Eventhub

Plataforma Transversal Kafka

Welcome Pack

Maig 2022

Generalitat de Catalunya
Centre de Telecomunicacions
i Tecnologies de la Informació

Índex

Introducció

El món es troba cada vegada més i més connectat, el que implica que els estils arquitectònics de les aplicacions van evolucionant per poder donar-hi una resposta adient. Les necessitats dels sistemes d'informació demanen cada cop més escalabilitat, temps de resposta baixos, estabilitat i fiabilitat. Les arquitectures basades en esdeveniments faciliten aquestes característiques i potencien la compartició d'informació en base a patrons simples com la publicació/subscripció d'esdeveniments o les cues de missatges.

Per a donar resposta a aquestes formes de comunicació entre serveis i sistemes, CTTI ha posat a disposició de tots els departaments de la Generalitat de Catalunya d'una plataforma transversal del gestor de missatgeria Kafka, promoguda inicialment pel Departament de Salut i l'Agència Tributària de Catalunya, basada en la plataforma Confluent. És un sistema crític, suportat pel fabricant, altament resilient, amb una oficina tècnica que governa la plataforma, la manté al dia i ajuda als consumidors de la mateixa a treure'n el màxim profit.

Què és i què es pot fer?

Kafka és una plataforma distribuïda de esdeveniments en *streaming* capaç de processar milions d'esdeveniments per hora. Originalment pensada per ser una cua de missatges, ha anat evolucionant fins a convertir-se en una plataforma de transmissió de alt rendiment.

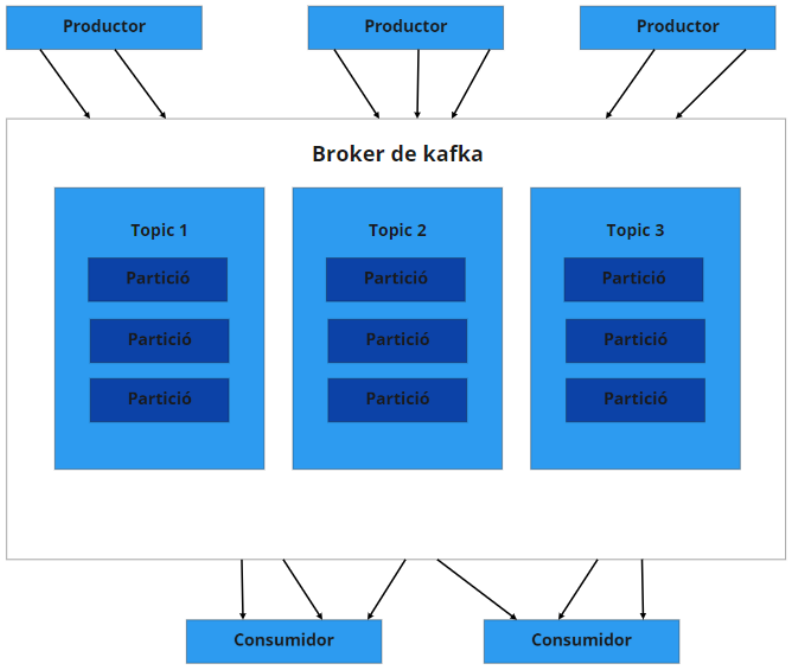
En Kafka, els missatges s'emmagatzemen en forma de *log*, a on s'enregistren amb un *timestamp* associat per tal de ser processats posteriorment amb el mateix ordre amb el que van a ser inserits.

Claus de l'arquitectura de Kafka

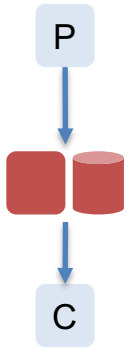
Els missatges (creats pels productors) es rebran via els punts d'entrada anomenats *brokers*.

Les dades s'emmagatzemen en *topics.* Aquests es divideixen en *particions* distribuïdes per la plataforma.

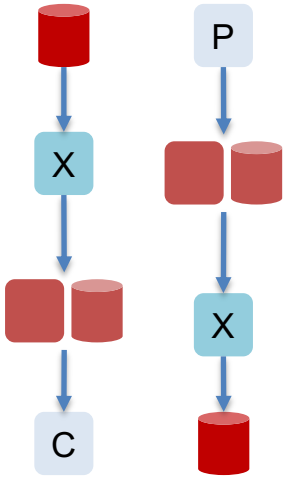
Els missatges són processats pels *consumidors subscrits* als *topics*.



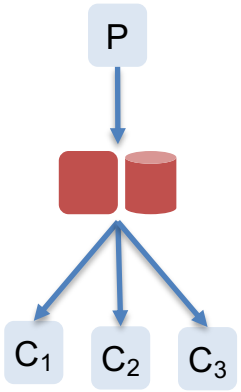
Què és i què es pot fer?



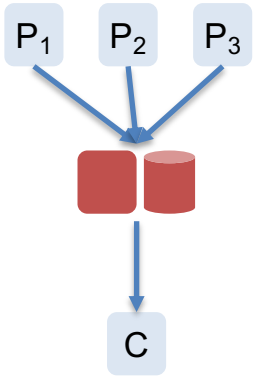
Comunicació entre un productor i un consumidor. El consumidor pot gestionar l'esdeveniment en "temps real" (stream) o en batch.
Exemple: esdeveniment de petició de proves diagnòstiques és consumit per programació de visites



Integració de dades: importació/exportació, stream/sink, online/batch mitjançant connectors 'X'.
Exemple: Captura d'esdeveniments IOT i emmagatzematge a un DataLake, bolcat d'una DB a un DWH (ETL).



Comunicació entre un productor i molts consumidors.
Exemple: esdeveniment de prescripció de medicament és consumit per infermeria, farmàcia i historial del pacient



Comunicació entre multiples productors i un o molts consumidors.
Exemple: Captura dels resultats de diversos laboratoris en un únic repositori de variable clíniques

Què és i què es pot fer?

En quins casos es pot emprar Kafka

- **Publicar i subscriure's** a un flux de dades. Ideal per a aplicacions que necessiten publicar i subscriure's a múltiples fluxos de dades i que, a més a més, sigui ràpid en el seu processament, escalable, tolerant a fallades i confiable.

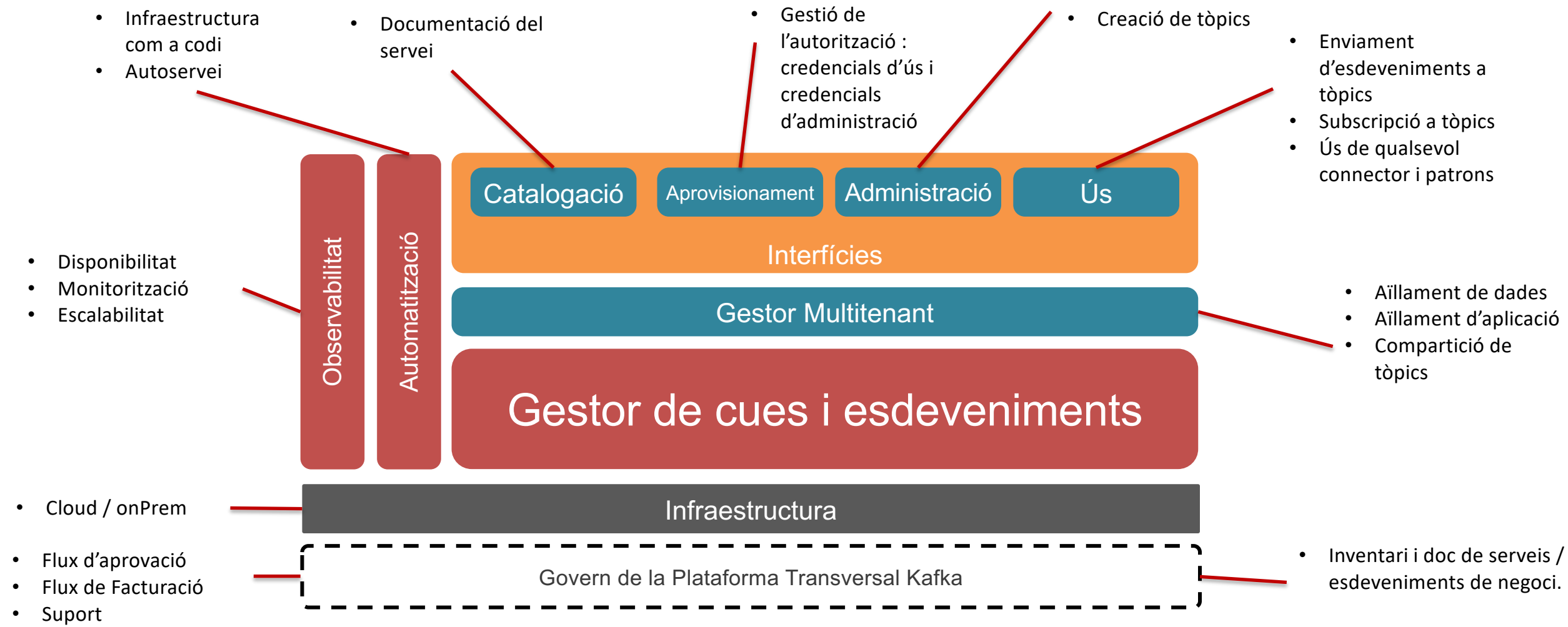
- **Capturar canvis en orígens de dades** i executar accions sobre altres repositoris o sistemes d'informació

- **Emmagatzemar dades**. Kafka permet emmagatzemar-hi dades, tantes com siguin necessàries. Les dades es poden mantenir, per exemple, per ser emprades en casos d'auditoria, per analitzar el que va passar en un cert moment en el passat.

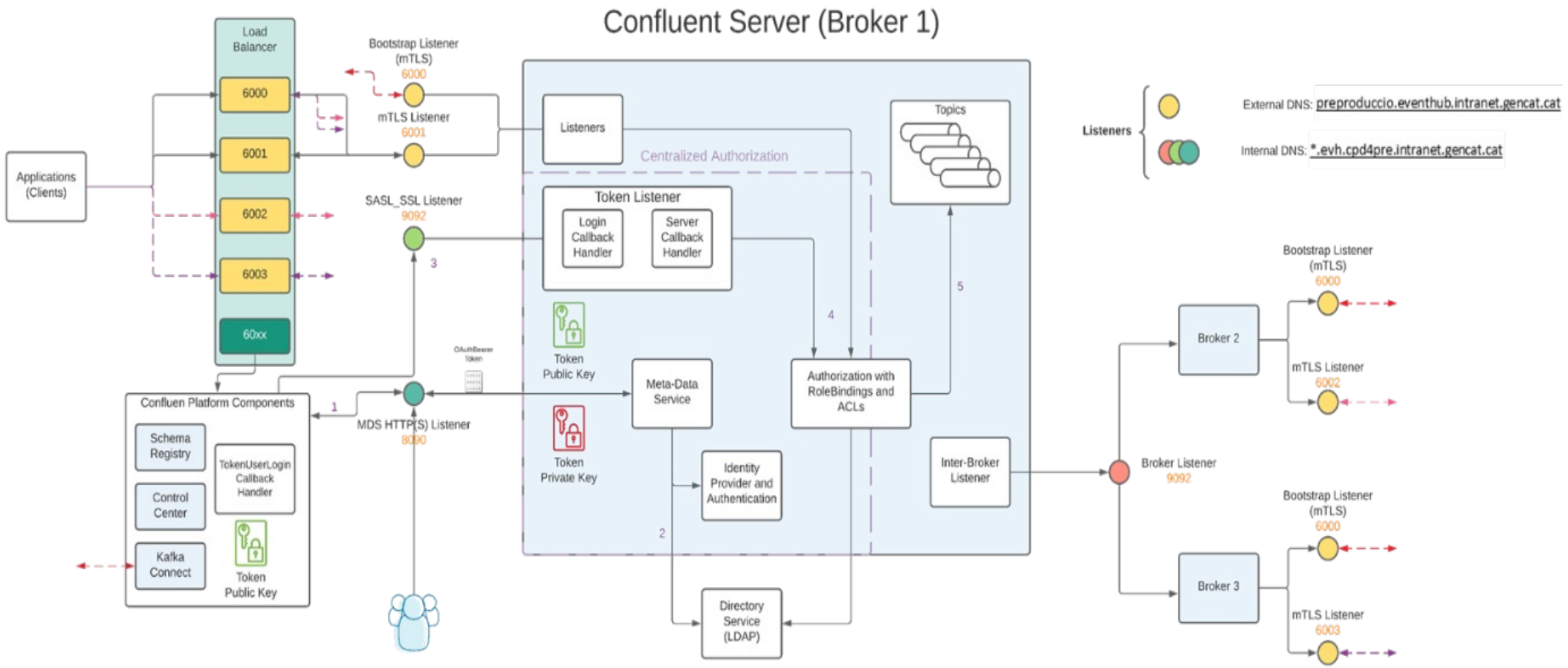
- **Processament de flux de dades**. L'API Streams de Kafka permet processar els missatges "al vol", permet fer agrupacions de dades, tractar finestres de temps, executar *joins* amb altres fonts de dades, enriquir d'informació els missatges, etc.

Casos d'us:

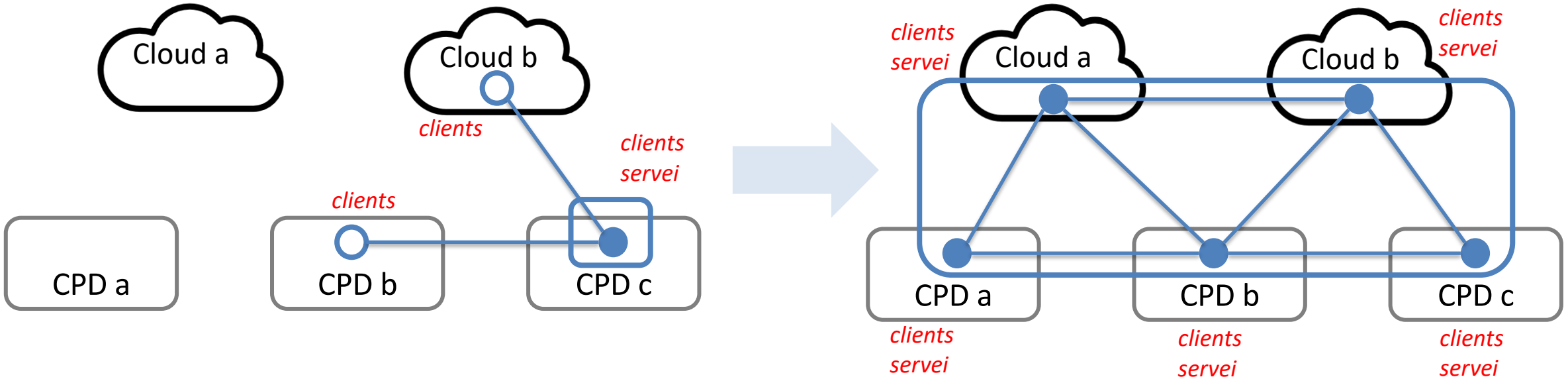
Arquitectura Eventhub



Arquitectura Eventhub



Arquitectura Eventhub



Implantació inicial: 1 CPD donant servei a tots els clients

Estat final: n CPD/cloud donant servei a tots els clients, gestionats coordinadament amb una consola única

Model de Seguretat

Com implementem la seguretat

- Els clients (productors i consumidors) i serveis del sistema s'autenticaran mitjançant certificat software, signat per l'autoritat pública de certificació Sectigo, amb el mètode mTLS d'autenticació (garanteix que les parts de cadascun dels extrems d'una connexió de xarxa són els que diuen ser, verificant que ambdues tenen la clau privada correcta. La informació continguda en els seus respectius certificats TLS/SSL proporciona una verificació addicional). La signatura del certificat es demanarà a l'Agència de Ciberseguretat (AC), prèvia creació de la clau privada i el certificat CSR corresponents.

- L'Oficina Tècnica proporcionarà un *script* de creació de la clau privada i CSR per facilitar aquesta tasca als clients. La clau privada s'ha d'emmagatzemar protegida i el CSR s'enviarà a l'AC, que el signarà i retornarà al client el certificat final (clau pública) signat amb Sectigo.

- Els administradors accediran al sistema i el Control Center de Confluent amb usuari/password.

- Els usuaris de consulta accediran al Control Center amb usuari/password.

- Els drets d'accés a cada recurs s'establiran segons les decisions de la persona responsable del mateix.

- Els drets d'accés de cada usuari es limitaran segons els següents principis: mínim privilegi, necessitat de conèixer i capacitat d'autoritzar.

- Els usuaris que vulguin treballar amb la plataforma han de sol·licitar els permisos adients segons les seves necessitats. Aquests permisos es demanaran a l'Oficina Tècnica, que podrà acceptar o rebutjar la petició en base als criteris anteriors.

Multitenancy i entorns

Com implementem el multitenancy

A la plataforma Eventhub implementem el multitenancy i aïllament de recursos a partir de quotes.

El clúster Kafka té la capacitat d'aplicar quotes a les sol·licituds per controlar els recursos del broker utilitzats pels clients. Els brokers de Kafka poden aplicar dos tipus de quotes de clients per a cada grup de clients que comparteix una quota:

- Les quotes d'amplada de banda de xarxa defineixen els llindars de velocitat de bytes.
- Les quotes de velocitat de sol·licitud defineixen els llindars d'utilització de la CPU com a percentatge dels fils d'E/S i de xarxa.

Amb la implementació de quotes evitarem:

- La monopolització dels recursos de la plataforma per part d'una aplicació
- La saturació de la xarxa
- Denegació del servei per altres clients

Entorns

Posem a disposició de les aplicacions 3 entorns de treball: INT, PRE i PRO (INT és un entorn opcional)

Avantatges

¿Quines avantatges te adherir-se a la plataforma transversal de Kafka?

- **Estalvi**. Al ser una plataforma compartida, el cost d'utilització es redueix considerablement. Per al repartiment del cost d'ús de la plataforma es tenen en compte diferents factors, com el tràfic de dades, l'emmagatzematge utilitzat, la quantitat de missatges dipositats, etc.

- **Temps de posada en producció.** El temps de posada en producció es redueix dràsticament, ja que no s'ha de fer cap aprovisionament d'infraestructura, desplegament del producte ni tot el que comporta una plataforma nova.

- **Robustesa.** La plataforma és altament disponible, tolerant a fallades i redundant.

- **Servei monitoritzat 24/7.** La plataforma està declarada com un sistema crític i per tant monitoritzada tot el dia tots els dies pel Centre del Control del CTTI.

- **Suport.** Equip de suport especialitzat en la tecnologia per ajudar-vos des de la definició de l'arquitectura, millors pràctiques de definició de *topics*, integració amb la plataforma, resolució de incidències i posada en producció. Compta amb suport de fabricant, Confluent, amb temps de resposta inferior a 1h per a incidents de severitat crítica en producció.

Oficina tècnica Eventhub

L'oficina tècnica Eventhub es va crear amb la finalitat de donar el suport necessari als departaments que es volen adherir a la seva plataforma.

L'oficina tècnica està pensada per ajudar en tot el procés d'integració, des de l'*onboarding* de la aplicació a integrar-se amb Kafka fins el desplegament en els diferents entorns de la plataforma (INT, PRE i PRO).

L'oficina tècnica s'encarrega de:

- Administrar la plataforma Confluent Kafka.
- Observabilitat de la plataforma.
- Afegir components d'arquitectura si calgués.
- Gestió de les peticions de manteniment dels esquemes (Schema Registry)
- Afegir nous plugins a Kafka Connect (mysql, oracle, sap, etc).
- Configurar connectors de Kafka Connect tant per *source* com per *sink*.
- Gestionar els usuaris d'aplicació i les seves autoritzacions.
- Ajudar a definir i configurar els *topics* necessaris per a la vostra aplicació.
- *Fine tuning* de *topics* i particions.
- Resolució de dubtes amb un equip d'experts en la tecnologia.
- Repositori de coneixement i experiències d'altres departaments.

Oficina tècnica Eventhub

L'oficina tècnica s'encarrega de (continuació):

- Generació d'informes detallats de consum dels *topics*.
- Suport a proves de rendiment.
- Donar suport a les aplicacions usuàries de la plataforma.
- Subscripció Gold amb Confluent, podem obrir tiquets de suport al fabricant
- Consultoria del fabricant en funció del cas d'ús. En cas que sigui necessari podem gestionar sessions de treball amb els consultors de Confluent.
- Donar accés per obrir tiquets a Confluent directament.

Serveis que ofereix l'oficina tècnica

Serveis actius a la plataforma i com demanar-los

Kafka Brokers, Schema Registry i Kafka Connect

- Onboarding per conèixer les seves necessitats, entendre el cas d'ús i tenir una visió de totes les peces. Ens podeu contactar a eventhub.ctti@gencat.cat
- Passes a seguir per integrar-se a la plataforma Eventhub
  - Obrir regles de firewall fins els següents endpoints:
    - integracio.eventhub.intranet.gencat.cat (10.53.141.134) ports: 9093
    - preproduccio.eventhub.intranet.gencat.cat (10.53.194.11) port: 6000, 6001, 6002, 6003
    - eventhub.intranet.gencat.cat (10.52.194.10) port: 6000, 6001, 6002, 6003
  - Demanar usuari a partir del codi de diàleg i nom d'aplicació.
  - Demanar certificats seguint el protocol en l'Annex I
  - Demanar els *topics* omplint el formulari en l'Annex II
- Aprovisionar, *topics* (veure l'Annex II)
- Aprovisionar *schemas* (veure l'Annex III)
- Ajudar en la definició dels *topics* (nombre de particions, rèpliques, etc). En cas de dubtes ens podeu obrir un tiquet i podem fer reunions de treball.

Serveis que ofereix l'oficina tècnica

- En cas necessari, demanar la configuració de Kafka Connect per fer transferències de registres entre bases de dades o sistemes d'informació
- Seguiment de les *Best practices* de l'arquitectura
  - Per la integració d'aplicacions (consumir / produir)
  - Ús de les llibreries i dependències per la integració
  - Knowledge base de Confluent
  - Assessorament per la implementació de microserveis
- Comptem amb l'experiència d'altres equips ja integrats a la plataforma

Temps de resposta de l'oficina tècnica

Nota: temps estimats tenint en compte que es disposen de tots els components i llicències requerits disponibles per l'oficina.
Afegir un component nou es tracta com a projecte i surt d'aquest nivell d'objectius

Tarifari (En definició)

Es proposa un model de tarifació per l'ús de la plataforma, el qual es calcularà a mes vençut per les següents mètriques d'utilització.

2022:

- Hi haurà una quota fixa de XX€ anuals per client (client és àmbit)

2023

- Hi haurà una quota fixa de XX€ anuals per client (client és àmbit)
- Mètriques per consum a estudiar durant el 2022:
  - Es facturarà per tràfic de GB, tant en producció de tòpics com en el seu consum, a raó d'x€/GB. Tràfic total durant el mes.
  - Es facturarà per mitjana d'ocupació de dades, a raó de x€/GB. Ocupació durant el mes
  - El cost global de la plataforma es repercutirà en funció de l'ús. Per tant a mesura que s'incorporin més àmbits el cost unitari anirà minvant.

Exemples d'integració

L'Àrea Tècnica compta amb un espai propi dins del portal d'arquitectura del CTTI (en construcció) a on es publica informació amb exemples d'integració, millors pràctiques i novetats en general de la plataforma.

La pàgina web es la següent:

https://canigo.ctti.gencat.cat/eventhub/

Més exemples es poden trobar als següents enllaços de Confluent:

- https://kafka-tutorials.confluent.io/creating-first-apache-kafka-producer-application/kafka.html
- https://kafka-tutorials.confluent.io/creating-first-apache-kafka-consumer-application/kafka.html

Glossari

- **Missatge**. Conjunt de dades. Per a Kafka un missatge no és més que una cadena de *bytes*.
- **Producer.** És una aplicació que envia missatges. Aquests missatges no s'envien directament al destinatari, sinó que s'envien als *topics* publicats al Kafka Server.
- **Consumer.** L'aplicació que llegeix els missatges dels *topics* publicats al Kafka Server. El consumer ha de tenir els permisos adequats per poder-los llegir, els missatges.
- **Kafka Broker.** És l'intermediari que fa possible l'intercanvi de missatges entre els Producers i Consumers.
- **Kafka *Topic***. Categoria en la que els missatges s'emmagatzemen, organitzen i publiquen.
- **Kafka *Partitions*.** Un *topic* pot estar dividit en tantes particions como siguin necessàries, ja que Kafka és un sistema distribuït, les particions s'emmagatzemen en els diferents servidors del clúster. Correspondria al nombre de consumidors en paral·lel que vols gestionar.
- **Offsets.** És una seqüencia d'identificadors que s'assignen als missatges en el moment de la seva arribada al sistema. Aquests identificadors són inamovibles i immutables durant tot el seu cicle de vida.
- **Kafka Consumer Group.** Un grup de consumidors que comparteix la carrega de treball. Els missatges, per ser processats, són consumits pels diferents membres del grup, cadascun associat a una *partició* del *topic*.

Annex I – Demanar nou client del sistema

Tiquet petició nou client Kafka
Quan un nou client vol integrar-se amb la plataforma Eventhub, el primer que ha de fer és realitzar una petició via tiquet aportant la següent informació:

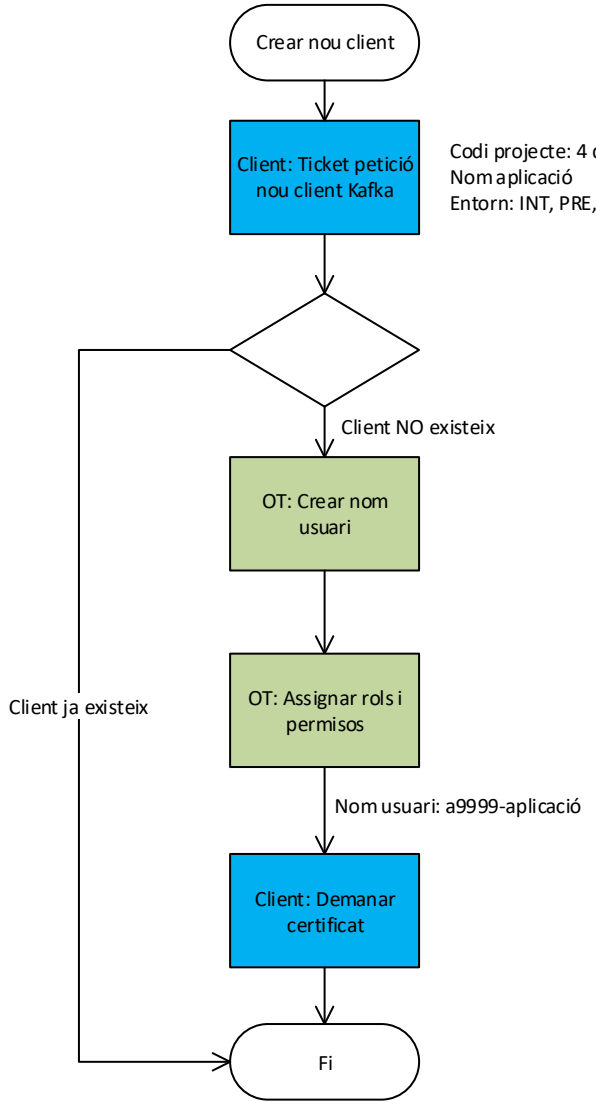
- Codi del projecte de 4 dígits.
- Nom de l'aplicació
- Entorn pel qual es vol: INT, PRE, PRO.

Tasques a fer:

Crear nom usuari
L'oficina tècnica crearà el nom de l'usuari segons les dades informades en el tiquet.

Assignar rols i permisos
L'oficina tècnica s'encarregarà de l'assignació dels permisos corresponents.

Demanar certificat
L'Oficina Tècnica proporcionarà un script de creació de la clau privada i CSR per facilitar aquesta tasca als clients. La clau privada s'ha d'emmagatzemar protegida i el CSR s'enviarà a l'AC, que el signarà i retornarà al client el certificat final (clau pública) signat amb Sectigo.



Annex I – Demanar nou client del sistema

Pla de capacitat
Un client que vulgui integrar-se a la plataforma Eventhub, haurà, en la mesura que sigui possible, presentar un pla de capacitat indicant una estimació de l'ús que farà de la plataforma.

Aquest pla haurà de tenir en compte la informació següent, per cadascun dels tòpics sol·licitats:

- Estimació de missatges produïts/període de temps. Ex.: 100 msg/s.
- Estimació de missatges consumits/període de temps. Ex.: 100 msg/s.
- Estimació de mida dels missatges. Ex.: 10 KiB.
- Estimació d'ús de disc. Ex.: 10 GiB.

En posteriors sol·licituds de tòpics, cal presentar l'estimació per a aquests nous tòpics.

Annex II – Gestionar *topics*

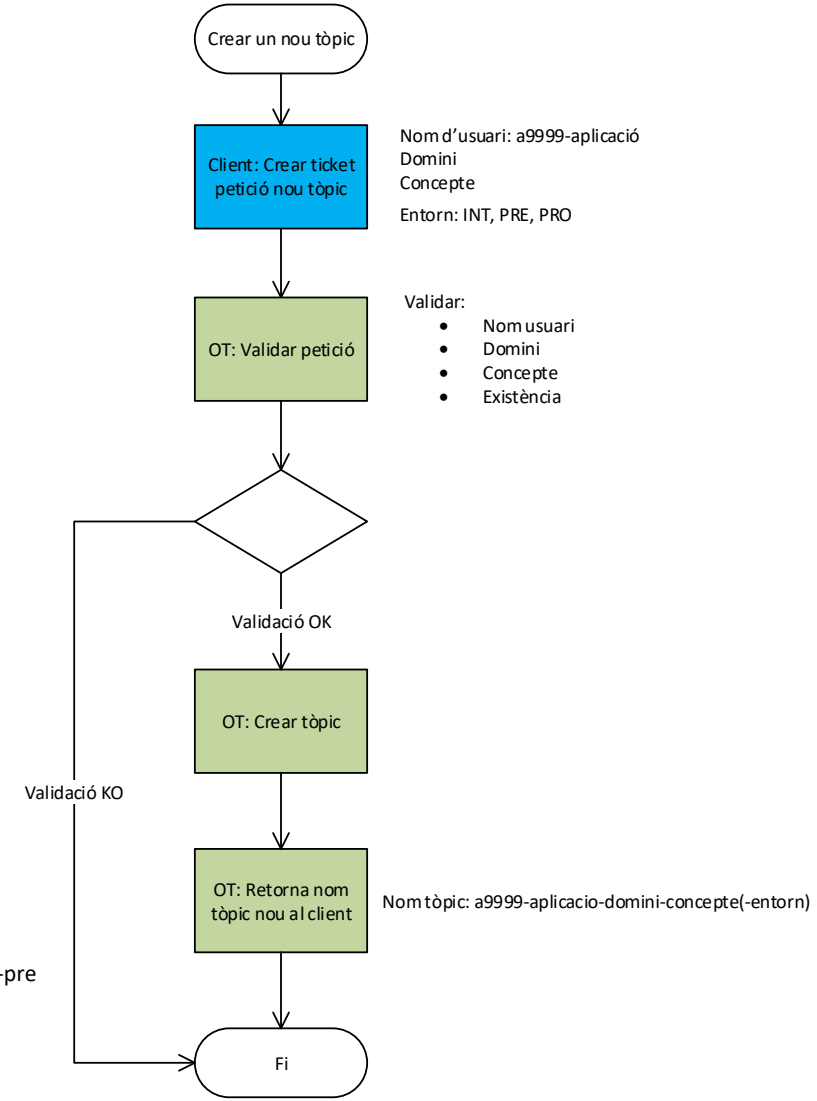
Tiquet de petició de gestió de *topics* Kafka

- El client haurà de sol·licitar via tiquet l'alta, esborrat o modificació del *topic*, omplint el formulari descrit a sota.
- L'oficina tècnica validarà la petició i farà les accions oportunes.

Formulari de gestió de topics:

Acció	Alta / Esborrar / Modficació
Codi de aplicació	Codi de l'aplicació propietària del topic. Serà un numèric de 4 dígits, que compleix amb l'expressió regular [0-9]{4}.
Nom aplicació	Nom de l'aplicació propietària del topic, que ha de complir amb l'expressió regular [a-z0-9\.]{1,20}. No pot contenir majúscules ni espais.
Domini	Domini de la missatgeria del topic. Ha de complir amb l'expressió regular [a-z0-9\.]{1,15}. No pot contenir majúscules ni espais.
Concepte	Descripció que permeti definir millor el contingut o propòsit del topic. Ha de complir amb l'expressió regular [a-z0-9\.]{1,30}. No pot contenir majúscules ni espais.
Entorn	int / pre / pro
Permisos	Lectura / Escriptura / LecturaEscriptura (valor per defecte)

Propiedad	Valor
Nombre de particions	Valor per defecte 3
Nombre de repliques	Valor per defecte 3
Nombre min in sync repliques	
Temps de retenció del missatge	



Exemples:
Topic per a l'aplicació Portal Tributari, amb codi 0205, domini "tributs", propòsit self assessment i entorn de preproducció: a0205-portaltributari-tributs-selfassessment-pre
Topic per a l'aplicació Portal Tributari, amb codi 0205, domini "tributs", propòsit actualitzar estats i entorn de producció: a0205-portaltributari-tributs-updatestate

Annex II – Gestionar *topics*

Aplicacions Kafka Streams

Les aplicacions Kafka Streams poden generar tòpics interns necessaris per al seu funcionament.

Un projecte que tingui intenció de fer ús d'aquesta tecnologia per al desenvolupament d'aplicacions, ho haurà de comunicar a l'Oficina Tècnica per assignar els permisos de RBAC necessaris.

El paràmetre **application.id**, definit per l'aplicació, és utilitzat com a prefix a l'hora de generar el nom dels tòpics interns (*<application.id>-<operatorName>-<suffix>*) i, per tant, serà tingut en compte a l'assignació de permisos de RBAC. El valor d'aquest paràmetre ha de seguir la nomenclatura **<a><codi aplicació>-<nom aplicació>-ks-<domini>** per poder garantir que sigui únic al clúster.

En aplicacions stateful, és molt recomanable el nomenat d'operadors per evitar problemes derivats de canvis de topologia. Veure [1] y [2] per a més informació.

[1] Naming Kafka Streams DSL Topologies
[2] Naming stateful operations in Kafka Streams

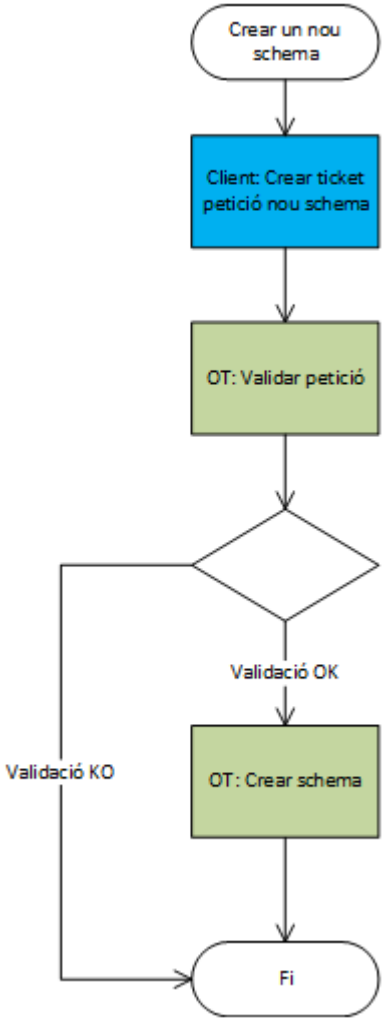
Annex III – Gestionar l'*Schema Registry*

Tiquet de petició de gestió de *l'Schema Registry*

- El client haurà de sol·licitar via tiquet l'alta, esborrat o modificació del *schema*, omplint el formulari descrit a sota.
- L'oficina tècnica validarà la petició i farà les accions oportunes.

Formulari de gestió de Schema Registry:

Acció	Alta / Esborrar / Modficació
Codi de aplicació	Codi de l'aplicació propietària del topic. Serà un numèric de 4 dígits, que compleix amb l'expressió regular [0-9]{4}.
Nom aplicació	Nom de l'aplicació propietària del topic, que ha de complir amb l'expressió regular [a-z0-9\.]{1,20}. No pot contenir majúscules ni espais.
Domini	Domini de la missatgeria del topic. Ha de complir amb l'expressió regular [a-z0-9\.]{1,15}. No pot contenir majúscules ni espais.
Concepte	Descripció que permeti definir millor el contingut o propòsit del topic. Ha de complir amb l'expressió regular [a-z0-9\.]{1,30}. No pot contenir majúscules ni espais.
Topic	Topic al que aplica l'schema
Schema	fitxer json amb l'schema
Entorn	int / pre / pro



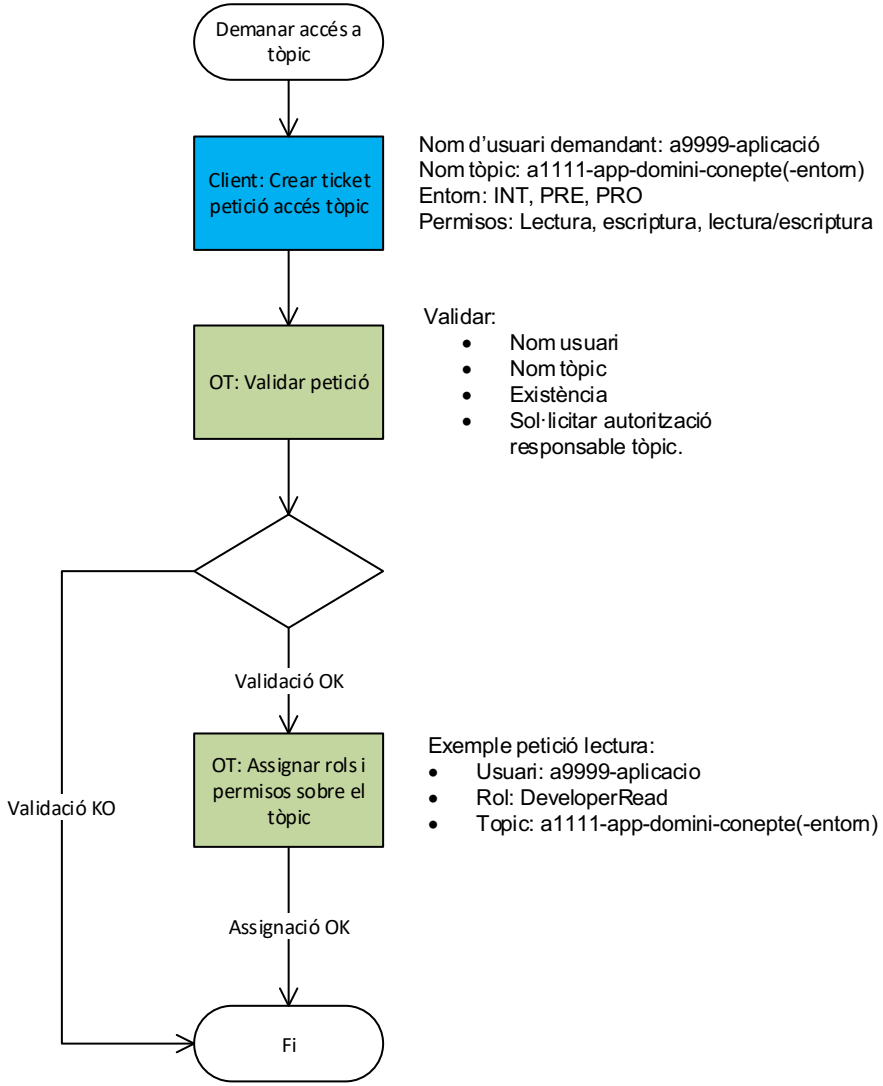
Annex IV – Demanar accés a un *topic*

Tiquet de petició d'accés a un *topic* Kafka

- El client haurà de sol·licitar per tiquet l'accés als *topics*, emplenant el formulari de sol·licitud i comptant amb l'autorització corresponent per part del gestor/PO del sistema.
- L'oficina tècnica validarà la petició i gestionarà l'assignació de permisos per l'usuari.
- L'oficina tècnica informarà en el tiquet la finalització de l'operació.

Formulari d'accés a un *tòpic:*

Topic	Tópic al que es vull tenir access
Codi de aplicació	Codi de l'aplicació propietària del topic. Serà un numèric de 4 dígits, que compleix amb l'expressió regular [0-9]{4}.
Nom aplicació	Nom de l'aplicació propietària del topic, que ha de complir amb l'expressió regular [a-z0-9\.]{1,20}. No pot contenir majúscules ni espais.
Entorn	int / pre / pro
Permisos	Lectura (valor per defecte) / Escriptura / LecturaEscriptura



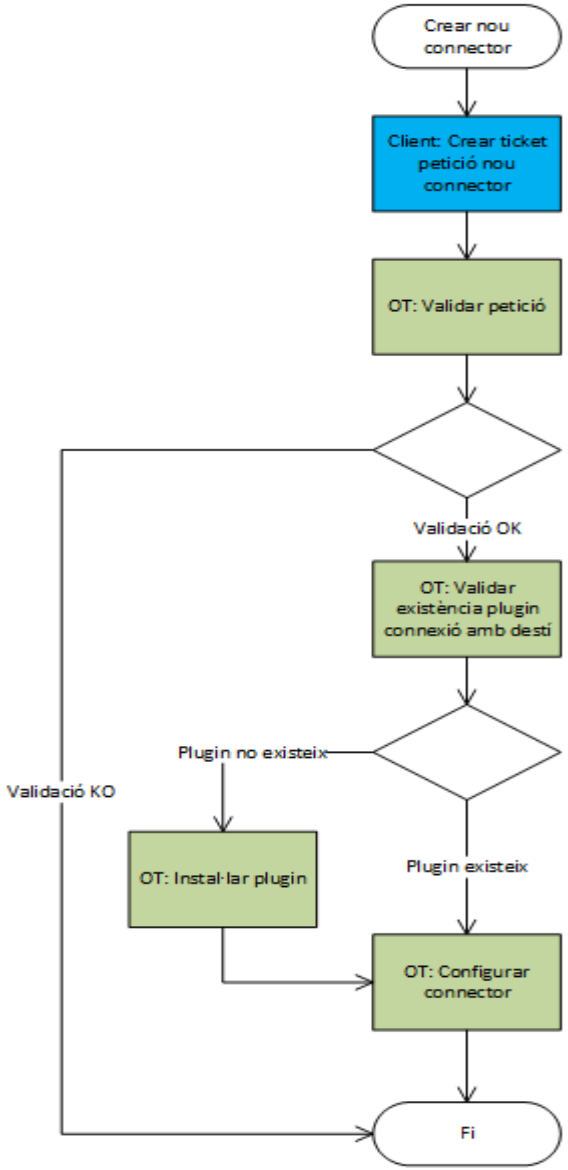
Annex V – Gestionar *connectors*

Tiquet de petició de gestió de *topics* Kafka

- El client haurà de sol·licitar via tiquet l'alta, esborrat o modificació del *connector*, omplint el formulari descrit a sota.
- L'oficina tècnica validarà la petició i farà les accions oportunes.
- En cas que el plugin no estigui disponible, caldrà una instal·lació per manteniment.

Formulari de gestió de connectors:

Tipus de sol·licitud	Creació / Modificació / Esborrat
Nom de aplicació	Nom de l'aplicació propietària del grup de consumidors. [a-z0-9\.]{1,20}
Codi de aplicació	Serà un numèric de 4 dígits, que compleix l'expressió regular [0-9]{4} *
Domini	Heu de complir amb l'expressió regular [a-z0-9\.]{1,15}
Entorn	Int / pre / pro
Sistema origen/destí	MongoDB / MySQL / etc
Tipus de connector	Source / Sink
Key Converter	
Value Converter	
Topic	
Connection URI	
Tipus de credencials	Kerberos / certificado / user-password
Credencials	



Annex VI – Llibreries client

Amb el propòsit d'evitar dependre d'un proveïdor específic, es recomana, sempre que sigui possible, fer servir les llibreries d'Apache un lloc de les de Confluent.

Exemples

Per a kafka-clients utilitzar:

```
<dependency>
      <groupId>org.apache.kafka</groupId>
      <artifactId>kafka-clients</artifactId>
      <version>3.1.1</version>
</dependency>
```

En lloc de:

```
<dependency>
      <groupId>org.apache.kafka</groupId>
      <artifactId>kafka-clients</artifactId>
      <version>7.1.1-ccs</version>
</dependency>
```

Per a kafka-streams utilitzar:

```
<dependency>
      <groupId>org.apache.kafka</groupId>
      <artifactId>kafka-streams</artifactId>
      <version>3.1.1</version>
</dependency>
```

En lloc de:

```
<dependency>
      <groupId>org.apache.kafka</groupId>
      <artifactId>kafka-streams</artifactId>
      <version>7.1.1-ccs</version>
</dependency>
```

Annex VII – Schema Registry, memòria cau local d'esquemes

Atès que actualment només existeix un node de Schema Registry a la plataforma, es recomana la memòria cau d'esquemes als clients.

Per a aplicacions productores/consumidores de Kafka, els serialitzadors/deserialitzadors de Confluent, com per exemple KafkaAvroSerializer, implementen la memòria cau local dels esquemes al costat del client.

Per a aplicacions que necessitin utilitzar directament un client de Schema Registry es recomana que facin ús de CachedSchemaRegistryClient, atès que els aportarà memòria cau local dels esquemes al costat del client.

www.gencat.cat