



Plataforma transversal de dades

Infraestructura i DevOps

Responsable del document: Raúl Chamizo
Gener 2025

Índex

1.	Introducció	3
1.1	Propòsit	3
2.	Context de la plataforma	4
2.1	Xarxes i firewall	4
2.1.1	DNS	6
2.2	Xarxes <i>Serverless</i> de Databricks	7
2.3	<i>Workspaces</i> de Databricks	7
2.4	Aplicacions en contenidors	9
3.	Requeriments de les aplicacions	11
3.1	Requeriments de les aplicacions de Databricks	11
3.2	Requeriments de les aplicacions en contenidors	14

1. Introducció

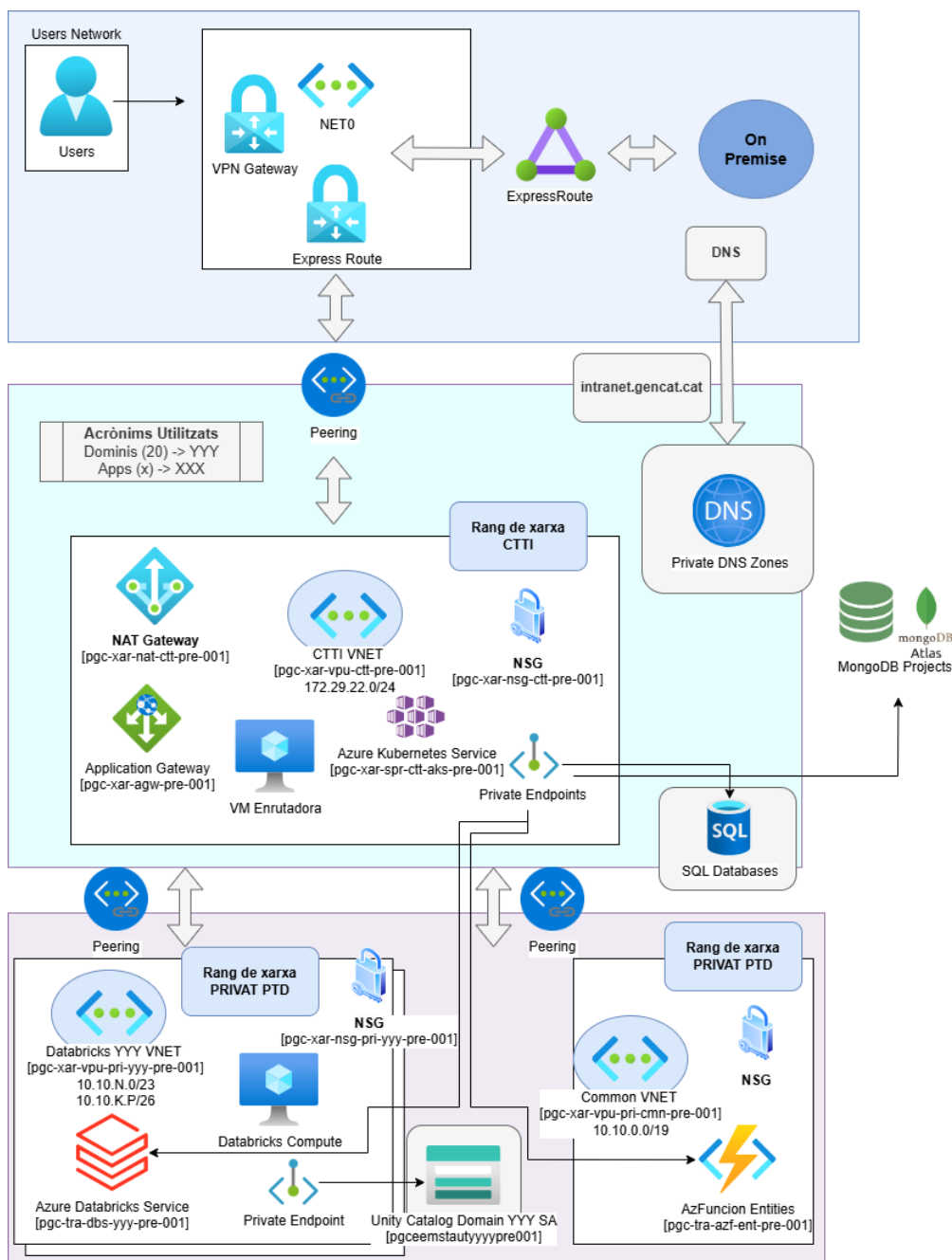
1.1 Propòsit

L'objectiu d'aquest document és proporcionar informació als diferents proveïdors que treballin a la Plataforma Transversal de Dades per a poder integrar els seus productes a la PTD des del punt de vista d'Infraestructura i DevOps.

2. Context de la plataforma

2.1 Xarxes i firewall

El següent diagrama representa de forma esquematitzada la plataforma en l'entorn de preproducció (preproducció i producció són idèntics)



- És important recalcar que la PTD és una arquitectura de xarxa privada, sense exposicions públiques. Des d'Internet no s'arriba a cap element de la PTD, encara que la plataforma sí que es capaç d'accedir a recursos d'Internet a través de IPs fixes i controlades (NAT Gateway). En cas d'accedir a recursos que implementen *firewalls*, aquestes són les IPs a les que s'ha de permetre l'accés:

Entorn	IP de sortida
Preproducció	20.224.22.183
Producció	4.231.8.211

- Del diagrama anterior, es poden distingir tres zones:
 - o La part de dalt, de **color blau més fosc**, representa la xarxa d'Azure NET0, aliena a la PTD, que fa de pont amb la resta d'entorn del CTTI. Els usuaris connectats al diferents perfils VPN de CISCO accediran a la plataforma a través d'aquesta connexió de la NET0. Permet utilitzar des de dins de la nostra xarxa serveis del CTTI com bases de dades Oracle.
 - o La zona central, de **color blau més clar**, mostra una xarxa connectada amb la NET0, per tant, es podrà accedir a qualsevol element amb una IP en aquesta xarxa sempre que les regles de seguretat / Firewall ho permetin. En cas contrari, des d'aquesta xarxa també es podrà contactar amb qualsevol servei dins de la xarxa del CTTI.

Des de l'entorn de la PTD deleguem la gestió del *firewall* cap a altres recursos del CTTI a la NET0 permetent l'accés sortint i entrant a les xarxes en els **rangs 10.0.0.0/8** per als **ports 53,22,80,443**.

No obstant, per accedir a qualsevol recurs des de la PTD cap a l'entorn CTTI s'haurà de sol·licitar l'obertura del *firewall* a GESNUS, ja que la NET0 sí que té un *firewall* implementat. El mateix aplica si des de la VPN no s'accedeix a cap element de la PTD, ja que els diferents perfils de la VPN de Cisco s'han de permetre dins de les regles de *firewall*.

En aquesta mateix zona de l'esquema és on s'executen les aplicacions en contenidors dins d'Azure Kubernetes Services.

- o La part inferior, de **color lila**, representa la reserva de rangs privats per a la PTD, per minimitzar problemes de saturació d'IPs. S'utilitza el rang **10.10.0.0/16** per a aquestes xarxes. Existeix solapament d'IPs al rang 10.10.0.0/16, impedit per aquest motiu la zona blau fosc i la zona lila es comuniquin per defecte.

Per a poder habilitar aquesta comunicació des de la zona lila s'ha de fer a través d'SNAT (passant per una màquina que fa d'enrutador de la zona blau fosc), permetent que tot el que hi ha dins d'aquesta xarxa pugui accedir als serveis de la xarxa del CTTI (zona blau fosc).

En aquesta zona és on s'executen els clústers de Databricks o serveis com els d'Azure Functions. Per exemple, si des de Databricks s'accedeix a un Oracle en un centre de dades, aquest últim veuria que des de l'IP de la màquina enrutadora s'ha intentat la connexió, però Databricks podria fer *queries* a Oracle.

Es important recalcar que no hi ha un accés directe en sentit contrari, és a dir, des de la zona blau fosc no es possible contactar amb cap servei a la zona lila, no existeixen rutes que permetin la connexió. Si es rep una petició per contactar amb una IP dins del rang **10.10.0.0/16**, aquesta arribarà a una altra zona de la xarxa del CTTI (blau fosc) que actualment s'està usant.

Per solucionar aquests casos es fan servir *private endpoints*: es publica l'accés a un recurs d'Azure que pertany a la xarxa lila a una altra xarxa que pertany a la zona blau clar dins del rang del CTTI. D'aquesta manera encara que els clústers de Databricks s'executin a la zona lila, la IP d'accés a l'API de Databricks està a la zona blau clar i és accessible des de la VPN i per altres serveis del CTTI.

- En resum, s'accedeix des d'on s'accedeixi tot està connectat (sempre que no s'implementin nous serveis que no puguin usar *private endpoints*).
- Sobre la màquina enrutadora mencionada, aclarir que no és una única sinó diverses amb un balancejador.

2.1.1 DNS

La plataforma utilitza el seu propi DNS, en concret per als registres que acaben en `intranet.gencat.cat` delega la resolució als DNS del CTTI (10.1.1.1). No obstant, si es vol accedir a un element privat d'Azure, per exemple, un *blob*, aquesta resolució es farà exclusivament a la PTD i per molt que estigui registrat als DNS de CTTI, no es resoldrà adequadament. Això passaria amb registres de tipus *privatelink*, per exemple, `'privatelink.blob.core.windows.net'`. En aquests casos serà necessari sol·licitar a la PTD que registri les entrades necessàries als DNS dins de la plataforma.

Rangs de xarxa de la plataforma:

Element	Entorn	IP de sortida
Xarxa CTTI assignada a la PTD (zona blau clar)	PRE	172.29.22.0/24
Xarxa CTTI assignada a la PTD (zona blau clar)	PRO	172.29.23.0/24
Rang privat usat a la PTD	PRE i PRO	10.10.0.0/16
IP de sortida cap a la Internet (Nat Gateway)	PRE	20.224.22.183
IP de sortida cap a la Internet (Nat Gateway)	PRO	4.231.8.211
Rang privat usats als AKS per als PODs	PRE i PRO	10.11.0.0/17
Rang privat usat als AKPS per als serveis	PRE i PRO	10.11.128.0/17

2.2 Xarxes *Serverless* de Databricks

Un cas especial no mencionat a l'apartat anterior són les xarxes *serverless* de Databricks. Quan s'executa un clúster *serverless* a Databricks, la màquina no es crea al nostre entorn d'Azure, sinó en un entorn extern a la infraestructura de la PTD.

Aquest punt és rellevant, ja que des d'aquest entorn extern no hi ha connectivitat amb la resta de la plataforma (excepte els permisos per ([Azure Private Link availability](#))). Per exemple, per accedir a les dades de cada domini allotjats als *storage account*, seria possible només des del nostre entorn, no des de fora, perquè tenen IPs públiques.

L'alternativa en aquests casos es sol·licitar la creació d'un enllaç privat (*private link*) per a accedir a recursos privats de la plataforma, sempre que els elements d'Azure permetin aquesta funcionalitat ([Azure Private Link availability](#)).

A l'entorn de producció es desaconsella la utilització del còmput *serverless* a Databricks.

2.3 *Workspaces* de Databricks

A la PTD es disposa d'un workspace (àrea de treball) de Databricks per a cadascun dels dominis de la dada. Es llisten els existents a continuació:

Codi	Acrònim	Domini	Abreviatura catàleg	nom
D01	ADM	Administració pública, govern i relacions institucionals	ADMIN_GOVERN	
D02	AGR	Agricultura, ramaderia, pesca i alimentació	AGRIC_ALIMENT	
D03	CCT	Comerç, consum i turisme	CONSUM_TURISME	
D04	CLT	Cultura, llengua i identitat	CULT_LLENGUA	
D05	ECO	Economia	ECONOMIA	
D06	EDU	Educació, formació i universitats	EDU_FORMACIO	
D07	ELL	Esports i lleure	ESPORT_LLEURE	
D08	FPH	Finances públiques i hisenda	FINANCES_HISENDA	
D09	IND	Indústria i energia	IND_ENERGIA	
D10	INF	Informació i comunicació	INFORM_COMUN	
D11	JUD	Justícia i dret	JUSTICIA_DRET	
D12	MAM	Medi ambient	MEDI_AMBIENT	
D13	MOB	Mobilitat i transports	MOBILITAT	
D14	SLT	Salut	SALUT	
D15	SEM	Seguretat i emergències	SEGUR_EMERG	
D16	SSO	Serveis socials	SERVEIS_SOCIALS	
D17	SCI	Societat i ciutadania	SOCIETAT	
D18	TEC	Tecnologia, recerca i innovació	TECNO_INNOVA	
D19	TER	Territori, infraestructures i urbanisme	TERRITORI	
D20	TRB	Treball	TREBALL	
D98	NCO	No consta	NO_CONSTA	
D99	ALT	Altres/Diversos	ALTRES	

Existeixen també *workspaces* que pertanyen a un determinat domini. És necessari estar connectat a la VPN de Cisco amb un perfil que permeti l'accés a la xarxa de la PTD:

Workspace Databricks	Entorn	Acrònim
https://adb-7139081274934771.11.azuredatabricks.net	PRE	EDU
https://adb-1917381938162982.2.azuredatabricks.net	PRO	EDU
https://adb-3789131903298711.11.azuredatabricks.net	PRE	IND
https://adb-2541301643624898.18.azuredatabricks.net	PRO	IND
https://adb-3048252599961395.15.azuredatabricks.net	PRE	INF
https://adb-948847523960118.18.azuredatabricks.net	PRO	INF
https://adb-3277095303563266.6.azuredatabricks.net	PRE	SCI
https://adb-334953087586491.11.azuredatabricks.net	PRO	SCI
https://adb-589894607047291.11.azuredatabricks.net	PRE	TUR
https://adb-4258240250330622.2.azuredatabricks.net	PRO	TUR

A continuació el llistat de *workspaces* especials que no pertanyen a cap domini:

Workspace Databricks	Entorn	Funció
https://adb-3032011656902762.2.azuredatabricks.net	PRE	Administració
https://adb-3583375544375164.4.azuredatabricks.net	PRO	Administració
https://adb-3807468366949474.14.azuredatabricks.net	PRE	Transversal
https://adb-415924557256886.6.azuredatabricks.net	PRO	Transversal
https://adb-7139081274934771.11.azuredatabricks.net	PRE	Laboratori

2.4 Aplicacions en contenidors

El desplegament de les aplicacions dins de de la PTD es realitza a través d'un clúster de Kubernetes gestionat per Azure, és a dir, un AKS (Azure Kubernetes Services).

Cadascun dels projectes disposa d'un *namespace* propi on es poden desplegar les aplicacions que es requereixin.

A dia d'avui no estan implementades regles de *firewall* entre els diferents *namespaces*, però està previst. En aquest cas, les aplicacions que requereixin accedir a un *namespace* diferent hauran de sol·licitar-ho a l'equip PTD.

Les aplicacions s'exposen a través de l'Application Gateway d'Azure. La gestió del certificat es gestiona per l'Application Gateway.

La metodologia utilitzada per al desplegament es GitOps utilitzant ArgoCD i Helm. No es requereixen coneixements en cap d'aquestes eines o de Kubernetes per a desenvolupar aplicacions dins de la PTD.

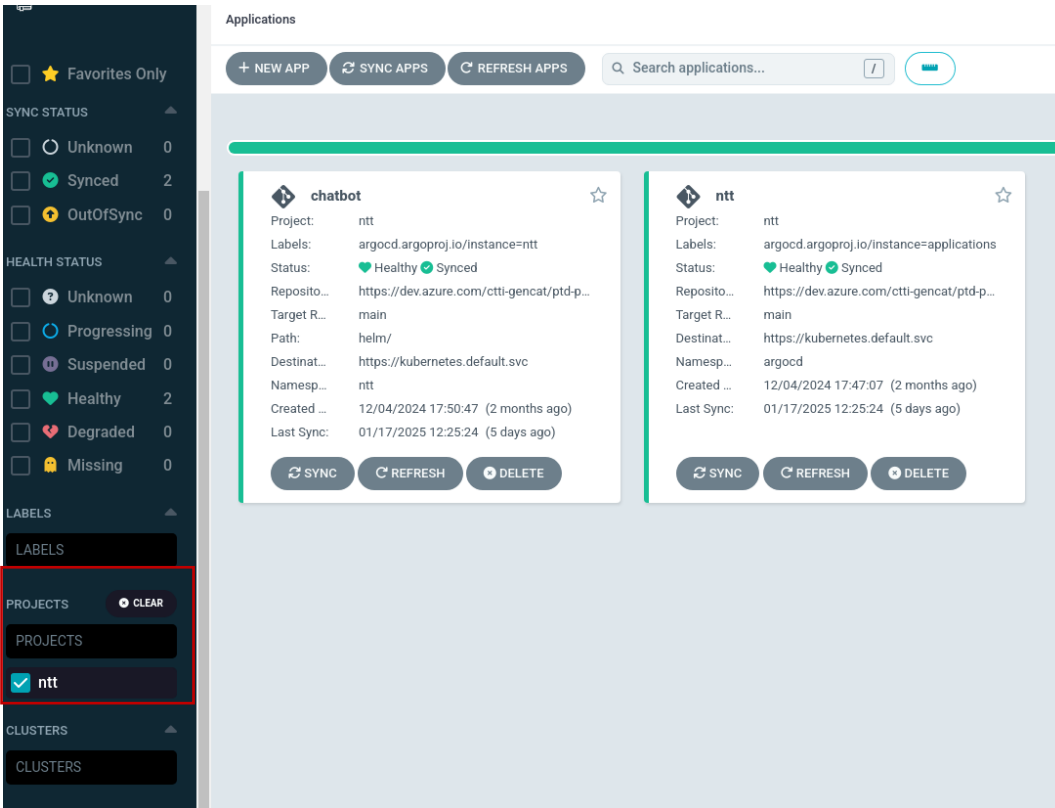
Per a consultar l'estat d'una aplicació s'haurà d'anar a ArgoCD ja que per defecte no es proporcionen usuaris de Kubernetes.

A continuació es llisten algunes de les URLs d'interès:

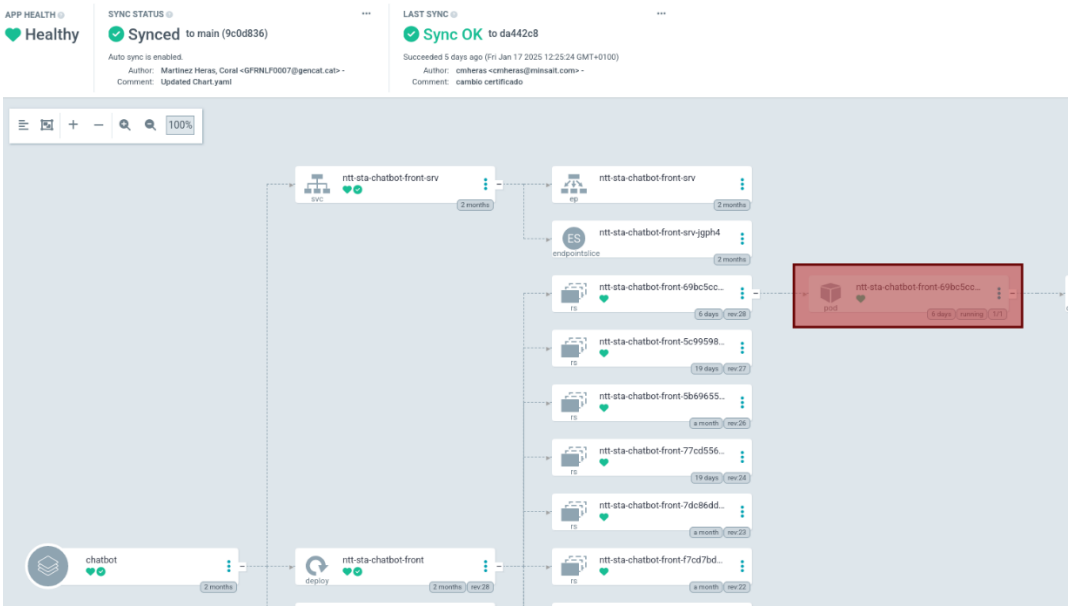
Elemento	Entorno	Recurso
https://argocd.preproduccio.ptd.ctti.intranet.gencat.cat	PRE	ArgoCD
https://argocd.ptd.ctti.intranet.gencat.cat	PRO	ArgoCD
https://grafana.preproduccio.ptd.ctti.intranet.gencat.cat	PRE	Grafana
https://grafana.ptd.ctti.intranet.gencat.cat	PRO	Grafana

Per poder fer login és necessari identificar-se a través de 'Keycloak', i triar 'Azure AD', és a dir, l'autenticació està gestionada a través del directori actiu d'Azure, i aquest al seu torn està federat amb el CTTI, pel que s'ha d'utilitzar el compte de Gencat. Per poder accedir ArgoCD és necessari que l'usuari estigui inclòs al grup del directori actiu 'PGC_PRE_AZURE-DEVELOPERS-UG' (s'ha de sol·licitar a la PTD).

Un cop s'hagi accedit es podrà navegar fins a les aplicacions o projectes desitjats. Al menú de l'esquerra, a 'Projects' es llisten els projectes als que es té accés; per exemple:



Dins de cadascuna es podran consultar els diferents manifestos de Kubernetes de l'aplicació, o consultar-ne els *logs*. Aquest punt és útil per consultar les variables d'entorn o configuracions de recursos de cada aplicació.



3. Requeriments de les aplicacions

3.1 Requeriments de les aplicacions de Databricks

Per poder desplegar aplicacions de Databricks és necessari encapsular totes les configuracions dins dels *bundles* ([Databricks Asset Bundles](#))

Aquests *bundles* permeten configurar tots els recursos necessaris de Databricks mitjançant configuracions en YAML. La *pipeline* de desplegament d'aplicacions de Databricks ho espera d'aquesta manera.

Exemple de databricks.yml:

```
26
27 targets:
28   dev:
29     mode: development
30     default: true
31     workspace:
32       host: https://adb-2626822259176962.2.azuredatabricks.net
33     variables:
34       environment: des
35       ownerCreation: [REDACTED]
36       groupWsView: [REDACTED]
37       groupWsViewPermissions: CAN_MANAGE
38       ownerProcesor: 890[REDACTED]
39       #ownerProcesor: 41[REDACTED]
40
41   pre:
42     mode: production
43     workspace:
44       host: https://adb-3807468366949474.14.azuredatabricks.net
45     run_as:
46       service_principal_name: c36a4[REDACTED]
47     variables:
48       environment: pre
49       denodo_enabled: false
50       groupWsView: pgc_[REDACTED]
51       groupWsViewPermissions: CAN_MANAGE_RUN
52       ownerProcesor: c36[REDACTED]
53       ownerCreation: 8d0[REDACTED]
54
55   prod:
56     mode: production
57     workspace:
58       host: https://adb-415924557256886.6.azuredatabricks.net
59     run_as:
60       service_principal_name: 6c6f[REDACTED]
61     variables:
62       environment: pro
63       denodo_enabled: false
64       groupWsView: [REDACTED]
65       groupWsViewPermissions: CAN_VIEW
66       ownerProcesor: 6c6[REDACTED]
67       ownerCreation: 676[REDACTED]
68
69 version=GBpreproduccio
```

Es pressuposa coneixement sobre l'operativa dels *bundles* per avançar en aquesta secció.

Requeriments:

- S'han de configurar com a mínim 3 *targets*: desenvolupament, preproducció i producció, els dos últims amb el mode '*production*'. Cadascun ha de tenir el *target* que pertanyi al domini corresponent. Per defecte es pressuposa que cada *bundle* ha de desplegar-se a un únic domini. Per desplegar en diferents dominis, si us plau contactar amb l'equip de la PTD.
- Els secrets que pugui necessitar l'aplicació han d'estar als Secret Scopes de Databricks, que per sota es connectaran als Azure Keyvaults. L'alta d'aquests secrets s'haurà d sol·licitar a l'equip de la PTD. Així mateix, la resta de variables han d'estar parametritzades per entorn.
- S'hauran de configurar adequadament els permisos amb els quals s'executen els *workflows*, és a dir, el paràmetre '*run_as.service_principal_name*'. Cada equip té un servei principal associat. Sol·licitar a l'equip de la PTD.
- Per a cadascun dels *workflows* s'hauran d'indicar a quins e-mails s'ha de notificar en cas de que fallin.

Exemple de notificacions:

```
1 resources:
2   jobs:
3     Ejemplo:
4       name: Ejemplo
5       email_notifications:
6         on_failure:
7           - outscaubcn@indracompany.com
8           - sistemasbcn@indra.es
9       permissions:
10        - service_principal_name: ${var.ownerProcesor}
11          level: IS_OWNER
12       run_as:
13         service_principal_name: ${var.ownerProcesor}
14       schedule:
```

- Fitxer de versió. A l'iniciar un *bundle* el *pipeline* espera trobar una carpeta '*src*' a l'arrel, i dins d'aquesta una segona carpeta amb el mateix nom que el repositori de codi font amb un fitxer '*__init__.py*' que contingui únicament la informació de versió; per exemple:

The image shows a code editor interface. On the left is a file explorer for a project named 'finops_databricks_impl'. The directory structure includes folders for 'CI', 'fixtures', 'resources', 'scratch', and 'src'. Under 'src', there is a sub-folder 'finops_databricks_impl' which is expanded to show a list of files and folders. A red arrow points to the file 'PY __init__.py'. Other files shown are '.DS_Store', 'PY main.py', and a folder 'MAPPING'. On the right, the code editor displays the content of the selected file, 'preproduccio / src / finops_databricks_impl / __init__.py'. The code contains two lines: '1 __version__ = "0.0.36"' and '2'. The editor has tabs for 'Contents', 'History', 'Compare', and 'Blame'.

3.2 Requeriments de les aplicacions en contenidors

Per a poder desplegar a la PTD una aplicació o arquitectura basada en contenidors els requeriments són bàsicament els mateixos que els de qualsevol entorn de Kubernetes:

- Aplicació o arquitectura *dockeritzada*, amb variables dependents de l'entorn parametritzades. Ha d'incloure referència a recursos externs, base de dades o entre diferents contenidors. És important recalcar que el *dockerfile* no el proporciona l'equip de la PTD, i que no pot contenir vulnerabilitats *high* o *critical* un cop analitzats per eines especialitzades (per exemple, [trivy](#)). Al [Dockerhub](#) es poden consultar les vulnerabilitats de les imatges base. Actualment no hi ha un catàleg d'imatges base aprovades per la PTD, pel que es podria utilitzar qualsevol que compleixi els requeriments de vulnerabilitats.
- Les imatges *Docker* no han de contenir secrets o informació sensible. Els secrets es muntaran com a fitxers/variables d'entorn en l'execució i la infraestructura ho tindrà en cuenta. L'aplicació a desplegar ha d'esperar trobar certs fitxers o variables d'entorn declarades. El clúster de Kubernetes recollirà els secrets a partir dels diferents Azure Keyvault i en cas de necessitar nous secrets s'haurà de sol·licitar l'alta dels mateixos a l'equip de la PTD.
- Actualment només disposem de *pipelines* per a desplegar aplicacions amb Maven i Angular. Per a fer-ho amb un altre tipus de tecnologia, s'ha de sol·licitar amb antelació a l'equip de la PTD.
- Les aplicacions han d'estar contingudes en sí mateixes al contenidor, és a dir, aplicacions amb estàtics html han d'incloure al *Dockerfile* l'Apache o Nginx que correspongui. En principi les aplicacions estàtiques s'instal·laran en contenidors, però es podria estudiar utilitzar els serveis propis d'Azure en cas de necessitar un CDN. Per defecte la solució preferent serà Kubernetes, ja que facilita la gestió.
- En projectes amb més d'un contenidor, s'haurà d'entregar un diagrama explicant les comunicacions entre els diversos components i el fluxe de peticions d'usuari. Per exemple, si la petició és cap a serveis *backend* s'enruta directament per Kubernetes, o en cas que les peticions vagin sempre al contenidor frontal i aquest disposi d'un Proxy per redirigir al *backend*.
- Actualment donem suport tant a construir una imatge genèrica per entorn, com a construir una imatge compilada para cada entoro, en funció de l'aplicació, pel que aquest punt no seria un requeriment en aplicacions Angular.
- Sobre la integració amb GICAR, en cas de ser requerida per part del CTTI, la PTD disposa d'un contenidor que per a algunes aplicacions s'interposa entre l'usuari i els contenidors finals que gestiona l'autenticació contra Gicar, permetent a les aplicacions gestionar directament els *tokens* JWT. Per a més informació consultar a l'equip PTD.
- Respecte a les configuracions de Kubernetes o plantilles d'HELM, aquestes es proveïran per part de la PTD, però en cas que l'aplicació sigui complexa o requereixi particularitats es pot facilitar a l'equip PTD un Helm Chart per a analitzar si es pot utilitzar.