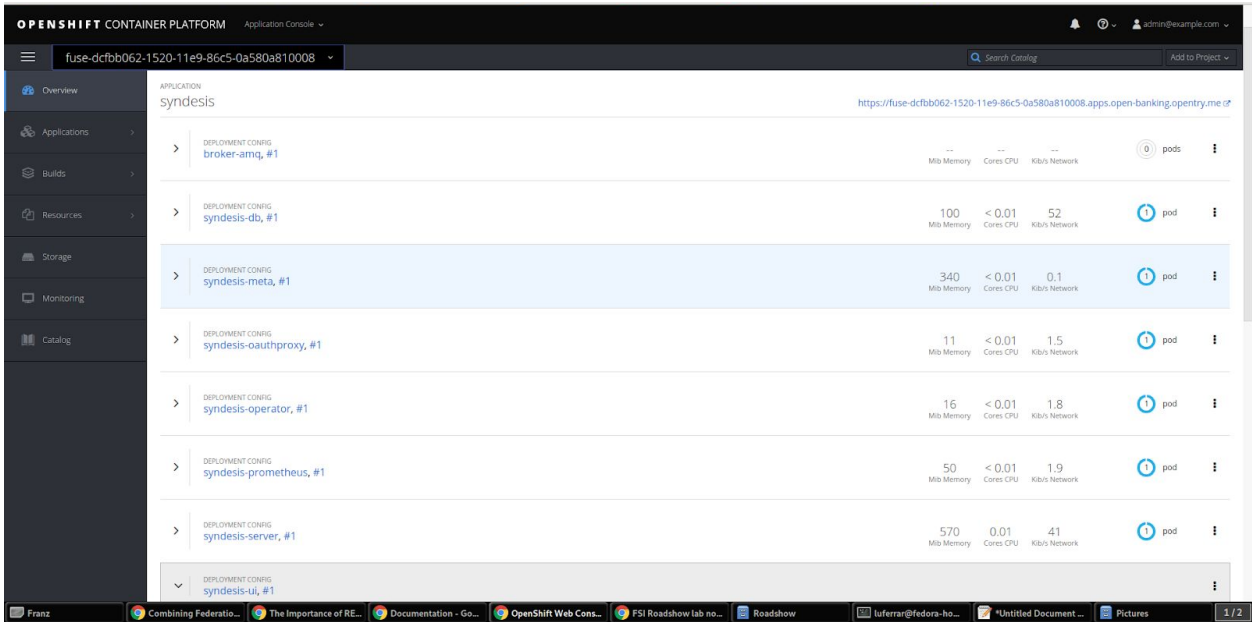




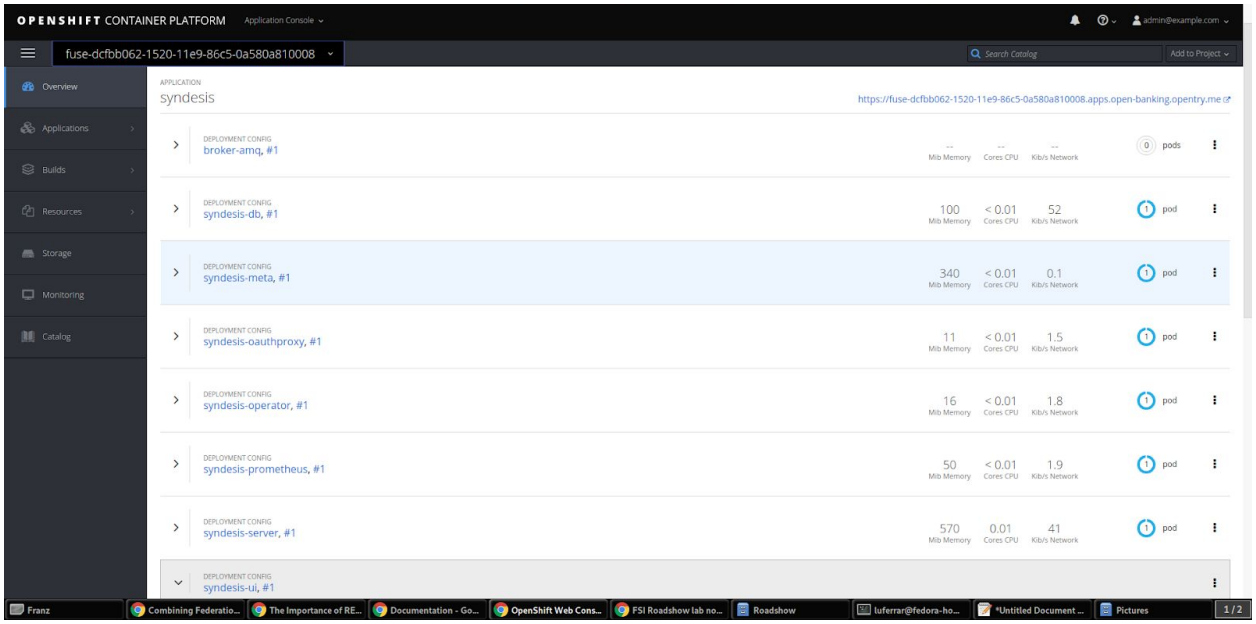
As we can see we tried to kill one of the running components of our integration platform with no success, because of the roles assigned to my user.
Let's see the magic introduced by OpenShift and login as administrator of the platform once again.



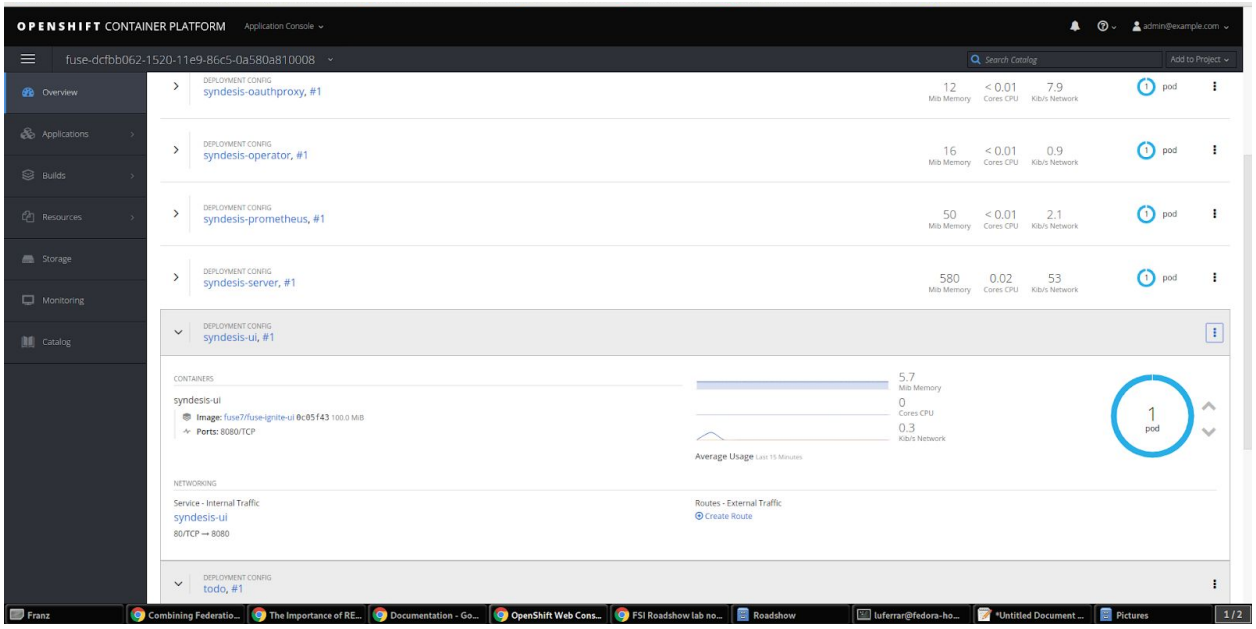
We now have full access to all the platforms from all users. We will open as admin one of the Fuse project

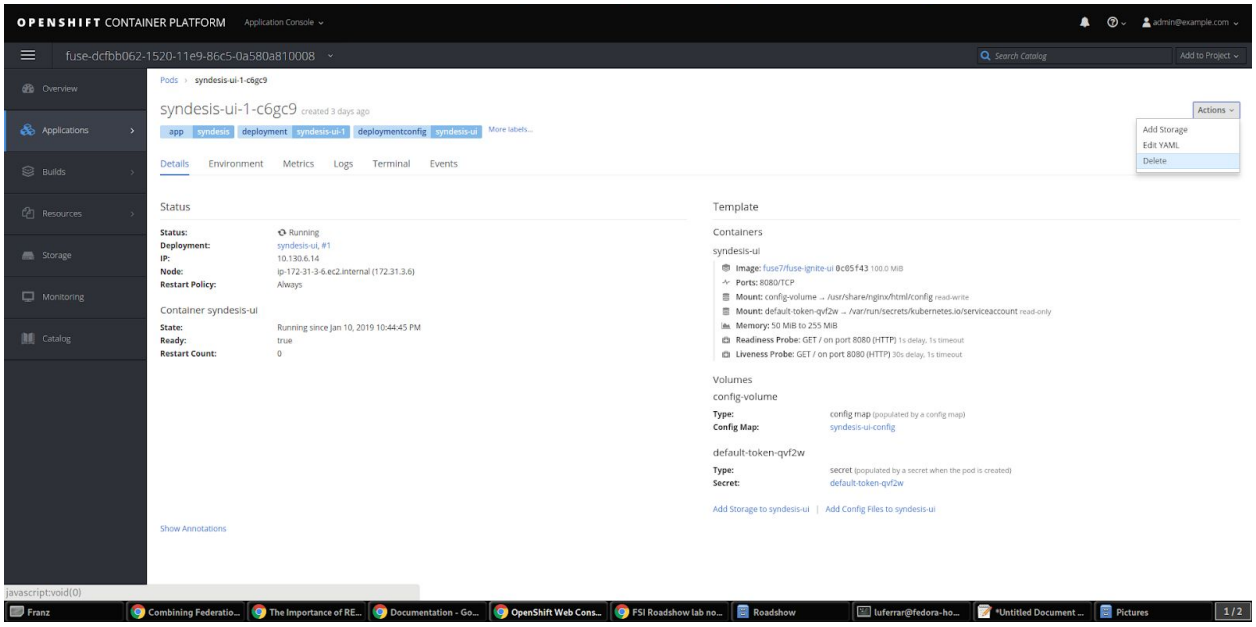


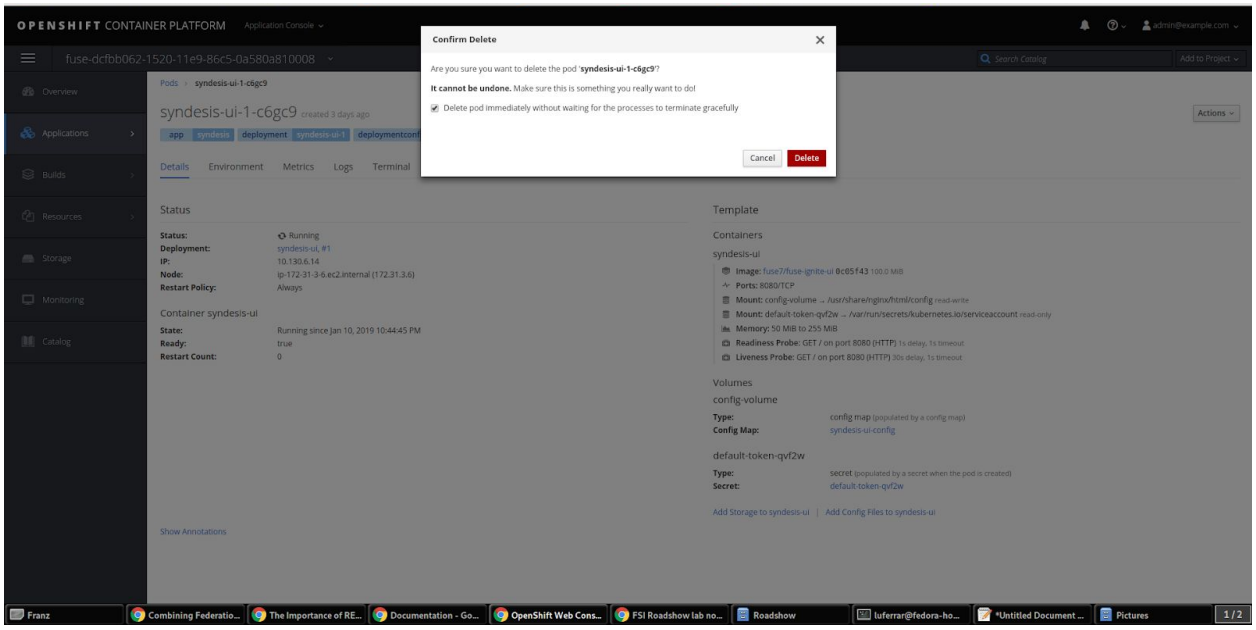
We can also open the relative Fuse Online installation.

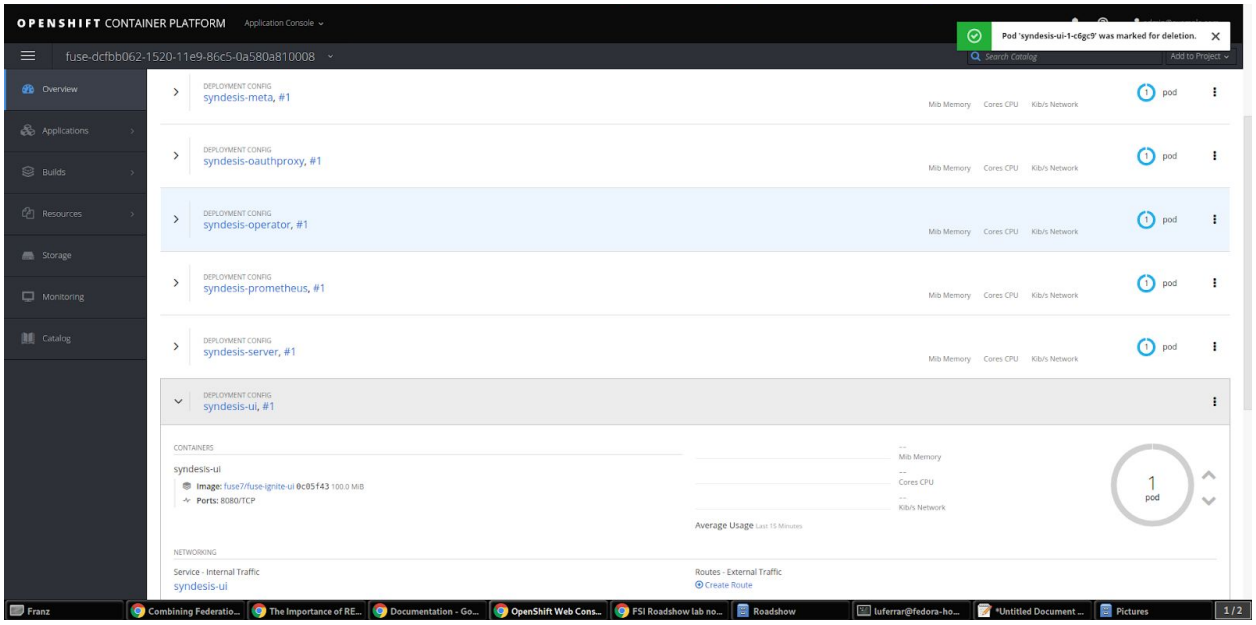


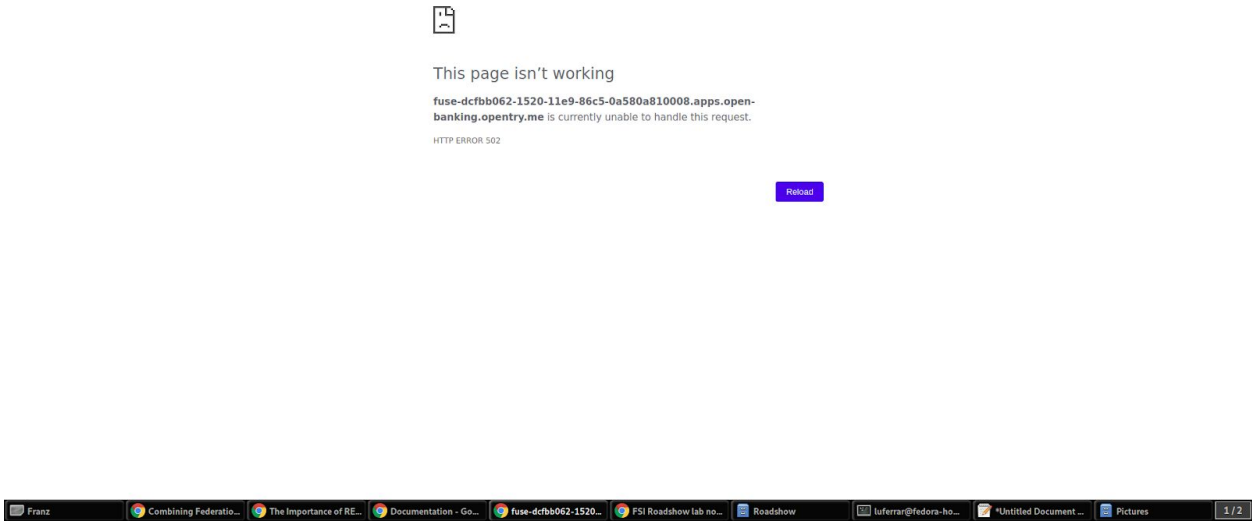
We are going to test the auto healing capabilities of the platform by killing one if its running components, in particular the one providing the UI service.

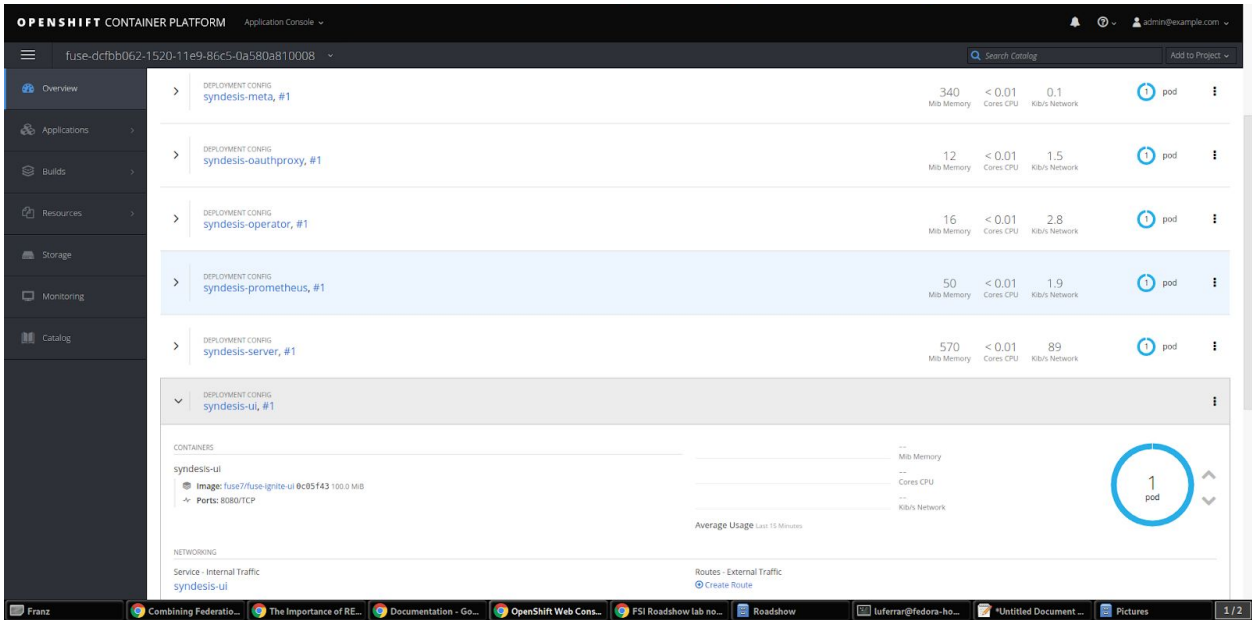


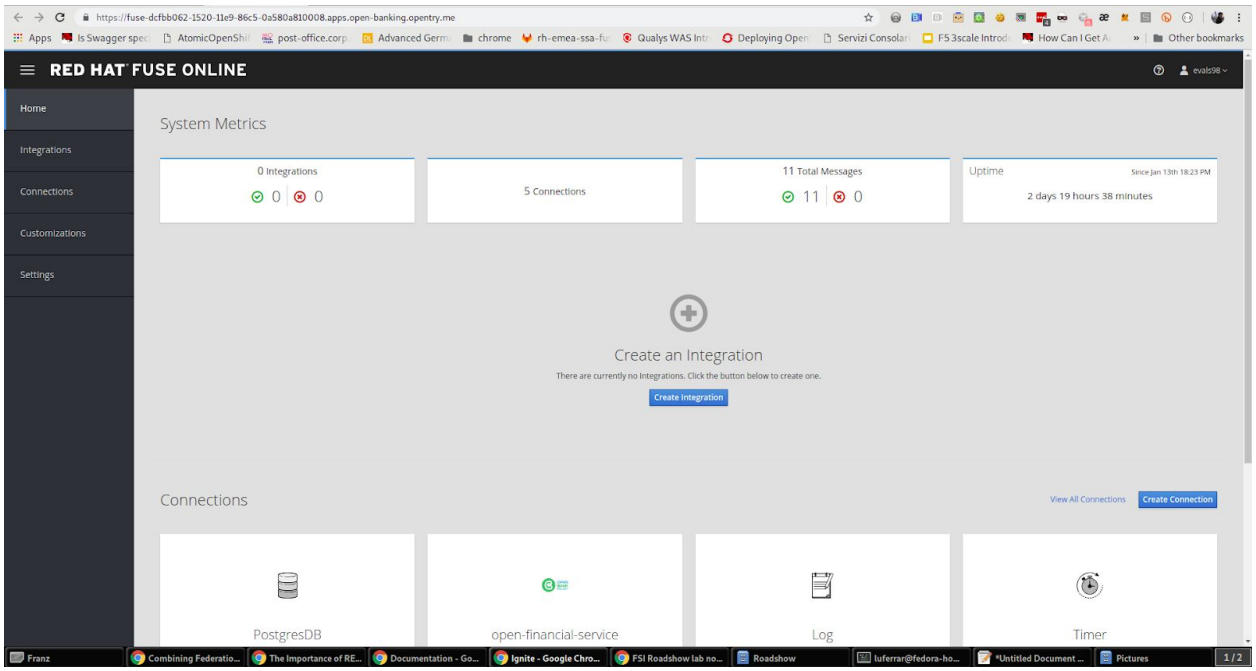

OPENSHIFT CONTAINER PLATFORM
Application Console
admin@example.com
fuse-dcfbb062-1520-11e9-86c5-0a580a810008
Search Catalog
Add to Project
Overview
Applications
Builds
Resources
Storage
Monitoring
Catalog
Pods
syndesis-ui-1-c6gc9
syndesis-ui-1-c6gc9 created 3 days ago
app syndesis deployment syndesis-ui-1 deploymentconfig syndesis-ui More labels...
Actions
Add Storage
Edit YAML
Delete
Details Environment Metrics Logs Terminal Events
Status
Status: Running
Deployment: syndesis-ui, #1
IP: 10.130.6.14
Node: ip-172-31-3-6.ec2.internal (172.31.3.6)
Restart Policy: Always
Container syndesis-ui
State: Running since Jan 10, 2019 10:44:45 PM
Ready: true
Restart Count: 0
Template
Containers
syndesis-ui
Image: fuse7/fuse-ignite-ui 0c05f43 100.0 MiB
Ports: 8080/TCP
Mount: config-volume → /usr/share/nginx/html/config read-write
Mount: default-token-qvf2w → /var/run/secrets/kubernetes.io/serviceaccount read-only
Memory: 50 MiB to 255 MiB
Readiness Probe: GET / on port 8080 (HTTP) 1s delay, 1s timeout
Liveness Probe: GET / on port 8080 (HTTP) 30s delay, 1s timeout
Volumes
config-volume
Type: config map (populated by a config map)
Config Map: syndesis-ui-config
default-token-qvf2w
Type: secret (populated by a secret when the pod is created)
Secret: default-token-qvf2w
Add Storage to syndesis-ui | Add Config Files to syndesis-ui
Show Annotations
javascript:void(0)
Franz
Combining Federatio...
The Importance of RE...
Documentation - Go...
OpenShift Web Cons...
FSI Roadshow lab no...
Roadshow
luferrar@fedora-ho...
*Untitled Document ...
Pictures
1 / 2


OPENSHIFT CONTAINER PLATFORM
Application Console
admin@example.com
fuse-dcfbb062-1520-11e9-86c5-0a580a810008
Search Catalog
Add to Project
Confirm Delete
Are you sure you want to delete the pod 'syndesis-ui-1-c6gc9'?
It cannot be undone. Make sure this is something you really want to do!
Delete pod immediately without waiting for the processes to terminate gracefully
Cancel
Delete
Overview
Applications
Builds
Resources
Storage
Monitoring
Catalog
Pods
syndesis-ui-1-c6gc9
syndesis-ui-1-c6gc9 created 3 days ago
Actions
Details Environment Metrics Logs Terminal
Status
Status: Running
Deployment: syndesis-ui, #1
IP: 10.130.6.14
Node: ip-172-31-3-6.ec2.internal (172.31.3.6)
Restart Policy: Always
Container syndesis-ui
State: Running since Jan 10, 2019 10:44:45 PM
Ready: true
Restart Count: 0
Template
Containers
syndesis-ui
Image: fuse7/fuse-ignite-ui 0c05f43 100.0 MiB
Ports: 8080/TCP
Mount: config-volume → /usr/share/nginx/html/config read-write
Mount: default-token-qvf2w → /var/run/secrets/kubernetes.io/serviceaccount read-only
Memory: 50 MiB to 255 MiB
Readiness Probe: GET / on port 8080 (HTTP) 1s delay, 1s timeout
Liveness Probe: GET / on port 8080 (HTTP) 30s delay, 1s timeout
Volumes
config-volume
Type: config map (populated by a config map)
Config Map: syndesis-ui-config
default-token-qvf2w
Type: secret (populated by a secret when the pod is created)
Secret: default-token-qvf2w
Add Storage to syndesis-ui | Add Config Files to syndesis-ui
Show Annotations
Franz
Combining Federatio...
The Importance of RE...
Documentation - Go...
OpenShift Web Cons...
FSI Roadshow lab no...
Roadshow
luferrar@fedora-ho...
*Untitled Document ...
Pictures
1 / 2


OPENSHIFT CONTAINER PLATFORM
Application Console
Pod 'syndesis-ui-1-c6gc9' was marked for deletion.
fuse-dcfbb062-1520-11e9-86c5-0a580a810008
Search Catalog
Add to Project
Overview
Applications
Builds
Resources
Storage
Monitoring
Catalog
DEPLOYMENT CONFIG
syndesis-meta, #1
syndesis-oauthproxy, #1
syndesis-operator, #1
syndesis-prometheus, #1
syndesis-server, #1
syndesis-ui, #1
Mib Memory
Cores CPU
Kib/s Network
pod
CONTAINERS
syndesis-ui
Image: fuse7/fuse-ignite-ui 0c05f43 100.0 MiB
Ports: 8080/TCP
Average Usage Last 15 Minutes
NETWORKING
Service - Internal Traffic
syndesis-ui
Routes - External Traffic
Create Route
Franz
Combining Federatio...
The Importance of RE...
Documentation - Go...
OpenShift Web Cons...
FSI Roadshow lab no...
Roadshow
luferrar@fedora-ho...
*Untitled Document ...
Pictures
1 / 2


This page isn't working
fuse-dcfbb062-1520-11e9-86c5-0a580a810008.apps.open-banking.opentry.me is currently unable to handle this request.
HTTP ERROR 502
Reload
Franz
Combining Federatio...
The Importance of RE...
Documentation - Go...
fuse-dcfbb062-1520...
FSI Roadshow lab no...
Roadshow
luferrar@fedora-ho...
*Untitled Document ...
Pictures
1 / 2





As we can see the component auto-healed based and in a few seconds we have a GUI running once again for the integration platform.

Q&A

Common issues

- While using Fuse Online it I have experienced some timeouts and slowness. If that happens too often you can always use the same URL that all the other attendees are using (from our open-bank demo portal) to test the API. Also make sure you use a different browser for Fuse Online scenario than the one used for Integr8ly demos
- openidconnect.net client might have an additional space in the redirect_uri field. That's a client bug, you can fix it by adding an additional redirect URIs in RH SSO with a space preceding the URL: " https://openidconnect.net/callback "
- The installation of RH SSO might have some certification issues, so might need to use instead a local or otherwise deployed installation