



Documentación Técnica
GSDPI - AVIB
v 1.0.0

Copyright

This document is Copyright © 2024 by its contributors as listed below. You may distribute it and/or modify it under the terms of either the GNU General Public License (<http://www.gnu.org/licenses/gpl.html>), version 3 or later, or the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/3.0/>), version 3.0 or later.

All trademarks within this guide belong to their legitimate owners.

Colaboradores

Miguel Salinas Gancedo: versión español

Realimentación

Por favor, dirija cualquier comentario o sugerencia sobre este documento a:
salinasmiguel@uniovi.es

Fecha de publicación y versión del software

Publicado 3 Octubre 2024. Basado en AVIB versión 0.0.1.SNAPSHOT.

Contenidos

Copyright.....	2
Introducción.....	5
Análisis.....	6
Dominio del problema.....	7
Metodología Agile: Azure Devops.....	8
Seguridad del sistema.....	10
Gestión de casos.....	11
Datasets y su estructura.....	12
Encodings: tipos.....	13
Pipeline de los datos.....	14
Ingesta de casos.....	15
Transformación de casos.....	16
Análisis de casos.....	17
Dashboard y kpis.....	18
Arquitectura.....	19
Tech Stack.....	19
Dominio del problema.....	19
Microservicios.....	19
Diagrama de despliegue.....	19
Código.....	20
Repositorios de código.....	21
Políticas desarrollo backend: patrones y buenas prácticas.....	22
Políticas desarrollo frontend: patrones y buenas prácticas.....	23
Arquetipo microservicios backend Java.....	24
Arquetipo microservicios backend Python.....	25
Arquetipo microservicios frontend Angular.....	26
Arquetipo Jobs Kubernetes.....	27
Arquetipo microservicio analítica.....	28
Empaquetando los arquetipos: Helm.....	29
Operaciones.....	30
Despliegue infraestructura kubernetes Introducción.....	31
Instalación del cluster de Kubernetes.....	32
Instalación gestor paquetes de Kubernetes.....	40
Introducción.....	40
Instalación del CLI de Helm.....	40
Despliegue servicio Database: MongoDB.....	42
Despliegue servicio IAM: keycloak.....	45
Despliegue servicio Object Storage: Minio.....	49
Configuraciones Kubernetes post-despliegue.....	53
Configuración reverse-proxy: HAProxy Introducción.....	55
Configuración kubernetes ingress.....	56
Reglas de ingress.....	57
Despliegue servicios de negocio.....	61
Introducción.....	61
Listado de paquetes Helm.....	61

Acceso al Service Registry de Azure.....	62
Acceso local a Azure.....	<u>62</u>

Introducción

Este es un documento técnico destinado a todo usuario con rol de Arquitectos o Desarrollador que tenga que comprender las diferentes partes en que está diseñado el sistema. Igualmente todo usuario que tenga que mantener y monitorizar el mismo con rol tipo devops también le será de gran ayuda.

Este documento está dividido en cuatro grandes secciones:

1. **Análisis:** en donde se intenta explicar el dominio del problema que quiere resolver este sistema.
2. **Arquitectura:** en esta sección se describen con texto y diagramas los frameworks y librerías escogidos así como están entre si relacionados y se comunican entre si, para resolver el dominio del problema que nos ocupa.
3. **Código:** en esta sección se enumeran los repositorios de código, buenas prácticas a la hora de desarrollar cada una de las piezas que forman los servicios de negocio que resuelven el dominio de problema antes indicado.
4. **Despliegue:** por último en esta sección se explica en detalle, como se debe de desplegar un sistema distribuido como este, indicando los pasos a seguir en caso de tener que desplegarlo desde cero.

Análisis

Vamos a explicar en esta sección que dominio de problema queremos solventar y que metodología herramientas hemos utilizado para implementar esta solución

Dominio del problema

Antes de empezar a analizar como queremos implementar esta solución, debemos de comprender que problema queremos resolver.

Actualmente el departamento GSDPI ha desarrollado durante años diferentes proyectos con un denominador común, ser capaces de analizar gran cantidad de datos visualmente utilizando la técnica de **Morphing Projections**. Esta técnica permite poder encontrar patrones de comportamiento en grandes Datasets de alta dimensionalidad, empleando para ello técnica de Inteligencia Artificial que permiten reducir esta alta dimensionalidad a 2 o tres dimensiones capaces de ser dibujadas en un canvas de 2 o tres dimensiones. Estas proyecciones en este canvas junto a técnicas visuales de color y movimiento gracias a esta técnica de Morphing o moviendo de estos puntos en el espacio, permiten que el analista pueda encontrar patrones de comportamiento en donde las técnicas numéricas no son capaces de mostrarnos con tanta claridad este comportamiento.

Por lo tanto una necesidad surgida de este desarrollo era como resolver un problema como este de forma escalable, dinámica y adaptada a cualquier dataset procedente de cualquier dominio: industrial, salud, marketing, etc.

El proceso necesario a la hora de adaptar las aplicaciones individuales de ingestar los datasets y visualizar el resultado de los mismos, es costoso en tiempo. Además la solución debiera de poder ser configurable y explotable en entornos Web fácilmente accesible desde cualquier navegador actual. Además debíamos de tener en cuenta la escalabilidad y el uso por diferentes usuarios al mismo tiempo, cada uno de ellos con un problema diferentes de un espacio distinto.

El análisis de todos estos requisitos han hecho posible el desarrollo de este sistema teniendo en mente estos puntos:

- Sistema amigable y fácilmente accesible vía Web
- Sistema configurable a cualquier dominio, creando un standard que se capaz de adaptarse a cualquier dominio.
- Un sistema escalable que pueda crecer según las necesidades
- Un sistema basado en datos, teniendo este concepto como piedra angular al rededor del cual diseñar todo el sistema.
- Un sistema resiliente capaz de mantener la integridad en todo momento.
- Un sistema seguro, por se consumido a través de internet, un canal no seguro a todas luces.
- Siguiendo los standards actuales del mercado, a nivel de diseño, arquitectura e implementación
- Utilizando herramientas OpenSource que sean mantenidas por la comunidad o empresas, dándonos una seguridad de su continuidad y soporte durante años.

Metodología Agile: Azure Devops

A la hora de desarrollar una herramienta como esta de carácter distribuida, debemos en primer lugar seleccionar el entorno y metodología para su análisis, desarrollo y despliegue.

Para resolver este primer dilema, se ha seleccionado la herramienta de Microsoft llamada Azure Devops. Esta plataforma de Microsoft cumple con todas las condiciones necesarias a la hora de abordar un proyecto como este:

1. Herramienta mantenida y soportada por Microsoft, lo que nos da la seguridad de su continuidad y soporte actual y futura.
2. Es una herramienta segura que está perfectamente integrada con el SSO de Microsoft de la Universidad de Oviedo, por lo que podemos utilizar nuestras mismas credenciales que actualmente nos definen en la Universidad de Oviedo, no teniendo que crear nuevas credenciales para ello.
3. Es una herramienta que esta formada por varios módulos integrados, que no utilizaremos en su totalidad pero que si permiten crear un seguimiento y control perfecto de un proyecto de la embergadura como este:
 - **Wiki:** Este módulo representa la parte documental del sistema, en donde podemos crear vistas y documentación digital fácilmente distribuible y mantenible. La división de esta documentación sigue la misma distribución que la de este documento.
 - **Board:** este módulo gestor de tareas y seguimiento del proyecto siguiendo la metodología agile. Este módulo permite crear un backlog de tareas, ordenarlas y ejecutarlas de forma controlada. Igualmente permite el seguimiento de las mismas, así como su evolución por medio de listados, kambas, diagramas y KPIs.
 - **Repos:** Esta sección es donde crearemos todos los repositorios de código de todos los servicios de negocio del sistema. Esta sección es un gestor de versiones distribuido como puede ser Github o Gitlab.
 - **Pipelines:** este módulo en principio no está siendo utilizada, pero representa aquella parte del sistema en donde podemos implementar los pipelines CI/CD de integración y despliegue del mismo de forma automática. Actualmente y como se explicará en otros capítulos, las etapas a la hora de integrar y desplegar nuestros servicios será manual siguiendo unos pasos detallados que veremos en próximos capítulos.
 - **Test Plan:** es otro módulo que no utilizaremos y sirve para diseñar pruebas de integración de nuestro sistema, para poder mantener un nivel de calidad continua. En nuestro caso estas pruebas unitarias y de integración se hacen manualmente en tiempo de desarrollo

- **Artefactos:** este es un módulo que no utilizaremos tampoco, pero que a futuro podría ser interesante a la hora de mantener una cache controlada para todas las dependencias, que son muchas, utilizadas por todos nuestros servicios de backend y frontend.

A todas estas herramientas debemos de añadir aquellas que son ofrecidas por la infraestructura de Azure, no confundir con Azure Devops. Actualmente la infraestructura de Azure es muy grande ofreciendo todo tipo de servicios, orientados a la ejecución, monitoreo, redes y mucho mas. De todos los servicios ofrecidos por Azure solamente utilizaremos uno, que es el **gestor privado de imágenes de Docker**, pues como iremos viendo en otros capítulos todos los servicios del sistema tienen en común ser contenedores de docker, por lo que todos ellos estan empaquetados como imágenes de Docker que deben de ser almacenadas y gestionadas por repositorios especiales. Azure ofrece este tipo de repositorios y será el que utilizaremos para almacenar nuestras imágenes de docker.

Seguridad del sistema

TODO

Gestión de casos

TODO

Datasets y su estructura

TODO

Encodings: tipos

TODO

Pipeline de los datos

TODO

Ingesta de casos

TODO

Transformación de casos

TODO

Análisis de casos

TODO

Dashboard y kpis

TODO

Arquitectura

TODO

Tech Stack

TODO

Dominio del problema

TODO

Microservicios

TODO

Escalabilidad: Jobs

TODO

Análítica: Algoritmos

TODO

Diagrama de despliegue

TODO

Código

TODO

Repositorios de código

TODO

Políticas desarrollo backend: patrones y buenas prácticas

TODO

Políticas desarrollo frontend: patrones y buenas prácticas

TODO

Arquetipo microservicios backend Java

TODO

Arquetipo microservicios backend Python

TODO

Arquetipo microservicios frontend Angular

TODO

Arquetipo Jobs Kubernetes

TODO

Arquetipo microservicio analítica

TODO

Empaquetando los arquetipos: Helm

TODO

Operaciones

En esta sección vamos a explicar en detalle todos los pasos y configuraciones que debemos de tener en cuenta a la hora de desplegar, configurar y mantener un sistema como es AVIB. Sabiendo que desde el punto arquitectónico es un sistema basado en microservicios que necesitan del apoyo de otros servicios no desarrollados internamente como pueden ser:

- **Dashboard:** esta herramienta es muy útil para visualizar y gestionar casi todos los recursos del cluster: Pods, contenedores, servicios, secrets, etc de forma visual. De todas formas siempre contaremos con el CLI de Kubernetes llamado kubectl que ya hablaremos de el posteriormente.
- **Base de datos** para gestionar los metadatos del sistema.
- **Gestores de ficheros** Object Storage para gestionar los datasources del sistema.
- **Servicio de Autenticación y Autorización** para implementar la seguridad.
- **Reverse Proxies** para redireccionar el tráfico procedente del exterior. En este apartado hablaremos de un servicio que aun no corriendo dentro del cluster de Kubernetes es de vital importancia pues estará corriendo en el Host dando entrada a todas las peticiones externas, tanto al sistema AVIB desplegado en un cluster de Kubernetes como a los servicios que actualmente ya están corriendo en el Host.

Despliegue infraestructura kubernetes

Introducción

En este capítulo se va a explicar como se debe debemos desplegar un cluster de Kubernetes. Como sabemos Kubernetes se define como un orquestador de contenedores, y por ellos su despliegue y correcta configuración es de vital importancia pues todos los servicios de infraestructura y servicios de negocio van a ser empaquetados como imágenes de Docker desplegadas en este entorno, que va a encargarse de gestionarlos correctamente en todo momento.

Debemos tener presente que el cluster de Kubernetes va a ser desplegado en una infraestructura hardware manejada por el departamento AVIB de la Universidad de Oviedo con sus limitaciones a nivel de recursos: memoria, CPU y disco, que la mismo tiempo va a ser un recurso compartido por otros otros servicios ya existentes que no van a correr dentro del espacio de Kubernetes. Dada esta situación se ha adoptado por seleccionar un despliegue de Kubernetes basado en un cluster mono nodo, pues el hardware no es escalable horizontalmente y por ello se ha escogido el servicio de [Minikube](#) por:

- Es el primer servicio desarrollado para desplegar Kuberbetes en entornos no escalables como el que nos ocupa.
- Servicio mantenido actualmente por la comunidad, con un roadmap muy activo.
- Permite desplegar Kubernetes en dos modos utilizando drivers: modo contenedor o modo Maquina Virtual utilizando un Hypervisor.
- Documentación amplia y comunidad activa, que permite consultar errores, casos de uso o enviar tickets en caso de dudas o errores.
- Gran cantidad de extensiones faciles de ser desplegadas a través de su consola.
- Poner en marcha un cluster de Kubernetes es rápido y sencillo desde cero.

Por todas estas razones se ha escogido Minikube. Debemos de hacer imcapié en el punto que habla sobre la forma de ser desplegado Minikube, en nuestro caso y viendo que el nodo hardware en donde va a ser desplegado Kubernetes ha de ser compartido por otros servicios se ha adoptado desplegar Kubernetes en modo Máquina Virtual que aísla por completo el cluster y cualquier servicio que corra dentro de el, evitando cualquier problema colateral a nivel de seguridad con el host y los servicios que puedan correr en paralelo en el mismo.

Instalación del cluster de Kubernetes

Vamos a listar todos los pasos y consideraciones que debemos de tener en cuenta a la hora de desplegar un cluster de Kubernetes con las consideraciones antes expuestas:

- **Paso 01: instalar el CLI de minikube**

Como ya se ha comentado hemos escogido la herramienta Minikube para desplegar y gestionar nuestro cluster de Kubernetes, por lo que lo primero que debemos hacer es instalar el CLI (Command Line Interface) de Minikube. Este CLI es un simple binario que debemos de bajarlo a nuestro Host e instalarlo en la carpeta compartida de binarios para poder acceder al mismo desde cualquier cuenta. En nuestro caso escogemos la arquitectura de nuestro Host de tipo amd64:

```
$ curl -LO https://storage.googleapis.com/minikube/releases/latest/minikube-linux-amd64
$ sudo install minikube-linux-amd64 /usr/local/bin/minikube && rm minikube-linux-amd64
```

Este comando instala el CLI de Minikube bajo el nombre minikube, siendo accesible desde nuestra cuenta. Para chequearlo podemos ejecutar simplemente este comando para ver que funciona correctamente:

```
$ minikube version
minikube version: v1.34.0
commit: 210b148df93a80eb872ecbeb7e35281b3c582c61
```

Este comando muestra la versión de minikube y mas adelante cuando despluguemos un cluster la versión del cluster desplegado en el Host

- **Paso 02: desplegar el cluster de kubernetes**

Antes de ejecutar el comando del CLI de Minikube que instalará el cluster debemos de tener algunas consideraciones respecto al Host en donde correrá el cluster:

- Vamos a utilizar el modo Máquina Virtual, y por ello necesitamos que el Host tenga instalado un Hypervisor que va a encargarse de gestionar las Máquinas Virtuales que correrán en el Host. Aunque Minikube soporta varias máquinas virtuales la que utilizar por defecto es la De VirtualBox de Oracle, por lo que será esta la que deba de estar instalada en el host antes de desplegar el cluster. La instalación de esta herramienta queda fuera del ámbito de este documento. Pero para más detalle puede consultar el link oficial de Oracle sobre [VirtualBox](#)

- El Host debe de tener los recursos suficientes para albergar el cluster de Kubernetes a nivel de: memoria, CPU y disco. Claro está este debe de tener acceso a Internet en todo momento.

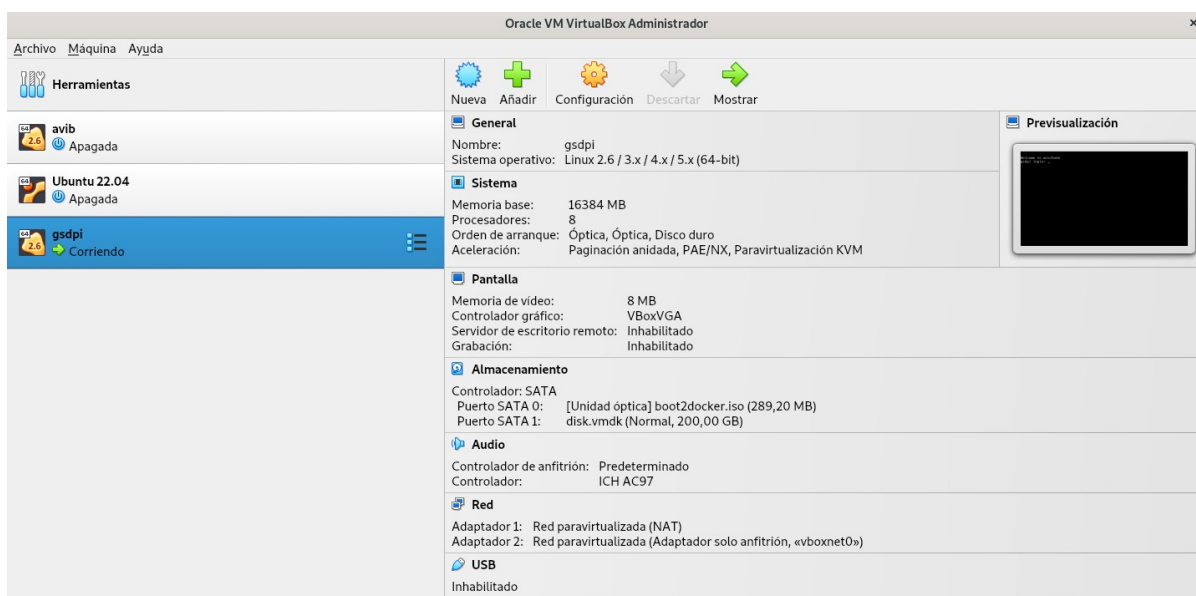
Con estos datos presentes vamos a describir los recurso mínimos y consideraciones que hemos escogido para nuestro cluster:

- **Memoria:** 16 gigabytes de memoria RAM, pues trataremos con datasources que en muchos casos van a requerir de memoria RAM para ser ejecutados correctamente. Este recurso es fácilmente escalable, teniendo en cuenta claro está las limitaciones del nodo hardware que cuenta con hasta 32 Gigas si fuera necesario ampliar la misma.
- **CPU:** máximo cores para que los proceso de machine leaningy proyecciones puedan correr de forma ágil. Al igual que en el caso anterior este recurso es fácilmente escalable desde el gestor de VirtualBox si fuera necesario ceder mas potencia de cálculo al cluster.
- **Disco:** 200 gigas para poder almacenar de forma agil ahora y en el futuro los datasources que utilizaremos en nuestros análisis. Este recurso aunque escalable posteriormente se ha definido la Máquina Virtual, no es tan sencillo de ser modificado a posteriori, con peligro de dejar la máquina Virtual no accesible si no se hacen los pasos correctos, por ello se ha escogido suficiente espacio de disco para que no nos quedamos cortos a medio plazo. En este [link](#) publico explico de todas formas como realizar los pasos si nos viéramos en la necesidad de ceder mas espacio de disco a la Maquina Virtual si fuera necesario.
- Como sabemos el acceso a cualquier servicio desde el Host se hace de forma segura utilizando el protocolo TLS. Como ya sabemos para ellos Minikube ofrece la opción de generar **certificados autofirmados** por el sistema, haciendo que el proceso de instalación sea mas sencillo. En este caso debemos tener en cuenta es la expiración del certificado auto-firmado que originalmente crea Minikube para nosotros. Por defecto Minikube utilizar 3 años para la misma, pero nosotros vamos a ampliarla hasta los 10 años para no tener que modificarla posteriormente que no es una tarea nada sencilla

```
$ minikube start --profile=gsdpi --driver=virtualbox --memory=16384 --cpus=max --disk-size=200g --cert-expiration=87600h0m0s:
```

Con estas consideraciones podemos ya ejecutar el siguiente comando de minikube desde la consola del Host. Podemos el driver escogido, los recursos antes listados y los 10 años de vida para los certificados creados por el cluster:

Tras unos segundos y no ha habido ningún problema veremos nuestro cluster corriendo dentro de una máquina virtual con los recurso antes descritos:



Una nota a destacar es que aunque el cluster es un servicio vital, pues dentro de el correrán todos los servicios del sistema, este pueda que tenga que ser parado por mantenimiento. Aunque este es una máquina virtual listada como cualquier otra máquina virtual box, no debemos de manejarla utilizando la herramienta de Virtual Box, sino el CLI de Kubernetes, **siempre deberemos de arracar o para el cluster desde el CLI y nunca desde Virtual Box, esto puede dejar la instancia corrupta o en estado no consistentes**

Para mayor detalle de como utilizar el CLI podemos consulta la ayuda del mismo desde la consola del host como cualquier comando de Linux:

```
$ minikube --help
```

- **Paso 03: Instalar el CLI de Kubernetes**

Tras desplegar nuestro cluster de Kubernetes, ahora debemos de instalar algunas herramientas para interactuar con el a la hora de desplegar y monitorear el estado de nuestros servicios desplegados dentro de el. Para ellos Kubernetes ofrece el CLI oficial llamado **kubectl**. Si es cierto que minikube en las últimas versiones ya viene preparado con esta herramienta para no tener que instalarla posteriormente, vamos a explicar como instalar el CLI por nuestra cuenta. Un dato que debemos de tener en cuenta antes de instalar este CLI es la versión de kubernetes que Minikube ha instalado en nuestro Host, pues el cliente debe de estar alineado con esta versión para no sufrir efectos desagradables a la hora de ejecutar este comando contra nuestro cluster.

```
$ minikube version --components
```

```
minikube version: v1.31.2
```

```
commit: fd7ecd9c4599bef9f04c0986c4a0187f98a4396e
```

```
buildctl:
```

```
buildctl github.com/moby/buildkit v0.11.6 2951a28cd7085eb18979b1f710678623d94ed578
```

```
containerd:
```

```
containerd g
```

Este comando nos da las versiones de todos los componentes de los que esta formado un cluste de Kubenetes, el que nos interesa el de minikube version que esta alineado con la versión de kubernetes en nuestro caso la 1.31.2, por lo tanto deberemos de instalar esta versión de CLI llamada kubectl, como sigue:

```
$ curl -LO "https://dl.k8s.io/release/1.31.2/bin/linux/amd64/kubectl"
```

```
$ sudo install -o root -g root -m 0755 kubectl /usr/local/bin/kubectl
```

```
$ kubectl version
```

```
WARNING: This version information is deprecated and will be replaced with the output from kubectl version --short. Use --output=yaml|json to get the full version.
```

```
Client Version: version.Info{Major:"1", Minor:"27", GitVersion:"v1.27.4",
```

```
GitCommit:"fa3d7990104d7c1f16943a67f11b154b71f6a132", GitTreeState:"clean",
```

```
BuildDate:"2023-07-19T12:20:54Z", GoVersion:"go1.20.6", Compiler:"gc",
```

```
Platform:"linux/amd64"}
```

```
Kustomize Version: v5.0.1
```

```
Server Version: version.Info{Major:"1", Minor:"27", GitVersion:"v1.27.4",
```

```
GitCommit:"fa3d7990104d7c1f16943a67f11b154b71f6a132", GitTreeState:"clean",
```

```
BuildDate:"2023-07-19T12:14:49Z", GoVersion:"go1.20.6", Compiler:"gc",
```

```
Platform:"linux/amd64"}
```

Aquí vemos como el comando de kubectl no solo nos da la versión suya sino también la versión del cluster de kubernetes ya funcionando. Esto es así, porque cuando minikube inicia el cluster también crea una configuración de acceso al cluster por defecto, con todas las credenciales necesarias para que un CLI como kubectl pueda lanzar comandos al cluster. Esta configuración se guarda por defecto en este fichero:

`~/.kube/config`

Comentar que si paramos el cluster estas credenciales se borrarán del fichero config, volviendo a recrearse en su arranque.

Activar addons kubernetes

Una vez el cluster esté funcionando deberemos de instalar un par de extensiones que minikube las llama addons.

Ahora que ya tenemos nuestro cluster corriendo y el CLI instalado para interactuar con él, vamos a terminar esta primera etapa de instalación del cluster desplegando un par de servicios necesarios para acceder externamente a nuestros servicios y poder monitorizar y configura el mismo visualmente:

Instalación de addons en el cluster Kubernetes

- **Paso 01: Instalar las extensión Kubernetes Dashboard**

Dashboard: este es el servicio que por defecto ofrece Kubernetes para poder visualizar y gestionar los recursos de un cluster de Kuberetes de forma visual, aunque como ya se ha comentado anteriormente, el CLI de Kubernetes llamado kubectl ofrece todo lo necesario para interactuar con el cluster desde linea de comandos, es mas, el Dashboar no ofrece todos los recursos para poder ser gestionados visualmente, pero el CLI si. De todas formas el Dashboard casi todos los recursos que manejaremos nosotros en nuestro sistema siendo mucho mas ágil utilizar esta herramienta en muchos casos frente a la linea e comandos ofrecida por kubectl. Para instalar este servicio Minikube la ofrece bajo la figura de addon, es decir Minikube tiene muchos addons que pueden ser desplegados fácilmente utilizando su CLI de minikube. Para list todos estos addons podemos ejecutar el comando. Este comando nos da una lista muy extensa con muchos addons entre ellos el llamado dashboard

```
$ minikube addons list
```

ADDON NAME	PROFILE	STATUS	MAINTAINER
ambassador	gsdpi	disabled	3rd party (Ambassador)
auto-pause	gsdpi	disabled	minikube
cloud-spanner	gsdpi	disabled	Google
csi-hostpath-driver	gsdpi	disabled	Kubernetes
dashboard	gsdpi	enabled	Kubernetes
default-storageclass	gsdpi	enabled	Kubernetes
efk	gsdpi	disabled	3rd party (Elastic)
....			

Ahora simplemente para instalar el addon llamado dashboard ejecutamos este comando:

```
$ minikube addon install dashboard
```

Tras unos minutos este addon será instalado, para poder acceder a el deberemos de crear un reverse proxy temporal. Esto lo haremos así porque por defecto el Dashboard viene sin seguridad alguna, y el acceso al mismo será temporal durante el despliegue del sistema, por ello utilizaremos un proxy temporal creado por el CLI minikube dará acceso al servicio del Dashboard, solamente desde el navegador del Host y nunca desde el exterior del mismo. En cuanto terminemos de monitorizar nuestro cluster podemos parar este proxy temporal en cuanto queramos. Vamos a crear este proxy temporal y ver un poco por encima la herramienta de Dashboard:

```
$ minikube dashboard
```

```
Verifying dashboard health ...
```

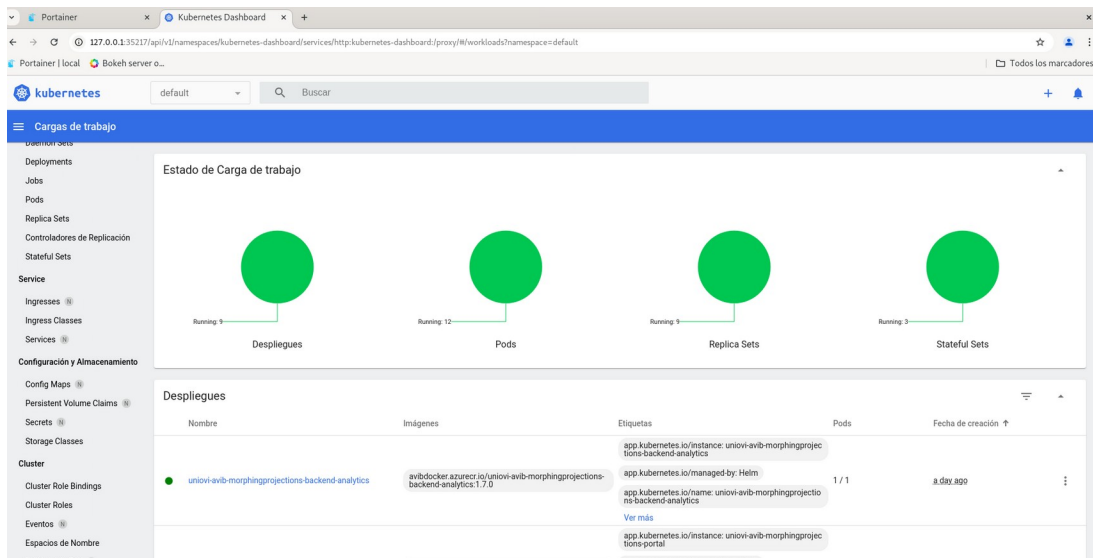
```
Launching proxy ...
```

```
Verifying proxy health ...
```

```
Opening http://127.0.0.1:35217/api/v1/namespaces/kubernetes-dashboard/services/  
http:kubernetes-dashboard:/proxy/ in your default browser...
```

Esta es una herramienta Web visual por lo tanto deberemos de tener en nuestro Host un navegador Web, que abrirá automáticamente una pestaña con acceso al Dashboard desde localhost y puerto aleatorio 35217. Este puerto es aleatorio como comento por lo que si paramos el proxy y lo arrancamos posteriormente este puerto será diferente. Pero como comentamos esta es una herramienta temporal que nos ayuda a ver los recursos y estado de los recursos de nuestro cluster, pero como comento, el CLI kubectl ofrece lo mismo y mas pero desde la consola de Linux.

En la siguiente captura podemos ver el Dashboard con todos los recursos y sus estados arrancados por defecto en el sistema. En este documento no se va a hablar de como manejar Kubernetes por estar fuera del ámbito del documento, pero para mayo detalle existe mucha documentación sobre esta herramienta, empezando por la oficial de [Kubernetes](#) a infinidad de links y libros sobre el tema.



- **Paso 02: Instalar las extensión Kubernetes Ingress:**

No voy a extenderme demasiado a la hora de definir que es Ingress, pero podemos resumir que Ingress es una especificacion creada para Kubernetes en donde se explica como debe de implementarse un proxy dentro de Kubernetes. Como toda especificación esta puede ser implementada por muchas empresas, en nuestro caso escogeremos la de referencia implementada por NGINX, por ser una de las primeras opciones ofrecidas como addon por Minikube y la mas madura de otras soluciones como Istio o HAProxy. Como en el caso anterior por ser un addon sersencillo instalarla ejecutando este comando

\$ minikube addons install ingress

Tras uno segundos el servicio del ingress estará desplegado en el cluster. De el hablaremos mas adelante cuando definamos las reglas de redireccionamiento a los servicios que el frontend debe de tener acceso. Por ahora podemos decir que Kubernetes ya cuenta con reverse proxy interno que podrá ser configurado por medio de una serie de reglas con un lenguaje específico del ingress.

Instalación gestor paquetes de Kubernetes

Introducción

Ahora que ya tenemos el cluster de Kubernetes funcionando con los addons ya instalados y los clientes de gestión de Minikube y Kubernetes también instalados, vamos a instalar otro CLI más llamado **helm**. Helm es una herramienta que sirve para instalar paquetes de Kubernetes, entiendo por paquetes como un conjunto de recursos de Kubernetes relacionados entre sí y necesarios para que un servicio pueda correr correctamente dentro del entorno de Kubernetes.

Dependiendo del servicio que vayamos a instalar este necesitará unos recursos u otros como por ejemplo: deployments, Pods, containers, services, volume claims, configmaps, secrets, service accounts o roles entre otros muchos. La necesidad de tener que instalar todos estos recursos de forma ordenada y de tener que ser actualizados igualmente si fuera necesario, hace que el uso de herramientas como Helm sean muy útiles. Esta herramienta no solo facilita el despliegue de estos paquetes sino que maneja el estado de las mismas llamadas releases, que son la instancia de un paquete de Helm llamados charts. En este documento no se va a explicar con detalle como crear paquetes chart para ser manejados por la herramienta Helm, pues está fuera del ámbito de este documento, pero para mayor detalle recomiendo leer la documentación oficial de la herramienta [Helm](#).

En este apartado voy a explicar brevemente como instalar el CLI de Helm con el cual podremos interactuar con Kubernetes a la hora de manejar estos paquetes Charts desplegándolos y actualizándolos si fuera necesario. Como sabemos el sistema está basado en el patrón de microservicios, donde cada uno de ellos está empaquetado como un paquete chart, preparados para ser desplegado en Kubernetes. Por lo que no solo utilizaremos esta herramienta inicialmente a la hora de desplegar los servicios de infraestructura del sistema ya comentados:

- Bases de Datos.
- Object Storage.
- Servicio de Autenticación y Autorización.

Sino que también será utilizado a la hora de desplegar todos los servicios de negocio propios del sistema tanto de backend como de frontend.

Instalación del CLI de Helm

Para instalar el CLI de Helm será tan sencillo como los otros CLI ya instalados de Minikube o el de Kubernetes. En este caso nos bajamos el CLI para nuestro entorno y

```
$ curl -fsSL -o get_helm.sh https://raw.githubusercontent.com/helm/helm/main/scripts/get-helm-3
$ chmod 700 get_helm.sh
$ ./get_helm.sh
```


lo instalamos en el sistema con estos comandos:
Ahora podemos probar que funciona correctamente

Este comando lista todas la releases desplegadas en el sistema, es decir todos los paquetes tipo Chart desplegados, en nuestro caso no hay ninguno, pero el resultado

```
$ helm list
NAME                                NAMESPACE REVISION    UPDATED
STATUS      CHART                                APP VERSION
```

indica que funciona correctamente, pues este CLI se alimenta la igual que el CLI de Kubernetes kubectl de la configuracion activa antes descrita y por ellos Kubernetes le esta respondiendo correctamente sin ninguna release desplegada.

Al final cuando desplaguemos todos los microservicios veremos que aparecerán muchas releases unas pertenecientes a nuestros servicios de negocio y otras pertenecientes a los servicios de infraestructura antes citados.

Despliegue servicio Database: MongoDB

Como se ha comentado podemos agrupar los servicios dentro del cluster en dos grupos:

- **Servicios de infraestructura:** son todos los servicios que no implementan lógica de negocio de nuestro dominio, pero que son necesarios o de apoyo a la hora de hacer posible esta implementación, por ejemplo implementar el estado de los servicios que lo requieran por medio de bases de datos, o object storages, o sistemas que implementan la autenticación Oauth como es el caso del servicio Keycloak
- **Servicios de negocio:** son por contra aquellos servicios que si implementan la lógica de negocio de nuestro dominio. En nuestro caso son todos los microservicios de backend y frontend que listaremos posteriormente en próximos capítulos, cuando hablemos de como desplegar esta lógica de negocio.

En este caso vamos a centrarnos en uno de estos servicios de infraestructura encargado de manejar el estado del sistema. Como es sabido el patrón microservicios aconseja utilizar una base de datos independiente para cada uno de estos microservicios, por temas relacionados con la escalabilidad y desacoplamiento dentro del modelo de datos. Nosotros no hemos seguido estrictamente este patrón, pues estamos utilizando en este caso una sola base de datos utilizada por dos microservicios implementada por la base de datos no relacional llamada MongoDB

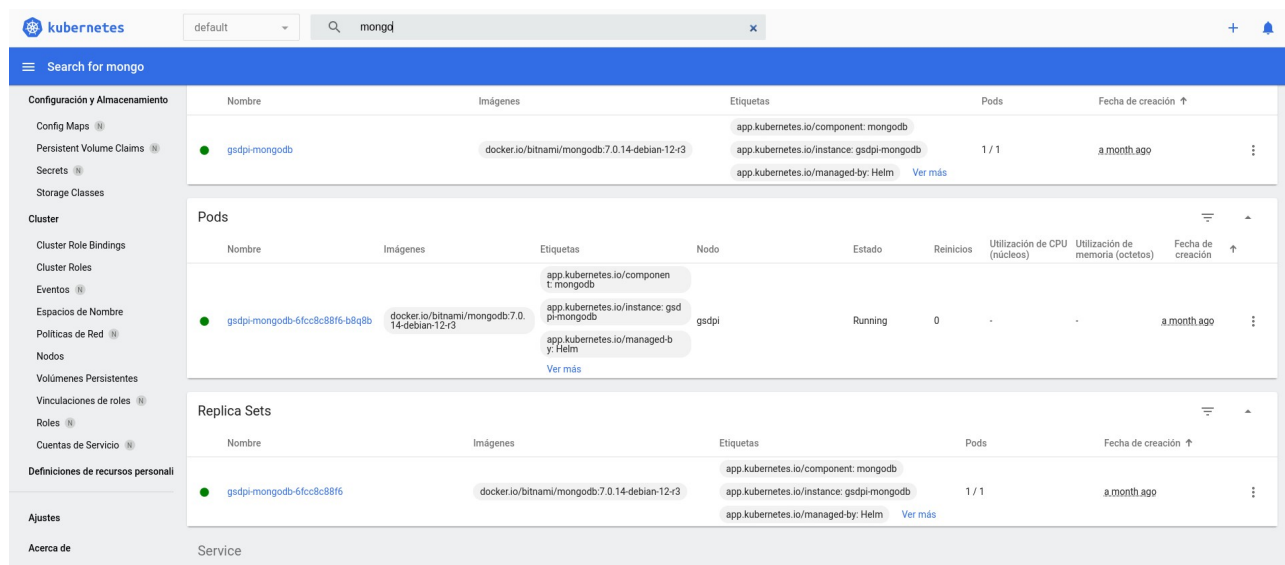
A la hora de desplegar este servicio hemos utilizado el paquete de helm standar mantenido por MongoDB, para que el despliegue sea lo mas sencillo posible, pues el número de recursos de Kubernetes necesarios para poner en marcha una base de datos como esta en Kubernetes es amplio y complejo. El uso de estos paquetes hacen que este despliegue sea mucho mas sencillo y mantenible. El comando que debemos ejecutar tratándose de un paquete helm es este:

```
$ helm install avib-mongodb oci://registry-1.docker.io/bitnamicharts/mongodb
```

Como podemos ver no hemos modificado ninguno de los parámetros que por defecto define el paquete. Normalmente estos paquetes son altamente configurables y se puede consultar todos estos parámetros desde el link oficial del paquete helm en este [link](#). Este paquete esta gestionado por el repositorio público de paquetes de helm llamado bitnami. Por defecto este repositorio no viene configurado con el CLI de helm, por lo que debemos añadirlo antes de ejecutar el anterior comando:

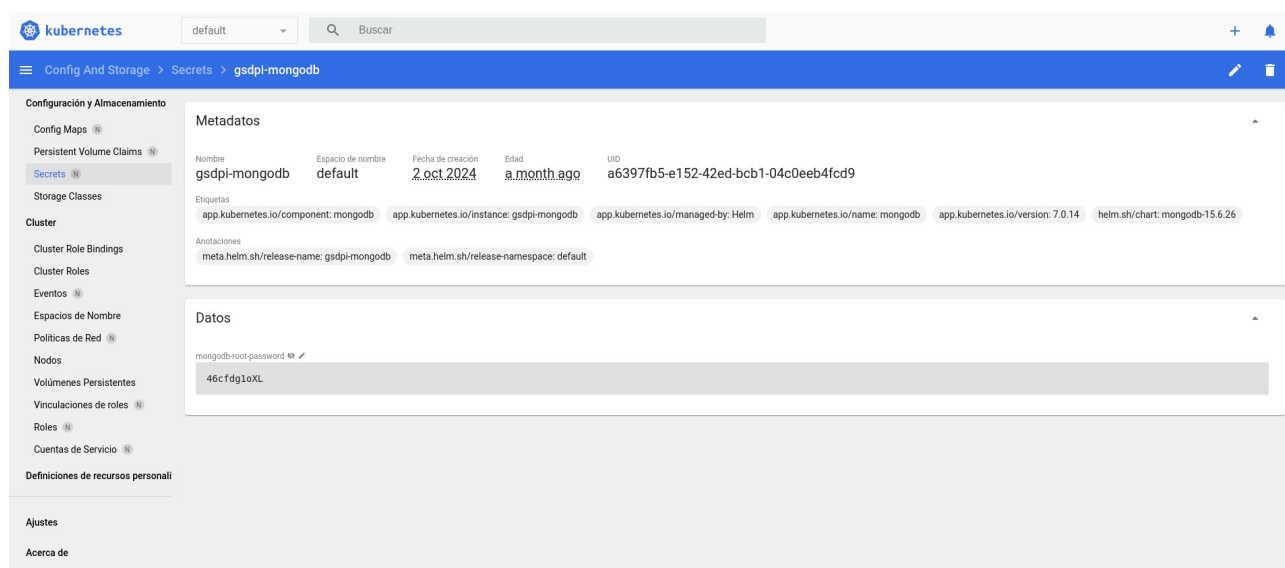
```
$ helm repo add bitnami https://charts.bitnami.com/bitnami
```

Por defecto no hemos escogido el namespace en donde desplegar estos recursos, pero escogera el de por defecto en Kubernetes llamado default. Tras unos segundos todos los recursos de la base de datos estarán desplegados en el cluster como se puede ver en la imagen siguiente:



Una vez desplegada la base de datos, debemos de recuperar las credenciales y el nombre del servicio, pues estos dos datos serán los que deberemos de utilizar a la hora de configura los microservicios que tengan que acceder a este recurso.

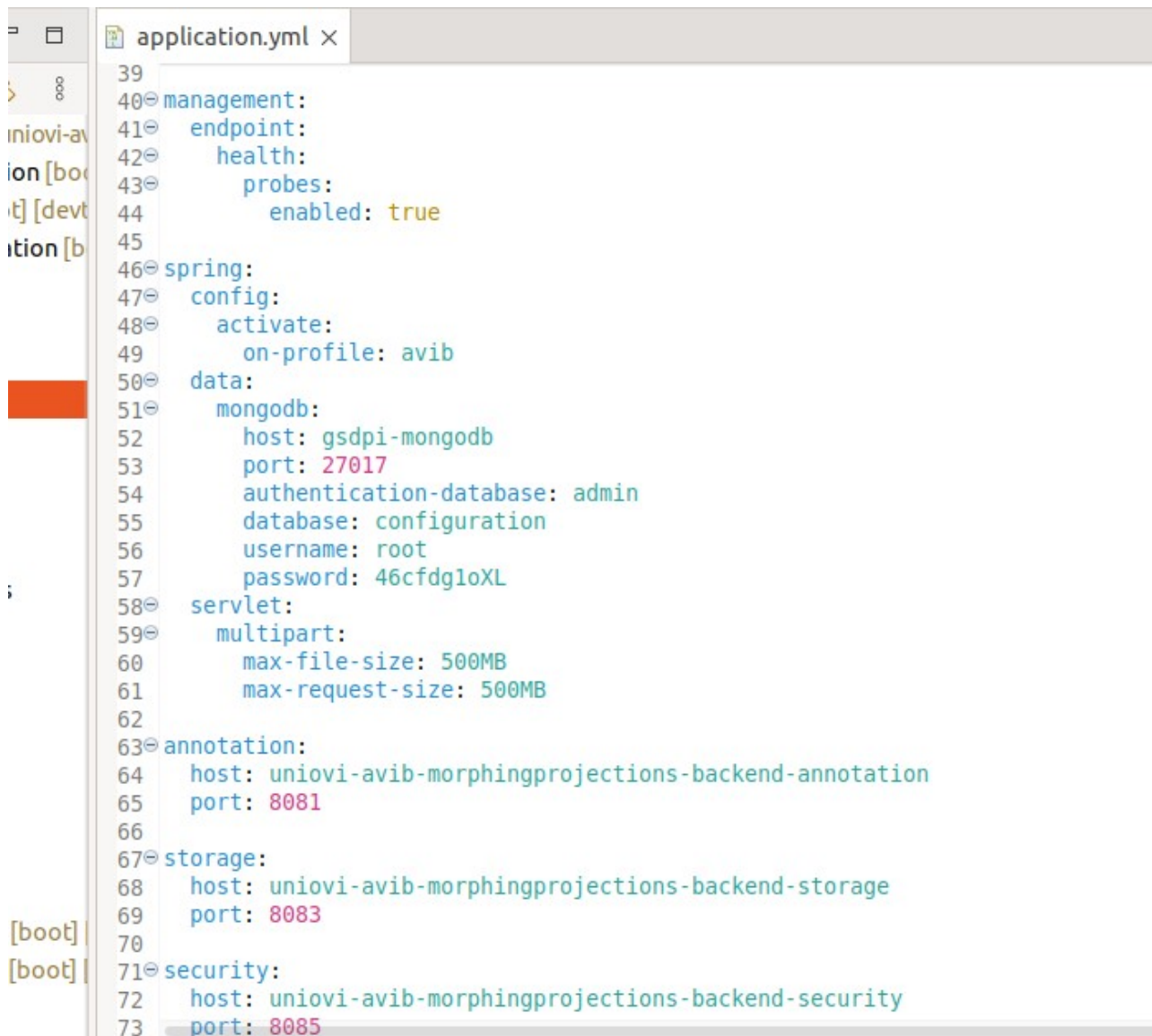
Las credenciales se pueden obtener del secreto creado en el proceso de despliegue llamado **gsdpi-mongodb** como se puede ver en la siguiente imagen, este es la clave del usuario de root con su clave, y esta será la cuenta que utilizaremos para nuestros microservicios:



Por último el servicio representa el nombre DNS interno que estos microservicios utilizaran para comunicarse con la base de datos, lo podemos consultarlo bajo el

servicio creado por el paquete helm llamado **gsdpi-mongodb**. Este nombre es el que utilizaremos como hemos dicho a la hora de configurar los micros de Java y Python que tengan que conectarse a la base de datos para manejar su estado.

Por ejemplo aquí podemos ver la configuración del microservicio de organización que gestiona su estado gracias a esta base de datos como se puede ver en la imagen inferior para el entorno de producción:



```
39
40 management:
41   endpoint:
42     health:
43       probes:
44         enabled: true
45
46 spring:
47   config:
48     activate:
49       on-profile: avib
50   data:
51     mongodb:
52       host: gsdpi-mongodb
53       port: 27017
54       authentication-database: admin
55       database: configuration
56       username: root
57       password: 46cfdgloXL
58   servlet:
59     multipart:
60       max-file-size: 500MB
61       max-request-size: 500MB
62
63 annotation:
64   host: uniovi-avib-morphingprojections-backend-annotation
65   port: 8081
66
67 storage:
68   host: uniovi-avib-morphingprojections-backend-storage
69   port: 8083
70
71 security:
72   host: uniovi-avib-morphingprojections-backend-security
73   port: 8085
```

Despliegue servicio IAM: keycloak

En este apartado vamos a explicar como desplegar este otro servicio de vital importancia desde el punto de vista de la seguridad del sistema, pues es el que implementa la especificación OAuth 2.1. Esta herramienta desarrollada y mantenida por Red-Hat es la versión Open Souce de su hermano comercial llamado RH-SSO desplegable en Openshift.

Al igual que en el caso anterior, el despliegue de este tipo de servicios es complejo y por ellos nos hemos apoyado nuevamente en los paquetes de helm mantenidos en este caso por Red-Hat. Al igual que en el caso anterior este paquete está mantenido por el repositorio privado de Bitnami, por lo que el repo ya lo tendremos dado de alta, como hemos explicado en el punto anterior. En este caso el comando que ejecutaremos será este:

```
$ helm install avib-keycloak --values values.yaml oci://registry-1.docker.io/bitnamicharts/keycloak
```

En este caso si hemos configurado algunos atributos que por defecto no existen y son de vital importancia, pues en este caso Keycloak debe de ser accesible através de un proxy corriendo en el host implementado por HAProxy. Estos parámetros se definen en un fichero que por defecto se llama values.yaml, en donde se pueden configurar estos parámetros extras necesarios en nuestro caso. El contenido de este fichero es este:

auth:

adminUser: admin

adminPassword: password

proxyHeaders: forwarded

En este caso hemos definido:

- Las credenciales del usuario admin con privilegios al Admin Console de Keycloak. Esta herramienta Web es la encargada de gestionar keycloak. La utilizaremos inicialmente para:
 - Crear nuestro Tenant, llamados por Keycloak como realms,
 - Crear los roles por defecto que el sistema maneja: ADMIN, USER y GUEST.
 - Crear el cliente que representa al microservicio que tiene acceso a Keycloak para poder autenticar a los usuarios, es decir, el microservicio Portal.
 - Existe otro microservicio que también necesita autenticarse actuando también como cliente, este microservicio es el de Security, pues es el encargado de gestionar los usuarios de nuestras organizaciones en el sistema, creando, actualizando o borrando los mismos. También este micro se encarga de modificar nuestra clave si fuera necesario. En este caso utilizaremos la misma cuenta de admin con privilegios suficientes a la hora de manejar estos recursos dentro del servicio de Keycloak.

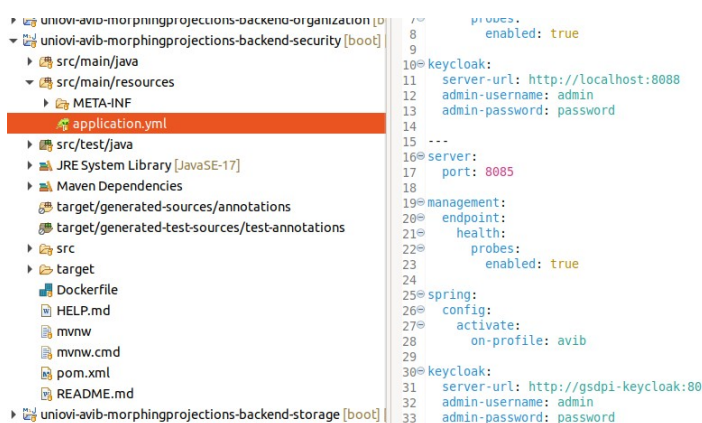
Para poder acceder al Admin Console hemos creado una regla de ingress para que su acceso sea directo desde internet. El acceso a esta herramienta es importante, en caso de que tengamos que borrar crear cuentas de emergencia, aunque como ya se ha comentado anteriormente el propio sistema AVIB cuenta con un módulo encargado de manejar estos recursos: usuarios y claves.

El acceso al Admin Console de Keycloak es a través de esta URI

<http://avispe.edv.uniovi.es/>

La cuenta de admin es la configurada previamente en el fichero de values.yaml. Mucho cuidado con cambiar esta clave por defecto, pues ya se ha comentado que el microservicio de Security la utiliza, y el cambio de la misma provocará que este micro ya no pueda desarrollar su trabajo. En caso de querer modificarla deberemos de modificar este dato en el micro y redespugarlo.

Aquí se puede ver esta configuración en el microservicio de Security:



Una vez desplegado Keycloak debemos de configurarlo utilizando la herramienta llamada **Admin Console** debemos de crear estos recursos para nuestro tenant

- Primero creamos un realm llamado avib, como se puede ver en la imagen inferior. Este dato es importante pues será utilizado por el microservicio Portal para autenticar cualquier usuarios

⚠ You are logged in as a temporary admin user. To harden security, create a permanent admin account and delete the temporary one.

KEYCLOAK

admin

avib

Manage

Clients

Client scopes

Realm roles

Users

Groups

Sessions

Events

Configure

Realm settings

Authentication

Identity providers

User federation

avib

Enabled

Action

General

Login

Email

Themes

Keys

Events

Localization

Security defenses

Sessions

Tokens

Client policies

User profile

User registration

Realm name *

avib

Display name

HTML Display name

Frontend URL ⓘ

Require SSL ⓘ

External requests

ACR to LoA Mapping ⓘ

No ACR to LoA Mapping have been defined yet. Click the below button to add ACR to LoA Mapping, key and value are required for a key pair.

Add ACR to LoA Mapping

User-managed access ⓘ

Off

Organizations ⓘ

Off

Save

Revert

- Una vez creado este realm, ya podremos crear los siguientes recursos. Primero los roles del realm, que como sabemos son tres: ADMIN, USER y GUEST.

⚠ You are logged in as a temporary admin user. To harden security, create a permanent admin account and delete the temporary one.

KEYCLOAK

admin

avib

Manage

Clients

Client scopes

Realm roles

Users

Groups

Sessions

Events

Configure

Realm settings

Authentication

Identity providers

User federation

Realm roles

Realm roles are the roles that you define for use in the current realm. [Learn more](#)

Q Search role by name

→

Create role

Refresh

1-6 < >

Role name	Composite	Description	
ADMIN	False	Admin Role	⋮
default-roles-avib ⓘ	True	role_default-roles	⋮
GUEST	False	Guest Role	⋮
offline_access	False	role_offline-access	⋮
uma_authorization	False	role_uma_authorization	⋮
USER	False	User Role	⋮

1-6 < >

- Y por último el cliente, que utilizará este realm para poder autenticar a los usuarios y gestionar sus AccessTokens de seguridad. Este cliente se llamará **portal-cli** y será otro dato importante a la hora de configurar el micro de portal. Debemos de configurar la URI que representa este cliente en nuestro caso **avispe.uniovi.es** como se puede ver en la captura inferior

⚠ You are logged in as a temporary admin user. To harden security, create a permanent admin account and delete the temporary one.

KEYCLOAK

admin

avib

Manage

Clients

Client scopes

Realm roles

Users

Groups

Sessions

Events

Configure

Realm settings

Authentication

Identity providers

User federation

Settings Roles Client scopes Sessions Advanced

General settings

Client ID *

portal-cli

Name

portal_cli

Description

Avispe Portal

Always display in UI

Off

Access settings

Root URL

https://avispe.edv.uniovi.es

Home URL

https://avispe.edv.uniovi.es

Valid redirect URIs

https://avispe.edv.uniovi.es/*
Add valid redirect URIs

Valid post logout redirect URIs

https://avispe.edv.uniovi.es/*
Add valid post logout redirect URIs

Web origins

https://avispe.edv.uniovi.es/*

Jump to section

General settings

Access settings

Capability config

Login settings

Logout settings

Save

Revert

- Por último vamos a crear un solo usuario administrador llamado **administrator** con clave **password**, con role ADMIN. Este usuario será unico en el sistema y es el único que puede crear organizaciones. El sistema solo permite crear usuarios de tipo USER y GUEST que pueden crear todo tipo de recursos a excepción de Organizaciones. De esto se hablará mas en detalle en el documento funcional que acompaña este documento técnico.

KEYCLOAK

admin

avib

Manage

Clients

Client scopes

Realm roles

Users

Groups

Sessions

Events

Configure

Realm settings

Authentication

Identity providers

User federation

Users > User details

administrator

Enabled Action

Details

Credentials

Role mapping

Groups

Consents

Identity provider links

Sessions

ID *

7ac64c68-faa8-456a-8d4b-9d14d7e350c6

Created at *

10/21/2024, 12:06:54 PM

Required user actions

Select action X

Email verified

On

General

Username *

administrator

Email

administrator@gsdpi.com

First name

Administrator

Last name

Portal

Jump to section

General

Save

Revert

Despliegue servicio Object Storage: Minio

Ya por último será necesario instalar el Object Storage implementado por Minio. Este servicio se encarga de manejar todos los datasets de nuestros casos en formato csv. Igualmente el resultado de la proyección de los mismo utilizando el algoritmo t-SNE o siendo previamente ya creado externamente a la herramienta, serán también ficheros csv manejados por esta herramienta de forma segura y consumidos por los clientes Portal, servicios de analítica y por los procesos Jobs encargados de proyectar los datasets de entrada. Para mayor detalle sobre estos datasets y su forma, se aconseja leer los primeros capítulos de este documento.

Como en casos anteriores este servicio consta de varios recursos de Kubernetes, difíciles de ser desplegados de forma individual, por lo que buscaremos el paquete de helm que nos facilite las cosas. Este caso es un poco diferente al anterior, pues a la hora de desplegar el servicio de Minio utilizaremos otra especificación de Kubernetes llamada Operadores. Estas aplicaciones son constructores de aplicaciones, en nuestro caso este operador se encarga de crear tenants de Minio, concepto semejante al hablado en el capítulo anterior, y al mismo tiempo cuenta con una herramienta capaz de monitorizar y gestionar visulamente todos los buckets (carpetas) y keys (ficheros) almacenados por Minio. Es una herramienta útil para poder ver estos recursos, aunque el sistema AVIB cuenta con su propio módulo de gestion de recursos integrados con los casos. **Por lo que no se recomienda ni crear ni borrar estos recursos directamente desde Minio**, pues esta herramienta como es lógico no está integrada con AVIB y no sabe nada relacionado con los casos. Se puede utilizar para monitorizar y visualizar los recursos, pero nunca modificarlos.

Para desplegar Minio ejecutaremos este comando de helm:

```
$ helm install avib-minio-operator --namespace minio-operator --create-namespace minio-operator/operator
```

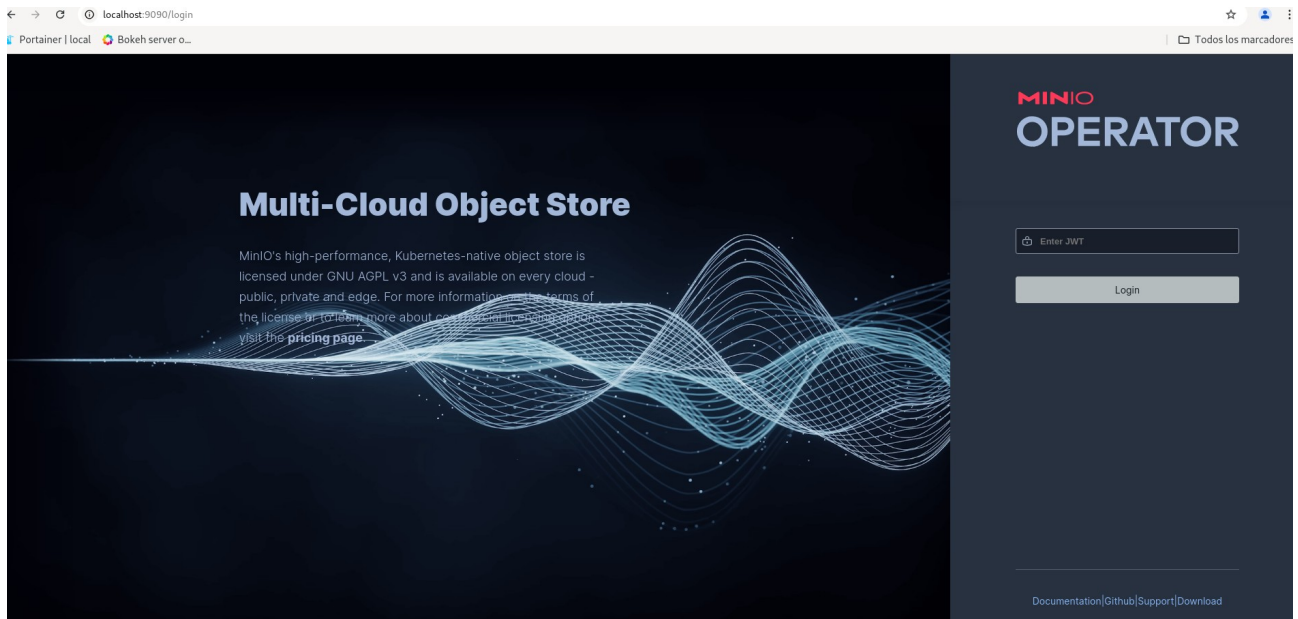
En este caso el repositorio utilizado no será el de Bitnami sino el oficial de Minio por lo que deberemos de registrar este repositorio antes de ejecutar el comando anterior:

```
$ helm repo add minio-operator https://operator.min.io
```

Tras unos segundos todos los recursos del operador serán instalados en este caso bajo el namespace de **minio-operator**. Se ha escogido este namespace pues esta herramienta no interviene directamente en la implementación del sistema, sino que es una herramienta auxiliar necesaria para crear el Tenant. Al igual que en caso anterior tras desplegar el operador debemos de crear el tenant para AVIB con unos recursos concretos. A diferencia del caso anterior esta herramienta no será accesible externamente, evitando puntos de acceso no necesarios, por lo que para poder acceder temporalmente para crear este Tenant, crearemos en el host un reverse proxy temporal como se ve en este comando:

El puerto de acceso al operador es 9090, para poder acceder a esta herramienta Web necesitamos la credenciales de admin, a diferencia al caso anterior hemos dejado que el paquete de helm cree un token aleatorio en este despliegue que puede ser consultado como secreto en el namespace de minio-operator. Este secreto se llama **console-sa-secret** y si lo abrimos utilizando el Dashboard veremos el valor de este token como se en la captura inferior:

Este valor será el utilizado a la hora de acceder a la consola de Administrador del Operador de Minio a través de la URI <http://localhost:9090>



Introducimos este token y ya podremos crear el Tenant para nuestro sistema:

Aquí podemos ver los valores escgidos a la hora de crear ese Tenant:

Estos son los datos del tenant:

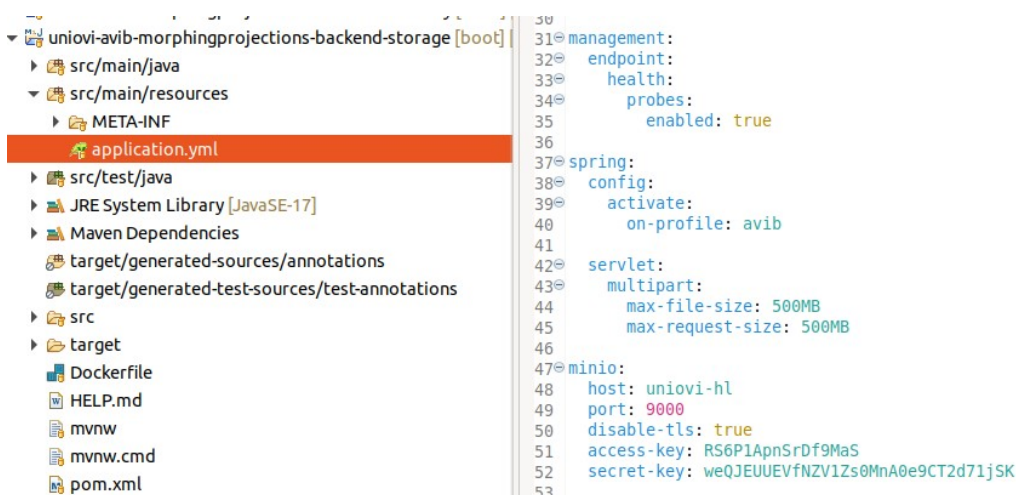
- Name: uniovi
- Namespace: default
- Number of Servers: 1
- Drives per Server (Volumes): 4

- Total Size (Size per drive): 30Gb
- Erasure Code Priority: EC:2 (Default).
- CPU Request: 2.
- Memory Request: 2.

Cuando guardemos el operador va a crear otros recursos de Kubernetes que representan al tenant, bajo el puerto por defecto 9000 en el namespace default, junto a los otros recursos. Al igual que en el caso de MongoDB el acceso a este recurso se guarda en forma de secretos que podemos recuperar, pues estos serán las credenciales utilizadas por el microservicio que se comunican con Minio. El microservicio de storage utilizado por:

- El Portal para gestionar la ingesta, gestión de los recursos de los casos y visualización del resultado proyectados
- El microservicio que implementa el algoritmo de proyección t-SNE, pues debe recuperar estos recursos y proyectarlos en 2D siguiendo la configuración previamente creada para nuestros casos.
- El microservicio que implementa algoritmos de analítica tipo histogramas y regresiones lineales sobre las muestras de los datasets ingestados previamente.

Para recuperar estas credenciales en el momento de crear el tenant el sistema te avisa que va a crear unas credenciales (access_key, secret_key) en formato json y que las guardes, pues estas serán las utilizadas a la hora de configurar el acceso al tenant recién creado para el sistema AVIB. Por ejemplo en esta captura se puede ver como se configura el microservicio de storage con estas credenciales :



```

30
31 management:
32   endpoint:
33     health:
34       probes:
35         enabled: true
36
37 spring:
38   config:
39     activate:
40       on-profile: avib
41
42 servlet:
43   multipart:
44     max-file-size: 500MB
45     max-request-size: 500MB
46
47 minio:
48   host: uniovi-hl
49   port: 9000
50   disable-tls: true
51   access-key: RS6P1ApnSrDf9MaS
52   secret-key: weQJEUUEVfNZV1Zs0MnA0e9CT2d71jsK
53

```

Configuraciones Kubernetes post-despliegue

Una vez desplegado el cluster de Kubernetes, y desplegados los addons necesarios para monitorizar los despliegues y permitir el acceso externo al cluster a nuestros servicios por medio del Ingress. Solamente nos queda por configurar un solo recurso muy importante y este es el acceso al Registro Privado de Contenedores de Azure.

Como explicaremos con mas detalles en capitulos posteriores, todos nuestros servicios de negocio, están empaquetados como imágenes de docker que pueden ser desplegadas en el cluster de Kubernetes. Pero estas imágenes residen en un repositorio espacial capaz de manejar y servir estas imágenes. Pero este repositorio es privado como es lógico, controlado por la infraestructura de Azure bajo una cuenta o service account con sus credenciales. En el momento que queramos desplegar una de estas imágenes utilizando un paquete de helm, este servicio encargado de desplegar todos los recursos necesarios, no solo la imagen sino otros mas, que se hablan de ellos posteriormente, tiene que conectarse al registro privado e Azure con estas credenciales.

Estas credenciales se guardan como un recurso especial dentro del cluster llamado **Image Pull Secret**, que representa las credenciales de acceso a la infraestructura de Azure y en concreto al servicio de Container Registry donde residen todas la paquetes de helm y las imágenes de docker que maneja cada uno de ellos. Este recurso ha de ser desplegado manualmente desde la consola utilizando el CLI de Kubernetes ejecutando este comando:

```
$ kubectl create secret docker-registry acr-avib-secret --docker-server=avibdocker.azurecr.io --
docker-username=avibdocker --docker-
password=BAqBdHVbrSmPOxH96lGHlcze7gx8lclS WJNxFyx/c+ACRB1+L5M
```

Este comando indica el nombre que le hemos dado a estas credenciales, en nuestro caso **acr-avib-secret**, este nombre es importante, pues este dato deberá de ser configurado en todos los paquetes de helm, para indicar a este servicio donde se encuentran las credenciales que debe utilizar para validarse contra Azure y bajar los paquetes de helm y las imágenes de docker que maneja cada uno de ellos. Igualmente se indica el nombre del host asociado con el espacio dentro del servicio privado del Container Registry que hemos creado en Azure para gestionar nuestros artefactos: imágenes y paquetes de helm llamado **aviddocker.azurecr.io** y por último las credenciales como es de esperar el username **avibdocker** y la password de de este servicio que nos da acceso al mismo.

Tenemos que tener en cuenta que este secreto con estas credenciales debe de existir en todos los namespace en donde despleguemos nuestros servicios. Como el cluster es solamente utilizado por lo servicios del sistema AVIB, todos los servicios son desplegados en el namespace por defecto llamado default. Es aquí en este namespace donde debemos de crear este recurso como se puede ver en la imagen siguiente:

The screenshot shows the Kubernetes dashboard interface. The top navigation bar includes the 'kubernetes' logo, a dropdown menu set to 'default', a search bar, and a notification bell. The main content area is titled 'Config And Storage > Secrets > acr-avib-secret'. On the left sidebar, under 'Configuración y Almacenamiento', the 'Secrets' link is highlighted. The main panel displays the details for the 'acr-avib-secret' resource. It includes a 'Metadatos' section with a table showing the secret's name, namespace, creation time, age, and UID. Below this is a 'Datos' section showing the secret's data in a base64-encoded format, which is decoded to show the Docker configuration JSON. The URL at the bottom of the page is '127.0.0.1:35217/api/v1/namespaces/kubernetes-dashboard/services/http:kubernetes-dashboard/proxy/#/secret/default/acr-avib-secret?namespace=default&container=uniovi-avib-morphingprojections-backend-analytics'.

Nombre	Espacio de nombre	Fecha de creación	Edad	UID
acr-avib-secret	default	2 oct 2024	a month ago	b8615ab7-3162-4f9d-b50e-ed2a6e1ed7c9

```
dockerconfigjson: {"auths":{"avibdocker.azurecr.io":{"username":"avibdocker","password":"BaqBdHvbrSmPoxH96LGHlcze7gx8LcIsWJNxFyx/c+ACRB1+LSM","auth":"YXZpYmRvY2t1cjc0QXFCZEhWYnJTbVBPeEg5NmoxH5GxjemU3Z3g4bGdU3c1dkTnNVRn14L2MfQUN5QjE7TDVN"}}}
```

Configuración reverse-proxy: HAProxy

Introducción

Como ya se ha comentado la herramienta AVIB esta corriendo en un nodo compartido por otras herramientas. Igualmente el acceso al cluster debe ser direccionado por un proxy, en nuestro caso hemos escogido HAProxy por estas razones:

- Es una herramienta OpenSource ampliamente utilizada en el mercado, con un soporte duradero.
- Tiene una documentación excepcional, si la comparamos con otras opciones como son Nginx o Apache Web.
- Tiene una comunidad amplia con muchos ejemplos, que pueden ser consultados fácilmente
- Tiene una sintaxis y configuración, mucho mas amigable sin la comparamos con las otras herramientas.
- Es fácilmente empaquetable como contenedor Docker
- A nivel de performance es muy parecido a NGInx y superior a Apache

Configuración kubernetes ingress

A la hora de configurar las reglas del ingress debemos de tener muy presente que servicio vamos a configurar y que conexión tiene con el proxy del Host implementado por HAProxy.

En principio de todos los servicios que corren en kubernetes solamente vamos a exponer tres servicios, aunque realmente podríamos hacer solo dos. Vamos a listar estos servicios:

- **Portal del sistema:** este servicio de negocio de frontend implementado bajo el nombre **uniovi-avib-morphingprojections-portal:<VERSION>** representa el frontend del sistema, es decir, la interfaz gráfica utilizada por los usuarios para interactuar con el sistema.
- **Gateway del sistema:** este servicio de negocio de backend implementado bajo el nombre **uniovi-avib-morphingprojections-backend<VERSION>** representa la puerta de entrada a todos los servicios de negocio del sistema, utilizado por portal para poder interactuar con el backend en todo momento y el resto de servicios de infraestructura del mismo
- **Gestor de autenticación y autorización del sistema:** este servicio de negocio de seguridad implementado por la herramienta Keycloak, bajo el nombre **gsdpi-keycloak-0<VERSION>** es el servicio encargado de gestionar las cuentas de usuario y la autenticación y autorización de las mismas implementado la especificación OAuth 2.1

Deberemos de crear una regla de redireccionamiento para cada uno de estos servicios tanto para cargar el portal, como para que este pueda autenticarse y posteriormente pueda acceder a todos los recursos del sistema implementados por todos los microservicios de negocio a través del gateway.

Aunque Ingress es una especificación como ya se ha comentado la forma y implementación de la misma puede diferenciarse un poco de un producto a otro. Nosotros utilizaremos el ingreso de NGInx por ser la de referencia y la ofrecida por Minikube como add-on.

Reglas de ingress

- **Paso 01: Regla de ingress para servicio Keycloak**

En este caso el servicio de Keycloak está desplegado en el Webcontext / (raíz), por lo que en este caso la regla para este servicio se puede expresar como esto bajo el fichero llamado avispe-keycloak.ingress.yaml

```
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: avib-keycloak-ingress
spec:
  rules:
  - host: avispe.edv.uniovi.es
    http:
      paths:
      - path: /
        pathType: Prefix
        backend:
          service:
            name: gsdpi-keycloak
            port:
              name: http
```

Lo más destacado de esta regla es:

- El nombre del **host** que debe de coincidir con el DNS ofrecido por el departamento a la hora de identificar nuestros servicios
- El **path** absoluto / (raíz) bajo el cual el servicio de Keycloak esta desplegado en Kubernetes
- El **nombre y puerto del servicio** de kubernetes representando a la herramienta Keycloak desplegada, en nuestro caso se llama **gsdpi-keycloak** y el puerto es el representado por el nombre **http** del mismo, en concreto se puede ver en kubernetes que es el 80, pero utilizando el nombre de forma indirecta es mas sencillo desacoplándonos del numero en concreto.

- **Paso 02: Regla de ingress para servicio Portal**

En este caso el servicio de Portal está desplegado en el Webcontext **/morphingprojections-portal**, por lo que en este caso la regla para este servicio se puede expresar como esto bajo el fichero llamado `avispe-portal.ingress.yaml`:

```
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: avib-portal-ingress
  annotations:
    nginx.ingress.kubernetes.io/use-regex: "true"
    nginx.ingress.kubernetes.io/rewrite-target: /$2
spec:
  rules:
    - host: avispe.edv.uniovi.es
      http:
        paths:
          - path: /morphingprojections-portal(/|$)(.*)
            pathType: ImplementationSpecific
            backend:
              service:
                name: uniovi-avib-morphingprojections-portal
                port:
                  name: http
```

Lo mas destacado de esta regla es:

- El nombre del **host** que debe de coincidir con el DNS ofrecido por el departamento a la hora de identificar nuestros servicios al igual que antes.
- El **path relativo morphingprojections-portal** bajo el cual el servicio de Keycloak esta desplegado en Kubernetes y todas las páginas ofrecidas por el mismo. De ahí el utilizar reglas de tipo regex para el redireccionamiento
- El **nombre y puerto del servicio** de kubernetes representando a la herramienta Keycloak desplegada, en nuestro caso se llama **uniovi-avib-morphingprojections-portal** y el puerto es el representado por el nombre **http** del mismo.

- **Paso 03: Regla de ingress para servicio Gateway**

En este caso el servicio de Portal está desplegado en el Webcontext /morphingprojections-portal, por lo que en este caso la regla para este servicio se puede expresar como esto bajo el fichero llamado avispe-backend.ingress.yaml

```
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: avib-backend-ingress
  annotations:
    nginx.ingress.kubernetes.io/use-regex: "true"
    nginx.ingress.kubernetes.io/rewrite-target: /$2
    nginx.ingress.kubernetes.io/proxy-body-size: 500M
spec:
  rules:
    - host: avispe.edv.uniovi.es
      http:
        paths:
          - path: /morphingprojections-backend(/|$)(.*)
            pathType: ImplementationSpecific
            backend:
              service:
                name: uniovi-avib-morphingprojections-backend
                port:
                  name: http
```

Lo más destacado de esta regla es:

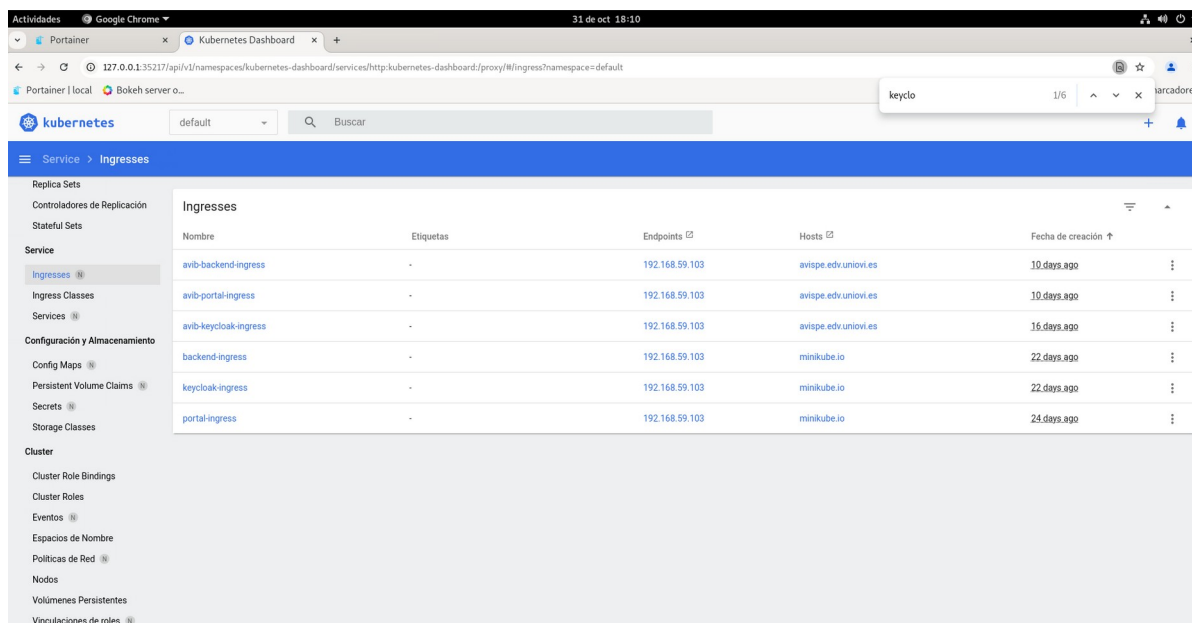
- El nombre del **host** que debe de coincidir con el DNS ofrecido por el departamento a la hora de identificar nuestros servicios al igual que antes.
- El **path relativo morphingprojections-backend** bajo el cual el servicio de Keycloak esta desplegado en Kubernetes y todas las páginas ofrecidas por el mismo. De ahí el utilizar reglas de tipo regex para el redireccionamiento
- El **nombre y puerto del servicio** de kubernetes representando a la herramienta Keycloak desplegada, en nuestro caso se llama **uniovi-avib-morphingprojections-backend** y el puerto es el representado por el nombre **http** del mismo.
- En este caso particular hay un **atributo llamado proxy-body-size** extra importante que son los megas máximo permitos a procesar en una petición a

través del ingress en este caso se ha puesto a 500Mb para permitir subir ficheros de entrada grandes.

Todas estas reglas deberán de ser desplegada en kubernetes utilizando el CLI de kubectl con este comando:

```
$ kubectl apply -f avispe-keycloak.ingress.yaml
$ kubectl apply -f avispe-portal.ingress.yaml
$ kubectl apply -f avispe-backend.ingress.yaml
```

Una vez desplegadas se pueden consultar utilizando el CLI kubectl o desde el Dashboard de Kubernetes en el namespace default:



Nombre	Etiquetas	Endpoints	Hosts	Fecha de creación
avib-backend-ingress	-	192.168.59.103	avispe.edv.uniovi.es	10 days ago
avib-portal-ingress	-	192.168.59.103	avispe.edv.uniovi.es	10 days ago
avib-keycloak-ingress	-	192.168.59.103	avispe.edv.uniovi.es	16 days ago
backend-ingress	-	192.168.59.103	minikube.io	22 days ago
keycloak-ingress	-	192.168.59.103	minikube.io	22 days ago
portal-ingress	-	192.168.59.103	minikube.io	24 days ago

Despliegue servicios de negocio

Introducción

Como ya se ha comentado todos los servicios de negocio se han empaquetado como paquetes de tipo Chart para ser desplegados por el CLI de Helm. Todos los servicios están formados por tres recursos:

- **Deployment:** gestión de la replicas del Pod
- **POD:** gestión del contenedor de Docker que empaqueta el servicio de negocio
- **Service:** acceso al servicio desde dentro del cluster y por las reglas del ingres en caso de ser necesario

Solamente el microservicio de Job tiene un recurso extra, llamado **service account**, pues este servicio debe de interactuar con Kubernetes bajo demanda para crear los jobs que el frontend le solicita, por ellos este service account tiene los roles y permisos necesarios para crear estos recursos de Kuberbetes llamados Jobs.

Todos estos recursos deberán de ser definidos en un paquete de tipo Chart y empaquetados y publicado como si de una imagen de Docker se tratara en Azure. Es mas todos estos principalmente son responsables de crear el contenedor asociado al mismo y por lo tanto deberán de bajarse la imagen de Docker correspondiente de Azure en el momento de Despliegue.

Listado de paquetes Helm

Vamos a ver como en el caso de los servicios de negocio hemos diseñado nosotros cada uno de estos paquetes, por contra en el caso de los servicio de infraestructura estos ya han sido diseñados por la propia casa: Base de Datos, Keycloak, etc

Acceso al Service Registry de Azure

Actualmente el número de recursos y servicios es enorme, pero como ya se ha comentado en apartados anteriores, solamente vamos a utilizar un recurso controlado por Azure y es el **Azure Container Registry**, que es el servicio en donde vamos a alojar todas las imágenes correspondientes a los microservicios de negocio del sistema. El resto de servicios de infraestructura formado por Bases de Datos, Gestores de Objetos o Servicios de Autenticación y Autorización, sus imágenes estarán gestionadas por registros de imágenes públicos y no por nosotros.

Con todo esto deberemos de tener acceso al portal de Azure para:

1. Toda imagen desarrollada localmente deberá de ser publicada en este registro privado de Azure
2. El cluster en el momento de desplegar una de estas imágenes deberá el tener también acceso al registro privado, por ello deberemos de crear dentro del cluster en el namespace donde despleguemos nuestras imágenes un recurso de tipo secreto en donde almacenemos las credenciales de acceso a nuestra cuenta de Azure

Acceso local a Azure

Como hemos comentado en el punto 1, localmente el equipo que utilicemos para compilar y publicar la imagen resultante de nuestro microservicio deberá de tener acceso a Azure con las credenciales correctas, para que en el momento de la publicar la imagen Azure nos de acceso al Container Registry.

Para poder autenticarnos contra Azure utilizaremos el CLI de azure llamado az, que podrá instalarse fácilmente, como podemos ver en la página de Microsoft, en este caso para un entorno [Linux](#)

```
$ curl -sL https://aka.ms/InstallAzureCLIDeb | sudo bash
```

Esto nos instalará en el entorno un CLI llamado az, como se puede ver viendo la versión del mismo:

```
$ az --version
azure-cli          2.23.0 *
```

```
core              2.23.0 *
telemetry         1.0.6
```

```
Extensions:
azure-devops      0.18.0
```

```
Python location '/opt/az/bin/python3'
Extensions directory '/home/miguel/.azure/cliextensions'
```

```
Python (Linux) 3.6.10 (default, Apr 29 2021, 12:10:04)
[GCC 9.3.0]
```

Legal docs and information: aka.ms/AzureCliLegal

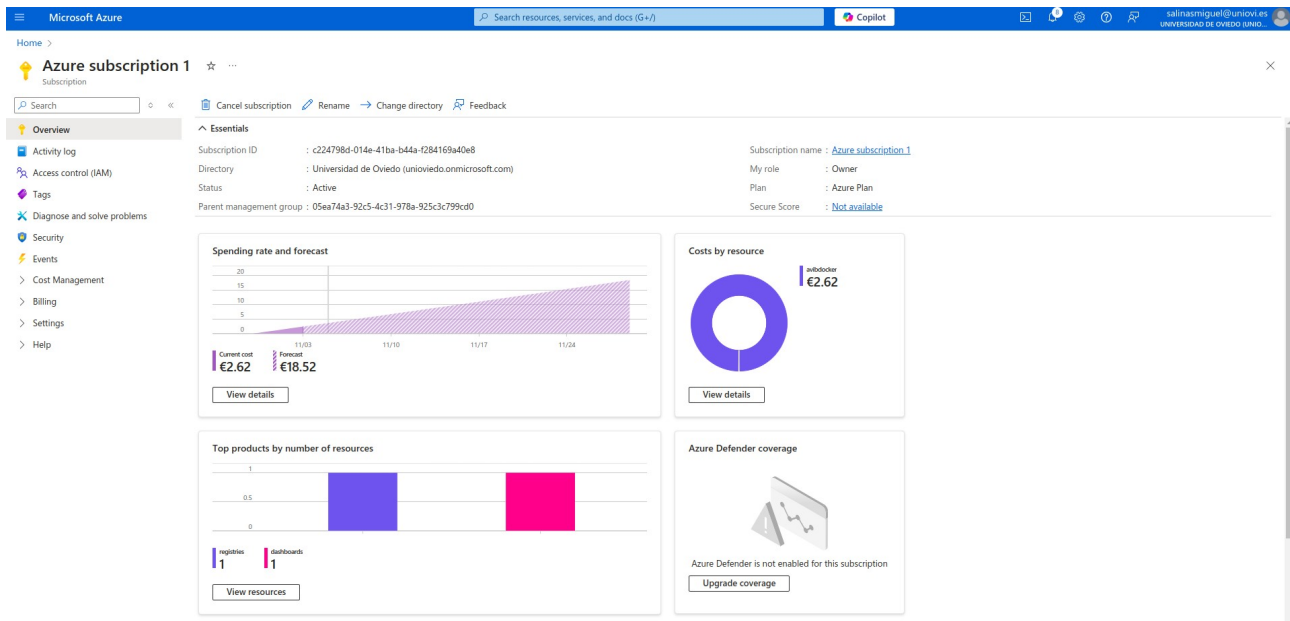
You have 2 updates available. Consider updating your CLI installation with 'az upgrade'

Please let us know how we are doing: <https://aka.ms/azureclihats>
and let us know if you're interested in trying out our newest features:
<https://aka.ms/CLIUXstudy>

Ahora solamente nos toca logearnos en la plataforma

```
$ az login
```

Esto nos abrirá un Login Web desde donde podremos meter nuestras credenciales para acceder a la suscripción de nuestro Directorio (Tenant). Como utilizaremos nuestras mismas cuentas de la Universidad de Oviedo, nuestro Directorio se llama **Universidad de Oviedo** y dentro de el hemos creado una suscripción propia para nuestro Sistema llamada **Azure subscription 1** como se puede ver en la siguiente captura:



Esta suscripción sirve para agrupar de forma lógica todos los recursos Azure que estamos utilizando para nuestro proyecto, que como se ha comentado solamente es el Registro Privado de Contenedores de Docker. Igualmente esta suscripción tiene asociado un owner, con un método de pago (tarjeta de crédito) que asume el gasto de los recursos utilizados.

Actualmente no se está cobrando nada pues el gasto incurrido hasta ahora solamente procede del Registro de Contenedores de Docker donde el espacio ocupado se está manteniendo al mínimo, sabiendo que estos gastos acumulados no deben de superar los 100 euros. En todo momento este owner puede ser cambiado por otra persona que asuma el método de pago y los gastos correspondiente si se superase ese límite de 100 euros.

Para ver todas las imágenes de Docker y gestionarlas, poder borrar versiones anteriores, para liberar espacio, por ejemplo, se ha creado dentro de nuestra suscripción, bajo el servicio Registro Privado de Contenedores un espacio llamado **avibdocker**, donde residen todas nuestras imágenes, como se puede ver en la siguiente captura:

Actualmente estas son las imágenes que manejamos. Podemos crear tres grupos:

- Grupo de imágenes para cada uno de nuestros microservicios:
 - **uniovi-avib-morphingprojections-backend**: Microservicio en Java Gateway
 - **uniovi-avib-morphingprojections-backend-analytics**: Microservicio en Python Analítica: histogramas, regresión lineal
 - **uniovi-avib-morphingprojections-backend-annotation**: Microservicio en Java configuración de anotaciones de casos

- **uniovi-avib-morphingprojections-backend-job:** Microservicio en Java que actúa como cliente de Kubernetes para lanzar y monitorizar las proyecciones de nuestros casos
- **uniovi-avib-morphingprojections-backend-organization:** Microservicio en Java que gestiona la organización, proyectos y casos
- **uniovi-avib-morphingprojections-backend-security:** Microservicio en Java que se integra con Keycloak como cliente, manteniendo usuarios y roles. Cliente del IAM Keycloak
- **uniovi-avib-morphingprojections-backend-storage:** Microservicio en Java que gestiona el acceso al Object Storage (Minio)
- **uniovi-avib-morphingprojections-job-projection:** este servicio implementa el algoritmo t-SNE y la lógica configurada a nivel de caso. Este proceso es disparado por el microservicio de **backend-job** en el momento que ejecutamos un caso.
- **Uniovi-avib-morphingprojections-portal:** este servicio implementa el Portal o interfaz de usuario con el cual el usuario interactúa a la hora de ingestar, ejecutar y explotar visualmente un caso.

Este otro grupo son los paquetes utilizados para desplegar cualquier servicio listado en el grupo anterior, podemos fijarnos como todos ellos están agrupados bajo la carpeta de helm, indicando que son precisamente paquetes de helm preparados para ser desplegados en el cluster de Kubernetes. Cada uno de ellos tiene encapsuladas las configuraciones propias de cada contenedor.

- helm/uniovi-avib-morphingprojections-backend
- helm/uniovi-avib-morphingprojections-backend-analytics
- helm/uniovi-avib-morphingprojections-backend-annotation
- helm/uniovi-avib-morphingprojections-backend-job
- helm/uniovi-avib-morphingprojections-backend-organization
- helm/uniovi-avib-morphingprojections-backend-security
- helm/uniovi-avib-morphingprojections-backend-storage
- helm/uniovi-avib-morphingprojections-portal

Por último podemos citar este último grupo que representan todos las imágenes que no son propias del sistema AVIB. Como ya hemos dicho varias veces, este sistema convive con otros servicios, en concreto con aplicaciones de tipo Bokeh, y esta imagen representa precisamente, la aplicación Bokeh llamada MP Tracción que sin correr dentro del cluster de Kubernetes, si corre como contenedor dentro del mismo host que el cluster:

- uniovi-gsdpi-bokeh-mp-traccion

Todos estos paquetes de Helm tienen en común el número de recursos creados por cada uno de ellos:

- **Deployment:** recurso encargado de crear replicas para los PODs que maneja. En nuestro caso hemos limitado la replica a uno, por ser suficiente para la carga de trabajo estimada para cada uno de ellos. El escalado de estos PODs y de sus contenedores internos es extramadamente sencillo hacerlo en caso de tener cargas de trabajo altas si fuera este el caso.
- **POD:** unidad mínima de despliegue de Kubernetes encargada de desplegar el contenedor propio manejado por el POD.
- **Service:** recurso de Kubernetes, encargado de balancear el acceso interno al contenedor que maneja

Solamente el paquete de helm llamado helm/uniovi-avib-morphingprojections-backend-job crea un recurso extra que los demás no hacen, y esto es un **service account** con los permisos necesarios, para que el microservicio que contiene pueda actuar de cliente de Kubernetes a la hora de crear y monitorizar los jobs encargados de ejecutar los algoritmos de proyección, como el t-SNE.

Microsoft Azure

Search resources, services, and docs (G+/I)

Copilot

salinasmiguel@uniovi.es
UNIVERSIDAD DE OVIEDO (UNED)

Home > avibdocker

avibdocker | Repositories

Container registry

Search

Refresh Manage Deleted Repositories

Overview

Activity log

Access control (IAM)

Tags

Quick start

Events

Settings

Services

Repositories

Webhooks

Geo-replications

Tasks

Connected registries (Preview)

Cache

Repository permissions

Tokens

Scope maps

Policies

Content trust

Retention (Preview)

Monitoring

Metrics

Diagnostic settings

New to ACR, Artifact streaming helps pull images faster from AKS clusters. The 'Artifact streaming status' column shows which repositories are using this feature. [Learn more](#)

Search to filter repositories ...

Repositories	Cache Rule
helm/uniovi-avib-morphingprojections-backend	...
helm/uniovi-avib-morphingprojections-backend-analytics	...
helm/uniovi-avib-morphingprojections-backend-annotation	...
helm/uniovi-avib-morphingprojections-backend-job	...
helm/uniovi-avib-morphingprojections-backend-organization	...
helm/uniovi-avib-morphingprojections-backend-security	...
helm/uniovi-avib-morphingprojections-backend-storage	...
helm/uniovi-avib-morphingprojections-portal	...
uniovi-avib-morphingprojections-backend	...
uniovi-avib-morphingprojections-backend-analytics	...
uniovi-avib-morphingprojections-backend-annotation	...
uniovi-avib-morphingprojections-backend-job	...
uniovi-avib-morphingprojections-backend-organization	...
uniovi-avib-morphingprojections-backend-security	...
uniovi-avib-morphingprojections-backend-storage	...
uniovi-avib-morphingprojections-job-projection	...
uniovi-avib-morphingprojections-portal	...
uniovi-gsdpi-bokeh-mp-traccion	...