



Generalitat de Catalunya  
**Centre de Telecomunicacions  
i Tecnologies de la Informació**

# **Estratègies de l'ús de l'API Manager**

**Octubre de 2024**

1	Introducció
2	Visió a Nivell Global
3	Elements Clau
4	Beneficis
5	Integració dins del CTTI
6	Desplegament de APIs
7	Guia d'ús

# 1. Introducció

Avui dia tothom disposa de dispositius mòbils, fent un ús massiu de les xarxes socials o compres per internet. A més, la irrupció de les startups tecnològiques, l'augment de plataformes en diversos sectors (retail, financer, segurs...) i l'impuls de noves tendències, com el Cloud, IoT o Big Data, han provocat el redescobriment de les API, no com a mers connectors, sinó com a potents ressorts de la transformació digital d'empreses i organitzacions.

Dins d'aquest context evolutiu de les APIs a nivell global, apareix el API Manager (gestió de API) dins de les architectures programari modernes, sent rara l'organització que avui no té en el seu full de ruta la implantació d'un sistema sota aquest propòsit, adoptant les seves estratègies en l'àmbit de les API, especialment per a cobrir i estendre la seva propietat intel·lectual, i fins i tot com a font d'ingressos.

## Els objectius principals són:

- Donar a conèixer una visió holística del API Manager, explorant el seu abast global i destacant la seva implementació estratègica dins del Centre de Telecomunicacions e Tecnologies de la Informació (CTTI).
- Mostrar com la implementació estratègica d'un API Manager pot impulsar el creixement empresarial de manera significativa. Descobrirem les virtuts inherents a aquesta poderosa eina, explorarem els beneficis tangibles que ofereix i analitzarem els diversos usos que poden transformar la dinàmica operativa de la nostra organització.





## 2. Visió a Nivell Global

---

# API Manager

## Visió a nivell global

### API MANAGER COM A GESTOR I PROVEÏDOR DE SERVEIS INFORMATICOS

En el vertiginós món de la tecnologia, on la connectivitat i la integració són essencials, els API Manager s'han convertit en fonaments sòlids per a organitzacions que busquen optimitzar i controlar les seves interfícies de programació d'aplicacions (API). Aquests elements exerceixen un paper crucial en facilitar la gestió, seguretat i eficiència en l'exposició i consum de serveis a través de API.

Els elements clau d'un API Manager són...

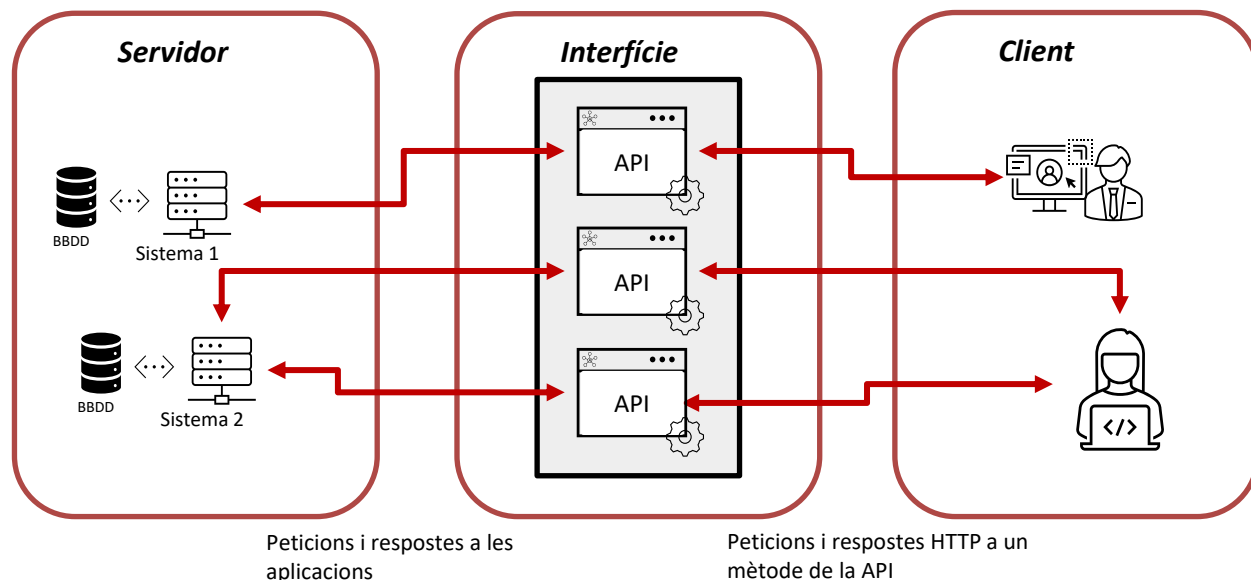
## 2. Visió a Nivell Global

# ¿Què és un API?

En essència, una **interfície de programació d'aplicacions (API)** facilita la comunicació entre un usuari i un sistema o servei, canalitzant les sol·licituds de l'usuari cap a aplicacions que poden estar dins o fora de la xarxa interna del client, i transmetent les respostes corresponents de tornada a l'usuari.

Les **API** permeten la comunicació entre aplicacions o serveis sense saber com s'implementen, la qual cosa simplificarà el desenvolupament d'aplicacions i permetrà l'estalvi de molt de temps i diners.

A més, les **API** aporten flexibilitat, oportunitats per a la innovació, una millor administració i eficiència, i permeten la integració eficaç entre sistemes de manera atòmica, compatible i àgil.



Una **API** defineix la forma en què altres aplicacions poden utilitzar els sistemes o serveis externs.

La interfície defineix:

- ❖ El tipus de sol·licituds que poden realitzar-se
- ❖ Els formats de dades compatibles
- ❖ Els fluxos de transformació de dades
- ❖ El maneig de les respostes
- ❖ ...

Bàsicament, una API envia la sol·licitud de l'usuari a un sistema o servei i retorna la seva resposta a l'usuari.

## 2. Visió a Nivell Global

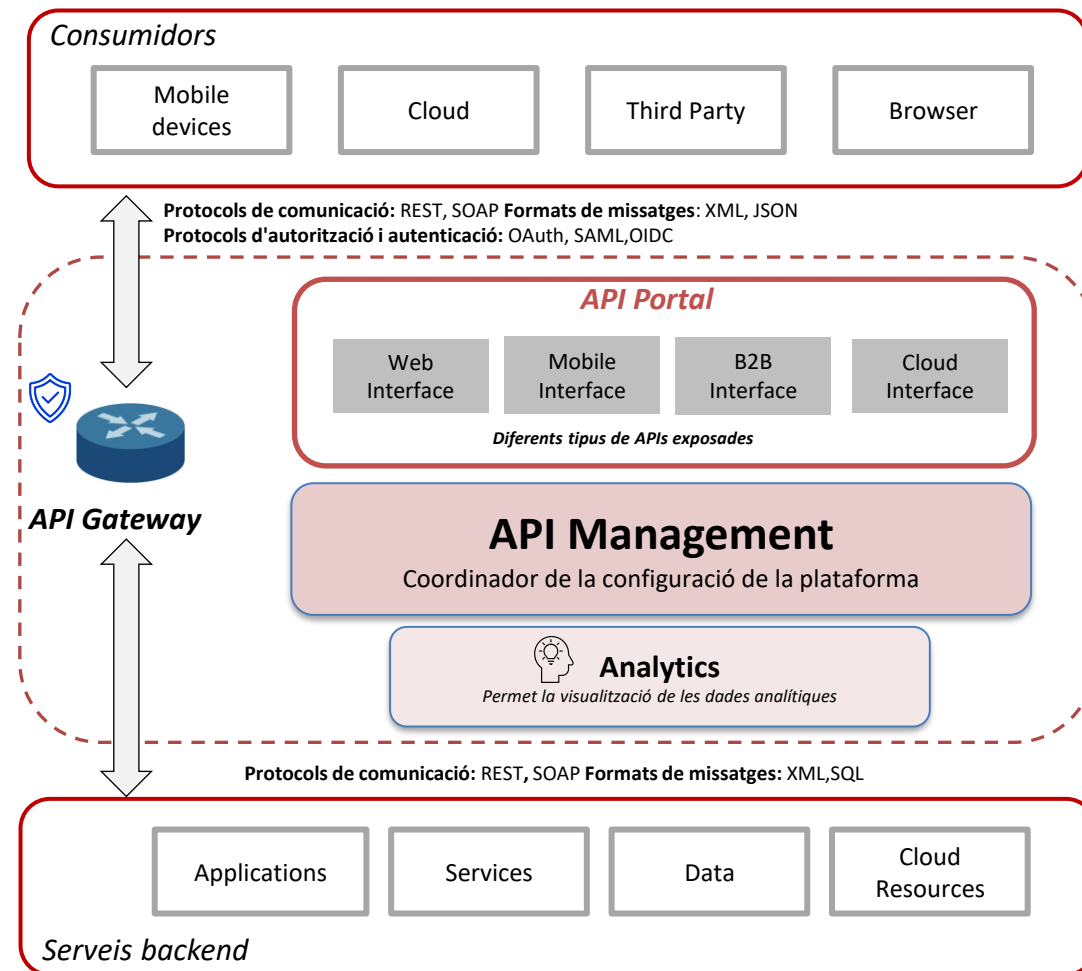
# ¿Què és un API Manager?

El API Manager és una eina programari que permet publicar, promocionar i supervisar APIs en un entorn segur i escalable. Així mateix, inclou tots aquells recursos enfocats a la creació, documentació i socialització de les mateixes, tant en Internet com a nivell local.

Les plataformes de API Manager proporcionen un conjunt bàsic de funcions que et permeten aplicar les bones pràctiques de gestió de les API, entre les quals s'inclouen:

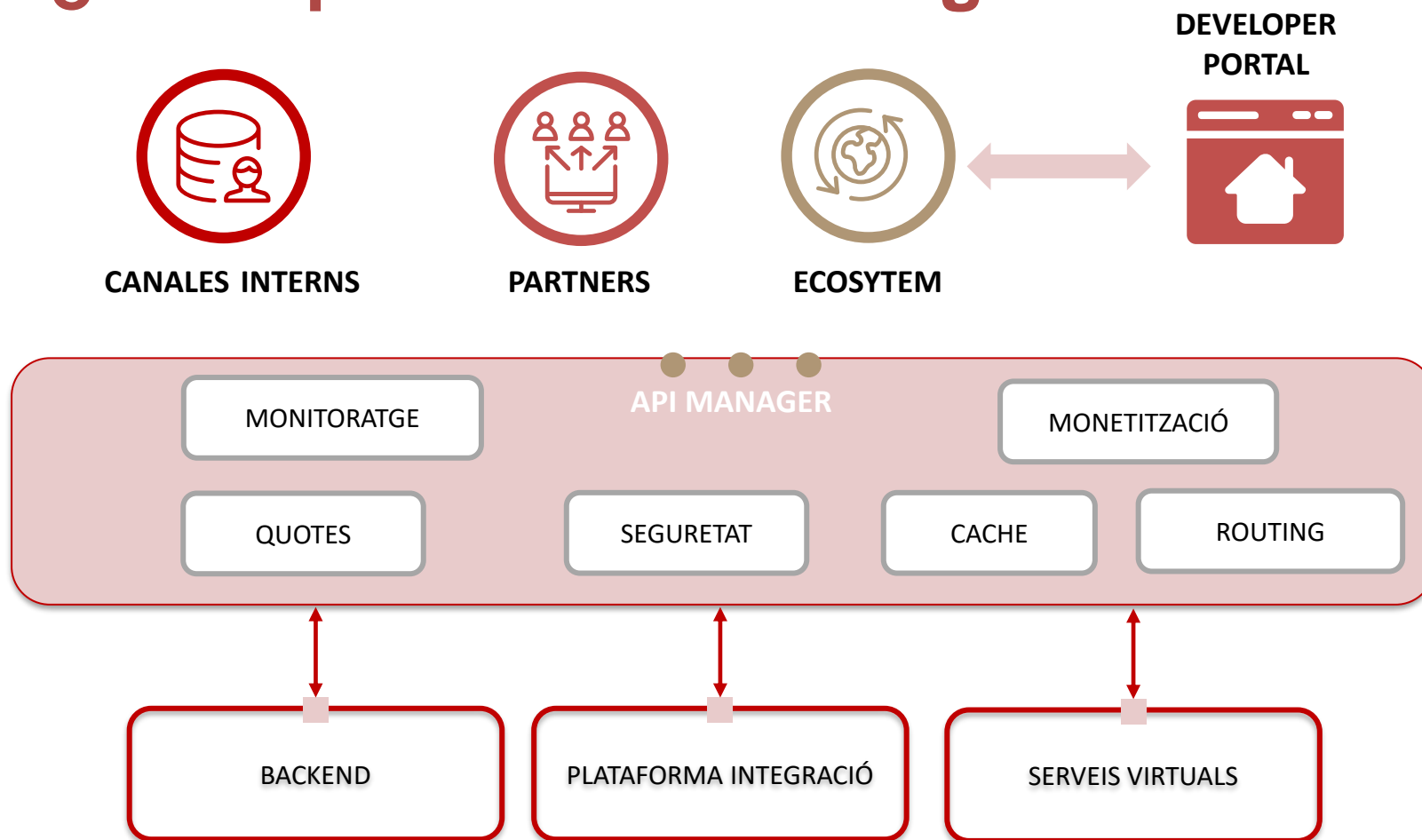
1. **Gestió de API:** Permet crear, publicar i administrar APIs de manera centralitzada. Això inclou la capacitat de definir polítiques de seguretat, autenticació, autorització i límits d'ús.
2. **Seguretat:** Proporciona mecanismes de seguretat per a protegir les APIs, com a autenticació d'usuaris, autorització d'accés, encriptació de dades i prevenció d'atacs.
3. **Monitoratge i anàlisi:** Permet realitzar un seguiment del rendiment de les APIs, com el temps de resposta, la taxa d'èxit i l'ús de recursos. També pot generar informes i anàlisis per a ajudar a prendre decisions basades en dades.
4. **Versionat i control de canvis:** Permet gestionar diferents versions d'una API i controlar els canvis realitzats en cada versió. Això facilita l'evolució de les APIs sense interrompre als consumidors existents.
5. **Portal de desenvolupadors:** Proporciona un portal o interfície perquè els desenvolupadors puguin descobrir, explorar i utilitzar les APIs disponibles. Això inclou documentació, exemples de codi, proves i eines de desenvolupament.
6. **Integració amb sistemes existents:** Un API Manager s'integra amb altres sistemes i tecnologies, com Gateways de API, sistemes de gestió d'identitat, sistemes de registre i anàlisi, entre altres.

Aquestes funcions et permeten aprofitar la plataforma de API Manager per a mantenir un ecosistema d'usuaris i desenvolupadors creixent i més fort.



## 2. Visió a Nivell Global

# ¿Qué aporta el API Manager?



### CAPACITATS OUT-OF-THE-BOX

- ESTANDARDITZACIÓ DE LA SEGURETAT
- MONETITZACIÓ DEL CONSUM
- DIFERENTS NIVELLS DE SERVEI
- VIRTUALITZACIÓ SERVEIS
- DESACOPLAMENT
- DOCUMENTACIÓ EN LÍNIA
- ENTORN SANDBOX
- INFORMACIÓ ANALÍTICA

### BENEFICIS

- TIME TO MARKET RÀPID
- APLICAR AGILE
- ORIENTACIÓ NEGOCI
- ASSEGURAR RENDIMENT BACKENDS



### 3. Elements Clau

---

# API Manager elements clau

## API MANAGER PEÇA ANGULAR DE LA TRANSFORMACIÓ DIGITAL

En l'era de la connectivitat, el API Manager s'erigeix com el director d'orquestra que permet a les organitzacions donar vida als seus serveis de manera segura i eficient. Des del control d'accés i la seguretat fins a la flexibilitat i el desacoblament, aquests elements no sols simplifiquen la interacció entre sistemes, sinó que també aplanen el camí per a la innovació i la col·laboració sense restriccions.

Els elements clau del API Manager són...





## 3. Elements Clau

# Portal de desenvolupadors

### Element Clau

#### PORTAL DE DESENVOLUPADORS

- Proporciona un portal o interfície perquè els desenvolupadors puguin descobrir, explorar i utilitzar les APIs disponibles. Inclou documentació, exemples de codi, proves i eines de desenvolupament
- Proporciona una experiència completa i col·laborativa per a facilitar la integració reeixida de les APIs en les aplicacions dels desenvolupadors.

### Camins d'aplicació

1

**DESCOBRIMENT DE APIS.** Els desenvolupadors poden accedir al Portal de desenvolupadors de CTTI per a descobrir les APIs disponibles. Poden explorar la documentació, llegir descripcions detallades de les APIs i comprendre com poden utilitzar-les en les seves pròpies aplicacions.



2

**REGISTRE I AUTENTICACIÓ.** Els desenvolupadors interessats a utilitzar les APIs de CTTI poden registrar-se en el Portal de desenvolupadors. Una vegada registrats, poden obtenir credencials d'accés, com a claus de API o tokens, per a autenticar-se i autoritzar-se correctament en consumir les APIs.



3

**DOCUMENTACIÓ I EXEMPLE DE CODI.** El Portal de desenvolupadors de CTTI proporciona informació completa i detallada sobre les APIs. Els desenvolupadors poden visualitzar la configuració de les APIs, exemples d'invocació a cada operació, així com la possibilitat de descarregar-se el YAML complet del API, per a poder comprendre com interactuar amb les APIs de manera efectiva.



4

**GESTIÓ DE SUBSCRIPCIONS.** A través del Portal de desenvolupadors, els desenvolupadors poden subscriure's a les APIs de CTTI que desitgin utilitzar. Això els permet rebre actualitzacions i notificacions sobre canvis en les APIs, com a noves versions o modificacions en les polítiques d'ús.



## 3. Elements Clau

# Gestió de API

### Element Clau

#### GESTIÓ DE API

- El API Manager permet crear, publicar i administrar APIs de manera centralitzada des de la consola d'administració. Això inclou la capacitat de definir polítiques de seguretat, autenticació, autorització i límits d'ús. Dins de CTTI, els desenvolupadors no fan ús d'aquestes funcionalitats, sinó que utilitzen l'eina **IBM API Designer toolkit** en local, per a assegurar-se que les APIs estiguin definides i implementades correctament abans de ser publicades
- A través d'aquestes funcionalitats, els projectes dins de CTTI poden gestionar de manera eficient i controlar el cicle de vida complet de les seves APIs. Des de la creació i configuració inicial, fins a la publicació, monitoratge, control de versions i gestió de subscripcions. A més, li brinda eines per a garantir la seguretat, controlar l'accés i obtenir informació valuosa sobre l'ús de les APIs. Això permet a CTTI oferir APIs d'alta qualitat, segures i ben administrades als desenvolupadors externs que desitgin utilitzar els seus serveis.

### Camins d'aplicació

1

**CREACIÓ DE API.** Els desenvolupadors utilitzen el API Manager per a crear una nova API. Podent definir la funcionalitat de la API, els punts d'entrada, els paràmetres de sol·licitud i resposta, i qualsevol altra configuració necessària.



2

**DEFINICIÓ DE POLÍTIQUES.** Utilitzant el API Manager, els projectes dins de CTTI podran disposar de Polítiques predefinides i custom, així com com la possibilitat de seleccionar la configuració requerida per als fluxos d'autenticació i autorització de les APIs.



3

**GESTION CICLE DE VIDA DEL API.** A través del API Manager, els projectes dins de CTTI poden gestionar totes les etapes del cicle de vida d'una API, com draft, publicació del API, manteniment, retirada del API per obsolescència, deprecació del API, etc.



4

**MONITORATGE I ANÀLISI.** Dins del API Manager, el **mòdul de Analytics**, permet als projectes de CTTI monitorar el rendiment dels seus APIs, podent realitzar un seguiment de mètriques, com el temps de resposta, la taxa d'èxit i l'ús de recursos. Això els ajuda a identificar possibles problemes i optimitzar el rendiment de les APIs.



5

**CONTROL DE VERSIONS.** A mesura que els projectes dins de CTTI realitzen actualitzacions o millores en les seves APIs, pot utilitzar el API Manager per a gestionar diferents versions de la API. Això els permet mantenir la compatibilitat amb les aplicacions existents mentre introdueixen canvis en la API.



6

**GESTIÓ DE SUBSCRIPCIONS.** A través del API Manager, els projectes dins de CTTI poden gestionar les subscripcions dels desenvolupadors als seus APIs. Poden controlar qui té accés a quin APIs i establir límits d'ús, com el nombre de sol·licituds per minut o el volum de dades permès.



7

**CONTROL DE L'ACCÉS I SEGURETAT.** El API Manager permet a CTTI implementar mesures de seguretat addicionals per a protegir les seves APIs. Poden utilitzar autenticació basada en tokens, encriptació de dades i altres tècniques de seguretat per a garantir que només els usuaris autoritzats puguin accedir a les APIs.





## 3. Elements Clau

# Seguretat

### Element Clau

#### SEGURETAT

- El API Manager ofereix configuracions de seguretat essencials per a salvaguardar les APIs. Aquests mecanismes inclouen autorització d'accés, xifrat de dades, prevenció d'atacs i autenticació d'usuaris. Aquestes funcionalitats es potencien mitjançant la capacitat de API Connect d'IBM per a integrar-se sense problemes amb gestors d'identitat, proporcionant una capa addicional de protecció i control sobre l'accés als nostres recursos.
- Aquestes funcionalitats treballen en conjunt per a garantir la seguretat de les APIs i protegir les dades sensibles d'accessos no autoritzats o atacs maliciosos.

### Camins d'aplicació

1

**AUTENTICACIÓ.** En el API Manager es poden implementar diferents mètodes d'autenticació per a les APIs. Per exemple, API Keys, Token d'accés, integració amb sistemes d'autenticació existents, etc. Això ajuda a verificar la identitat de l'usuari i assegurar que només els usuaris autoritzats puguin accedir a les APIs.



2

**AUTORITZACIÓ.** El API Manager permet definir polítiques d'autorització per a controlar quins usuaris o rols tenen accés a quin APIs i recursos. Per exemple, els projectes dins de CTTI pot establir regles que permetin a uns certs usuaris accedir a APIs concretes o limitar l'accés a funcionalitats dins d'una API, basant-se en tokens d'autorització, on els desenvolupadors han d'obtenir un token d'accés vàlid per a consumir les APIs. Per a això, han d'haver-se autenticat correctament primer.



3

**ENCRIPACIÓ DE DADES.** El API Manager pot proporcionar encriptació de dades per a protegir la confidencialitat de la informació transmesa a través de les APIs. Això assegura que les dades sensibles estiguin protegits i no puguin ser interceptats o llegits per tercers no autoritzats.



4

**PREVENCIÓ D'ATACS.** El API Manager pot incloure mecanismes de seguretat per a prevenir atacs, com a atacs de denegació de servei (DDoS) o atacs d'injecció de codi. Pot implementar filtres i regles de seguretat per a detectar i bloquejar activitats sospitoses o malicioses.



5

**GESTIÓ DE CLAUS I CERTIFICATS.** El API Manager facilita l'administració de *perfils de certificats TLS*, els quals són fonamentals per a garantir la seguretat en la transmissió de dades entre el servidor de gestió i altres subsistemes i serveis externs.



6

**AUDITORIA I REGISTRES D'ESDEVENIMENTS.** A través del component *Gateway* dins del API Manager, es poden registrar els esdeveniments/activitats relacionades amb les APIs, com a sol·licituds, respostes i accions dels usuaris. Posteriorment, a través del component *Analytics*, es pot explotar aquesta informació, permetent realitzar un seguiment de les activitats i detectar possibles intents d'accés no autoritzat o comportaments anòmals.



7

**INTEGRACIÓ AMB SISTEMES DE GESTIÓ D'IDENTITAT.** El API Manager té la capacitat d'integrar-se amb sistemes de gestió d'identitat existents, usant protocols com OAuth o OIDC, per a aprofitar l'autenticació i autorització centralitzades. Això simplifica l'administració d'usuaris i garanteix la coherència en la seguretat en tota l'organització.



## 3. Elements Clau

# Gestió de trànsit

### Element Clau

#### GESTIÓ DE TRÀNSIT

A través de les diferents funcionalitats integrades en l'eina, es pot coordinar i distribuir de manera eficient el trànsit dels seus APIs, assegurant un acompliment òptim i una disponibilitat elevada.

### Camins d'aplicació

1

#### PLANS I THROTTLING

CTTI té la capacitat d'establir restriccions en les anomenades a les seves APIs mitjançant la implementació de plans en els productes corresponents. Aquests plans, al seu torn, imposen límits de throttling (anomenades per hora) i burst (anomenades per minut). Aquesta configuració s'executa amb el propòsit d'evitar la superació del límit de crides associat al servei contractat per CTTI, garantint un ús controlat i eficient dels recursos disponibles.



2

**CAIXET.** A través del API Manager, CTTI pot utilitzar una capa de caixet que emmagatzema en memòria les respostes de les sol·licituds freqüents. Aquesta estratègia té el propòsit de reduir la càrrega i optimitzar els temps de resposta per a aquelles sol·licituds que s'efectuen de manera repetitiva a través de les APIs.



3

**MONITORATGE I ANÀLISI.** Dins del context del API Manager, el mòdul de Analytics permet als projectes de CTTI monitorar de manera exhaustiva l'acompliment dels seus APIs. Això implica el seguiment detallat de mètriques clau, com el temps de resposta, la taxa d'èxit i l'ús de recursos. Aquesta funcionalitat proporciona la capacitat d'identificar possibles problemes i optimitzar eficientment el rendiment de les APIs.



## 3. Elements Clau

# Integració amb sistemes existents

### Element Clau

#### INTEGRACIÓ AMB SISTEMES EXISTENTS

- El API Manager simplifica i potència la integració amb sistemes o serveis gràcies a les seves capacitats predefinides com, per exemple:
  - Integracions a través de serveis SOAP permetent la importació directa de definicions WSDL (Web Services Description Language), facilitant la creació ràpida de APIs basades en SOAP en aprofitar la informació estructurada i els mètodes definits en el WSDL. A més, el API Manager ofereix capacitats avançades de transformació i mapatge, permetent adaptar les estructures de dades i els formats entre les APIs SOAP importades i els requisits específics de l'ecosistema.
  - En el cas de serveis REST, el API Manager també simplifica la creació i gestió de APIs en proporcionar eines intuïtives per a importar definicions, realitzar transformacions i mapatges, permetent així una integració àgil i robusta amb sistemes o serveis que segueixin el paradigma RESTful.

### Camins d'aplicació

- 1 DEFINICIÓ DE ENDPOINTS.** Mitjançant el API Manager, CTTI defineix els endpoints de les APIs connectades a aquests serveis existents. Per exemple, considerem un servei de base de dades exposat mitjançant una URL, amb endpoints específics per a obtenir informació de clients i productes; aquests endpoints es defineixen en el API per a facilitar el consum d'aquests serveis. 
- 2 TRANSFORMACIÓ DE DADES.** Els projectes poden utilitzar eines de transformació de dades proporcionades pel API Manager per a adaptar la informació al format requerit pel sistema existent, o per a enviar la informació a aquest sistema. Per exemple, podria convertir les dades de format XML a format JSON i enviar-los. 
- 3 SEGURETAT I AUTENTICACIÓ.** CTTI configura la seguretat i l'autenticació en el API Manager per a garantir que només els usuaris autoritzats puguin accedir a la API. Això pot implicar la configuració de tokens d'accés o autenticació basada en claus. 
- 4 DOCUMENTACIÓ.** Els projectes poden utilitzar les eines de documentació del API Manager per a descriure clarament com altres desenvolupadors poden interactuar amb la API, quines dades poden esperar i com han d'autenticar-se. 
- 5 MONITORATGE I ANÀLISI.** Els projectes poden realitzar monitoratge en el API Manager, concretament via modulo Analytics, amb la finalitat de rastrear el rendiment de les APIs i detectar possibles problemes. Això podria incloure el monitoratge del temps de resposta, la taxa d'èxit de les sol·licituds i altres indicadors clau. 
- 6 GESTIÓ DE VERSIONS.** Si hi ha canvis en el sistema extern, i això canvia la lògica de la API, CTTI pot utilitzar les capacitats de gestió de versions del API Manager per a assegurar una transició suau sense afectar les aplicacions que ja depenen de la API. 



## 3. Elements Clau

# Polítiques

### Element Clau

#### POLÍTIQUES

El API Manager ofereix la capacitat de definir i aplicar polítiques a les APIs, proporcionant als desenvolupadors una sèrie de beneficis significatius.

- Entre ells, s'inclouen la possibilitat d'establir límits d'ús per a gestionar eficaçment la càrrega, quotes per a controlar l'accés, i la capacitat de realitzar transformacions i enriquiment de dades.
- Aquestes polítiques no sols faciliten un major control i gestió sobre la API, sinó que també ofereixen als desenvolupadors eines poderoses per a optimitzar el rendiment, millorar la seguretat i assegurar el compliment d'estàndards i regulacions específics de la indústria.

### Camins d'aplicació

1

**AUTORITZACIÓ.** Política d'Autorització, que garanteix la validació d'un token d'autorització vàlid per a accedir a la API, ja sigui mitjançant l'ús d'un protocol d'autorització OAuth o OIDC, segons es tingui configurat el proveïdor.



2

**LÍMITS DE TAXA.** Política enfocada a restringir la quantitat de sol·licituds que un usuari pot fer en un període específic per a evitar abusos de consum sobre una API (Throttling).



3

**VALIDACIÓ DE DADES.** Política per a verificar que les dades enviades a través de la API compleixen amb uns certs criteris abans de ser processats.



4

**TRANSFORMACIÓ DE DADES.** Política per a convertir formats de dades, per exemple de XML a JSON, per a complir amb els estàndards de la API i d'aquells sistemes que requereixin un format determinat.



5

**CAPÇALERES ARQUITECTURA.** Política que genera les capçaleres d'arquitectura que poden ser útils en integracions amb un Backend, de cara a garantir la seguretat i eficiència de les comunicacions.



6

**LOGGING I AUDITORIA.** Política per a registrar esdeveniments i accions importants per a un seguiment i auditoria efectius.



7

**MANEIG D'ERRORS.** Política per a definir com es manejaran els errors, quina informació es retornarà al client i com es registraran els errors internament.



8

**RECUPERACIÓ DE VARIABLES.** Política que permet la recuperació de variables emmagatzemades en els Gateways a partir d'un fitxer donat. Tenint les següents properties:

- **fichero-variables:** Nom del fitxer que conté les variables que volem recuperar.
- **get-variables:** Llistat de variables que es volen recuperar separades per “,”.



## 3. Elements Clau

# Cicle de vida de les APIs

### Element Clau

#### CICLE DE VIDA DE LES APIs

- El API Manager facilita la gestió del cicle de vida complet de les APIs, des de la creació i publicació inicial fins a la retirada o desactivació d'una API, de tal forma que s'agilitzi, homogenitzi, estandarditzi i controli el treball realitzat per cadascun dels proveïdors sobre les APIs.
- El cicle de vida de les APIs en el API Manager abasta des del disseny i desenvolupament fins al retir i desactivació. El API Manager facilita la gestió de cada etapa, des de la publicació i consum de les APIs fins al monitoratge i anàlisi del seu rendiment i ús. A més, permet l'actualització i versionat de les APIs, assegurant una transició suau per als consumidors. Finalment, el API Manager també facilita el retir i desactivació de APIs o versions antigues quan ja no són necessàries.

### Camins d'aplicació

1

**DISSENY I DESENVOLUPAMENT.** En aquesta etapa, els equips de desenvolupament de CTTI dissenyen i desenvolupen les APIs utilitzant eines i estàndards adequats. Poden utilitzar el API Manager per a definir les especificacions de la API, com els endpoints, els paràmetres i les respostes esperades.



2

**PUBLICACIÓ I CONSUM.** Una vegada que les APIs estan llestes, es publiquen en el portal del API Manager de CTTI, on els consumidors poden descobrir-les i fer ús d'elles. Els consumidors poden sol·licitar claus de API o tokens d'accés per a autenticar-se i autoritzar-se correctament. El API Manager gestiona l'accés i garanteix que només els consumidors autoritzats puguin utilitzar les APIs.



3

**MONITORATGE I ANÀLISI.** Dins del API Manager, el *mòdul de Analytics* permet als projectes de CTTI monitorar el rendiment dels seus APIs, podent realitzar un seguiment de mètriques, com el temps de resposta, la taxa d'èxit i l'ús de recursos. Això els ajuda a identificar possibles problemes i optimitzar el rendiment de les APIs.



4

**ACTUALITZACIÓ I VERSIONAT.** A mesura que les necessitats i requisits canvien, CTTI pot realitzar actualitzacions en les APIs existents. Utilitzant el API Manager, poden crear noves versions de les APIs i gestionar la transició dels consumidors cap a les versions actualitzades. Això permet introduir millores i noves funcionalitats sense interrompre als consumidors existents.



5

**RETIR I DESACTIVACIÓ.** En algun moment, CTTI pot decidir retirar una API o desactivar una versió antiga. Això pot ocórrer quan la API ja no és rellevant o quan s'ha migrat a una versió més recent. El API Manager permet gestionar aquest procés de manera controlada, assegurant que els consumidors estiguin informats i tinguin temps suficient per a adaptar-se als canvis.





## 4. Beneficis

---

# API Manager Beneficis

### API MANAGER COM A CATALITZADOR DE L'ÈXIT EMPRESARIAL

En el teixit digital de l'era actual, on la connectivitat i l'agilitat són imperatius comercials, l'adopció d'un API Manager emergeix com un catalitzador essencial per a l'èxit empresarial. En simplificar la gestió, seguretat i exposició de les Interfícies de Programació d'Aplicacions (API), el API Manager ofereix una sèrie de beneficis que impulsen la innovació, la col·laboració i l'eficiència operativa.

Els beneficis clau d'un API Manager són...



## 4. Beneficis

# Elements

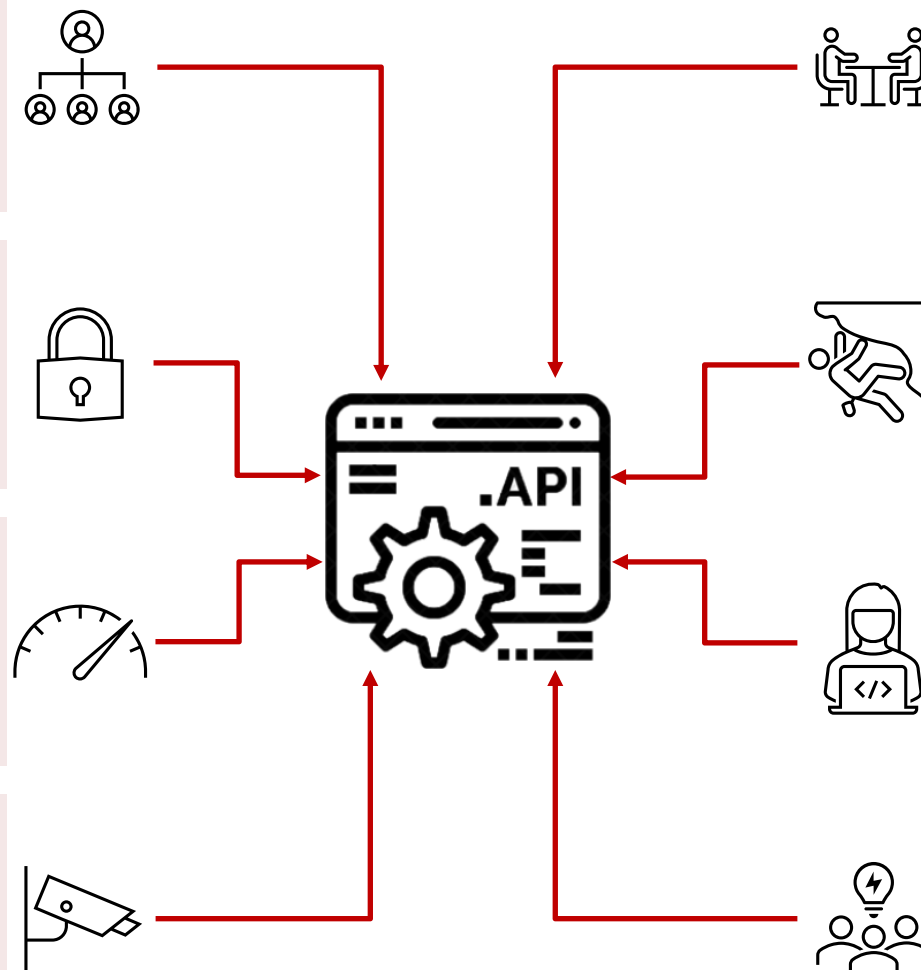
### Centralització i gestió simplificada:

El API Manager permet centralitzar i gestionar les APIs de tots els projectes dins del CTTI en un sol lloc. Això facilita l'administració i el control de les APIs, ja que es poden definir polítiques de seguretat, límits d'ús i monitoratge de rendiment de manera centralitzada.

**Seguretat i control d'accés:** El API Manager proporciona capacitats de seguretat robustes per a protegir les APIs i les dades sensibles. Això ajuda a prevenir accessos no autoritzats i protegir la informació confidencial.

**Monitoratge i anàlisi:** El API Manager recopila mètriques de rendiment i ús de les APIs, la qual cosa permet als projectes dins de CTTI, a través del mòdul de Analytics, monitorar i analitzar el rendiment de les APIs en temps real. Això permet prendre mesures correctives ràpidament i optimitzar el rendiment de les APIs per a brindar una millor experiència als consumidors.

**Control de versions i canvis:** El API Manager facilita el control de versions i canvis de les APIs. Això els permet realitzar millores i actualitzacions en les APIs sense interrompre als consumidors existents.



**Facilita la col·laboració:** El API Manager proporciona un portal on els consumidors poden descobrir i accedir a les APIs de l'organització de CTTI. Això fomenta la col·laboració i l'adopció de les APIs per part dels consumidors.

**Escalabilitat i flexibilitat:** El API Manager permet als projectes dins de CTTI escalar i adaptar els seus APIs segons les necessitats canviants del negoci, proporcionant d'aquesta manera la possibilitat de realitzar configuracions en les APIs i que aquestes es vegin reflectides de manera immediata per als consumidors.

### Millora l'experiència del consumidor:

El API Manager ajuda a millorar l'experiència del consumidor en proporcionar documentació clara i completa de les APIs, així com exemples d'ús. Això facilita als consumidors comprendre i utilitzar les APIs de CTTI de manera efectiva.

### Impulsa la innovació i la col·laboració:

El API Manager fomenta la innovació i la col·laboració en permetre a CTTI compartir les seves APIs amb socis externs i desenvolupadors de tercers. Això pot portar a la creació d'ecosistemes de desenvolupadors i a la generació de noves idees i solucions.



## 5. Integració dins del CTTI

---

# API Manager Integració dins del CTTI

### API MANAGER COM A GESTOR I PROVEÏDOR DE SERVEIS INFORMATICOS

En un món impulsat per la connectivitat i la interacció entre sistemes, la gestió efectiva de APIs s'ha convertit en un pilar fonamental per a l'èxit de les organitzacions. CTTI (Centri de Telecomunicacions i Tecnologies de la Informació) ha exercit un paper destacat en aquesta dinàmica, aprofitant la plataforma API Connect per a administrar i orquestrar les seves APIs de manera eficient.

Els punts destacats del API Manager dins de CTTI serien:

- ❖ Infraestructura
- ❖ Arquitectura de la plataforma
- ❖ Topologia d'IBM del API Connect

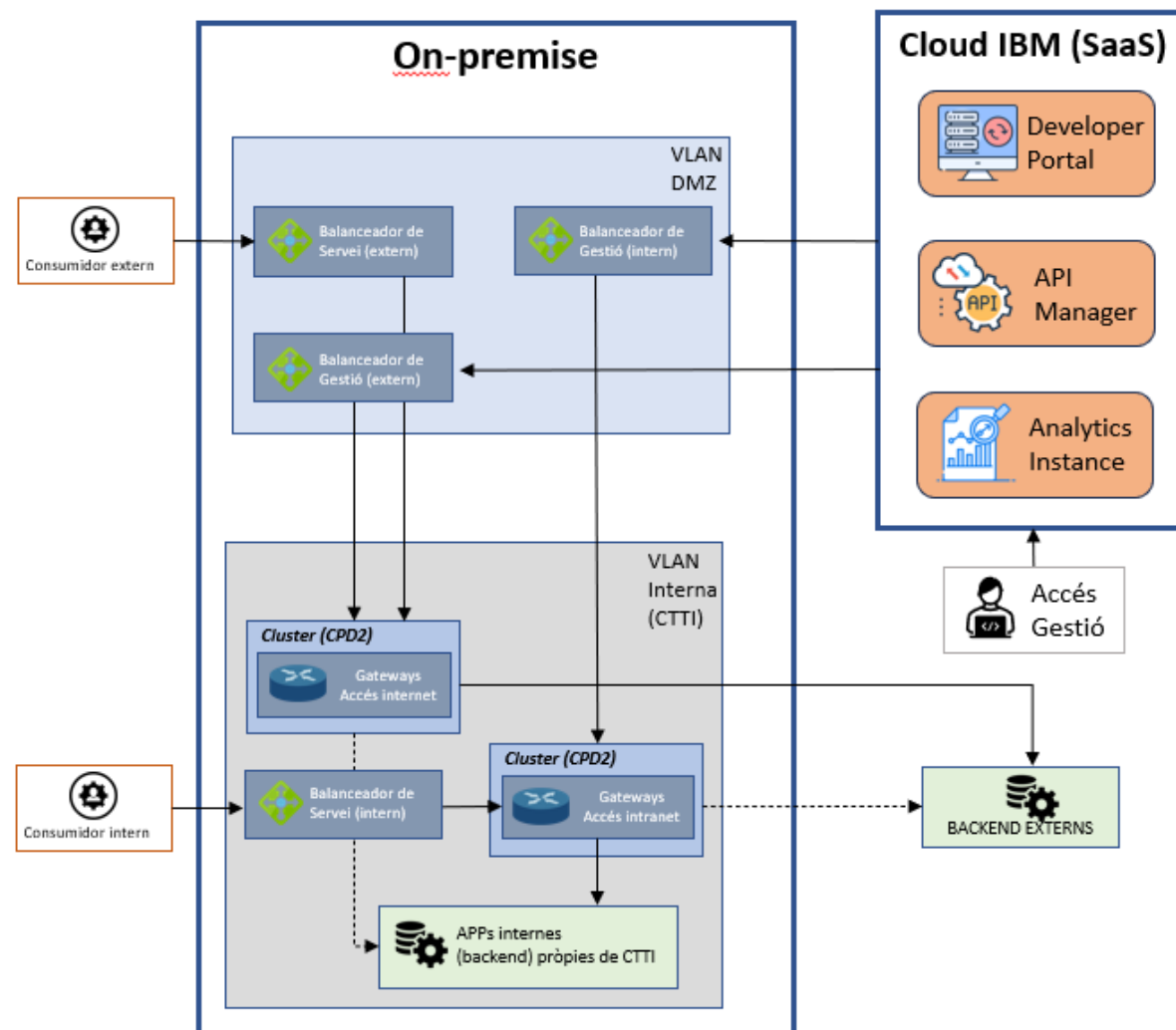
## 5. Integració dins del CTTI

# Infraestructura

CTTI basa la seva infraestructura per al **APIM** en un model de cloud “híbrid”, amb capacitat de gestionar i connectar APIs tant en entorns locals (on-premise) com en el núvol, diferenciant-se clarament dos grans blocs. D'una banda, estaria la part **Cloud** subscrita a un servei **SaaS (IBM API Connect Reserved Instance)** ofert per IBM, des d'on es realitza la gestió i control de les APIs, brindant monitoratge, anàlisi i administració de les APIs.

D'altra banda, estaria el bloc On-Premise que comprèn tots aquells components necessaris per a la comunicació i interconnexió (segments de xarxa, balanceadores, Gateways, etc..) i els elements del backend amb les funcionalitats dels serveis a explotar oferts per CTTI, tant a nivell intern (intranet) com a extern (internet). D'aquest bloc, destacar que les Gateways es troben desplegades en CPD2.

A nivell de connexió, els consumidors accedeixen als diferents segments de xarxa a través dels balanceadores de servei corresponents (intern i extern), els quals connecten amb les respectives Gateways, els quals realitzen el control i redirecció de les peticions als elements backends corresponents, ja sigui a nivell intern de CTTI, com a nivell extern.



## 5. Integració dins del CTTI

---

# Infraestructura

### Característiques clau de la instància API Connect Reservada

- 1 Inici de sessió comuna amb altres serveis d'IBM Cloud mitjançant GICAR via integració OIDC o IBMid
- 2 Aïllament d'uns altres que utilitzen el servei públic
- 3 Gestionada, supervisada i operada per l'equip d'Operacions d'API Connect
- 4 Desplegada en diversos servidors dins de la zona de centre de dades a efectes de resiliència

### Principals components del mòdul SaaS d'instància reservada

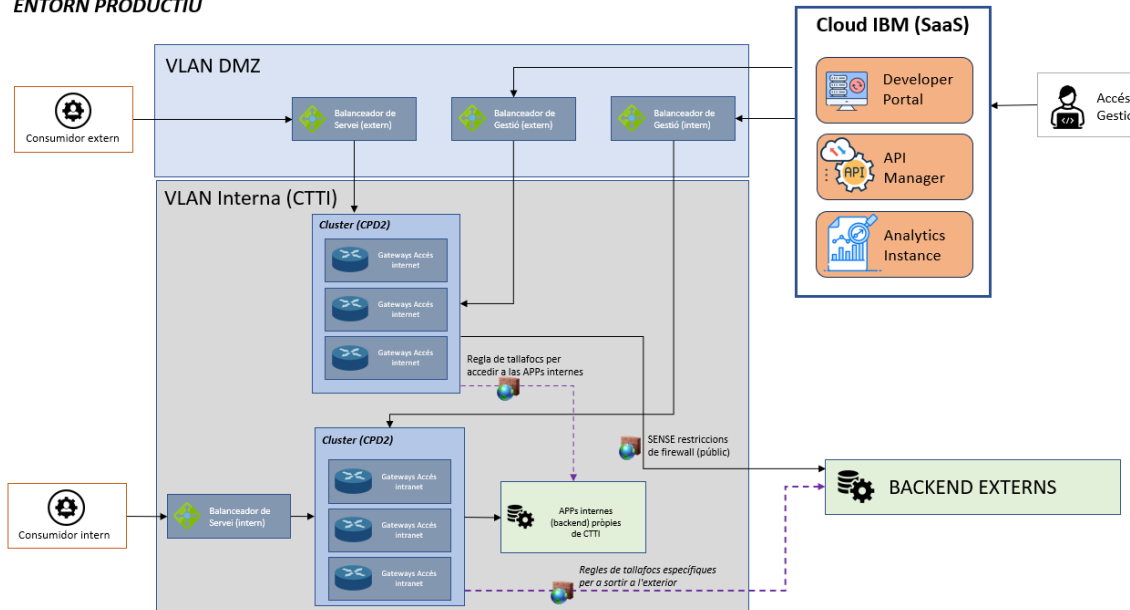
- 1 **Mòdul de gestió de APIs.** En dita modulo, es realitzen totes les tasques d'administració (gestió transversal de les APIs i el seu cicle de vida, gestió d'accessos, veure analítiques, configuracions)
- 2 **Portal de Desenvolupadors.** Plataforma per on els desenvolupadors podran accedir i consultar les APIs disponibles per al seu consum, subscriuint-se a les adequades
- 3 **Gateways.** Són portes d'enllaç empresarial dissenyades per a exposar de manera segura les dades i les aplicacions empresarials onsevulla que resideixin: en local i en clouds. *En concret, CTTI usa Gateways propis on-premise, en lloc d'usar els Gateways de la instància reservada.*
- 4 **Analytics.** Permet als usuaris obtenir informació sobre el rendiment de les APIs, l'ús dels recursos ajuda a l'organització a la detecció de problemes de rendiment, la identificació de patrons d'ús i la presa de mesures per a millorar la seguretat

## 5. Integració dins del CTTI

# Arquitectura de la plataforma

A nivell d'arquitectura, la plataforma de API Manager en CTTI compta amb dos entorns definits, **entorn productiu** i **entorn no productiu**, distribuïts en dos segments de xarxa (VLAN Interna i VLAN DMZ). Les VLAN són una manera de dividir una xarxa física en xarxes lògiques separades, la qual cosa permet segmentar el trànsit i millorar la gestió i seguretat d'una xarxa

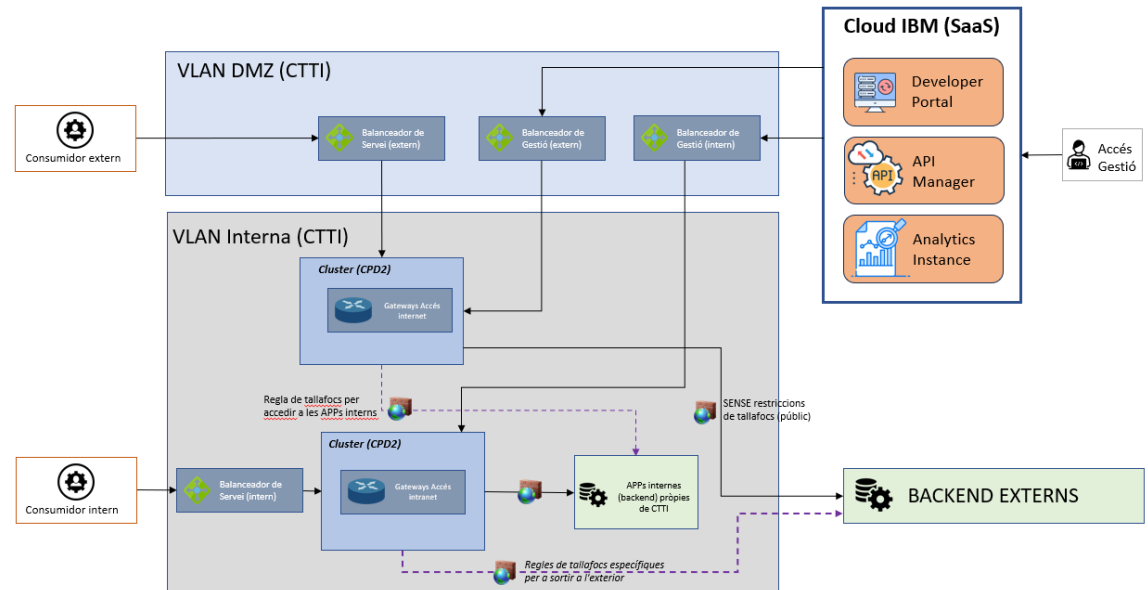
### ENTORN PRODUCTIU



**Entorn productiu (PRO).** És l'entorn que es troba a la disposició dels usuaris finals per al consum de les APIs en un model d'alta disponibilitat. Amb la següent distribució:

- 6 Gateways: distribuïdes en 2 clusters de 3 Gateways cadascun, un donant servei a peticions des de la DMZ i un altre a peticions des de la VLAN Interna.
- 4 Balanceadores:
  - 2 Balanceadores per a distribuir les peticions a nivell de gestió sobre els components que conformen la plataforma.
  - 2 balanceadores per a distribuir les peticions a nivell de servei, és a dir, les aplicacions manen les peticions a aquests balanceadores per a després accedir a les endpoints de les APIs publicades en els Gateways.

### ENTORN NO PRODUCTIU



**Entorn no productiu (PRE).** Ofereix un entorn similar al de producció tant a nivell de gestió com de servei, encara que no està configurat amb alta disponibilitat. Així, la distribució en el CPD2 que conforma aquest entorn és la següent:

- 2 Gateways: un donant servei a peticions des de la DMZ i un altre a peticions des de la VLAN Interna
- 4 Balanceadores amb la mateixa configuració que en l'entorn productiu

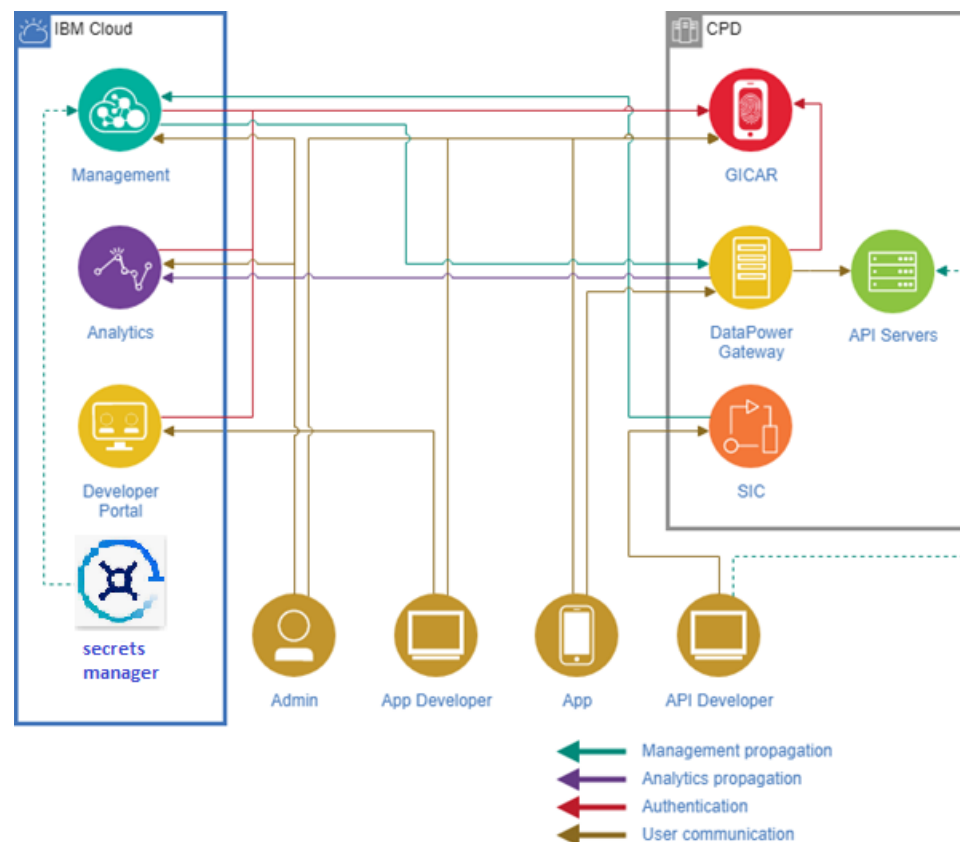
Els proveïdors usen aquest entorn per a desplegar els seus APIs en una primera fase, i realitzar totes les proves necessàries com són proves d'integració, proves d'acceptació d'usuaris prèvies per a assegurar el posterior desplegament en producció.

## 5. Integració dins del CTTI

# Topologia

Capa d'IBM Cloud, inclou la instància reservada d' API Connect, que és el servei de SaaS (Programari as a Service) contractat, del qual IBM és l'encarregat de realitzar el manteniment. Està composta pels següents serveis

- ❖ **IBM API Connect (Management).** Coordina la configuració de la plataforma
- ❖ **IBM API Connect (Analytics).** Permet la visualització de les dades analítiques
- ❖ **IBM API Connect (Developer Portal).** Permet la visualització dels catàlegs de APIs
- ❖ **IBM Secrets Manager.** Gestiona els certificats TLS a usar en els serveis Gateways configurats



Capa de CPD de CTTI, en la qual estan desplegats els següents components

- ❖ **GICAR.** Servei d'autenticació intern (OpenID i SAML)
- ❖ **API Servers.** Backends de les APIs
- ❖ **SIC.** Servei d'Integració contínua per a desplegar les configuracions de les APIs a exposar

Quant als actors del sistema, es poden apreciar els següents:

- ❖ **API Developer.** Desenvolupador de APIs a exposar. S'autentiquen mitjançant el clau proporcionat per GICAR
- ❖ **Application.** Aplicacions consumidores que invocaran les APIs desplegades pels API Developers.
- ❖ **App Developer.** Desenvolupador de les aplicacions consumidores. S'autentiquen mitjançant protocol OpenID corresponent (GICAR, VÀlid,...)
- ❖ **Admin.** Usuari administrador de la plataforma. Autenticat mitjançant GICAR/IBMid



## 6. Desplegament de APIs

---

# API Manager Desplegament de APIs

### INTEGRACIÓ AMB LA PLATAFORMA DE DESPLEGAMENTS DEL CTTI

En la gestió efectiva de APIs, el desplegament juga un paper fonamental. Integrar APIs de manera eficient i consistent és essencial per a garantir un flux de treball àgil i un desenvolupament continu. Per a l'eina de API Manager, hem optimitzat aquest procés mitjançant la implementació d'un pipeline dedicat al desplegament de APIs sobre els diferents entorns.

Aquest enfocament permet un lliurament ràpid i segur, assegurant que les actualitzacions i millores s'integrin de manera fluida en el nostre ecosistema, mantenint la coherència i l'eficàcia en tot moment.

## 6. Desplegament de APIs

# Metodologia de desenvolupament i desplegament

A continuació, es detallen les fases de desenvolupament del API fins al seu desplegament en producció:



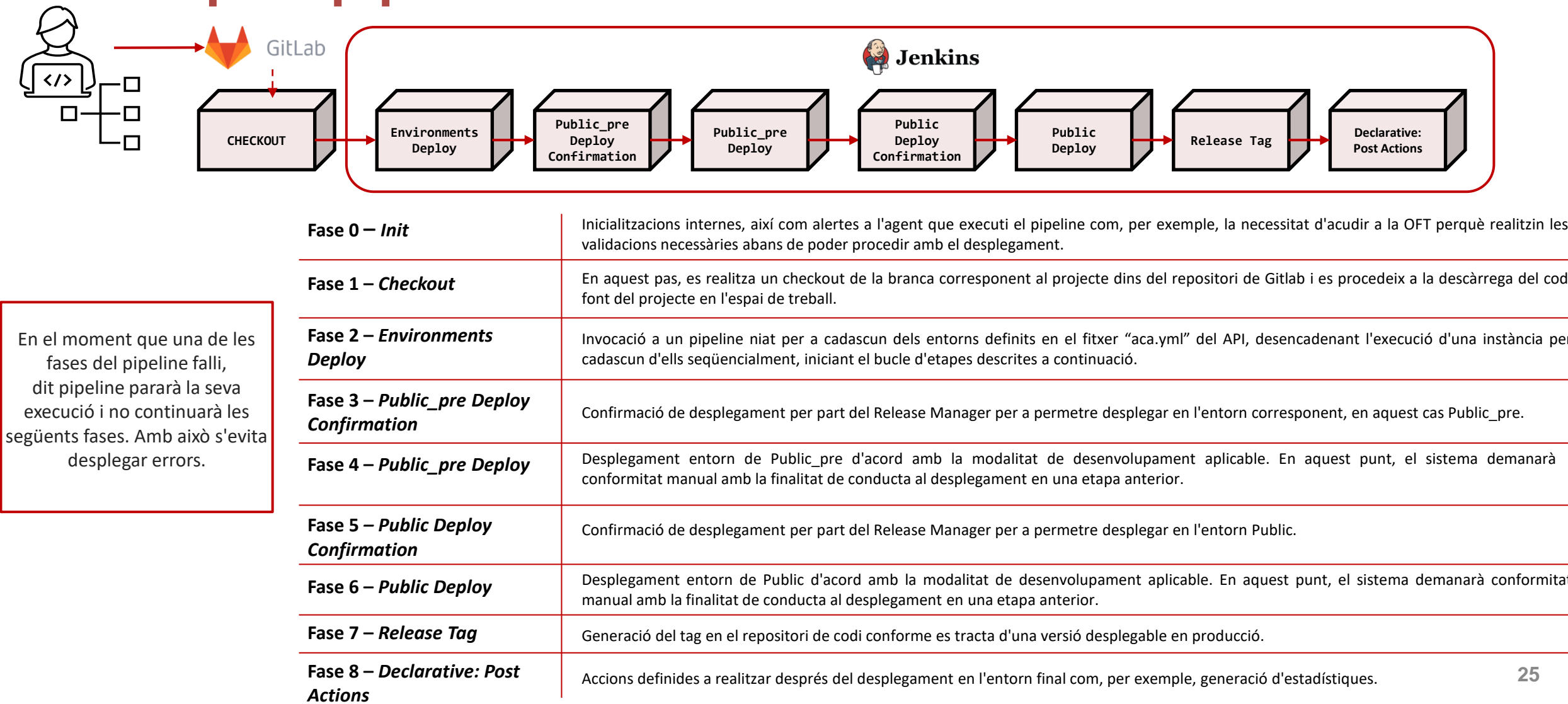
- **Desenvolupament de APIs i Productes:** Els projectes utilitzen l'eina API Designer Toolkit, proporcionada per IBM API Connect, per a desenvolupar i crear els APIs i Productes requerits pel projecte; realitzant les possibles configuracions necessàries de seguretat, plans etc.
- **Proves a través de LTE:** Els projectes poden configurar el **Local Test Environment** proporcionat per IBM (requereix de Docker Desktop), per realitzar les proves unitàries dels APIs i Productes desenvolupats en l'entorn local, de cara a depurar i solucionar qualsevol error previ al desplegament en un entorn del CTTI.
- **Configuració del repositori:** Cada projecte té assignat un repositori de Gitlab, en el qual s'hauran de pujar els fitxers de definició YAMLS, tant de les APIs com dels Productes desenvolupats, així com el fitxer aca.yml, amb la corresponent configuració necessària per al desplegament per part del SIC.
- **Desplegament:** Els proveïdors executen, a través de Jenkins, dels pipelines per a desplegar els APIs i Productes desenvolupats a l'entorn de preproducció i producció de CTTI. Els fitxers YAML hauran d'estar pujats a la branca Màster corresponent del repositori assignat de Gitlab.

Per a veure més detalladament sobretot el procés del desplegament d'un projecte, consultar el document **Guia de desplegament** en <https://canigo.ctti.gencat.cat/plataformes/apim/desplegament/>



## 6. Desplegament de APIs

# Descripció pipeline API



En el moment que una de les fases del pipeline falli, dit pipeline parará la seva execució i no continuarà les següents fases. Amb això s'evita desplegar errors.



## 7. Guia d'ús

---

# API Manager

## Guia d'ús

### API MANAGER COM A EINA DE TREBALL

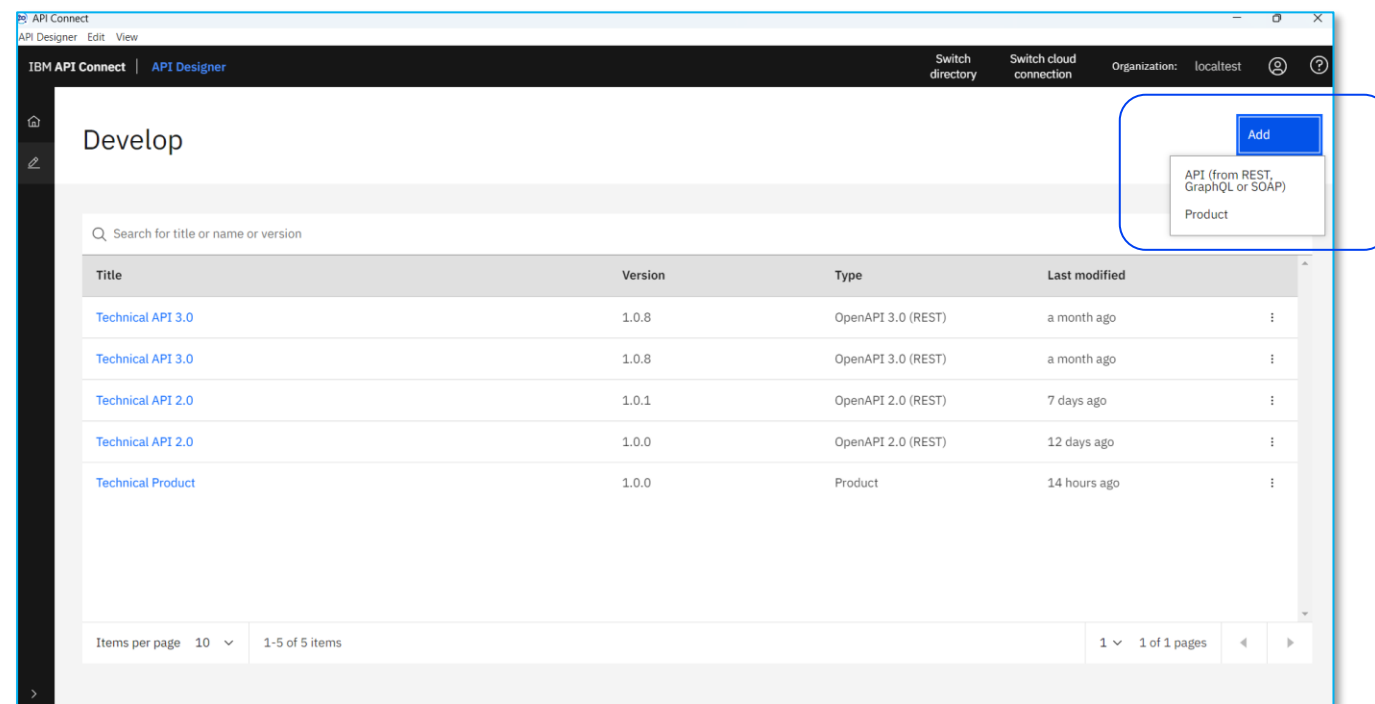
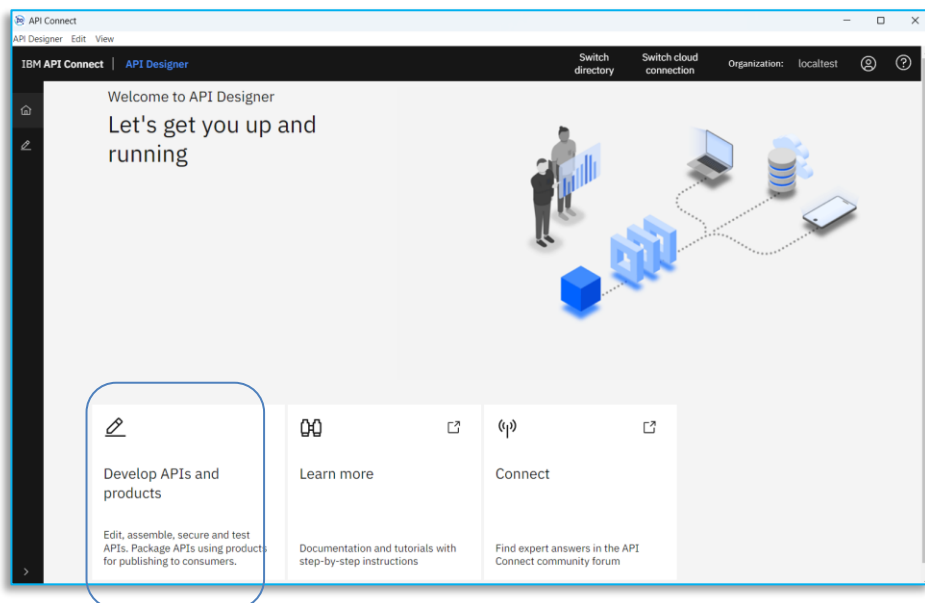
L'eina Toolkit de API Connect potència la creació i gestió de APIs de manera eficient per a dissenyadors i desenvolupadors, simplificant el procés des de la concepció fins a la implementació de APIs robustes a través d'un disseny intuïtiu.

A continuació, es detallaran els passos a seguir per a poder treballar amb l'eina Toolkit API Connect...

## 7. Guia d'ús

# Passos

- ❖ Accedim a l'eina del Toolkit en local. Una vegada en la finestra principal, accedim a **Develop APIs and products** per a començar amb el desenvolupament de nostra API

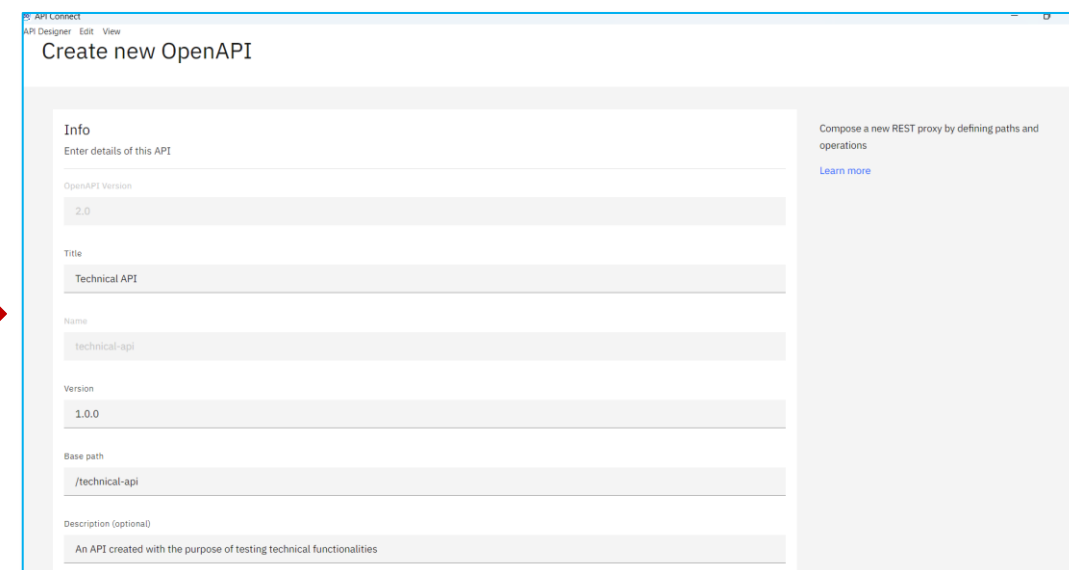
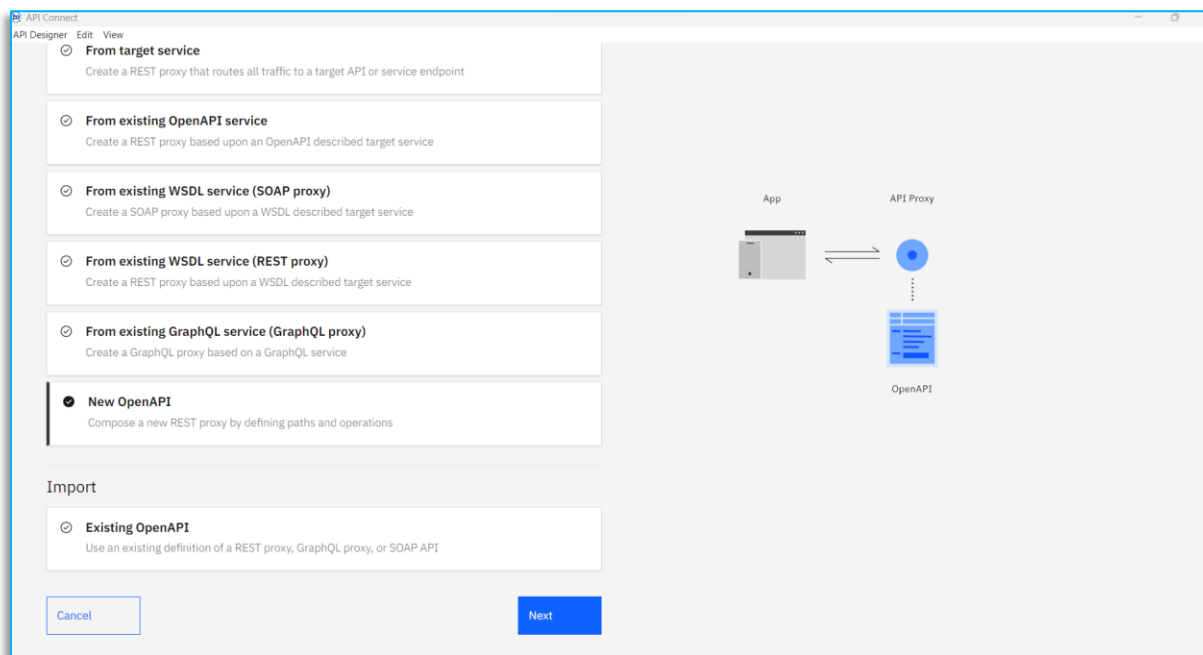


- ❖ Una vegada en **Develop**, indiquem que volem implementar/desenvolupar una API nova, a través del botó **Add** de la dreta i seleccionant **API (from REST GraphQL or SOAP)**

## 7. Guia d'ús

# Passos

- ❖ A continuació, s'ha de seleccionar el tipus de API que volem construir. Per al nostre cas, seleccionarem **New OpenAPI** perquè sigui de tipus REST, i li donem a **Next**

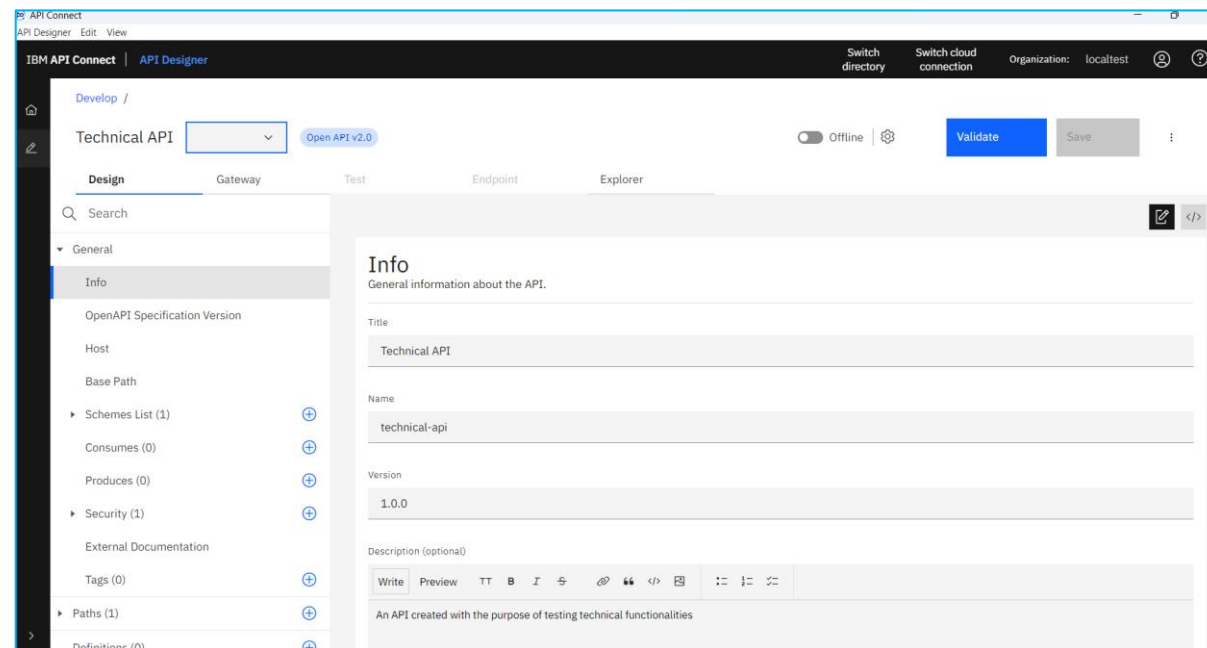
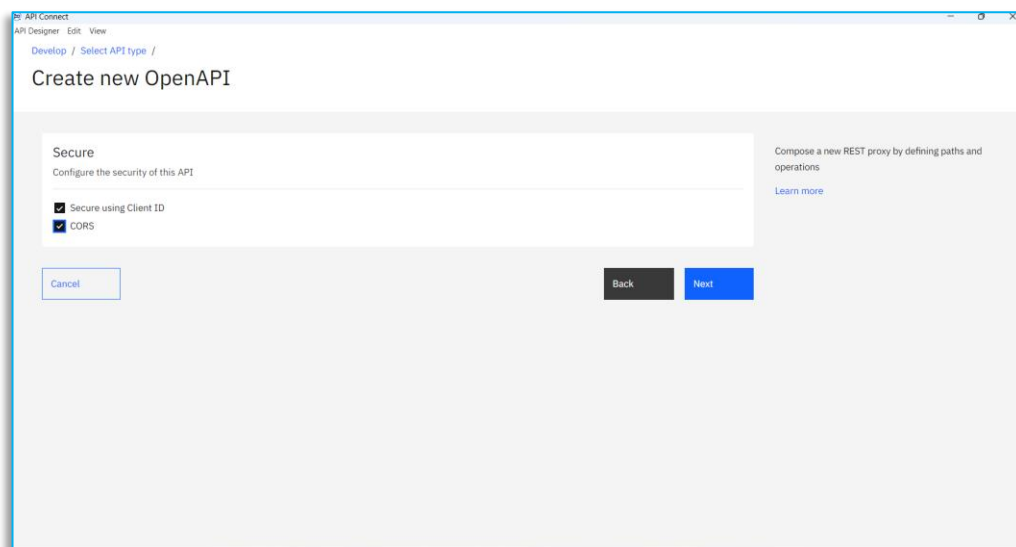


- ❖ Després de continuar, s'haurà d'emplenar el nom de la API en el camp **Title**, i automàticament s'emplenarà el Base path. La versió s'ha de deixar com apareix, ja que seria la 1.0.0

## 7. Guia d'ús

# Passos

- ❖ El següent pas és indicar la seguretat que tindrà nostra API com a base, encara que posteriorment es podrà modificar. Com a bona pràctica, es recomana posar el CORS, i dins de CTTI es requereix que sempre aquest inclòs el ClientID

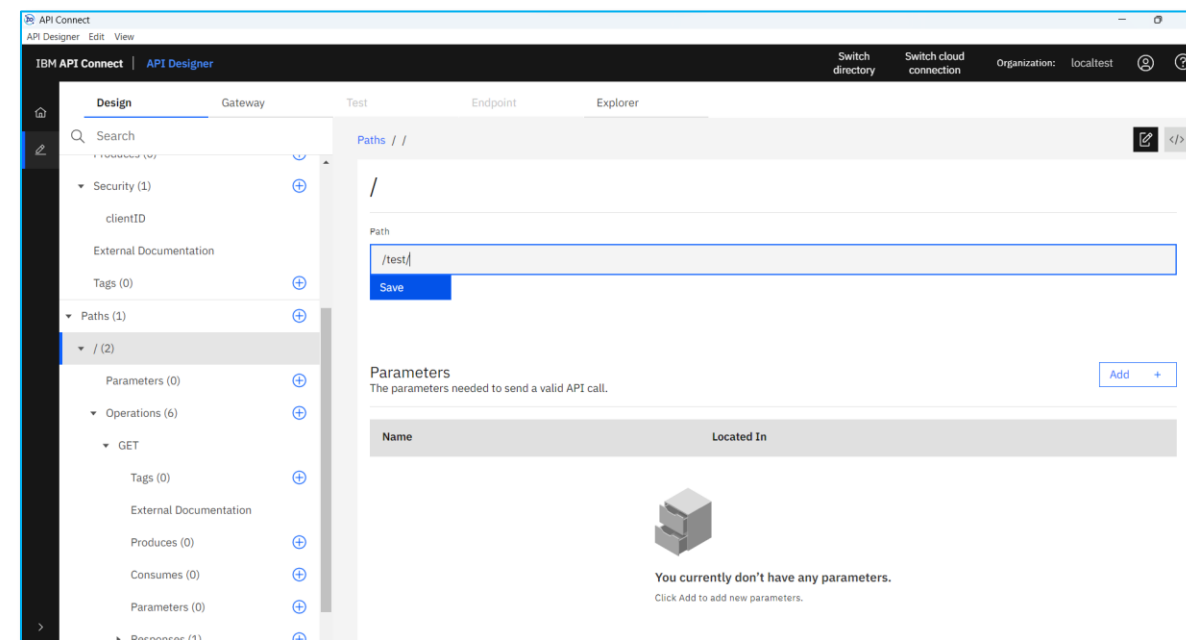
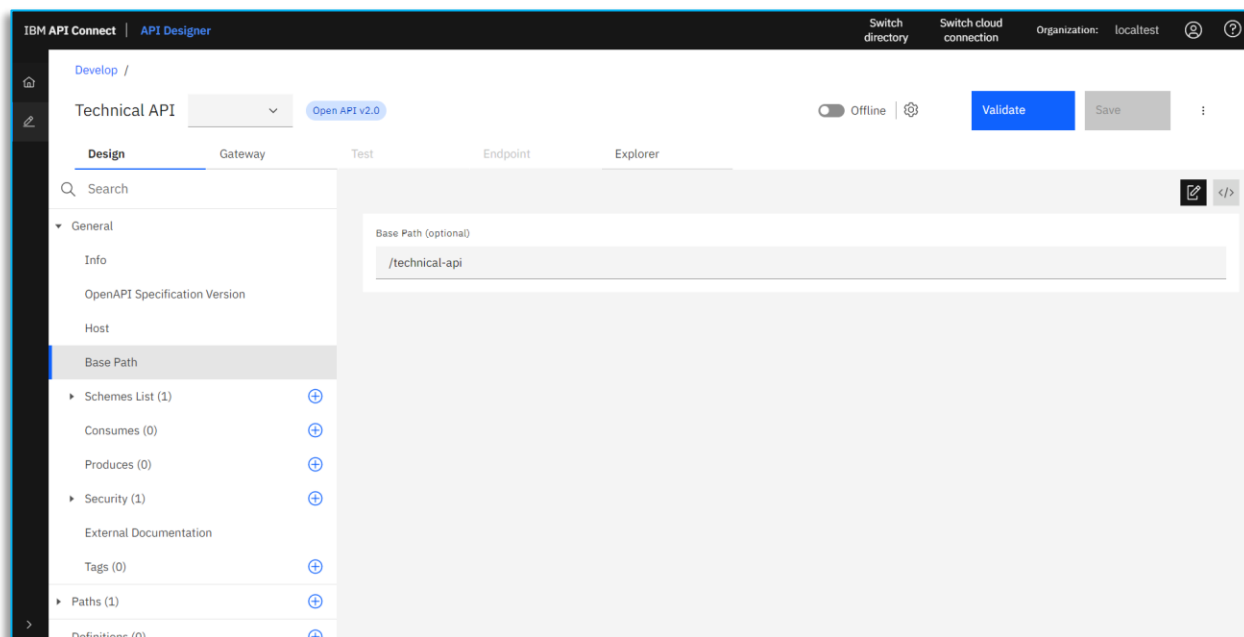


- ❖ A continuació, s'obrirà la finestra de nostra API, on estaran indicades totes les informacions descriptives del API, en la secció de **Info**

## 7. Guia d'ús

# Passos

- ❖ D'altra banda, en la secció **Base Path**, és on ve definit l'identificador del API per a invocar-la. El basePath es pot modificar les vegades que es necessiti, sempre que se segueixi les bones pràctiques i regles de nomenclatura del CTTI, que es poden trobar en altres documents en <https://canigo.ctti.gencat.cat/plataformes/apim/documentacio/>

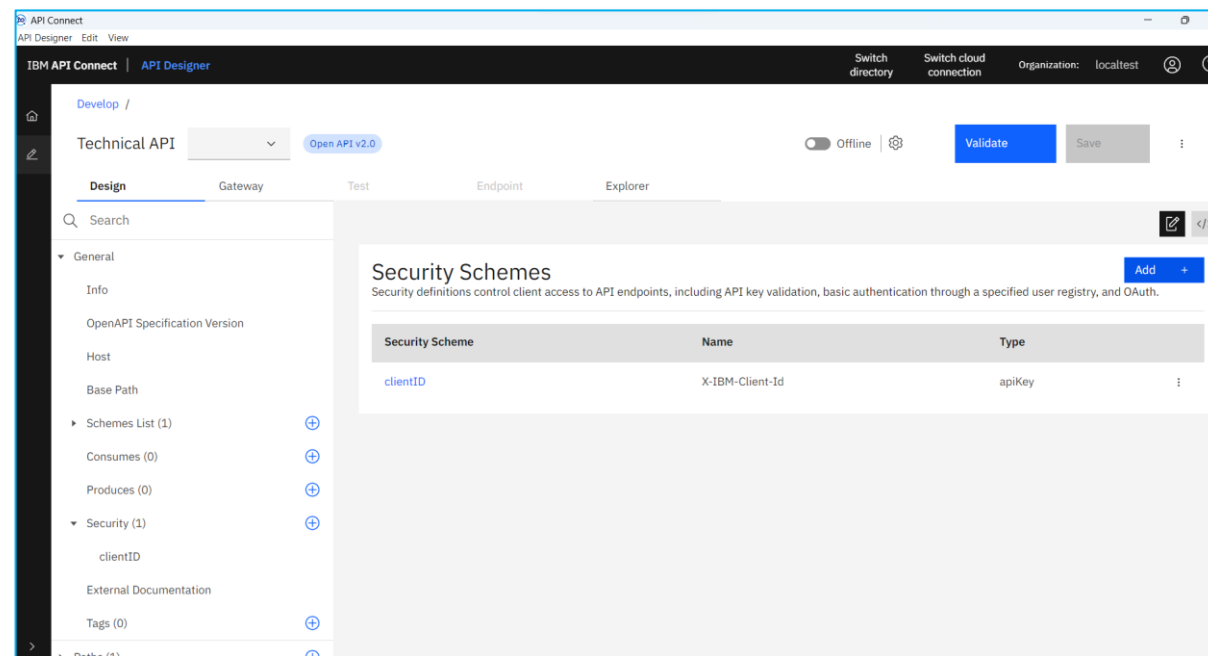
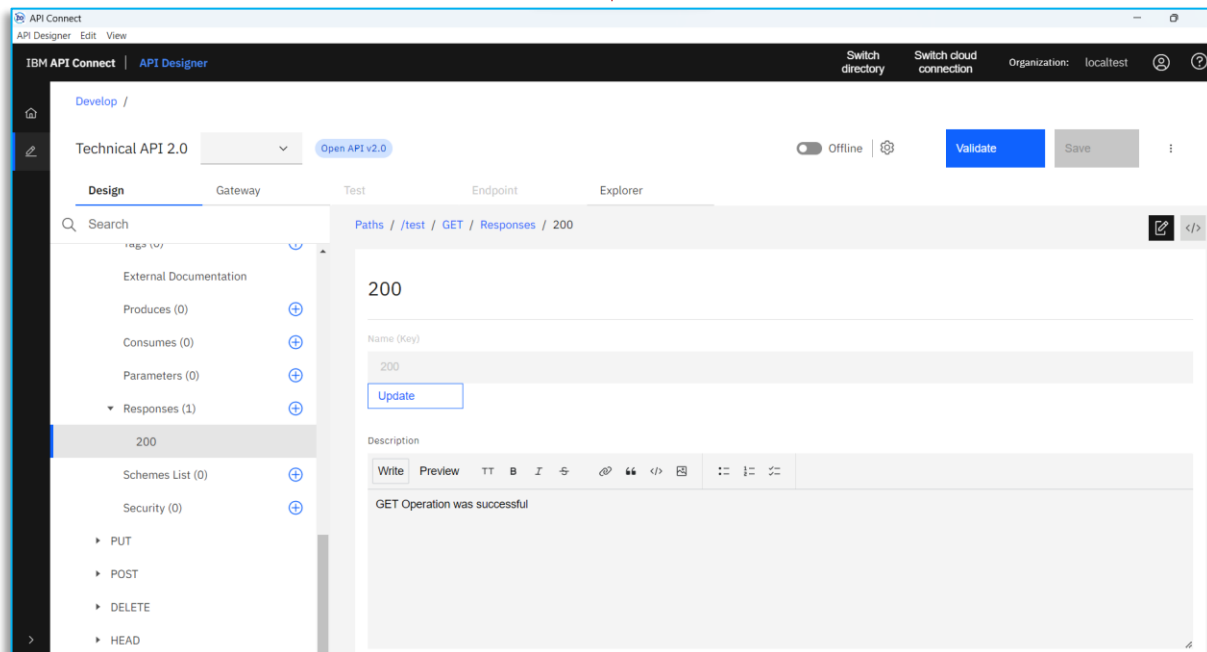


- ❖ En la secció de **Paths**, podem definir els paths de la API, juntament amb els paràmetres necessaris per a invocar a aquests, així com les operacions que contindran.

## 7. Guia d'ús

# Passos

- ❖ Les operacions es generen de manera automàtica per al path que ve definit per defecte. Dins de cada operació, com ara GET, podem definir les respostes que poden arribar-se a generar en cas de OK o de KO. Les definicions han de seguir la nomenclatura del CTTI.

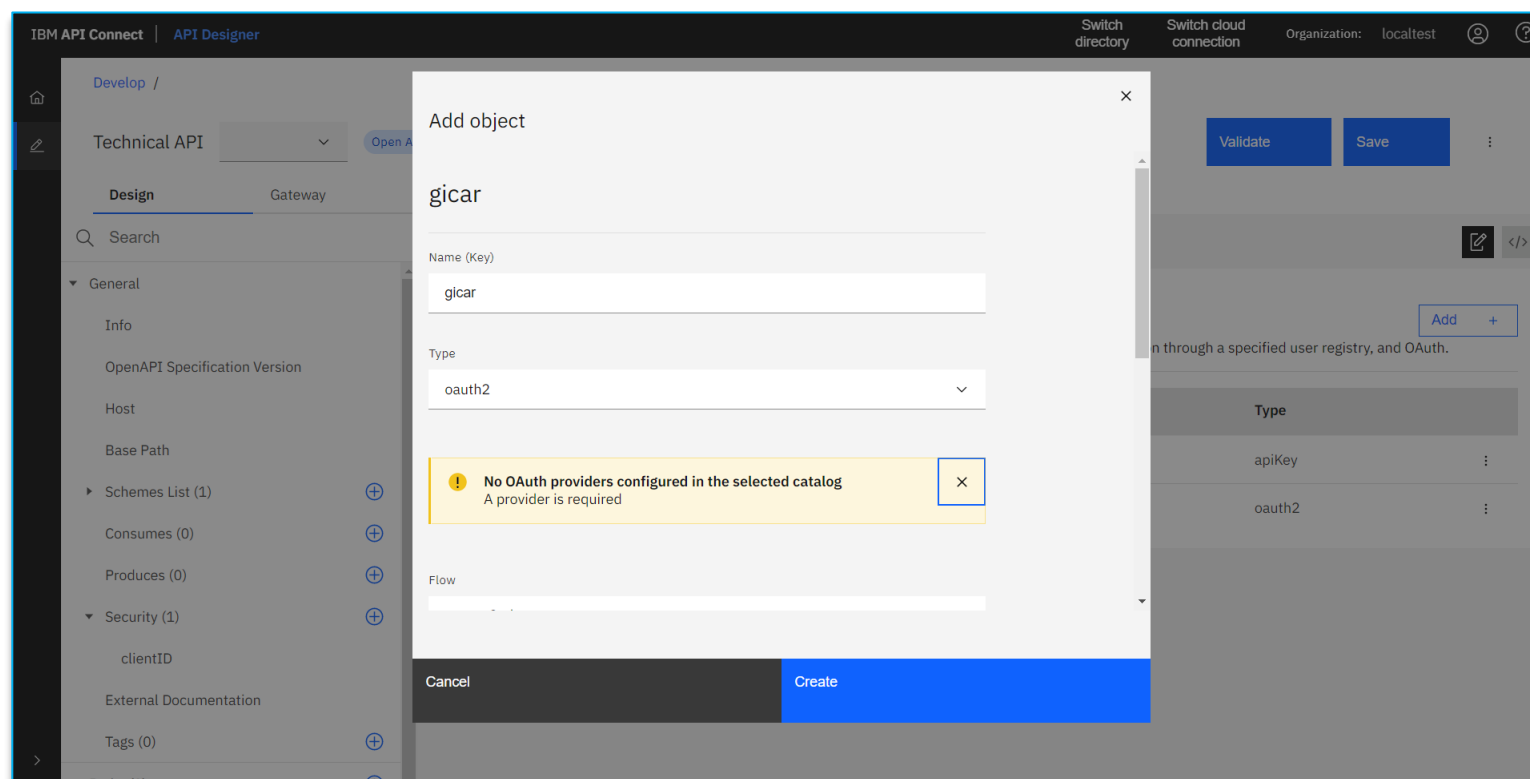


- ❖ Una vegada definit el path amb les seves operacions, procedim a definir els esquemes de seguretat en la secció **Security Schemes**. Per a això, li donem al botó **Add**

## 7. Guia d'ús

# Passos

- ❖ Configurem el protocol de seguretat OAuth2. Per a això, triem el tipus de seguretat **oauth2** i emplenem dins del camp Name (Key), el valor **gicar**

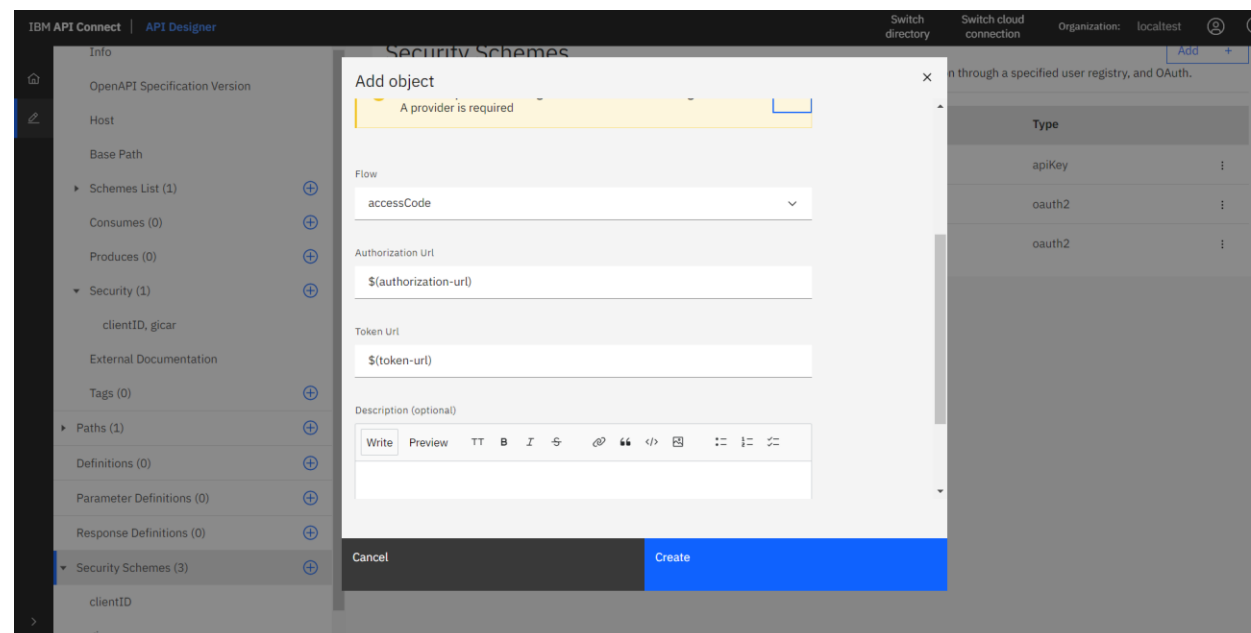


- ❖ **Nota:** Es pot veure que per pantalla es mostra l'alerta de “No OAuth providers configured in the selected catalog”. Continuarem i aquest punt el deixarem així ja que es tractarà més endavant



## 7. Guia d'ús

# Passos



- ❖ Emplenem la resta dels camps corresponents. El valor de cada camp dependrà del proveïdor de OAuth que es vagi a usar.
- ❖ A continuació, es presenta un exemple de com s'emplenaria els camps:
  - En el camp **Flow**, triem el flux de AccessCode
  - En el camp **Authorization Url**, emplenem la següent variable: `$(authorization-url)`
  - En el camp **Token Url**, emplenem la següent variable: `$(token-url)`
  - El camp **Description** es pot deixar en buit

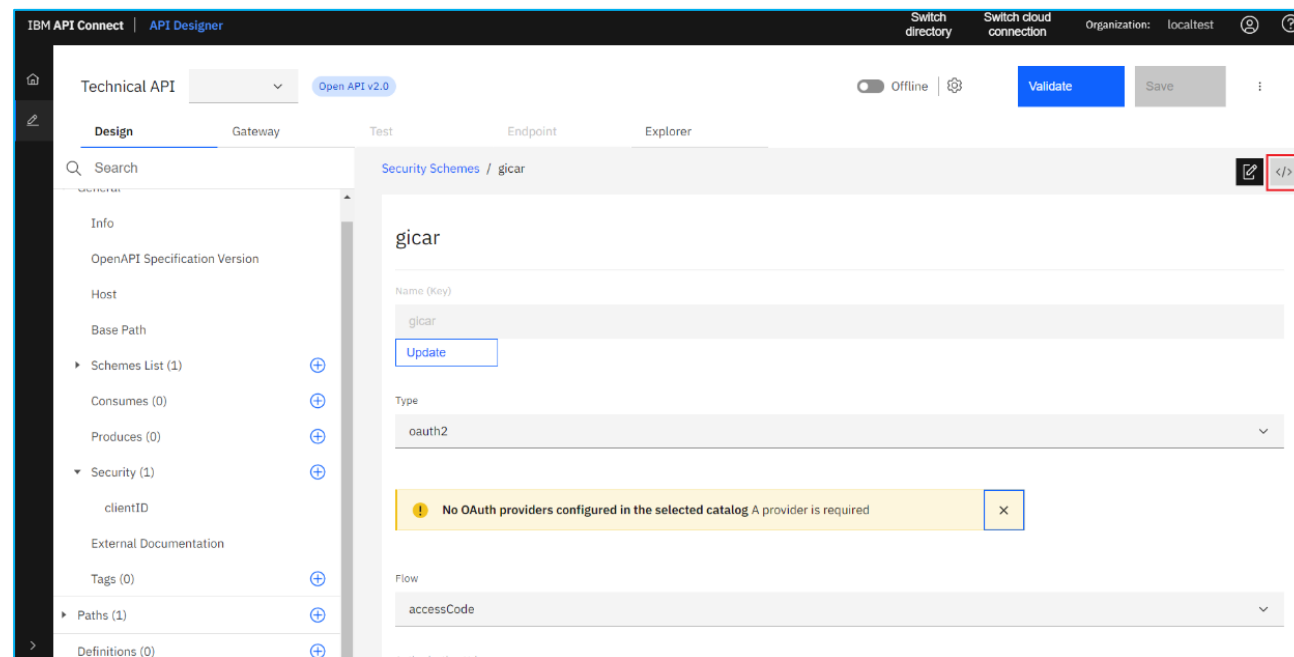
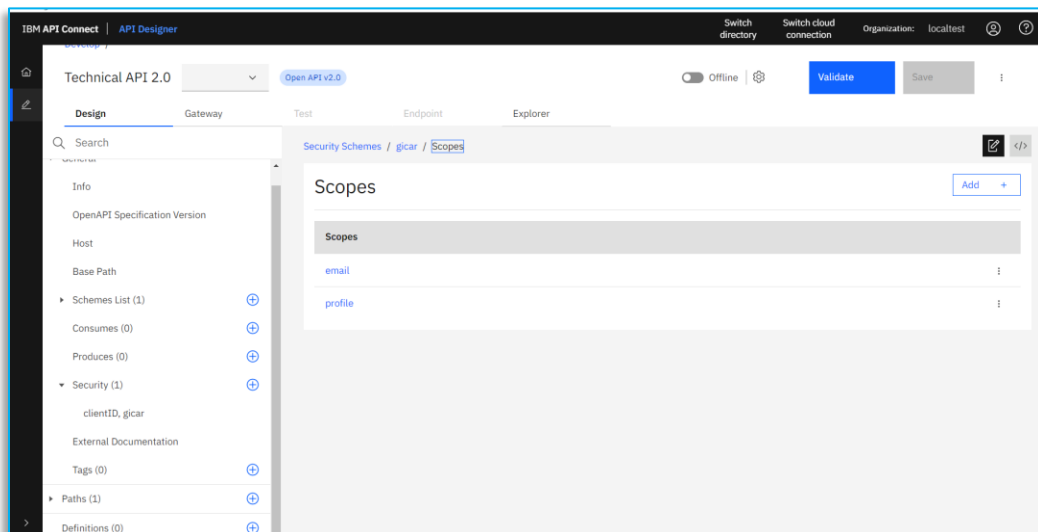
Després d'emplenar aquests camps, li donem al botó **Create**.

## 7. Guia d'ús

# Passos

❖ Dins del OAuth2, es poden definir els **Scopes** necessaris. En aquest cas, s'ha configurat els següents Scopes juntament amb les seves descripcions:

- **email**: email
- **profile**: dades bàsiques d'usuari

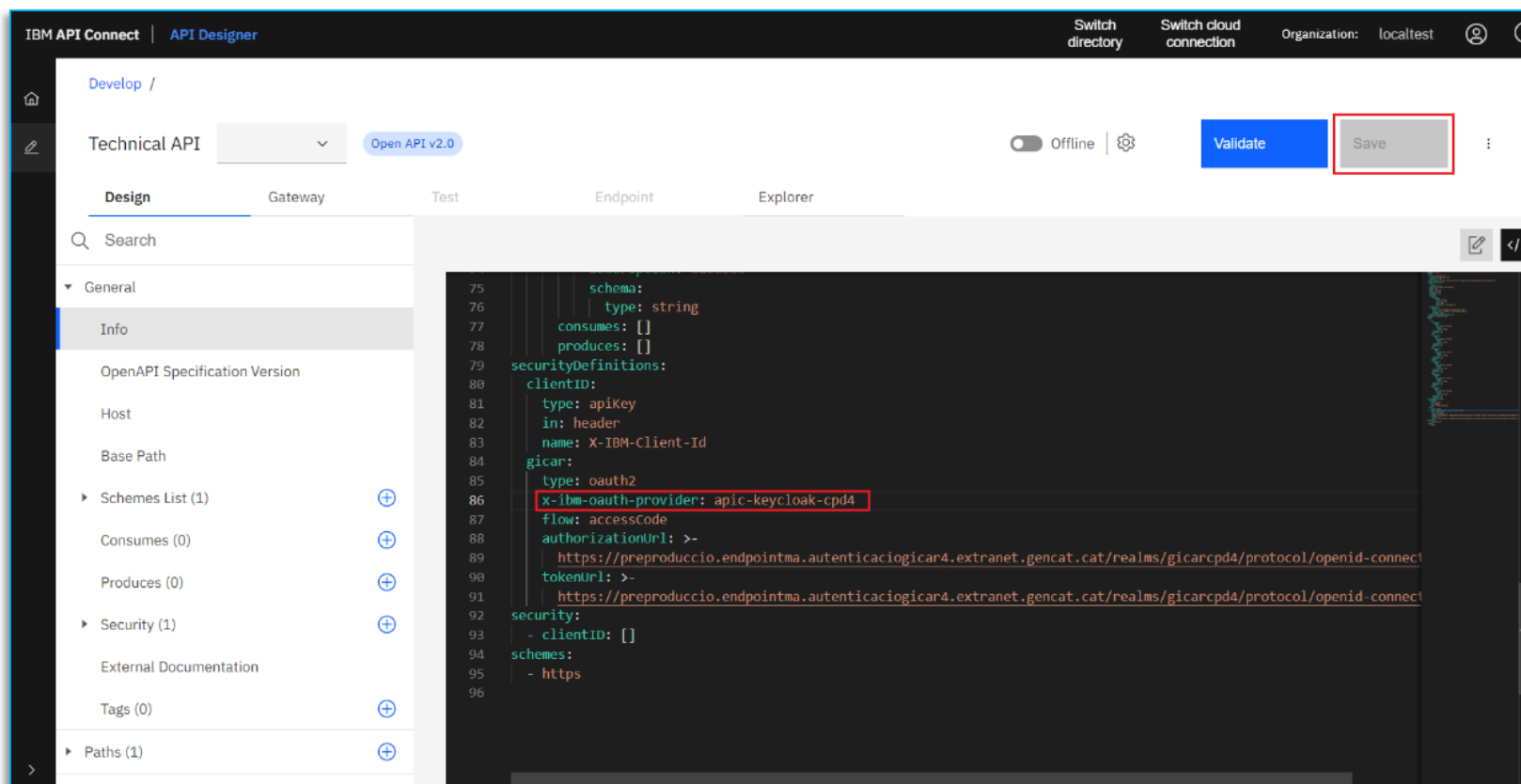


❖ Per a llevar l'alerta que es mostra per pantalla de “No OAuth providers configured in the selected catalog”, accedim al YAML del API mitjançant el botó **Source**

## 7. Guia d'ús

# Passos

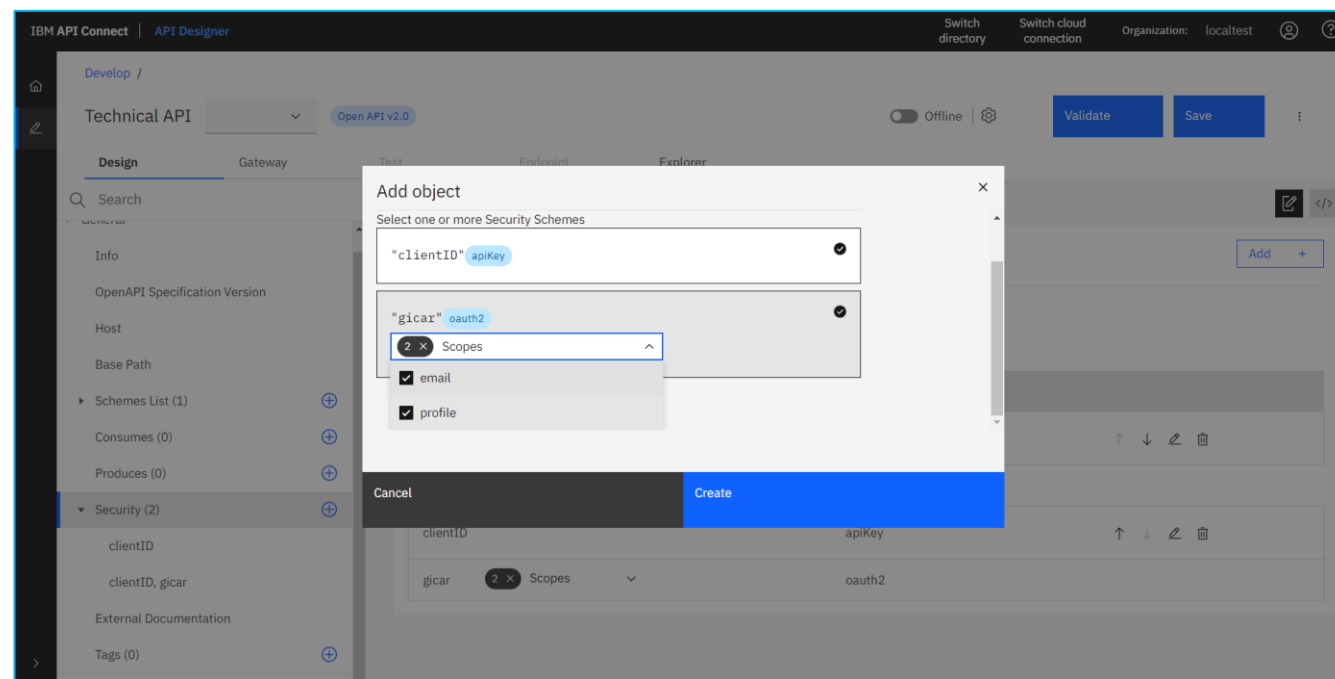
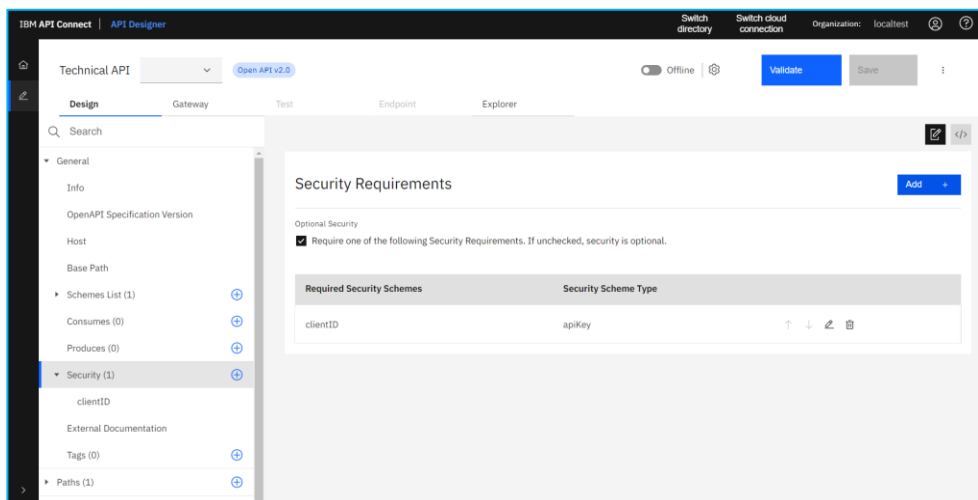
- ❖ Per sota de la línia “**type: oauth2**” posem el proveïdor de OAuth que es vagi a usar. Per al nostre exemple, tenint a KEYCLOAK com el proveïdor de OAuth2, s'ha indicat la següent línia de text en el YAML: **x-ibm-oauth-provider: apic-keycloak-cpd4**. Posteriorment li donem al botó de **Save** per a guardar els canvis



## 7. Guia d'ús

# Passos

- ❖ Una vegada definit l'esquema de seguretat, procedim a configurar nostra API amb aquest esquema. Per a això, accedim a la pestanya **Security**

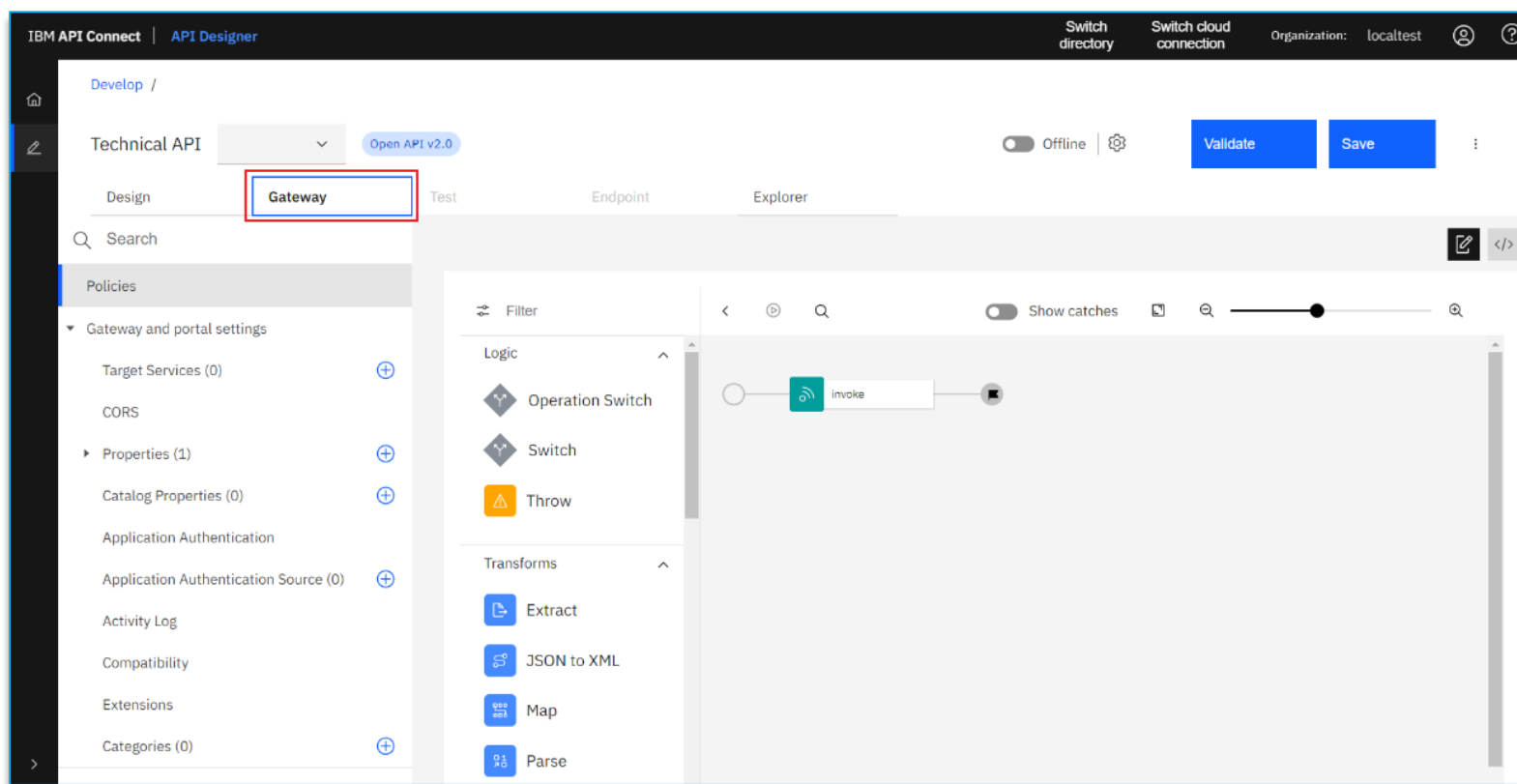


- ❖ Premem sobre el botó **Add** per a afegir el nou protocol de seguretat. Seleccionem la combinació de **ClientID + OAuth2** (amb els 2 Scopes seleccionats) i premem el botó **Create**

## 7. Guia d'ús

# Passos

- ❖ Una vegada que hem acabat de dissenyar les configuracions bàsiques del API, procedim a dissenyar l'acoblat. Per a això, ens dirigim a la pestanya **Gateway**



## 7. Guia d'ús

# Passos

❖ Dins de l'acoblament, es pot incloure les polítiques que es considerin necessàries, d'entre les que pot ser:

- ❖ **Invoke:** Per a cridar a un altre servei des de l'acoblament.
- ❖ **Map:** Per a aplicar transformacions al flux d'acoblament i especificar relacions entre variables.
- ❖ **GatewayScript:** Per a executar un programa de Datapower GatewayScript, codificat per l'usuari.
- ❖ **SetVariable:** Per a agregar una variable d'encapçalat o llevar/establir una variable de temps d'execució.

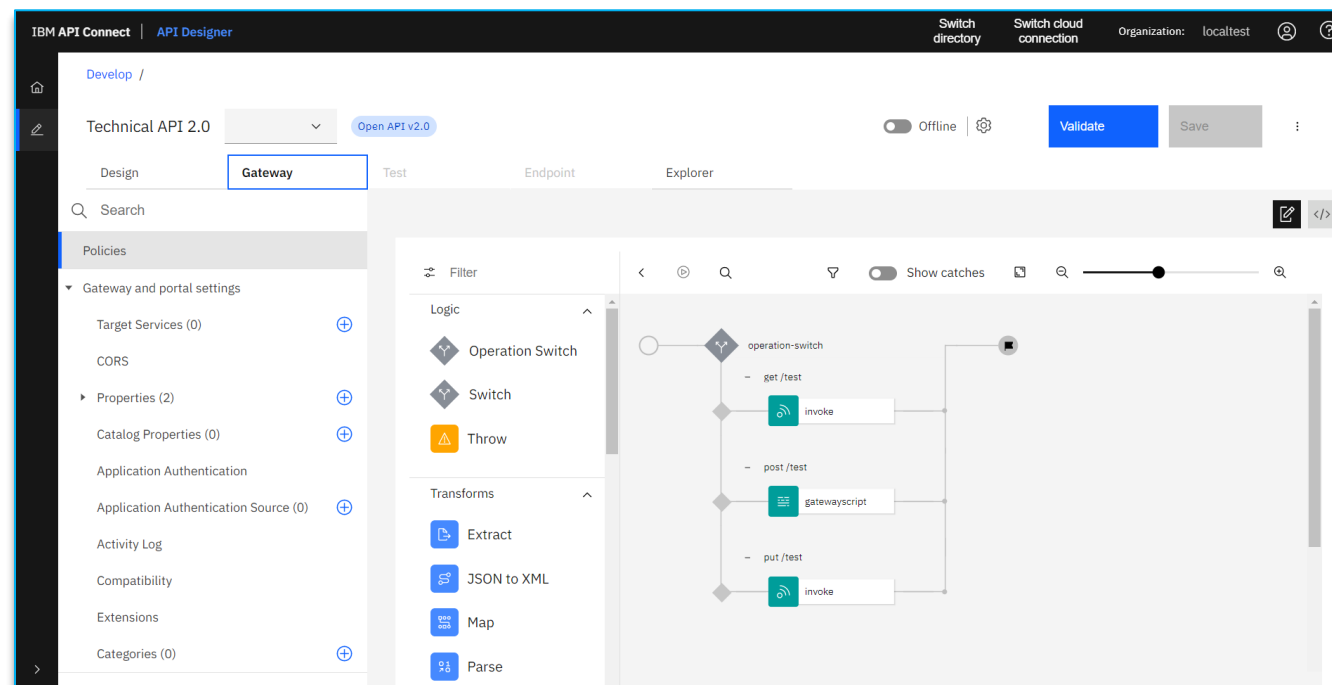
Per a consultar les informacions sobre l'ús i funcionament de les polítiques, revisar la [documentació oficial d'IBM](#).

❖ En aquest exemple, s'ha definit les següents polítiques per a l'acoblament:

- ❖ **Invoke (GET):** Redirigeix a la pàgina especificada en la variable target-url en realitzar una anomenada al API amb l'operació GET.
- ❖ **GatewayScript (POST):** S'executa un script que genera com a resposta el missatge de 'ok' en realitzar una anomenada al API amb l'operació POST. El seu contingut és el següent:

```
1 var response = {};  
2 response.prueba = 'ok';  
3 session.output.write(response);|
```

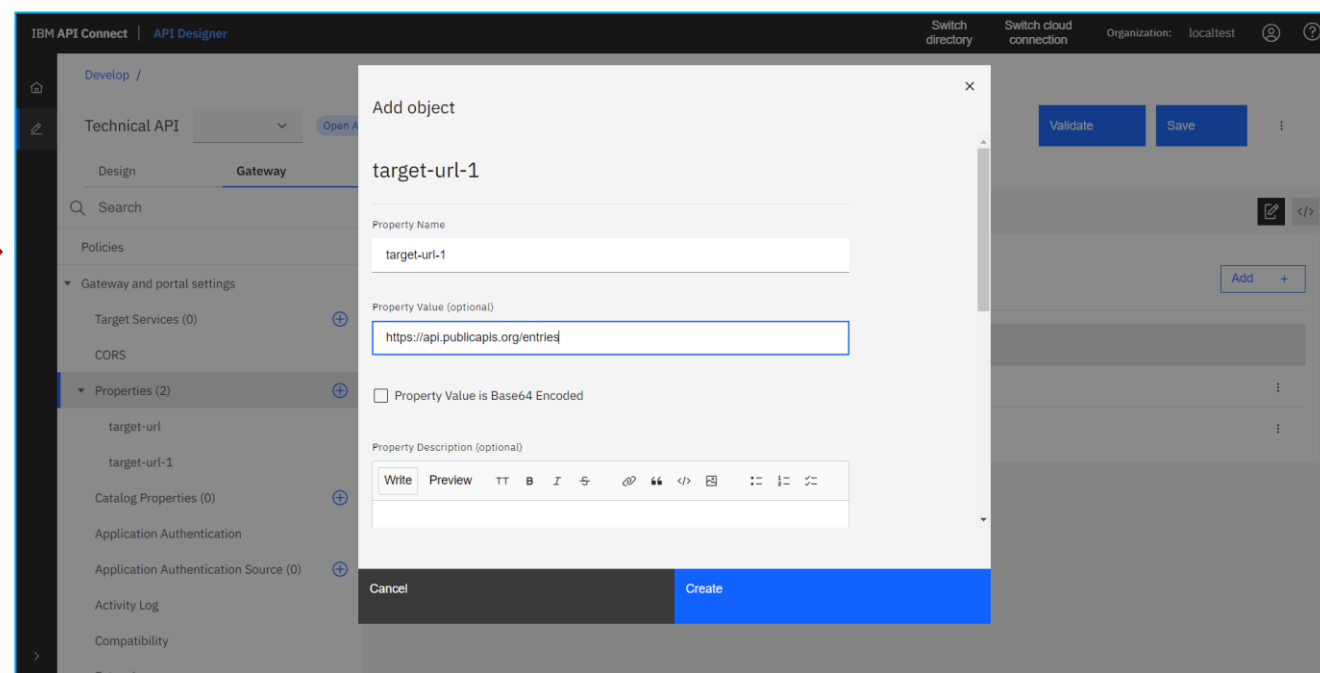
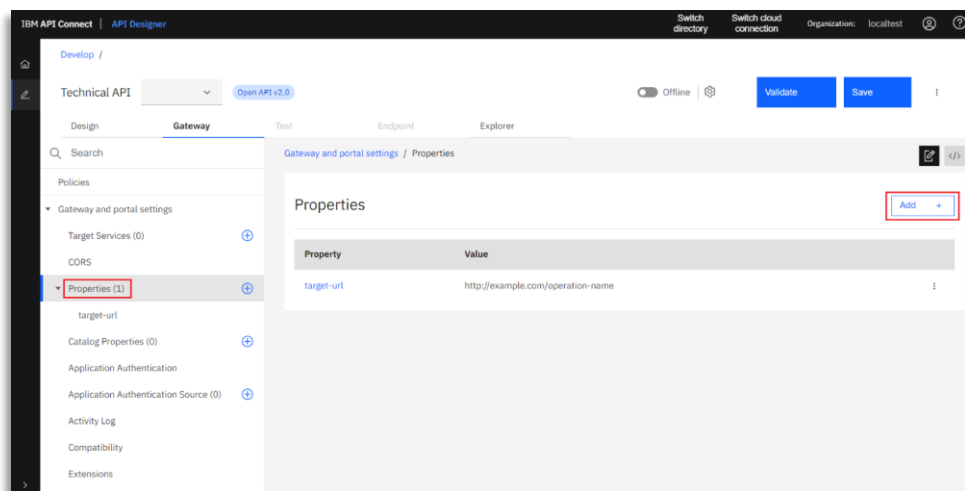
- ❖ **Invoke (PUT):** Redirigeix a la pàgina especificada en la variable target-url-1 en realitzar una anomenada al API amb l'operació PUT.



## 7. Guia d'ús

# Passos

- ❖ Perquè els invokes de l'acoblament anterior puguin funcionar correctament, definim el valor de les variables **target-url** i **target-url-1**. Per a això, ens dirigim a **Properties** i li donem al botó **Add**



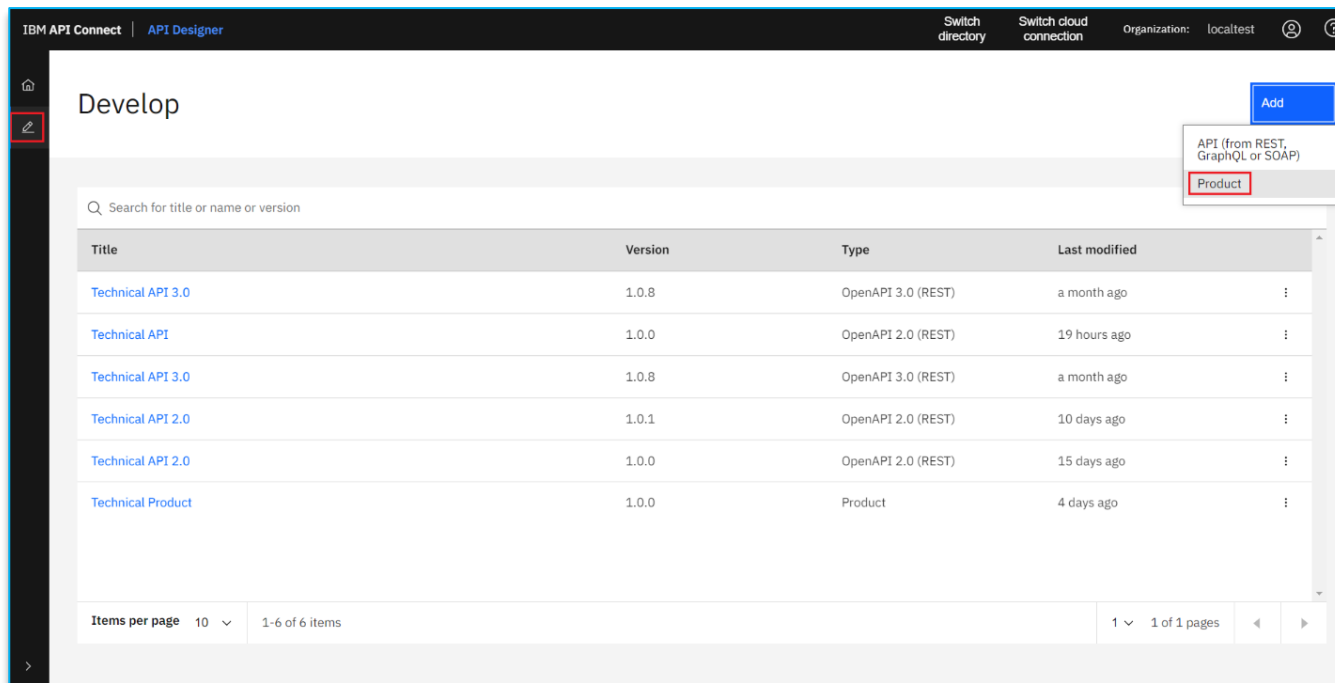
- ❖ Creem la variable **target-url-1** i introduïm la url al qual volem redirigir el API com a valor de la variable (Property Value). En aquest cas, es defineixen els següents valors a les variables

- ❖ **target-url-1**: Emplenem una url vàlida. Exemple: <https://www.google.es>
- ❖ **token-url**: buit (s'assignarà el valor configurat en Catalog Properties)
- ❖ **authorization-url**: buit (s'assignarà el valor configurat en Catalog Properties)

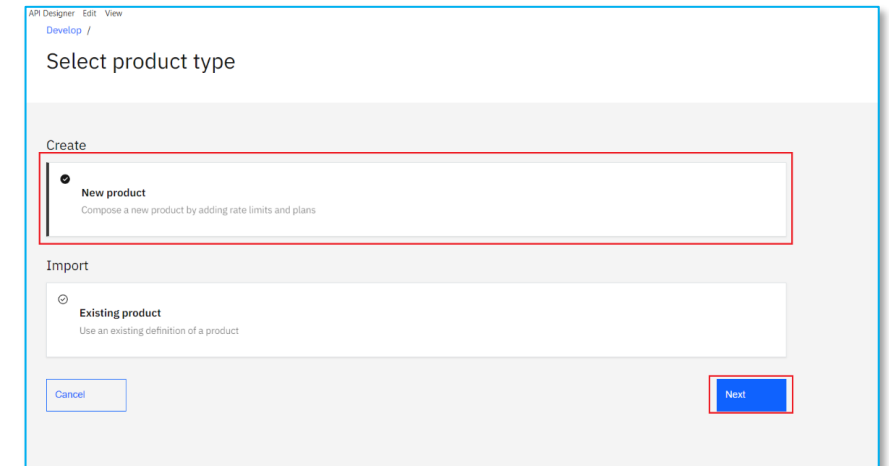
## 7. Guia d'ús

# Passos

- ❖ Després de finalitzar el disseny del API, procedim amb la **creació del producte**. Per a això, tornem a la secció principal prement sobre al botó  i posteriorment li donem als botons **Add – Product**



Title	Version	Type	Last modified
Technical API 3.0	1.0.8	OpenAPI 3.0 (REST)	a month ago
Technical API	1.0.0	OpenAPI 2.0 (REST)	19 hours ago
Technical API 3.0	1.0.8	OpenAPI 3.0 (REST)	a month ago
Technical API 2.0	1.0.1	OpenAPI 2.0 (REST)	10 days ago
Technical API 2.0	1.0.0	OpenAPI 2.0 (REST)	15 days ago
Technical Product	1.0.0	Product	4 days ago



API Designer Edit View  
Develop /

### Select product type

Create

**New product**  
Compose a new product by adding rate limits and plans

Import

**Existing product**  
Use an existing definition of a product

Cancel Next

- ❖ Seleccionem **New product** i li donem a continuar



## 7. Guia d'ús

# Passos

❖ Introduïm el títol del producte i li donem a **Next**

API Designer Edit View  
Develop / Select product type /

### Create new product

Info  
Enter details of the product

Title  
Product

Name  
product

Version  
1.0.0

Summary (optional)

Cancel Next

Create a new product by adding APIs and plans.  
Rate limits are only applied to enforced APIs.  
[Learn more](#)



API Designer Edit View  
Develop / Select product type /

### Create new product

APIs  
Select APIs to add to this product

<input type="checkbox"/>	Title	Version	Type	Enforced
<input type="checkbox"/>	Technical API 3.0	1.0.8	OpenAPI 3.0 (REST)	Enforced
<input checked="" type="checkbox"/>	Technical API	1.0.0	OpenAPI 2.0 (REST)	Enforced
<input type="checkbox"/>	Technical API 3.0	1.0.8	OpenAPI 3.0 (REST)	Enforced
<input type="checkbox"/>	Technical API 2.0	1.0.1	OpenAPI 2.0 (REST)	Enforced
<input type="checkbox"/>	Technical API 2.0	1.0.0	OpenAPI 2.0 (REST)	Enforced

Items per page 10 1-5 of 5 items 1 1 of 1 pages

Cancel Back Next

Create a new product by adding APIs and plans.  
Rate limits are only applied to enforced APIs.  
[Learn more](#)

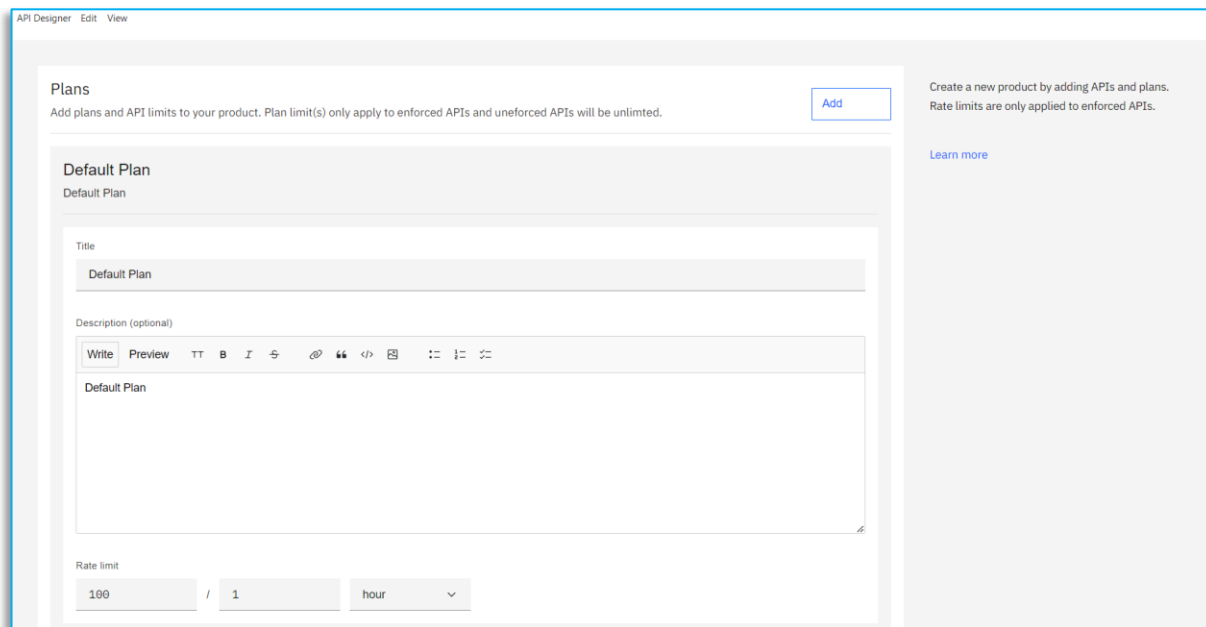
❖ Triem els APIs que es vagin a associar a aquest producte i li donem **Next**. En aquest cas, triem a “Technical API”

## 7. Guia d'ús

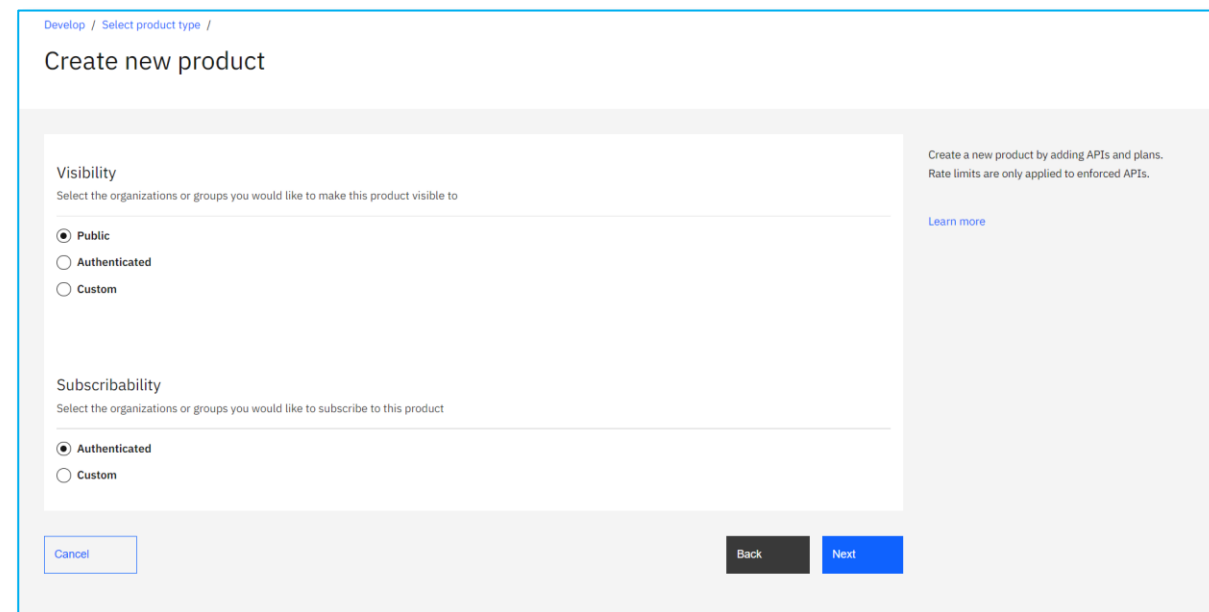
# Passos

❖ A continuació, es defineixen els plans del producte, juntament amb els límits de **Rate** i **Burst**. Un exemple del pla podria ser el següent:

**Title:** Default Plan **Rate Limit:** 100 anomenades/hora **Burst Limit:** 10 anomenades/minut



The screenshot shows the 'Plans' configuration interface in API Designer. It includes a title field set to 'Default Plan', a description field with a rich text editor, and a rate limit configuration set to '100' requests per '1' hour. A sidebar on the right provides instructions on creating a new product by adding APIs and plans, with a 'Learn more' link.



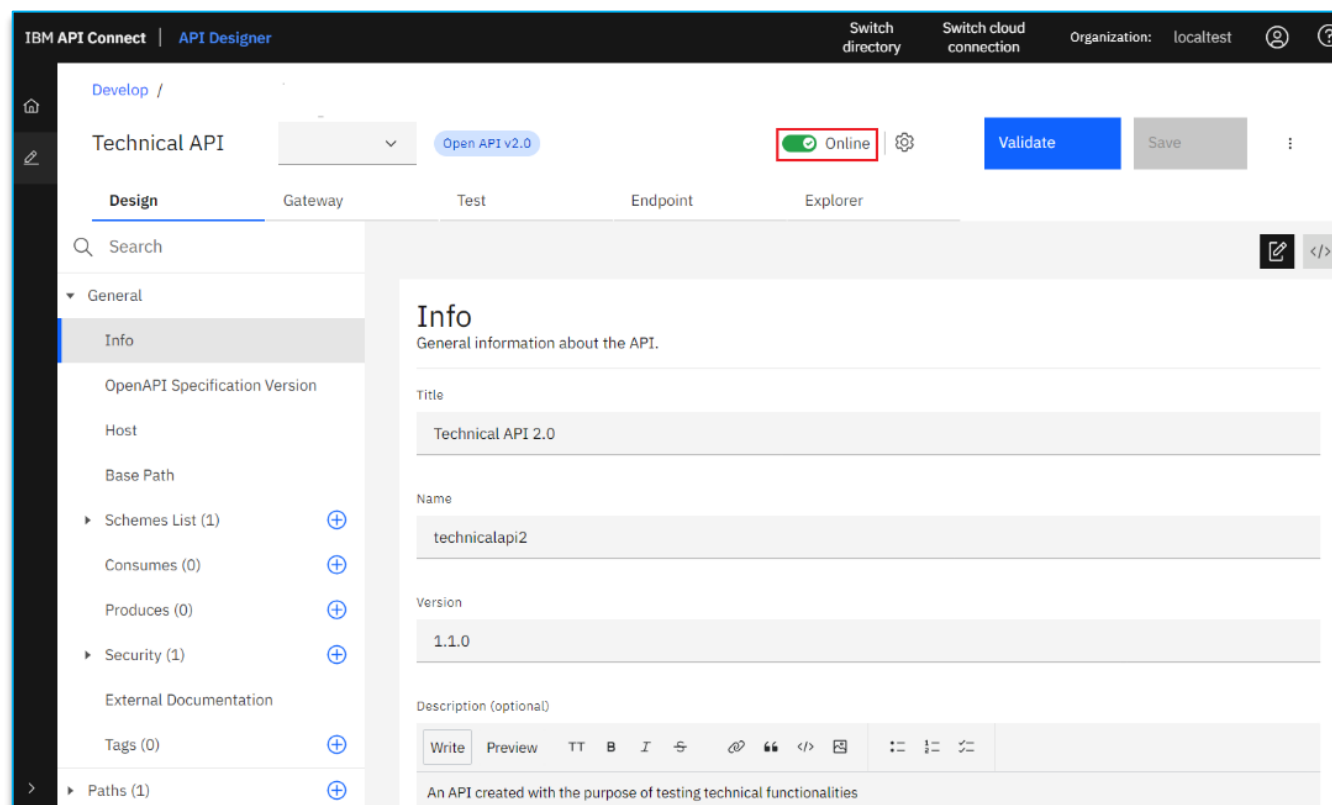
The screenshot shows the 'Create new product' screen. It features two sections: 'Visibility' with radio buttons for 'Public' (selected), 'Authenticated', and 'Custom'; and 'Subscribability' with radio buttons for 'Authenticated' (selected) and 'Custom'. Navigation buttons 'Cancel', 'Back', and 'Next' are at the bottom.

❖ Triem la **visibilitat** del producte i el seu **Subscribability** per a procedir. Continuem a través del botó **Next**, i en la finestra **Summary** següent, podem repassar els passos que hem realitzat i només hauríem de prémer el botó **Done**

## 7. Guia d'ús

# Passos

❖ Finalment, **activem nostra API per a procedir a realitzar les proves en l'entorn local**. Per a això, accedim a nostra API i li llisquem el **botó Offline a Online**



❖ Amb això el API, ja estaria llest per a procedir amb les proves en l'entorn local. Per a això, es poden usar eines de testing com [Postman](#).



**Gràcies !**