

# manual sygox (extret del wiki de sistemes)

## Índex Manual Sygox (Usuari/Operacions/Desenvolupament)

### Sygox

[Introducció a Sygox i terminologia](#)

[Arquitectura de Sygox](#)

### Sygox Manual d'Usuari

Secció orientada als usuaris de Sygox com ara tècnics de la DTI, caps de projecte o desenvolupadors d'aplicacions PHP que hi tenen accés.

[Accés a Sygox](#)

[Trobar un desplegament a Sygox](#)

[Crear un desplegament PHP Consolidat a Sygox](#)

[Comprovar l'estat d'una tasca](#)

[Afegir i actualitzar les url d'un PHP Consolidat](#)

[Alta i edició de paràmetres PHP a un servidor consolidat](#)

[Baixa de paràmetres PHP a un servidor consolidat](#)

[Gestió d'usuaris SSHail i sFTP en desplegaments PHP Consolidats](#)

[Donar d'alta BD MySQL a un desplegament PHP Consolidat](#)

[Exportació i importació de bases de dades](#)

[Configuració de correu a un desplegament PHP Consolidat](#)

[Alta de un monitor HTTP a un PHP Consolidat](#)

[Baixa d'un monitor HTTP a un PHP Consolidat](#)

[Visualitzar estat dels monitors des de UptimeRobot](#)

[Alta d'un cron a un desplegament d'un servidor consolidat](#)

[Baixa d'un cron a un desplegament d'un servidor consolidat](#)

[Anonimitzar dump de sygox](#)

[Afegir noves dades a anonimitzar a l'script de anonimitzat](#)

[Gestió d'equips de Sygox](#)

[Gestió de repositoris amb Sygox](#)

[Gestió de PHPackages amb Sygox](#)

[Publicació dades feed opendata](#)

[Visualitzar escriptures de les aplicacions](#)

[Sincronització de permisos de Sygox](#)

[Baixa i Arxivat de desplegament amb Sygox](#)

[Alta, edició i eliminació de redireccions de campanya amb Sygox](#)

[Escàner de vulnerabilitats amb Trivy a Sygox](#)

[Escàner Mozilla Observatory a Sygox](#)

[Gestió d'un canary deploy: Alta, baixa i pas a producció](#)

## **Sygox Manual d'Operacions**

Secció orientada als administradors de Sygox els quals fan operacions avançades com desplegaments de codi i manteniment de la propia eina

[Actualitzar codi de l'aplicació](#)

[Preparació Sygox CLI](#)

[Donar d'alta un rol d'usuari](#)

[Donar d'alta usuari a l'aplicació](#)

[Accedir al PostgreSQL de producció](#)

[Modificació de camps tipus JSON a BD](#)

[Modificar els fils de PHP per a una aplicació](#)

[Afegir un servei docker associat a una aplicació](#)

[Exposar un servei docker al port 80 \(HAproxy\)](#)

[Debug de Sygox en producció](#)

[Extreure llistat ids d'aplicació consolidada i URL dels deployments](#)

[Gestió d'equips de Sygox per operadors APSL](#)

[Esborrar desplegament de la BD de Sygox](#)

[Desplegament dels SSHail](#)

[Afegir un nou servidor d'aplicacions a Sygox](#)

[Sygox en mode lectura](#)

[Canviar l'aplicació a la que pertany un desplegament a Sygox](#)

[Depurar plugin redireccions de campanya](#)

[esborrar-vinculaci0-repositori-aplicacio-php-consolidada-a-repositori-gitlab](#)

[Sygox canviar versió per defecte PHP](#)

## **Sygox Manual de Desenvolupament**

Secció orientada als desenvolupadors de Sygox, els quals n'amplien les seves funcionalitats.

[El model de dades](#)

[Entorn de desenvolupament local](#)

[Dump de la base de dades de dev](#)

[Flux de feina](#)

[Autenticació a l'entorn de desenvolupament de Sygox](#)

[Implementació dels permisos de Sygox](#)

[Llibreries de Sygox](#)

[Desenvolupament de plugins](#)

[Enllaços útils pel desenvolupament de Sygox](#)

---

# **Manual Sygox**

## **Sygox**

Introducció-a-Sygox-i-terminologia

**Sygox** és una eina de govern de sistemes, aplicacions i desplegaments amb l'objectiu és oferir una eina modular fàcil d'ampliar i ajustar a diferents arquitectures de sistemes i desplegaments.

Amb Sygox s'ofereix als usuaris una capa d'abstracció per tal de crear desplegaments d'aplicacions sense preocuparse de l'arquitectura o proveïdor de Infraestructura (servidors) on s'executen les aplicacions.

## Terminologia

- **Aplicació:** Una aplicació és un conjunt d'un o més desplegaments que comparteixen un propòsit. Les aplicacions tenen un nom. Tots els desplegaments estan associats a una aplicació i és habitual que una mateixa aplicació tingui diversos desplegaments, per exemple del de desenvolupament i el de producció.
- **Desplegament:** Un desplegament és la instància d'una aplicació desplegat sobre una plataforma. Els desplegaments no tenen nom, són identificats per la seva URL. Es poden executar accions sobre les desplegaments.
- **Plataforma:** Una plataforma és un tipus infraestructura de servidors on es poden efectuar desplegaments d'aplicacions. Cada plataforma té característiques tècniques concretes i tenen accions associades per executar sobre els desplegaments.
- **Acció:** Una acció és una operació que es pot efectuar sobre un desplegament. Tots els desplegaments tendan l'acció de creació. Les accions no sempre s'apliquen instantàniament, el més habitual es que generin una tasca i aquesta es processa en segon pla.
- **Tasca:** Una tasca és la materialització d'una acció sobre un desplegament concret. Les tasques tenen estat, fases, tant per cent de completitud i un registre tipus text del que ha passat.

## Il·lustració dels conceptes

Un usuari crea l'aplicació "Mobilitat", a continuació l'usuari crea un desplegament d'aquesta aplicació sobre la plataforma "PHP Consolidated". És un desplegament productiu per tant és marca com a producció. L'URL del desplegament és <http://ajuntament.barcelona.cat/mobilitat>.

Al disparar-se l'acció de creació del desplegament s'haurà generat la tasca de creació associada al desplegament. Passats uns instants el desplegament haurà estat creat sobre la plataforma PHP Consolidat.

La plataforma PHP Consolidat permet crear usuaris sFTP i SSH per els desenvolupadors.

L'usuari dona d'alta un usuari sFTP i un SSH per l'aplicació. L'acció de crear cada un dels usuaris crea una tasca que serà processada els instants següents.

És necessari també un entorn de desenvolupament per l'aplicació "Mobilitat", així doncs l'usuari crea un altre desplegament associat a l'aplicació Mobilitat. El desplegament de desenvolupament es identificat amb la URL <http://dev-ajuntament.barcelona.cat/mobilitat>.

A l'igual que el desplegament productiu es sobre la plataforma PHP Consolidat, per tant és podran crear els usuaris sFTP i SSH corresponents.

Es pot veure que els dos desplegaments comparteixen un sentit, per això estan agrupats baix la mateixa aplicació: "Mobilitat"

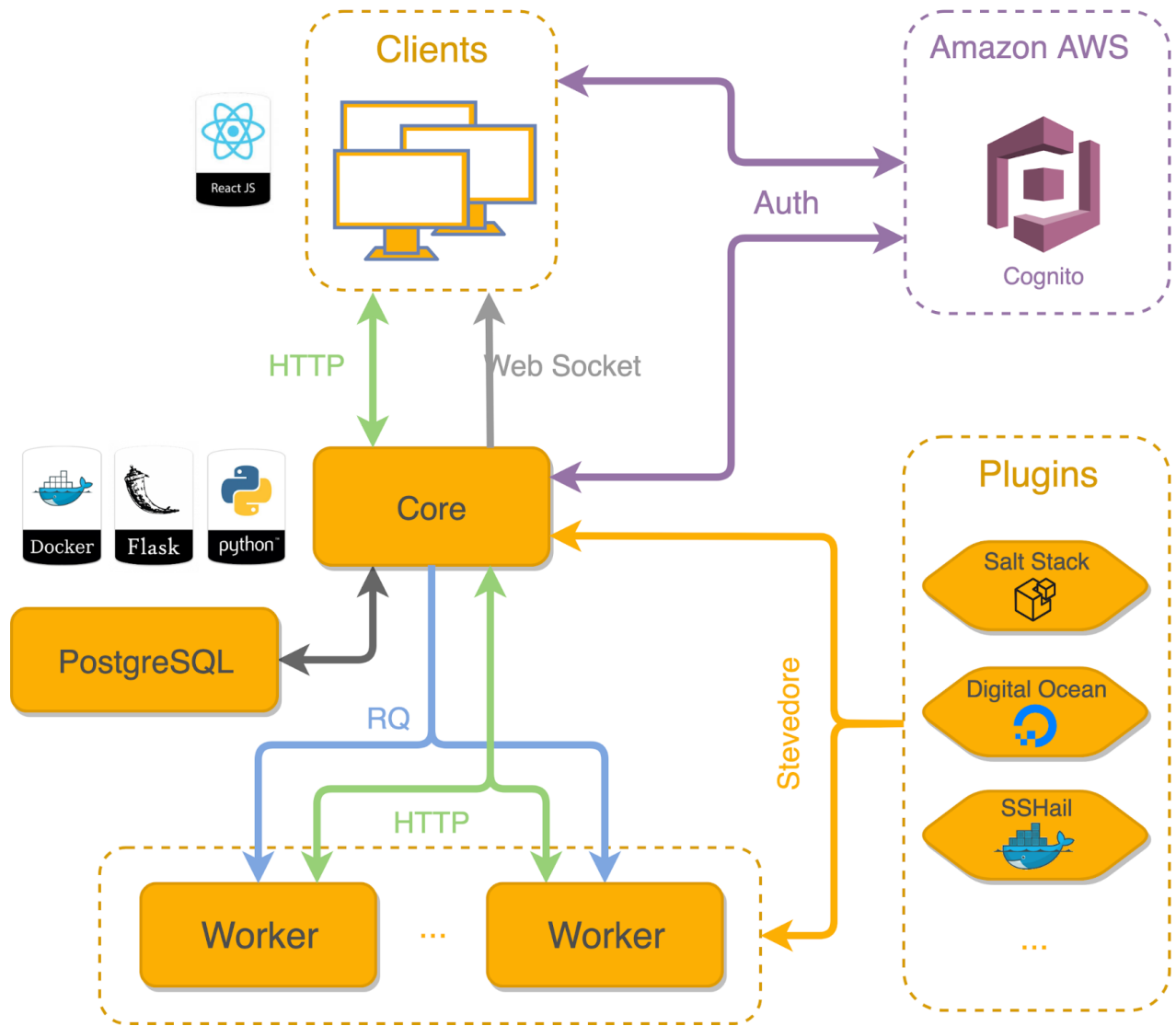
Si passat un temps es vol fer una nova versió de l'aplicació "Mobilitat" es pot crear un nou desplegament i un cop s'hagi acabat de desenvolupar modificar la seva URL.

### Arquitectura-de-Sygox

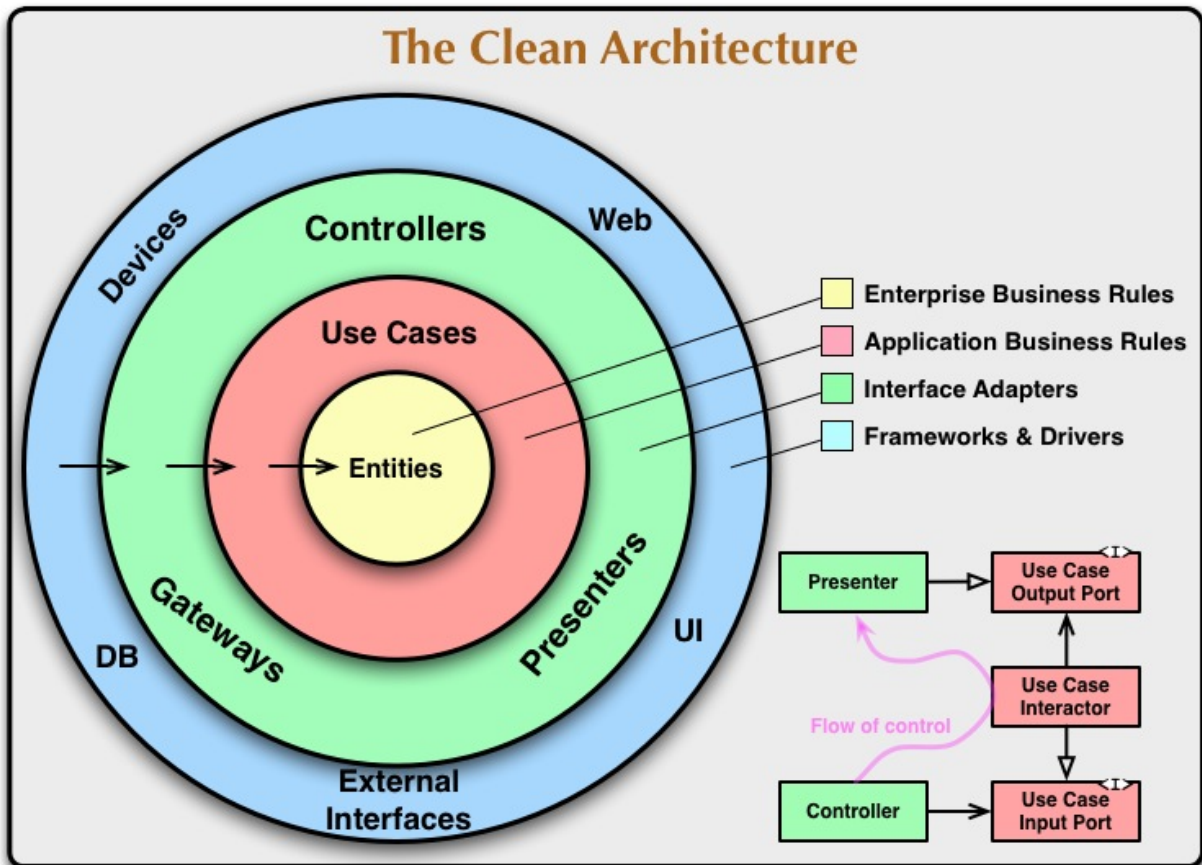
El servei està desplegat emprant `docker-compose` sobre el servidor `intern-sygox` al compte isoc de DigitalOcean.

El projecte també es connecta amb `intern-salt-master` el qual te instal·lat `SaltStack` al host i l'API de sygox-salt amb docker gestionada amb `docker-compose`.

# SyGoX Architecture



El diseny de l'aplicació segueix [The Clean Architecture](#).



És recomenable entendre, com a mínim a alt nivel, aquest disseny abans d'intentar entendre el codi de l'aplicació.

Exemples d'aplicació de Clean Architecture a [Flask](#) i a [Django](#).

## Sygox Manual d'Usuari

Secció orientada als usuaris de Sygox com ara tècnics de la DTI, caps de projecte o desenvolupadors d'aplicacions PHP que hi tenen accés.

Accés-a-Sygox

Podem accedir a Sygox a la URL: <https://sygox.dtibcn.cat>

Per seguretat abans del login d'usuari s'ha de passar una autenticació HTTP amb les credencials `web:ajuntament`. Un cop passada la fase d'autenticació HTTP s'ha de fer login amb l'usuari nominal. Aquest usuari s'ha de donar d'alta a AWS al pool de Cognito.

Trobar-un-desplegament-a-Sygox

Ens pot interessar trobar un desplegament per tal de veure en quin servidor es troba o quins usuaris associats té.

En l'apartat d'aplicacions podem trobar un cercador. Aquest cercador cerca per nom d'aplicació. Si el nom d'aplicació ha estat posat amb cura segurament tindrà relació amb la URL del desplegament que volem cercar.

Suposant que volem cercar el desplegament <http://ajuntament.barcelona.cat/mobilitat> cercarem "mobilitat" al cercador. Això ens mostrarà les aplicacions que contenen mobilitat al nom.

Llistat d'aplicacions [Filtre aplicat](#)

CERCAR APLICACIONS

NOM	SLUG
<a href="#">Mobilitat</a>	mobilitat
<a href="#">Mobilitat Tramvia Connectat</a>	mobilitat-tramvia-connectat
<a href="#">Mobilitat Redireccions</a>	mobilitat-redireccions

[Anterior](#) **1** [Següent](#)

Entrant a dins podem trobar els seus desplegaments.

Mobilitat - Desplegaments

URL PRINCIPAL	ENTORN
<a href="http://dev-ajuntament.barcelona.cat/mobilitat">http://dev-ajuntament.barcelona.cat/mobilitat</a>	environment:development
<a href="http://www.barcelona.cat/mobilitat">http://www.barcelona.cat/mobilitat</a>	environment:production
<a href="http://dev-mobilitat.ajuntament.barcelona.cat/">http://dev-mobilitat.ajuntament.barcelona.cat/</a>	environment:development

[Anterior](#) **1** [Següent](#)

Un cop s'ha trobat el desplegament es poden veure on està desplegat, si te usuaris etc.

En l'exemple d'un servidor consolidat es poden veure els detalls del PHP.

Desplegament

[Main](#) [PHP Consolidated](#) [HTTP Monitors](#) [MySQL Database](#) [Cron](#) [Email](#) [sFTP](#) [SSHail](#)

Actions ▾

PHP Consolidated info

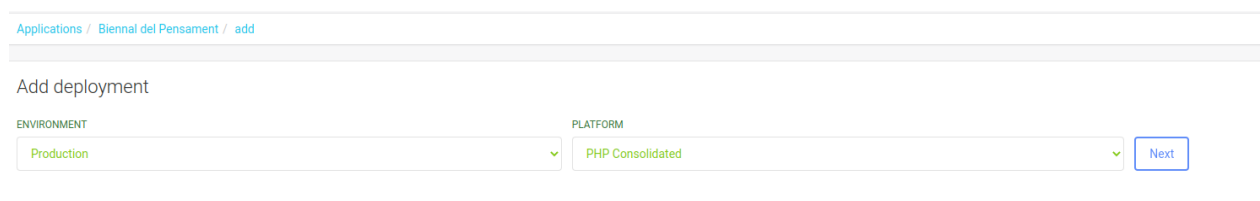
<b>HTTP endpoint</b>	http.app0247-2e37caf7.c10d.dtiibcn.cat
<b>Consolidated App Name</b>	app0247
<b>Consolidated ID</b>	247
<b>Server</b>	appserver-php-static-09
<b>Framework</b>	other
<b>PHP Version</b>	5.6

## Crear-un-desplegament-PHP-Consolidat-a-Sygox

Aquest procediment explica els passos a seguir per afegir un nou desplegament a Sygox PHP Consolidat i donar-lo d'alta a Sygox.

1. Accedim a [Sygox](#).
2. Busquem si ja existeix algun desplegament amb el mateix nom, similar o relacionat amb el que s'ha de crear. Fent servir el cercador que hi ha a [Applications](#)
3. Cliquem per crear un nou desplegament i emplenem els camps de la següent manera:

Cal posar quin és l'entorn (Productiu o Desenvolupament) i que es tracta del tipus `PHP Consolidated`



Applications / Biennial del Pensament / add

Add deployment

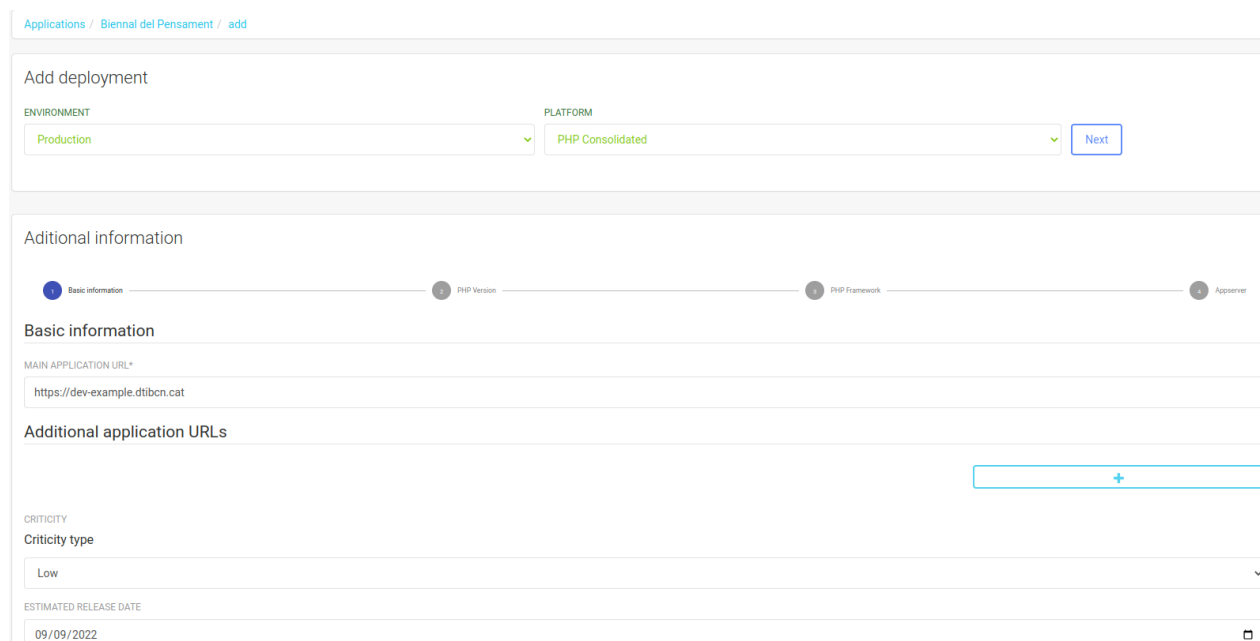
ENVIRONMENT: Production

PLATFORM: PHP Consolidated

Next

Fem click a **Next**

Seguidament s'haurà d'afegir la url del desplegament al camp **Main Applications URL** i la criticitat (Low per entorns DEV i medium per entorns de PROD). El camp **Estimated Release Date** es pot posar la mateixa data de creació del desplegament.



Applications / Biennial del Pensament / add

Add deployment

ENVIRONMENT: Production

PLATFORM: PHP Consolidated

Next

Additional information

Basic information

MAIN APPLICATION URL\*

https://dev-example.dtibcn.cat

Additional application URLs

CRITICITY

Criticality type

Low

ESTIMATED RELEASE DATE

09/09/2022

Fem click a **Next**

Seguidament ens demanarà la versió de PHP (7.4, 8, 8.1, etc) i el tipus de framework que utilitzarà el desplegament (Drupal, WP, altres). Aquestes dades les sol subministrar el peticionari de la creació en el següent [document](#)

Finalment haurem d'escollir a quin appserver es crearà el desplegament. Actualment estem fent servir el **PHP c10d Static 17** per nous desplegaments. Si no es te clar a quin es pot desplegar, sempre millor consultar amb un dels membres de KISSIS.

Add deployment

ENVIRONMENT: Production | PLATFORM: PHP Consolidated | Next

---

Additional information

Basic information | PHP Version | PHP Framework | Appserver

Appserver

APPSERVER\*

Appserver to deploy the app.

PHP c10d Static 09 (AWS) (eu-west-1)

PREVIOUS | SUBMIT

Fem click a **Submit** i es crearà un nou job a Sygox. Si aquest finalitza correctament ja tindrem creat el nou desplegament a Sygox

## Desplegaments Particulars:

- Els desplegaments de blocs en residència s'han de fer al `php-c10d-static-04`
- Els desplegaments de Biblioteques s'han de fer al `php-c10d-static-05`
- Els desplegaments CI/CD nou- haurien de crear-se amb `enviroment:production` `criticity:medium`

### Comprovar-l'estat-d'una-tasca

Les accions del Sygox generen tasques.

Si obrim una tasca podrem veure el seu estat, fases, tant per cent de completitud i un registre tipus text del que ha passant.

Podem veure les tasques associades a un desplegament al menú `Main` del propi desplegament.

SYGOX bmiro

Applications / Subtest / <http://dev-ajuntament.barcelona.cat/drupal-ci-test>

### Desplegament Eliminar

Main [PHP Consolidated](#) [MySQL Database](#) [Email](#) [sFTP](#) [SSHail](#)

Actions ▾

#### Deployment info

<b>Main URL</b>	http://dev-ajuntament.barcelona.cat/drupal-ci-test
<b>Environment</b>	development
<b>Platform</b>	platform:php-consolidated
<b>Criticality</b>	low
<b>Created at</b>	Fri, 09 Nov 2018 16:10:18 GMT
<b>Updated at</b>	Wed, 28 Nov 2018 14:23:07 GMT

#### Llista de tasques

#	NAMESPACE	ACCIÓ	ESTAT	PERCENTATGE	CREAT A	ACTUALITZAT A
20482fc0f31911e8953a0242ac160003	php_consolidated_salt	edit_deployment	SUCCESS	100%	Wed, 28 Nov 2018 14:23:07 GMT	Wed, 28 Nov 2018 14:24:16 GMT
2a2d874cf26111e8b75e0242ac160003	php_consolidated_salt	force_salt_apply	SUCCESS	100%	Tue, 27 Nov 2018 16:26:16 GMT	Tue, 27 Nov 2018 16:27:21 GMT
68c36a24f25e11e8b1d40242ac160003	php_consolidated_sshail	add_user_SSHail	SUCCESS	100%	Tue, 27 Nov 2018 16:06:33 GMT	Tue, 27 Nov 2018 16:07:42 GMT

Si s'ha executat una acció que ha disparat una tasca s'ha d'esperar que sigui executada i amb estat `SUCCESS`. En cas que no sigui així i aparegui com finalitzat amb un altre estat com ara `FAILED` s'ha de notificar immediatament a l'administrador de Sygox enviant la URL de la tasca que ha fallat.

SYGOX

APLICACIONS

Applications / Subtest / http://dev-ajuntament.barcelona.cat/drupal-ci-test / edit\_deployment.php\_consolidated\_salt

Job #20482fc0f319

Created At	Wed, 28 Nov 2018 14:23:07 GMT
Percentage	100
Stages	
Status	SUCCESS
Updated At	Wed, 28 Nov 2018 14:24:16 GMT
Username	bmiro

Completed steps

TIMESTAMP	STEP
[2018-11-28 14:23:08]	Sent salt task
[2018-11-28 14:23:13]	All stages of Sygox job '%s' added to SygoxSaltDaemon Queue.
[2018-11-28 14:23:14]	Stage (sygox job_id: 20482fc0f3191e8953a0242ac160003). Persited pillar php-server/appserver-php-static-03/apps/app0057.yaml:
[2018-11-28 14:23:14]	--- /srv/pillar/php-server/appserver-php-static-03/apps/journal/app0057_201811271626_2a2d074cf26111e8b75e0242ac160003.yaml 2018-11-27 16:26:18.430072766 +0000
[2018-11-28 14:23:14]	+++ /srv/pillar/php-server/appserver-php-static-03/apps/journal/app0057_201811281423_20482fc0f3191e8953a0242ac160003.yaml 2018-11-28 14:23:13.953654291 +0000
[2018-11-28 14:23:14]	@@ -8,7 +8,7 @@
[2018-11-28 14:23:14]	name: dev-ajuntament.barcelona.cat
[2018-11-28 14:23:14]	baseurl: /drupal-ci-test
[2018-11-28 14:23:14]	php:
[2018-11-28 14:23:14]	- version: '5.6'

## Afegir-i-actualitzar-les-url-d'un-PHP-Consolidat

Per tal de modificar o actualitzar les url d'un desplegament seguirem els següents passos.

Primer de tot cal accedir al desplegament en concret, cliquem **Actions** i **Update Deployment Info** :

Desplegament

Eliminar

Main PHP Consolidated HTTP Monitors MySQL Database Cron Email sFTP SSHail

Actions -

- Update Deployment Info
- Delete Deployment Main
- Update Job Info

Main URL	http://dev-guia.dtibcn.cat/
Environment	environment:development
Platform	platform:php-consolidated
Criticality	low
Created at	Fri, 09 Nov 2018 16:03:27 GMT
Updated at	Fri, 09 Nov 2018 16:03:27 GMT

En la nova pantalla podem o bé modificar la url principal, canviant **Main application URL** o bé afegir-ne de addicionals clicant al botó de **+** :

Update Deployment Info

Additional application URLs

CRITICITY  
Criticity type

Low

ENVIRONMENT  
Development

ESTIMATED RELEASE DATE  
dd / mm / aaaa

MAIN APPLICATION URL\*

http://dev-guia.dtibcn.cat/

## Alta-i-edició-de-paràmetres-PHP-a-un-servidor-consolidat

Aquest procediment descriu com canviar el paràmetre d'un valor PHP. Inicialment, l'app a Sygox no tindrà cap paràmetre PHP definit. Això no vol dir que el servidor no els tingui configurats, significa que porta els valors per defecte. La imatge que es veurà serà:

Despliegament

Main PHP Consolidated MySQL Database Email sFTP SSHail

Actions

PHP Consolidated info

Server	appserver-php-static-18
Framework	drupal_7
PHP Version	7.2

No params settled, using defaults.

Els paràmetres que es voldran afegir poden ser de l'estil `max_input_vars` o `memory_limit`. Farem l'exemple amb aquests dos paràmetres.

Per afegir-los cal anar a la pestanya `PHP Consolidated` i clicar a `Actions` -> `Set PHP Params`. Aquí podrem veure un desplegable on per defecte apareix `New`. Però també hi apareixeran tots els noms de paràmetres que prèviament s'hagin inserit al sistema per tal de minimitzar errors a l'hora de tornar a escriure els paràmetres. Si es vol editar un paràmetre caldrà posar de nou el nom amb el nou valor. Es poden afegir tants paràmetres com es vulguin d'una sola vegada afegint nous camps amb el botó de `+`. Cliquem `submit`.

## Set PHP Params

### PHP Parameters

Parameter\* ↑ ↓ ✕

EXISTING PARAMETER  
New

VALUE\*  
2000

PARAMETER NAME\*  
max\_input\_vars

Parameter\* ↑ ↓ ✕

EXISTING PARAMETER  
New

VALUE\*  
256

PARAMETER NAME\*  
memory\_limit

+

Submit

I ara a la pantalla inicial ja veurem els nous paràmetres:

Desplegament Eliminar

Main PHP Consolidated MySQL Database Email sFTP SSHail

Actions ▾

PHP Consolidated info

Server	appserver-php-static-18
Framework	drupal_7
PHP Version	7.2

PHP Params

KIND	PARAMETER	VALUE
php_admin_value	max_input_vars	2000
php_admin_value	memory_limit	256

## Baixa-de-paràmetres-PHP-a-un-servidor-consolidat

Aquest procediment descriu com donar de baixa un paràmetre de PHP a un servidor consolidat prèviament donat d'alta a Sygox.

Per donar de baixa un o diversos paràmetres cal anar a la pestanya `PHP Consolidated` i clicar a `Actions` -> `Remove PHP Params`. En la nova vista caldrà afegir un o més desplegable i triant el paràmetres que s'ha de suprimir i clicat `submit`. Es poden afegir més paràmetres a eliminar clicant el `+` o traient-los de la supressió amb el botó `x` si ens hem equivocat.

Remove PHP Params

PHP Parameters to remove

Un cop eliminat deixarà d'aparèixer a la pestanya de PHP Consolidated.

## Gestió-d'usuaris-SSHail-i-sFTP-en-desplegaments-PHP-Consolidats

Els desplegaments PHP consolidats permeten dos tipus d'usuaris per accedir al servidor: els sFTP i els SSHail.

Els sFTP permeten només manipular els fitxers del servidor, per altra banda amb l'accés SSHail es pot fer un SSH dins d'un contenidor on hi ha els fitxers del servidor i executar comandes per modificar-los emprant eines com `git`, `drush` o `composer`. Cal dir que dins del SSHail no és té accés als processos de sistema ni web que serveixen el desplegament.

Cada tipus d'usuari té la seva entrada de menú. Els usuaris SSHail i sFTP es gestionen per separat. Que un desenvolupador tingui usuari SSHail no significa que hagi de tenir sFTP i viceversa.

Per facilitat i donat que hi ha força usuaris que treballen en més d'un desplegament Sygox guarda una llista dels usuaris associats a altres desplegaments. D'aquesta manera al fer l'alta de l'usuari en un desplegament es pot mirar abans si ja està a la llista d'usuaris introduïts al sistema sense haver de re-introduir les seves dades.

Cal remarcar que el llistat d'usuaris sFTP i SSHail són separats, així doncs s'afegeixi l'usuari per primer cop en un dels dos no apareixerà automàticament a l'altre.

### Alta dels usuaris

Per fer l'alta dels usuaris a un desplegament haurem de cercar el desplegament i accedir-hi tal i com es mostra al procediment [Trobar un desplegament](#).

Un cop estem al desplegament ens situam al menú sFTP o SSHail, desplegam les accions i clicam a `Add user sFTP` o `Add user SSHail` segons correspongui.

Applications / Subtest / <http://dev-ajuntament.barcelona.cat/drupal-ci-test>

## Desplegament

[Eliminar](#)

[Main](#) [PHP Consolidated](#) [MySQL Database](#) [Email](#) [sFTP](#) [SSHail](#)

Actions ▾

No sFTP users has been assigned assigned to this deployment yet.

En la pàgina de l'acció podrem veure un símbol +. Si el clicam veurem un formulari amb dues parts.

SYGOX bmiro ▾

APLICACIONES

Applications / Subtest / <http://dev-ajuntament.barcelona.cat/drupal-ci-test> / <http://dev-ajuntament.barcelona.cat/drupal-ci-test>

### Add User SFTP

Existing User

User\* ✕

EXISTING USER\*

Create New ▾

EMAIL\*

NAME\*

MANAGER EMAIL\*

PLATE\*

The user's plate i.e. a123456

[+](#)

[SUBMIT](#)

En la primera part hi ha el desplegable Existing user . És recomanable cercar si l'usuari ja ha estat donat d'alta. L'ordenació es alfabètica i un cop desplegat és pot pitjar al teclat la lletra inicial a cercar.

En cas d'haver-hi un usuari duplicat per derivacions del nom o la matrícula intentar seleccionar el que es consideri correcte.

Quan està marcat el valor del camp `Existing user` és `Create new` s'està indicant que l'usuari s'ha de donar d'alta de nou al Sygox i es mostren els camps a emplenar:

Camp	Descripció	Exemple
Email	Correu electrònic de l'usuari	<a href="mailto:joanmiquelartiquesvalls@example.com">joanmiquelartiquesvalls@example.com</a>
Name	Nom i cognoms de l'usuari	Joan Miquel Artigues Valls
Plate	Matrícula de l'usuari	s482745
Manager email	Correu electrònic del cap de l'usuari o responsable de la petició	<a href="mailto:pnicolau@example.com">pnicolau@example.com</a>
Home Subdirectory	Només en el cas dels usuaris sftp. És opcional. Si es deixa en blanc l'usuari sftp tindrà accés des de l'arrel del directori d'aplicació. Si es posa un path més restrictiu tindrà accés a partir d'aquell path. Cal posar només el path relatiu. És a dir, obviar la part del path <code>/var/www/apps/appXXXX</code>	<code>www/aplicacio/serveis_sftp</code>

Es poden donar d'alta diversos usuaris a la vegada, ja siguin pre-existents al sistema o nous.

Senzillament s'ha d'anar clicant al símbol + i emplenar els camps del formulari.

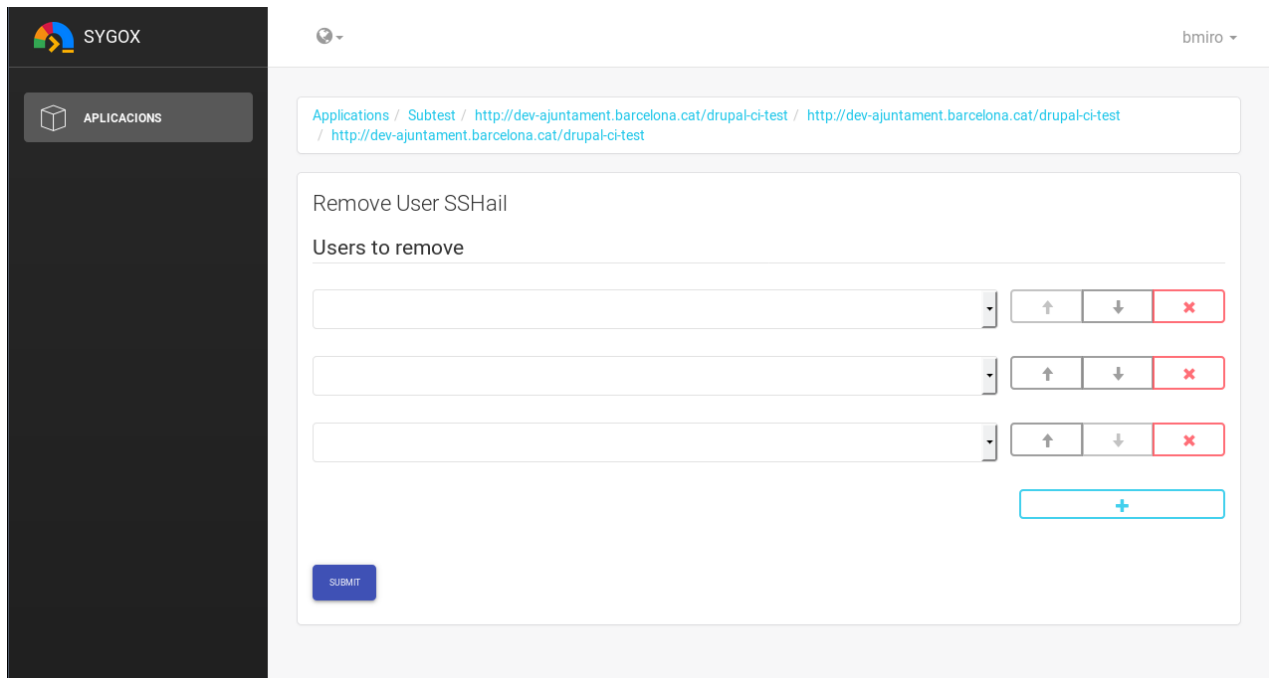
Un cop acabat clicar a Submit.

Haurem de la tasca s'executa correctament [comprovant l'estat de la tasca](#).

### Baixa dels usuaris

Si es vol donar de baixa un usuari d'un desplegament ens hem de situar al menú sFTP o SSHail desplegar el menú d'accions i executar `Remove SSHail User` o `Remove sFTP User` segons correspongui.

A continuació clicam el símbol + i seleccionam l'usuari a esborrar. Podem afegir usuaris a esborrar amb els símbol + .



Un cop tinguem la llista d'usuaris a esborrar clicam a `Submit` .

Haurem de la tasca s'executa correctament Comprovant l'estat de la tasca.

### **Regenerar usuari (canviar contrasenya)**

Si es vol canviar la contrasenya d'un usuari es pot esborrar l'usuari i tornar-lo a crear. D'aquesta manera el sistema li canviarà la contrasenya.

### **Donar d'alta-BD-MySQL-a-un-desplegament-PHP-Consolidat**

Aquest procediment descriu com donar d'alta una base de dades MySQL associada a un desplegament PHP Consolidat.

Com a resultat del procediment obtindrem una base de dades associada al desplegament i les credencials d'accés a la mateixa.

L'única dada que necessitam saber per donar d'alta la BD és a quin clúster la volem donar d'alta.

Per fer l'alta de la base de dades a un desplegament haurem de cercar el desplegament i accedir-hi tal i com es mostra al punt [Trobar un desplegament](#).

Con cop dins del desplegament ens situam al menú `MySQL Database` .

Hem de comprovar si ja hi ha alguna base de dades que puguem emprar. Si no és el cas en fem una de nova.

Per crear la base de dades desplegam el menú `Actions` i clicam a `Add MySQL Database` .

## Desplegament

Main

PHP Consolidated

MySQL Database

Email

sFTP

SSHail

Actions ▾

Add MySQL Database

Remove MySQL Databases

Add MySQL Database

No databases assigned to this deployment yet

Un cop dins l'acció haurem de seleccionar el clúster on vulguem la BD.

The screenshot shows a web browser window with the Sygox application. The address bar shows the URL: [https://sygox.dtibcn.cat/#/applications/fa5ecc06e43911e8a9990242ac160003/deployments/fa81c942e43911e89e7e0242ac160003/action/add\\_My](https://sygox.dtibcn.cat/#/applications/fa5ecc06e43911e8a9990242ac160003/deployments/fa81c942e43911e89e7e0242ac160003/action/add_My). The page title is 'Add MySQL Database'. Below the title, there is a label 'MYSQL SERVER\*' and a sub-label 'Where to create the DB'. A text input field is present, but it is empty. A tooltip message 'Please select an item in the list.' is visible over the input field. At the bottom of the form, there is a blue 'SUBMIT' button. The left sidebar shows the 'SYGOX' logo and a menu item 'APLICACIONS'.

Haurem de la tasca s'executa correctament [Comprovant l'estat de la tasca](#).

En acabat podem veure les credencials que s'han generat per la BD.

Desplegament Eliminar

Main PHP Consolidated MySQL Database Email sFTP SSHail

Actions ▾

Databases

DB NAME	USER	PASSWORD	DB ENDPOINT
db_foo	u_foo	*****	mysql-cluster01.c

## Exportació-i-importació-de-bases-de-dades

Es recomana fer els *exports* i *imports* de les bases de dades amb la línia de comandes.

Per exportar una base de dades:

```
mysqldump --single-transaction -quick -u <u_usuari_de_bd_origen> -p -P 3406 -h <endpoint_db> <db_nom_de_bd> | gzip -c > db_nom_de_bd_origen.sql.gz
```

Per importar una base de dades:

```
zcat db_nom_de_bd_origen.sql.gz | mysql -u <u_usuari_de_bd_desti> -p -P 3406 -h <endpoint_db_desti> <db_nom_de_bd_desti>
```

## Configuració-de-correu-a-un-desplegament-PHP-Consolidat

En ocasions, les aplicacions necessitaran fer enviaments de correu electrònic. En aquest cas, també s'haurà de configurar a través de Sygox. En primer lloc, cal [trobar l'aplicació](#) en la qual volem configurar el correu i cliquem a la pestanya `Email`.

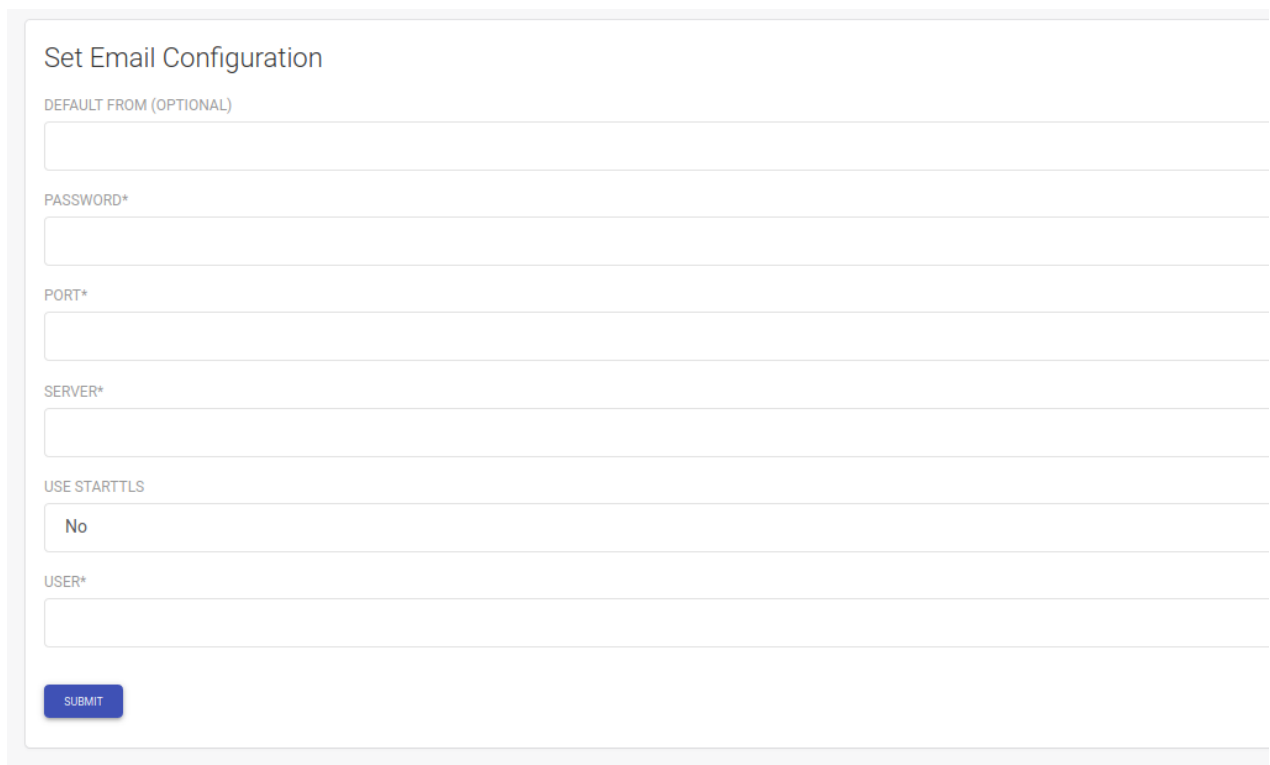
Desplegament

Main PHP Consolidated HTTP Monitors MySQL Database Cron **Email** sFTP SSHail

Actions ▾

No email configuration set yet.

Cliquem a `Actions` i `Set email configuration`.



Set Email Configuration

DEFAULT FROM (OPTIONAL)

PASSWORD\*

PORT\*

SERVER\*

USE STARTTLS

No

USER\*

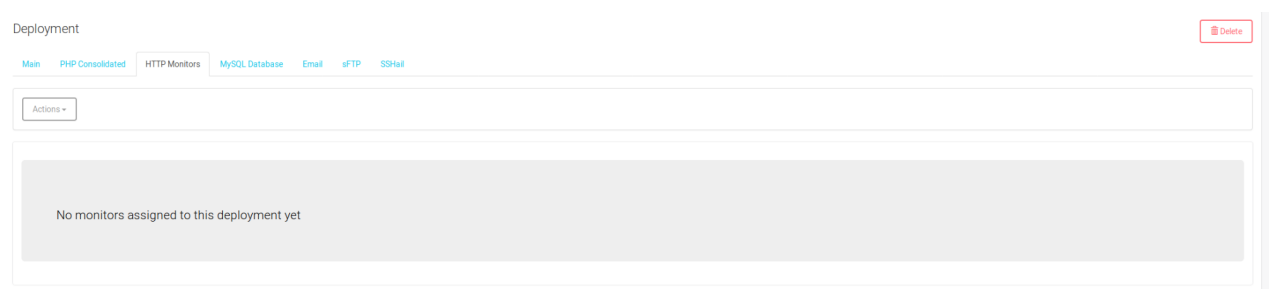
SUBMIT

Els paràmetres que s'han d'emplenar hauran de ser facilitats per l'administrador de sistemes del servidor de correu.

### Alta-de-un-monitor-HTTP-a-un-PHP-Consolidat

Aquest procediment consisteix en donar d'alta un monitor HTTP per una url i que comprovi que l'aplicació funciona correctament mitjançant UptimeRobot.

Per a donar-ho d'alta, anam al sygox, i [entram al desplegament](#) on volem donar el monitor d'alta. Seguidament, entram a la pestanya de `HTTP Monitors`.



Deployment Delete

Main PHP Consolidated HTTP Monitors MySQL Database Email sFTP SSHel

Actions -

No monitors assigned to this deployment yet

Cliquem a `Actions` i a `Add HTTP Monitor`. Com a default, ens sortirà la main url del desplegament, pero podem monitoritzar qualsevol subpath de la mainUrl o qualsevol url secundària.

El tipus de monitor pot ser `HTTP` o `Keyword`. El primer comprova que el codi de retorn sigui 200, mentre que el segon busca un string a la pàgina. En aquest cas, podem configurar l'alarma tant que salti en cas que no trobi aquest string, com en el cas que sí el trobi. Com a norma, posarem monitors de tipus `Keyword` triant una paraula que sigui

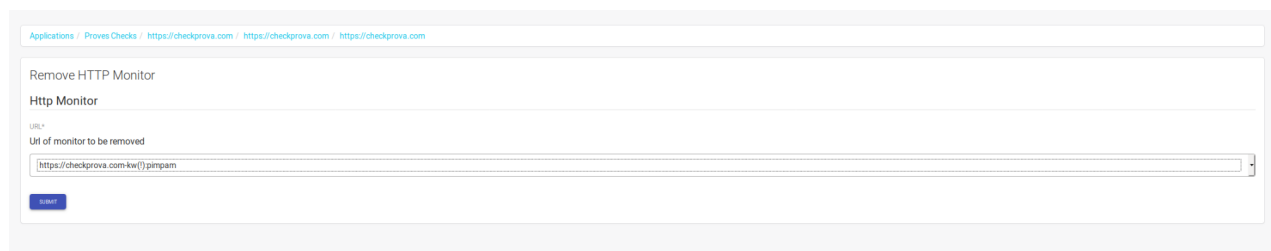
el més estàtica possible. És a dir, que no canviï amb la generació de continguts però que tampoc sigui molt comuna, com "Barcelona" o "Ajuntament".

Finalment, cliquem `Submit` per crear el monitor. Podem veure la [tasca que s'ha generat](#) per comprovar que el procés hagi acabat satisfactòriament.

## Baixa-d'un-monitor-HTTP-a-un-PHP-Consolidat

Aquest procediment consisteix en donar de baixa un monitor.

Per a donar-ho de baixa, anam al sygox, i entram al desplegament on volem donar el check de baixa, i entram a la pestanya de `HTTP Monitors` i clicam a `Actions ->> Remove HTTP Monitor`. Posteriorment escollim El `friendly name` del monitor a esborrar i clicam `submit`.



## Visualitzar-estat-dels-monitors-des-de-UptimeRobot

En cas de voler visualitzar l'estat dels desplegaments es poden visitar els panells d'estat.

Disposem de 3 panells:

- <https://status-high.d10n.dtibcn.cat> on apareixen els desplegaments classificats com estratègics. Aquests es comproven cada minut i dispren alarmes en 24x7.
- <https://status-medium.d10n.dtibcn.cat> on apareixen els desplegaments classificats com estàndard. Aquestes es comproven cada 5 minuts i es mostren a panells d'alarmes però no dispren alarma en 24x7.
- <https://status-all.d10n.dtibcn.cat> on apareixen tots els monitors donats d'alta independentment de la seva criticitat.

\*El password per accedir a aquests panells és **voltornegre**\*

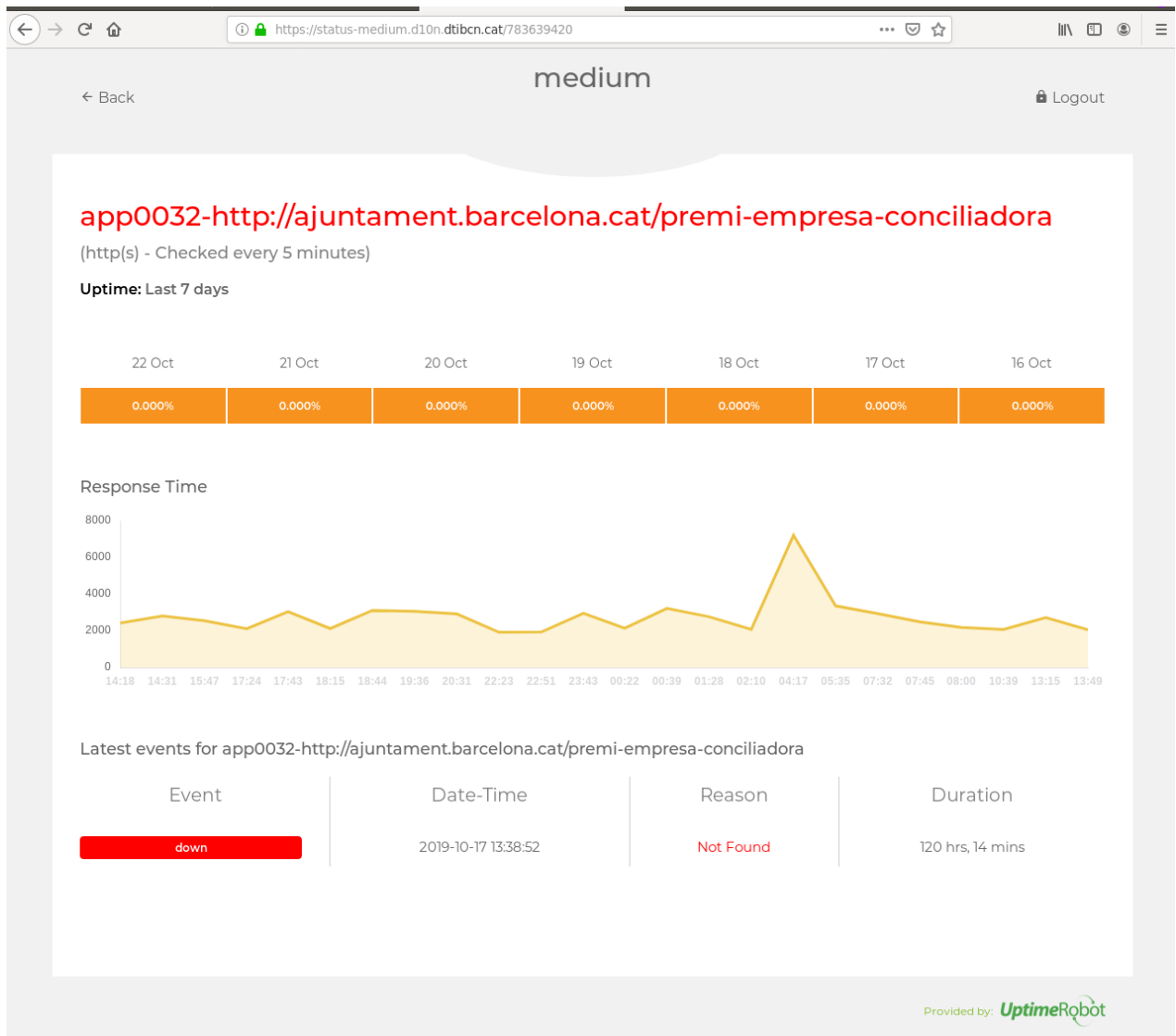
Els monitors estan ordenats mostrant primer els caiguts. D'aquesta manera ràpid si hi ha cap incident.

medium Logout

## Monitors

Status	Last 7 days		Type	Last 7 days						
				22 Oct	21 Oct	20 Oct	19 Oct	18 Oct	17 Oct	16 Oct
●	0.000%	app0032-http://ajuntame...	http(s)	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%
●	0.000%	app0137-http://ajuntamen...	http(s)	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%
●	0.000%	app0153-http://discapacita...	http(s)	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%
●	0.000%	app0294-http://ajuntame...	http(s)	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%
●	0.000%	app0502-http://ajuntame...	http(s)	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%
●	0.000%	app0525-https://ajuntame...	http(s)	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%
●	0.000%	app0577-https://ajuntame...	http(s)	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%
●	0.000%	app0578-https://ajuntame...	http(s)	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%
●	100.00%	app0001-http://lameva.ba...	http(s)	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	0.000%
●	100.00%	app0002-http://ajuntame...	http(s)	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	0.000%
●	100.00%	app0003-http://lameva.ba...	http(s)	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	0.000%
●	100.00%	app0004-http://ajuntame...	http(s)	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	0.000%
●	100.00%	app0005-http://barcelona...	http(s)	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	0.000%

Si es clica a un monitor es pot veure el detall del mateix:



## Alta-d'un-cron-a-un-desplegament-d'un-servidor-consolidat

Aquest procediment consisteix en l'alta d'un cron a un servidor consolidat. Sovint es demana l'execució d'un script en una certa freqüència.

Per tal de donar-lo d'alta caldrà anar a la pestanya Cron i clicar l'acció Add Cron . En aquesta vista tenim els camps de Name , Schedule i Command :

## Add Cron

COMMAND\*

CRON NAME\*

SCHEDULE\*

SUBMIT

El nom del cron és trivial i serveix per a identificar-lo. La comanda serà la línia que s'executarà en la freqüència indicada. Un exemple de comanda podria ser:

```
/usr/bin/php5.6 /var/www/apps/app0197/www/Modulos/import/auto_import.php
```

Es recomana no fer ús de `path` relatiu per tal de minimitzar errors.

El tercer camp, `Schedule`, és la freqüència. El format és el mateix que el del fitxer `crontab`. Per facilitar la feina, a més, podeu trobar un generador de freqüències [aquí](#). Un exemple de freqüència seria:

```
0 16 */3 * *
```

Aquesta freqüència implica l'execució de l'script cada 3 dies a les 16h.

### Baixa-d'un-cron-a-un-desplegament-d'un-servidor-consolidat

Aquest procediment defineix les passes a seguir per esborrar un cron d'un desplegament a un servidor consolidat. Per tal de fer-ho, només cal anar a la pestanya `Cron` i seleccionar l'acció `Remove Cron`.

En aquesta vista es pot afegir un o diversos crons per esborrar alhora. Se seleccionen i es clica `Submit`.

Remove Cron

Crons to remove

Search

## Anonimitzar-dump-de-sygox

Si es vol fer un dump de la base de dades de sygox per a poder fer un sygox-dev per a fer proves, és necessari l'anonimització de les dades, per això hem creat l'script `anonymitzer`.

El dump és necessari fer-ho amb les opcions `--inserts --column-inserts --attribute-inserts` per a que l'anonimitzador funcioni correctament, quedant així:

```
~/sysgov2-core$ sudo docker-compose exec postgres pg_dump -U usygox -Fp sygoxdb --inserts --column-inserts --attribute-inserts | ./scripts/anonymitzer > anon_dump-$(date -I).sql
```

Aquesta comanda anonimitzarà el dump sencer, però es pot fer amb el paràmetre `--reduce` i passar-li el nombre d'aplicacions a mantenir. El que farà és només fer un dump del nombre d'aplicacions que se li passi més els appservers i bases de dades. La resta de dades no s'importaran:

```
~/sysgov2-core$ sudo docker-compose exec postgres pg_dump -U usygox -Fp sygoxdb --inserts --column-inserts --attribute-inserts | ./scripts/anonymitzer --reduce 15 > anon_dump-$(date -I).sql
```

## Afegir-noves-dades-a-anonimitzar-a-l'script-de-anonimitzat

L'script d'anonimitzat de dades de sygox es pot variar afegint i llevant diferents dades a anonimitzar.

L'anonimitzador conté una llista de diccionaris anomenada `REGEX_CONFIG`, on es ficaran les diferents regles per tal que certes dades s'anonimitzin.

L'estructura del diccionari és la següent:

```
{
  "regex": ".*WHAT_TO_MATCH.*",
  "name": "NAME_OF_RULE",
  "description": "Description of rule",
```

```
"action": {
  "action": "Action",
},
},
```

`regex` serà una regex que indiqui que, en cas de match, es farà una acció `action`.

`action` pot tenir dos valors: `replace` o `remove`. `remove` no necessita cap altre key ni paràmetre, i indica que la línia que ha fet match no serà escrita al dump final. `replace` indica que la línia necessita una substitució i serà necessari afegir dues keys més al diccionari de `action`:

```
{
  "regex": '.*"password"\: "[^\,]*".*',
  "name": "anon-password",
  "description": "Anonymitze Passwords",
  "action": {
    "action": "replace",
    "replace": '"password"\: "[^\,]*"',
    "substitution": '"password": "anon_{random_password}"',
    "random_func": "random_8_password",
  },
},
```

Farà match amb qualsevol string que contengui `password:`, i substituirà `password: xxxxxx`, per `password": "anon_{random_password}` on `random_password` serà donat per la funció `random_8_password`.

## Gestió-d'equips-de-Sygox

### Descripció

El plugin d'equips permet la integració de desenvolupadors i líders d'equip a la plataforma. D'aquesta manera, qualsevol desenvolupador tindrà accés a Sygox i consultar de forma granular la informació de les aplicacions que té assignades. Aquesta funcionalitat hauria de descarregar de pes els tècnics de la DTI que a dia d'avui estan gestionant l'alta de tots els accessos i el traspàs d'informació.

Així, els tècnics només hauran de donar d'alta els equips i afegir-hi usuaris.

Posteriorment, seran els líders d'equip qui crearan els accessos SSHail i sFTP als desenvolupadors i aquests mateixos podran consultar les bases de dades creades, els seus propis accessos i altre informació rellevant per la seva feina.

# Què és un equip

Un equip és un tipus de desplegament especial en el qual se li poden assignar membres. Cada membre té un rol: O bé líder d'equip o bé desenvolupador. En un equip hi pot haver més d'un líder.

Quan s'assigna un equip a un desplegament (veure més abaix procediment) els seus membres obtenen una sèrie de permisos. Les seves característiques són:

- **Desenvolupador:**
  - Pot veure els paràmetres PHP.
  - Pot veure quins membres estan assignats al desplegament.
  - Pot consultar la configuració de bases de dades.
  - Pot veure si hi ha crons configurats.
  - Pot veure la configuració de correu.
  - Pot veure els seus propis accessos SSHail i sFTP.
- **Líder:**
  - Tot el que un desenvolupador pot fer.
  - Pot veure tots els accessos SSHail i sFTP dels membres de l'equip (però no la contrasenya).
  - Pot crear accessos SSHail i sFTP per als membres del seu equip.
  - Pot eliminar accessos SSHail i sFTP per als membres del seu equip.
- **Project Manager:**
  - Pot veure l'informació general del desplegament, però no informació tècnica.
  - Pot veure els monitors, per saber si l'aplicació està monitoritzada.
  - Pot fixar la data de publicació estimada.

L'assignació i eliminació de membres a un equip o l'assignació i eliminació d'equips a desplegaments és una operació privilegiada que només tècnics de la DTI i administradors podran dur a terme.

## Alta d'equip

Per donar d'alta un equip cal que busquem l'aplicació `Equips`. A dins hi podrem veure tots els equips que hi ha. Cliquem a `+ Desplegament` i emplenem els següents camps:

- **Environment:** `Development`
- **Platform:** `Team`
- **Main application url:** `team://nom-equip`
- La resta de camps per defecte
- Cliquem `Next` i donem nom a l'equip.

Add deployment

ENVIRONMENT: Development PLATFORM: Team Next

Additional information

Basic information

MAIN APPLICATION URL\*: team://apsl-sistemas

Additional application URLs: +

CRITICITY

Criticality type: Low

ESTIMATED RELEASE DATE: dd / mm / aaaa

Next

## Assignar usuari a equip

Per assignar un nou membre a un equip anirem a l'aplicació **Equips** i seleccionarem l'equip en qüestió. Cliquem la pestanya **Members**, **Actions** i **Assign Member**.

En el següent formulari haurem d'emplenar els camps referents a l'usuari:

Assign Member

**Member**

ROLE\*  
Leader

EXISTING MEMBER\*  
Create New

EMAIL\*  
vladimir@apsl.net

NAME\*  
Vladimir Iltix

MANAGER EMAIL\*  
admin@apsl.net

PLATE\*  
The user's plate i.e. a123456  
a123456

SUBMIT

Tot i així, és recomanable seleccionar-lo del desplegable si ja ha estat donat d'alta prèviament en algun altre equip, per estalviar temps però, sobretot, per evitar errors d'escriptura en el nom i matrícula:

Assign Member

Member

ROLE\*

Leader

EXISTING MEMBER\*

vladimir.a123456

SUBMIT

## Edició del rol d'un membre de l'equip

Anàlogament al procediment anterior, també es pot editar el rol d'un usuari d'un equip en aquells casos en què sigui necessari canviar-lo.

## Eliminació d'usuari de l'equip

Per eliminar un membre d'un equip anirem a l'aplicació `Equips` i seleccionarem l'equip en qüestió. Cliquem la pestanya `Members`, `Actions` i `Refuse Member`. El seleccionem del desplegable i acceptem:

Refuse Member

Refuse member

INFORMATION

This action will remove the member from the team and his/her sshail and sftp accesses where the team was assigned.

MEMBER TO REFUSE\*

vladimir.a123456

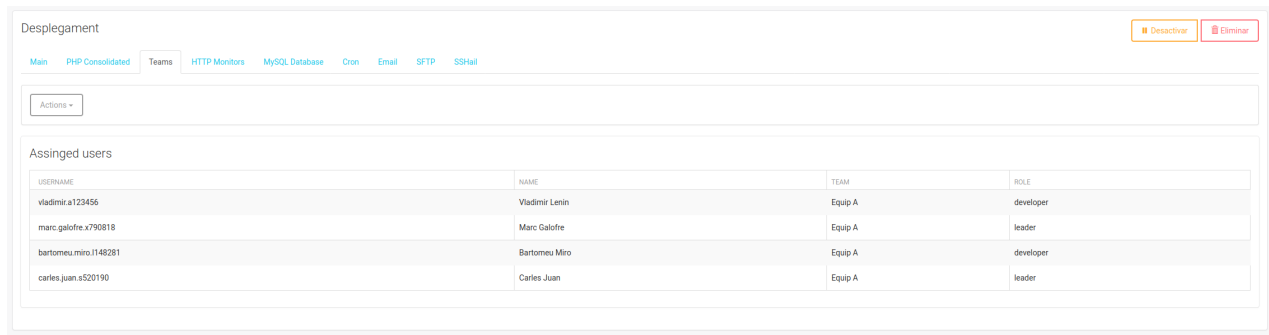
SUBMIT

**Cal tenir en compte que aquesta acció esborrarà tots els permisos que tenguí l'usuari a sobre de tots els desplegaments que té assignats l'equip. Això implica que els seus accessos SSHail i sFTP també seran esborrats per tots els desplegaments assignats.**

## Assignar equip a desplegament

L'assignació d'equips a desplegaments es fa des del desplegament de l'aplicació. Per tant, caldrà que busquem l'aplicació i entrem al desplegament en qüestió i cliquem a

sobre de la pestanya `Teams` . En aquesta pestanya hi sortiran tots els membres dels equips assignats. Per afegir un equip (i per tant, tots els seus membres), cliquem `Actions` , `Assign Team` i triem l'equip del desplegable.



The screenshot shows the 'Desplegament' interface with the 'Teams' tab selected. At the top right, there are buttons for 'Desactivar' and 'Eliminar'. Below the navigation bar, there is an 'Actions' dropdown menu. The main content area is titled 'Assinged users' and contains a table with the following data:

USERNAME	NAME	TEAM	ROLE
vladimir.a123456	Vladimir Lenin	Equip A	developer
marc.galofre.x790818	Marc Galofre	Equip A	leader
bartomeu.miro.1148281	Bartomeu Miro	Equip A	developer
carles.juan.s520190	Carles Juan	Equip A	leader

## Assign Team

TEAM\*

Select which team you want to assign

Equip B

SUBMIT

## Desassignar equip de desplegament

La desassignació d'equips de desplegaments es fa des del desplegament de l'aplicació. Per tant, caldrà que busquem l'aplicació i entrem al desplegament en qüestió i cliquem a sobre de la pestanya `Teams` , `Actions` i `Refuse Team` . Només haurem de seleccionar l'equip i acceptar.

## Refuse Team

TEAM\*

Select which team you want to refuse

Equip A

SUBMIT

**Cal tenir en compte que aquesta acció esborrarà tots els permisos que tinguin els usuaris de l'equip a sobre del desplegament. Això implica que els accessos SSHail i sFTP també seran esborrats per tots els membres de l'equip.**

## Gestió-de-repositoris-amb-Sygox

El plugin de Gitlab gestiona la integració de Sygox i el servei de repositoris gitlab.dtibcn.cat. D'aquesta manera, es facilita la creació de repositoris que queden vinculats a desplegaments de Sygox.

Només tenen permisos els tècnics de l'Oficina Tècnica (OT) i els administradors del sistema.

## Cas d'ús: Flux de creació del repositori

Per tal de crear un repositori de Gitlab al Sygox associat a un desplegament, caldria seguir una sèrie de passes.

1. Quan se sol·licita un nou espai per a una aplicació cal indicar si és necessari o no la creació d'un repositori i quin perfil base s'empra.
2. Si el repositori no està creat es preferible crear-lo a Sygox. Si ja està creat al Gitlab s'ha d'anar a Sygox i vincular-lo.
3. Una vegada creat o associat el repositori a Sygox cal assegurar-se que l'equip està associat al desplegament de Sygox i després propagar aquesta associació al Gitlab amb l'acció de Sygox corresponent.
4. L'OT enviarà la informació al desenvolupador que haurà de confirmar que hi té accés i és correcte.
5. Els desenvolupadors podran veure a través de Sygox el nou repositori creat i fer les accions pertinents.

## Donar d'alta un nou repositori

Per tal de donar d'alta un nou repositori caldrà clicar a la pestanya de Gitlab i posteriorment, a `actions` clicar `Create Git Project`. S'haurà de triar del desplegable a quin projecte correspon i triar el nom del repositori.

### Create Git Project

GIT GROUP\*

GIT PROJECT NAME\*

Un cop creat apareixerà la informació amb l'enllaç corresponent per poder fer el git clone.

Desplegament

[Main](#) [PHP Consolidated](#) [Teams](#) [HTTP Monitors](#) [MySQL Database](#) [Cron](#) [Email](#) [SFTP](#) [SSHail](#) [Gitlab](#) [PHPackages](#)

#### Gitlab Info

PROJECT NAME	GROUP	PROJECT URL	CLONE
Això era i no era	APSL	http://localhost:8929/apsl/aixo-era-i-no-era	ssh://git@localhost:2224/apsl/aixo-era-i-no-era.git

## Assignar un repositori ja creat

Pot passar que el repositori ja estigui creat de forma convencional al gitlab i simplement es vulgui assignar al desplegament. En tal cas, l'opció per a fer-ho és `Assign To Existent Git Project`. Caldrà inserir la ID del projecte a gitlab (consultar aquest identificador al gitlab mateix).

### Assign To Existent Git Project

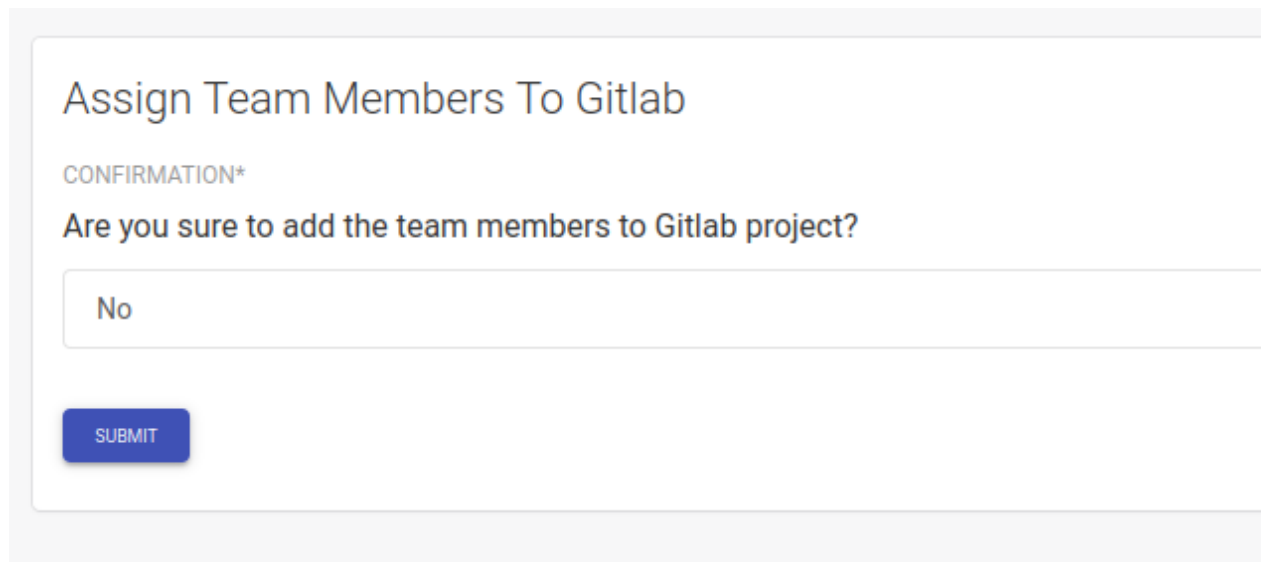
GITLAB PROJECT ID\*

Check the ID at Gitlab. It will overwrite previous assignment

Mentre que l'opció de crear un repositori no es pot editar, aquesta acció sí. Per tant, si s'introdueix una nova ID s'editarà l'assignació (sense fer cap tipus d'acció al Gitlab en el repositori anterior).

## Crear usuaris

Si els desenvolupadors de l'equip no tenen usuaris creats al Gitlab es pot seleccionar l'opció `Assign Team Members to Gitlab` que revisarà els membres de l'equip i si no tenen usuaris els en crearà un. Posteriorment, donarà permisos a aquests usuaris a sobre del repositori en funció del rol que tenen a l'equip.



The screenshot shows a confirmation dialog box with the title "Assign Team Members To Gitlab". Below the title, it says "CONFIRMATION\*" and "Are you sure to add the team members to Gitlab project?". There is a text input field containing the word "No". At the bottom left of the dialog, there is a blue button labeled "SUBMIT".

### Gestió-de-PHPackages-amb-Sygox

El plugin de PHPackages permet la integració de PHPackages amb Sygox. D'aquesta manera, des del desplegament serà possible crear les credencials d'aplicació i d'usuari al Satis.

## Cas d'ús: Flux de creació de credencials PHPackages / Satis

1. Quan un desenvolupador tengui necessitat d'un accés al Satis contactarà amb la OT informant que necessita l'accés i per quin projecte és.
2. L'OT haurà de subministrar un accés nominal al desenvolupador (o cada un d'ells) perquè és configurin els seus equips.
3. També ha de crear un accés per l'aplicació en cas que no estiguin creades. L'accés d'aplicació es configura automàticament al servidor i serveix per dur a terme les mateixes accions però des del propi servidor (això evita tenir credencials de desenvolupador al servidor). Aquestes credencials es donen d'alta des del desplegament pel qual ha demanat accés el desenvolupador.
4. L'OT enviarà les credencials al desenvolupador amb un secret d'un sol ús. Si el desenvolupador té accés a Sygox no es necessari enviar-ho només cal informar que l'accés ja està creat i ell mateix el veurà al Sygox.
5. El desenvolupador una vegada reb les credencials haurà de confirmar l'accés.

**Atenció: L'alta del projecte (que no els accessos) s'ha de vehicular com a petició des d'OT a APSL seguint els mecanismes fins ara establerts**

## Crear credencials

L'acció `Create Project Credentials` crearà les credencials d'aplicació i les desarà al servidor on hi ha l'aplicació en el fitxer `$HOME/.config/composer/auth.json`, de tal manera que totes les accions de composer de servidor ja estaran autenticades. En canvi, l'acció `Create User Credentials` només crearà les credencials per cada un dels membres de l'equip perquè les pugui configurar al seu equip.

Les credencials d'aplicació seran visibles per a tothom, mentre que les d'usuari només ho seran per l'usuari en qüestió.

### Create Project Credentials

CONFIRMATION\*

Are you sure you want to create main PHPackages credentials fot this deployment?

SUBMIT

### Create User Credentials

CONFIRMATION\*

Are you sure you want to create users PHPackages credentials fot this deployment?

SUBMIT

Actions ▾

### Main project credentials

Main project user	app0279
Password	9A3MrJA26Ms5QsbbQZ5JicraHZGECW

No user info available

Les credencials nominals encara que es crein associades a un desplegament apareixeran a tots els desplegaments on aquell desenvolupador participi, així doncs les credencials nominals son transversals i nomes cal que el desenvolupador en tingui una.

Publicació-dades-feed-opendata

**[- AQUEST SERVEI HA ESTAT DESACTIVAT. S'HA ELIMINAT LA PART DEL CRON QUE EXPORTAVA LES DADES AL SERVIDOR DE SYGOX. MÉS INFORMACIÓ A HOSTLAMP-2286 -]**

.  
. .  
. .  
. .

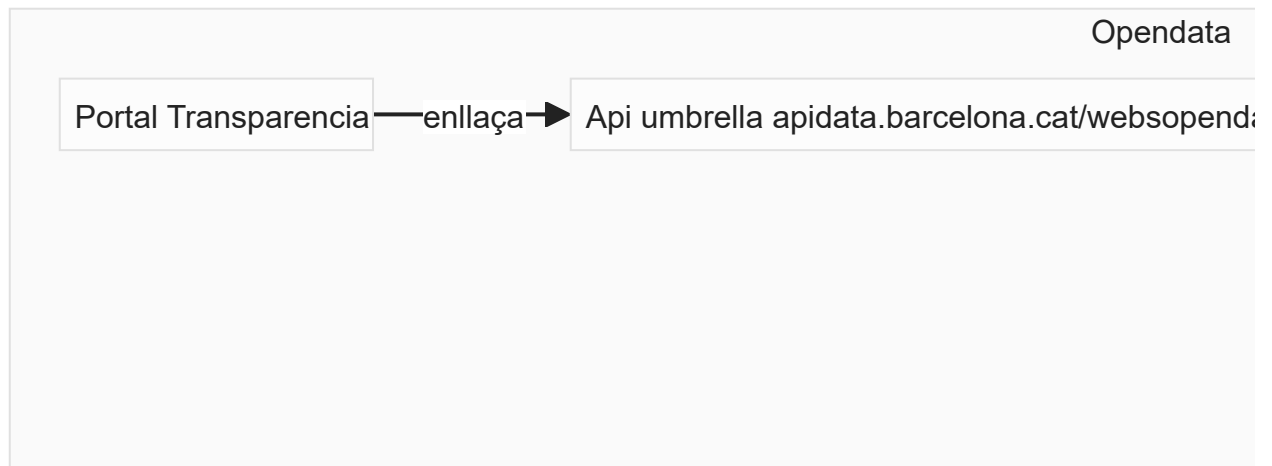
### Entregable de codi:

El codi es troba al repositori (<https://gitlab.dtiicn.cat/sygox/sysgov2-core>)

L'script es troba a scripts/opendata-weblis-report

### Descripció

L'objectiu és elaborar periòdicament un llistat de les web allotjades de manera automatizada.



Per això s'ha desenvolupat un script que ataca l'API de Sygox (eina de govern per desplegar les webs) demanant totes les webs amb determinades característiques.

El llistat es filtra exclouent projectes de desenvolupament, eines internes i d'altres webs que no son públiques cara a l'usuari.

L'script s'executa diàriament i genera un fitxer JSON el format:

```
{
  "weblist": [
    "https://ajuntament.barcelona.cat/biblioteques/bibcanyelles",
    "https://ajuntament.barcelona.cat/sants-montjuic/pla-desenvolupament-
economic",
    "http://ajuntament.barcelona.cat/noubarris/pla-desenvolupament-economic",
    "http://www.barcelona.cat/smart-city-week",
    "https://ajuntament.barcelona.cat/alcaldesa",
    ...
  ]
}
```

Un cop generat el JSON es puja a un bucket de S3:

(<https://opendata.dtibcn.cat/weblist.json> )

Aquest bucket s'exposa públicament al Portal de Transparència mitjançant API Umbrella

(<https://apidata.barcelona.cat/websopendata/>)

### Implicacions derivades

A banda del desenvolupament de la consulta s'ha hagut d'implementar una manera de filtrar les URL podent especificar un llistat de patrons a no publicar.

També ha definit una manera per tal de poder executar còmodament aquest tipus de reports extraient consultes a Sygox.

S'ha definit el domini `opendata.dtibcn.cat` per publicar aquestes informacions.

S'ha hagut de coordinar amb els administradors l'actualització del destí de l'API Umbrella cosa que ha portat més temps de l'esperat ja que no havien entès la petició i el seu API Umbrella no suportava fer connexions per HTTPS emprant SNI, la qual cosa va portar haver d'ajustar algunes configuracions.

### Accés a l'script opendata

L'script que actualment està funcionant a producció, es pot accedir entrant al servidor de sygox, actualment allotjat dins `sygox.aws.dtibcn.cat`.

Es pot entrar emprant `ajbssh` (`ajbssh sygox`).

L'script es troba a `/srv/sysgov2-core/scripts/opendata-weblist-report`

### Crons

S'ha configurat un cron dins `/etc/cron.d/sygox-opendata-weblist-report` que executa:

```
/usr/local/bin/docker-compose -f /srv/sysgov2-core/docker-compose.scripts.yml  
run opendata-weblist-report
```

Amb una periodicitat de: `22 14 * * *`

### Arguments

```
--exclude
```

Es pot passar una sub/string o list de sub/strings que vols excloure

```
--exclude-file
```

Es pot passar un fitxer on hi hagi tots els strings o substrings a excloure. És compatible amb `--exclude` a la vegada.

```
--config
```

Argument que dona un fitxer de configuració per passwords/keys per a connectar-se al servei emprats (s3, sygox)

```
--weblist
```

Argument per a indicar que vols extreure una list amb els resultats de l'script

```
--criticity
```

Argument per a treure una llista de les url amb certa criticitat (low, medium, high)

```
--upload-to-s3
```

Argument per a indicar que s'han de pujar els resultats a s3 i no per print a la consola.

```
--s3-bucket
```

Bucket de s3 on s'ha de enviar el resultat

```
--s3-path
```

Path del bucket S3 on enviar el resultat

```
--environment
```

Argument que indica quin environment concret han de tenir les url a cercar (development, production)

```
--appserver
```

Indicar quin appserver es vol cercar (appserverXX), tan sols les urls de l'appserver concret seran extretes.

Visualitzar-escriptures-de-les-aplicacions

## Descripció

Per tal de monitoritzar el volum d'escriptura a base de dades que fan les aplicacions es va dissenyar el `binloganal`. Es pot consultar la descripció d'aquesta monitorització a [Binloganal: Monitorització de bases de dades](#).

Aquest sistema s'ha integrat a Sygox per tal de tenir descrit a nivell d'aplicació quines són les taules amb més escriptures de la base de dades, ordenades per volum de dades.

## Consultar l'estat de la base de dades

Per tal de veure l'estat de cada taula s'ha implementat una acció. Aquesta acció executa el `binloganal` i reb les dades pertinents a la base de dades de l'aplicació. Aquestes dades són actualitzades cada 24 hores. Això significa que si s'executa l'acció més d'un sol cop durant el mateix dia retornarà la mateixa informació. S'haurà d'esperar al dia següent per veure'n les diferències. Això es així perquè el cron que hi ha al darrera s'executa cada 24 hores a la matinada (veure procediment anteriorment esmentat per a més informació).

Per tal d'executar l'acció cal que entrem a un desplegament concret, a la pestanya MySQL Database i executem l'acció `Update DB Info`. Cal fer notar que aquesta acció

només està disponible per les bases de dades que es troben en clústers d'AWS.

Desplegament

Main PHP Consolidated Teams HTTP Monitors **MySQL Database** CMS Info Cron Email SFTP SSHail Gitlab PHPackages

Actions ▾

- Add MySQL Database
- Remove MySQL Database
- Update Db Info**

DB NAME	USER	PASSWORD	DB ENDPOINT
db_alimentacio926766	u_alimenta		db.app.a.c10d.dtibcn.cat
db_alimentacio8d745a	u_alimer		db.app.a.c10d.dtibcn.cat

## Update Db Info

CONFIRMATION\*

Are you sure you want to update the DB information for this deployment?

Yes

**SUBMIT**

El resultat obtingut serà una taula similar a la següent:

Modified MB last day (2021-11-04 07:36:28)

DB NAME	TABLE	MODIFIED MB
db_alimentacio926766	cache_render	2548.51
db_alimentacio926766	cache_page	1751.9
db_alimentacio926766	cache_entity	284.04
db_alimentacio926766	cache_data	198.65
db_alimentacio926766	watchdog	143.04
db_alimentacio926766	node_field_data	24.17
db_alimentacio926766	node_field_revision	21.6
db_alimentacio926766	cache_default	16.73
db_alimentacio926766	search_index	6.72
db_alimentacio926766	node_revision	3.69
db_alimentacio926766	taxonomy_index	3.51
db_alimentacio926766	key_value_expire	3.31
db_alimentacio926766	node	3.25
db_alimentacio926766	key_value	2.9

## Sincronització-de-permisos-de-Sygox

És possible que després de la implementació de nous plugins alguns equips no tenguin els permisos actualitzats. És per això que hi ha l'acció per sincronitzar, que revisa els permisos que haurien de tenir els rols d'equip i els assigna.

Per tal d'iniciar l'acció haurem d'entrar al desplegament, pestanya de `Teams` i clicar a `Sync Permissions`:

## Desplegament

Main

PHP Consolidated

Teams

HTTP Monitors

MySQL Database

Actions ▾

Assign Team

Refuse Team

Sync Permissions

Posteriorment, indicarem a quin equip volem actualitzar els permisos:

### Sync Permissions

CONFIRMATION\*

Are you sure you want to sync permissions for this deployment?

No

TEAM\*

Select which team you want to update permissions

SUBMIT

Baixa-i-arxivat-de-desplegament-amb-sygox

[\\_TOC\\_](#)

## Definicions

En aquest procediment s'explica com efectuar la baixa, arxivat o eliminació d'un desplegament. Abans de tot, però, s'explicarà la diferència entre ells.

- **Baixa:** La baixa d'un desplegament es podria entendre com a un *soft delete*. Serà el tipus d'acció en la gran majoria dels casos quan l'Ajuntament ens demani donar de baixa alguna aplicació. La baixa implicarà la deshabilitació total de l'aplicació i l'eliminar dels accessos associats. Però **es mantindrà l'equip associat a mode d'històric així com també les bases de dades**.
- **Arxivat:** L'arxivat és una acció que sempre es farà després de la baixa i consistirà en efectuar un backup del codi i base de dades.
- **Eliminat:** L'eliminat, o *hard delete*, només es farà en casos excepcionals i implica l'esborrat d'absolutament tota la informació associada (tots els storages). En general només s'aplicarà a desplegaments creats per error o alguna casuística similar. El desplegament quedarà com a esborrat i quedarà en aquest estat al registre de Sygox.

## Baixa d'un desplegament (*soft delete*)

Per tal de dur a terme la baixa d'un desplegament ho farem de la següent manera. Clicarem a la pestanya de `Main -> Disable deployment`. Aquesta baixa, o deshabilitat, només acabarà bé si prèviament s'han eliminat tots els storages associats al desplegament a excepció de l'equip assignat i les bases de dades que pugui tenir. També es permet que tenguem crons **però han de quedar deshabilitats**, així com els outputs dels escàners de seguretat.

Una vegada el desplegament estigui marcat com a deshabilitat caldrà fer els canvis necessaris al frontal per tal que retorni el codi http 410.

Accedirem al servidor de SaltStack i editarem el fitxer de l'aplicació

```
/srv/pillar/frontal/<FRONTAL>/sites/<DOMINI>/apps.d/400-app-<APLICACIO>.yaml
```

I posar quelcom similar a:

```
<DOMINI>:
  app-<APLICACIO>:
    ssl: True
    insecure: True
    path: '/PATH-APLICACIO'
    custom: |
      return 410;
```

Finalment aplicam el canvi al frontal.

Aplicar recepta:

```
salt <minion_frontend> state.sls http-frontend pillar="{ 'apply_sites': ['Aplicacio'] }" test=True
```

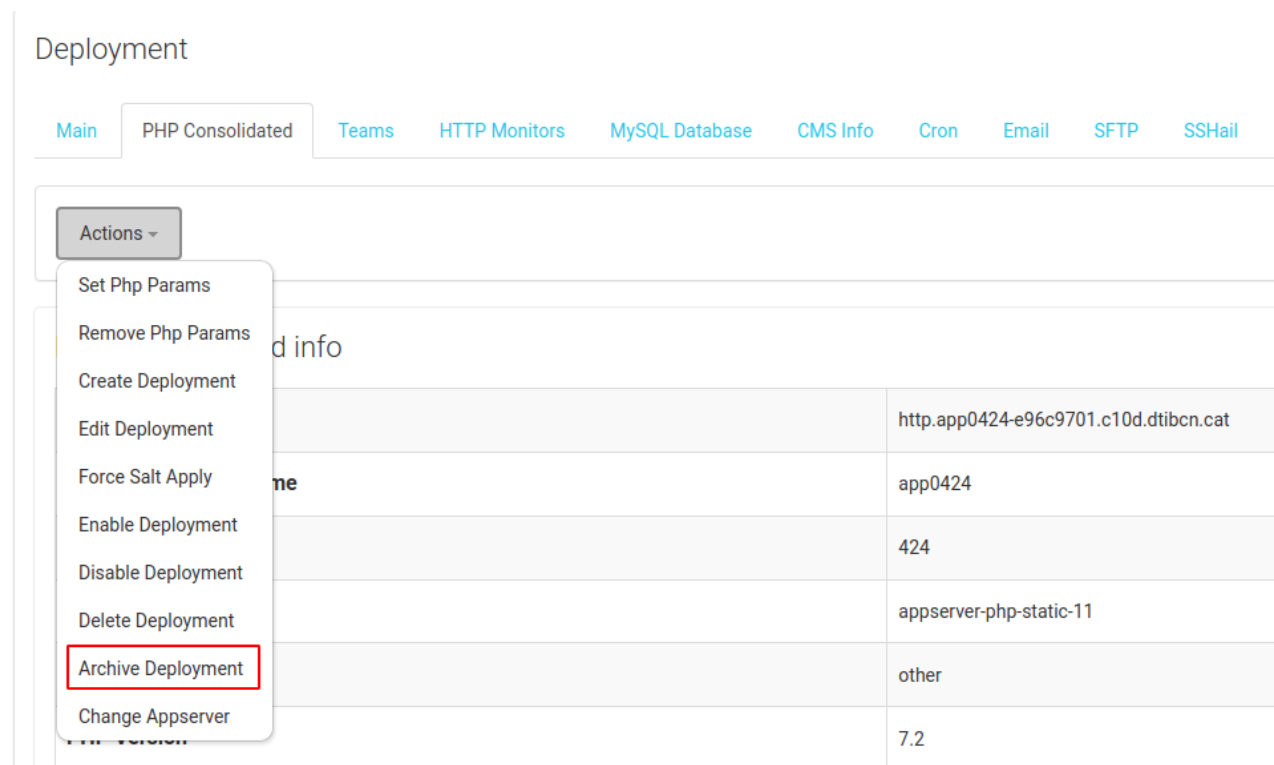
```
salt <minion_frontal> state.sls http-frontend pillar="{ 'apply_sites': ['Aplicacio'] }"
```

## Arxivat d'un desplegament

L'arxivat com s'ha dit és una acció de backup quan es vol donar de baixa una aplicació. Amb posterioritat al seu deshabilitat del punt anterior es podrà executar.

### 1. Arxivat del desplegament a Sygox

Accedim a la pestanya **PHPConsolidated/Actions/Archive Deployment** i s'inicia l'arxivat del desplegament:

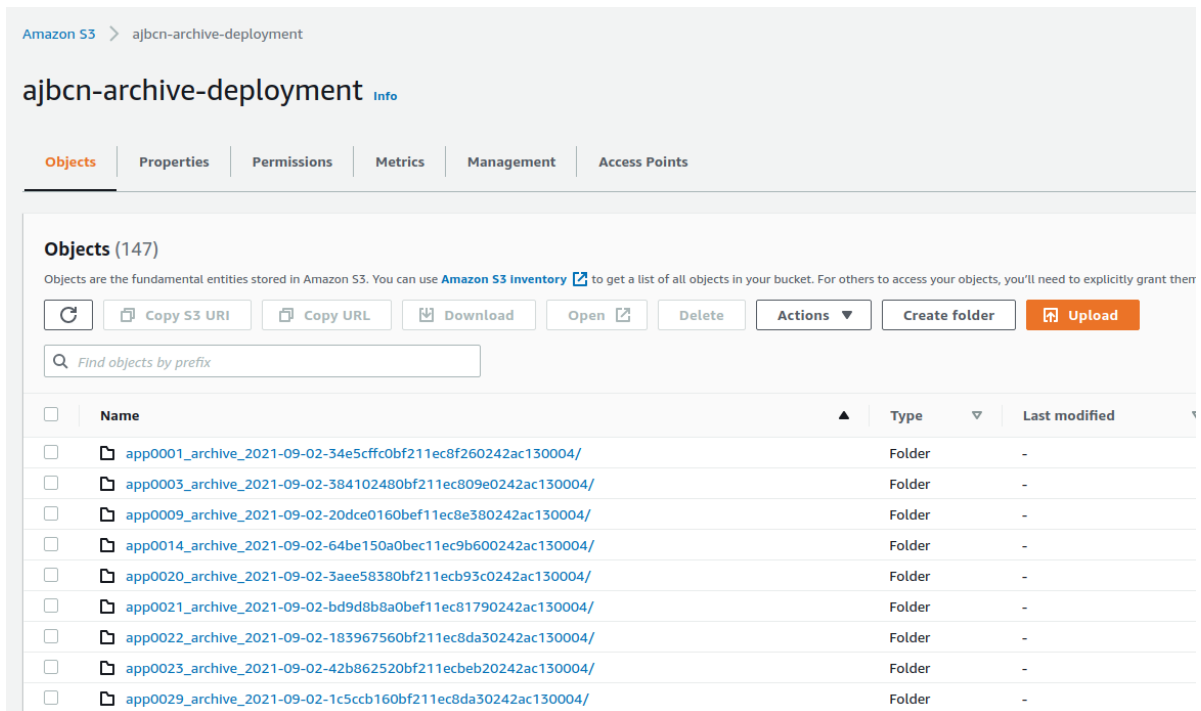


The screenshot shows the 'Deployment' management interface. At the top, there are navigation tabs: 'Main', 'PHP Consolidated', 'Teams', 'HTTP Monitors', 'MySQL Database', 'CMS Info', 'Cron', 'Email', 'SFTP', and 'SSHail'. Below the tabs, there is a table of deployments. A dropdown menu is open over the table, listing various actions. The 'Archive Deployment' action is highlighted with a red border. The table contains the following data:

Deployment Name	Deployment ID
http.app0424-e96c9701.c10d.dtibcn.cat	app0424
app0424	424
appserver-php-static-11	other
7.2	

### 2. Comprovacions a S3

- Accedim a la consola d'AWS: <https://ajbcn-isoc.signin.aws.amazon.com/console>
- Anem a **S3/ajbcn-archive-deployment**



- Busquem el número de app i comprovem que hi hagi els arxius i els tar que ha generat el procés d'arxivat.
- Revisar els logs d'S3 (**falta revisar çon es poden veure**) per veure si hi ha hagut algun problema amb el procés.

## Eliminat d'un desplegament (*hard delete*)

**AQUESTA ACCIÓ NOMÉS ES DURÀ A TERME EN CASOS MOLT DETERMINATS, COM CREACIONS DE DESPLEGAMENTS PER ERROR O SIMILAR.**

Només es podrà eliminar un desplegament que prèviament hagi estat deshabilitat i poder poder-ho dur a terme s'hauran d'haver esborrat absolutament tots els storages, incloses les bases de dades que pugui tenir i els equips associats. Ho farem clicant a `Main -> Delete Deployment`.

En cas que hi hagi configuracions al frontal també s'hauran d'esborrar completament.

## Eliminar desplegaments duplicats al haproxy

A vegades si hi ha un desplegament prèviament eliminat amb la mateixa url, pot ser que les peticions hi vagin a parar i no es serveixin els arxius. En aquest cas s'ha d'esborrar el symlink de configuració del desplegament a salt:

```
/srv/pillar/php-server/<server-que-toqui>/appXXXX.yaml
```

I actualitzar el desplegament:

Applications / La Capella / <https://nou-www.lacapella.barcelona/>

Despliegue

Main PHP Consolidated Teams MySQL Database HTTP Monitors CMS Info Security Canary SSHail SFTP Cron Email Gitlab PHPackages

Actions -

- Set Php Ini Overrides
- Remove Php Ini Overrides
- Set Php Settings
- Remove Php Settings
- Edit Deployment
- Force Salt Apply**
- Archive Deployment
- Change Appserver

Info	
http.app1527-030d15e2.c10d.dtibcn.cat	
app1527	
1527	
php-c10d-static-17	
<b>Framework</b>	drupal_9
<b>PHP Version</b>	8.1

No params settled, using defaults.

Alta,-edició-i-eliminació-de-redireccions-de-campanya-amb-Sygox

## Descripció

El plugin sygox-redirector té per objectiu gestionar les redireccions de campanya. Permet donar d'alta, editar o esborrar redireccions. S'entén una redirecció de campanya com aquella que redirigeix el trànsit que li arriba a una ruta concreta cap a un altra domini on hi ha l'aplicació. Generalment s'usa un domini més curt, per exemple `https://www.barcelona.cat/exemple` que redirigeix el trànsit cap a `https://ajuntament.barcelona.cat/nova-campanya-exemple`

Aquestes redireccions són de tipus 302 i redirigeixen (seguint l'exemple anterior) el que és exactament igual a `/exemple` o `/exemple/` i no pas qualsevol subruta. És a dir, no faria redirecció de `/exemple/hola-mon`.

## Configuració general

Totes les redireccions es gestionen a l'aplicació `App Redireccions de Campanya`. Aquí dins, cada desplegament correspon a un domini diferent. Per exemple, `www.barcelona.cat` o `ajuntament.barcelona.cat`.

## Nova redirecció

Per donar d'alta una nova redirecció cal que anem a l'aplicació `Redireccions` i triem el desplegament que es correspongui amb el domini. Un cop seleccionat, anirem a la pestanya

Applications / Redirections / https://www.barcelona.cat

Desplegament Desactivar Eliminar

Main Campaign redirections

Actions

Deployment info

Status	enabled
Main URL	https://www.barcelona.cat
Environment	environment.development
Platform	platform.http-front-campaign-redirector
Criticality	low
Created at	Thu, 23 Dec 2021 16:01:29 GMT
Updated at	Thu, 23 Dec 2021 16:01:29 GMT

Posteriorment, anem a la pestanya Campaign redirections i triem l'acció Add campaign redirection i emplenem els camps corresponents. Cal notar que s'ha de posar el destí com a url completa, però el path d'origen només a partir de la barra (per exemple /exemple):

Applications / Redirections / https://www.barcelona.cat

Desplegament Desactivar Eliminar

Main Campaign redirections

Actions

- Add Campaign Redirection
- Edit Campaign Redirection
- Remove Campaign Redirection

PATH	DESTINATION	USER OF LAST EDITION	CREATED	EDITED
/aaaravijjs	https://example.com/gwjooumao	demo	2021-12-28 07:33	2021-12-28 07:33
/aalyqphj	https://example.com/lpjfsgjud	demo	2021-12-28 07:33	2021-12-28 07:33
/aavfghaad	https://example.com/wlmygwevb	demo	2021-12-28 07:33	2021-12-28 07:33
/abdolojyu	https://example.com/hdtjgufbmg	demo	2021-12-28 07:33	2021-12-28 07:33
/abdpwkdff	https://example.com/boatwvjff	demo	2021-12-28 07:33	2021-12-28 07:33

Applications / Redirections / https://www.barcelona.cat / Add campaign redirection

## Add Campaign Redirection

DESTINATION URL\*

Destination URL (eg https://example.com/hello)

ORIGIN PATH\*

Origin path (just the path, for example /hello)

SUBMIT

Posteriorment, es comprovarà que la redirecció que s'intenta aplicar no genera conflictes. En cas que generi conflictes s'avortarà l'aplicació. Cal revisar si ja hi ha una altra redirecció igual i en cas de no trobar el conflicte caldrà avisar l'equip de sistemes d'APSL.

## Edició de redirecció

De la mateixa manera que en el cas anterior, caldrà que anem a la pestanya `Campaign redirections` i en aquest cas triem l'opció `Edit campaign redirection`. A continuació triem del desplegable quin és el path d'origen i la nova redirecció que es vol aplicar:

[Applications](#) / [Redirections](#) / <https://www.barcelona.cat> / [Edit campaign redirection](#)

### Edit Campaign Redirection

DESTINATION URL\*

Destination URL (eg <https://example.com/hello>)

REDIRECTION TO EDIT\*

## Eliminació de redireccions

De la mateixa manera que en el cas anterior, caldrà que anem a la pestanya `Campaign redirections` i en aquest cas triem l'opció `Remove campaign redirection`. A continuació, triem del desplegable quina és la redirecció que volem eliminar:

[Applications](#) / [Redirections](#) / <https://www.barcelona.cat> / [Remove campaign redirection](#)

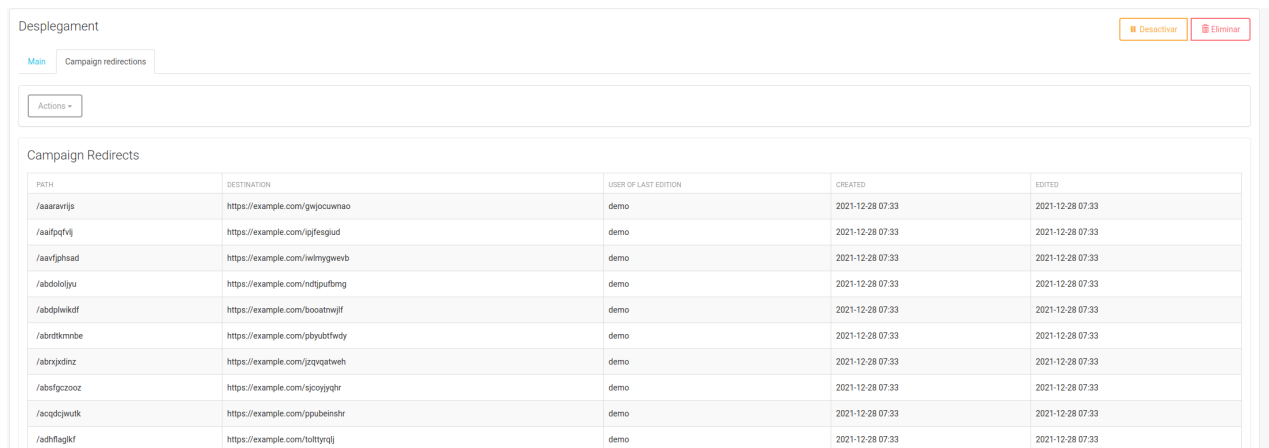
### Remove Campaign Redirection

REDIRECTION TO REMOVE\*

## Consulta de redireccions

Es poden consultar totes les redireccions de campanya aplicades a la mateixa pestanya `Campaign redirections`. La taula mostra quin és el path d'origen, la url de destí, la data

de creació, la data de modificació i quin ha estat l'usuari que ha creat o editat per últim cop aquella redirecció:



The screenshot shows the 'Desplegament' interface with a 'Campaign Redirects' table. The table has columns for PATH, DESTINATION, USER OF LAST EDITION, CREATED, and EDITED. It lists ten redirect entries, each with a unique path and a destination URL, all created and edited by 'demo' on 2021-12-28 07:33.

PATH	DESTINATION	USER OF LAST EDITION	CREATED	EDITED
/aaarvrijs	https://example.com/gwjocuwmao	demo	2021-12-28 07:33	2021-12-28 07:33
/aalfpofvj	https://example.com/igflesgiud	demo	2021-12-28 07:33	2021-12-28 07:33
/aavijghsad	https://example.com/wimrygwevb	demo	2021-12-28 07:33	2021-12-28 07:33
/abdolojju	https://example.com/ndtjpuftmg	demo	2021-12-28 07:33	2021-12-28 07:33
/abdpjwikdf	https://example.com/boostatwjjf	demo	2021-12-28 07:33	2021-12-28 07:33
/abrdtkmibe	https://example.com/pbyustfwjy	demo	2021-12-28 07:33	2021-12-28 07:33
/abrxjdinz	https://example.com/jzqvqatweh	demo	2021-12-28 07:33	2021-12-28 07:33
/abstfgzcooz	https://example.com/sjcoyqghr	demo	2021-12-28 07:33	2021-12-28 07:33
/acqdcjwutk	https://example.com/spubeinahr	demo	2021-12-28 07:33	2021-12-28 07:33
/adhftagktf	https://example.com/holttyrqlj	demo	2021-12-28 07:33	2021-12-28 07:33

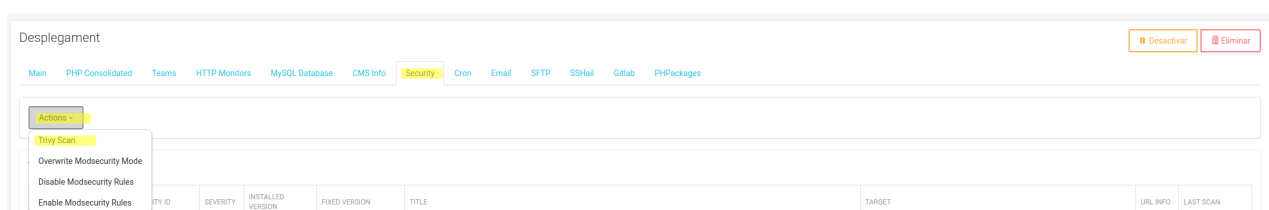
## Escàner-de-vulnerabilitats-amb-Trivy-a-Sygox

### Descripció

El mòdul de seguretat de Sygox permet entre d'altres accions escanejar el desplegament per buscar vulnerabilitats al projecte. Per fer-ho s'utilitza l'eina de [Trivy](#). Trivy és un programari que busca vulnerabilitats donat una ruta concreta del sistema de fitxers i pot comprovar imatges de contenidors, sistema de fitxers, repositoris i fitxers de configuració.

### Iniciar un escaneig

Per tal d'iniciar un escaneig del desplegament caldrà anar a la pestanya de Seguretat i clicar a l'acció de `Trivy Scan`:



The screenshot shows the 'Desplegament' interface with the 'Security' tab selected. A dropdown menu is open under the 'Actions' button, showing the 'Trivy Scan' option. Below the menu is a table with columns for ID, SEVERITY, INSTALLED VERSION, FIXED VERSION, TITLE, TARGET, URL INFO, and LAST SCAN.

ID	SEVERITY	INSTALLED VERSION	FIXED VERSION	TITLE	TARGET	URL INFO	LAST SCAN
----	----------	-------------------	---------------	-------	--------	----------	-----------

L'output que obtindrem reportarà la llibreria afectada, així com la versió actual i la versió que soluciona el problema. També informa del fitxer afectat i la URL amb més informació sobre la vulnerabilitat, entre d'altres:

Applications / Grafitx Castell de Montjuïc / https://www.barcelona.cat/grafitxcastellmontjuic/

Desplegament Desactivar Eliminar

Main PHP Consolidated Teams HTTP Monitors MySQL Database CMS Info Security Cron Email SFTP SSHail Gitlab PHPackages

Actions -

Trivy Scan

LIBRARY	VULNERABILITY ID	SEVERITY	INSTALLED VERSION	FIXED VERSION	TITLE	TARGET	URL INFO	LAST SCAN
acorn	GHSA-6chw-6fng-f759	HIGH	5.5.3	5.7.4, 7.1.1, 6.4.1	Regular Expression Denial of Service in Acorn	grafitxcastellmontjuic/wp-content/themes/understrap-child/package-lock.json	<a href="#">More info</a>	2022-01-10 09:34
axios	CVE-2019-10742	HIGH	0.17.1	0.18.1	Denial of Service in axios	grafitxcastellmontjuic/wp-content/themes/understrap-child/package-lock.json	<a href="#">More info</a>	2022-01-10 09:34
axios	CVE-2020-28168	HIGH	0.17.1	0.21.1	nodejs-axios: allows an attacker to bypass a proxy by providing a URL that responds with a redirect to a restricted host or IP address	grafitxcastellmontjuic/wp-content/themes/understrap-child/package-lock.json	<a href="#">More info</a>	2022-01-10 09:34
axios	CVE-2021-3749	HIGH	0.17.1	0.21.2	nodejs-axios: Regular expression denial of service in trien function	grafitxcastellmontjuic/wp-content/themes/understrap-child/package-lock.json	<a href="#">More info</a>	2022-01-10 09:34
bl	CVE-2020-8244	HIGH	1.2.2	2.2.1, 1.2.3, 4.0.3, 3.0.1	nodejs-bl: buffer over-read vulnerability leads to corrupted BufferList which can result in uninitialized memory being leaked	grafitxcastellmontjuic/wp-content/themes/understrap-child/package-lock.json	<a href="#">More info</a>	2022-01-10 09:34
cryptiles	CVE-2018-1000620	CRITICAL	2.0.5	4.1.2	nodejs-cryptiles: Insecure randomness causes the randomDigits() function returns a pseudo-random data string biased to certain digits	grafitxcastellmontjuic/wp-content/themes/understrap-child/package-lock.json	<a href="#">More info</a>	2022-01-10 09:34

## sygox-mozilla-observatory

El [Mozilla Observatory](#) és un software que permet fer un anàlisi de seguretat a nivell d'HTTP. Aquestes eines han estat integrades a Sygox per tal que els desenvolupadors siguin conscients de què poden millorar.

## Iniciar un escàner

Per iniciar un escàner de seguretat HTTP cal anar a Sygox, al desplegament en qüestió, a la pestanya `Security` i clicar a `Analyze HTTP Security`:

Desplegament

Main PHP Consolidated Teams HTTP Monitors MySQL Database CMS Info Security Cron Email SFTP SSHail Gitlab PHPackages

Actions -

- Overwrite Modsecurity Mode
- Disable Modsecurity Rules
- Enable Modsecurity Rules
- Trivy Scan
- Analyze Http Security

de not modified. Using default settings.

## Consultar els resultats

Per consultar els resultats només cal anar a la pestanya `Security`. Aquí hi podem veure dos widgets. Un de general amb la nota global i un de més específic amb els tests que l'eina ha dut a terme, així com veure si l'ha passat o no.

Widget general. Hi podem veure la nota numèrica i en lletra, així com la data de l'últim escàner.

## Mozilla Observatory Score

Score	45
Grade	C-
Last scan	2022-04-12 08:06 (UTC+0)

El segon widget, de detall, es pot veure quins tests s'han fet. En cas que s'hagi fallat, a la darrera columna es pot trobar l'enllaç a la wiki per tal de poder-lo solventar.

### Mozilla Observatory Details

NAME	PASS	SCORE	DESCRIPTION	WIKI
content-security-policy	false	-25	Content Security Policy (CSP) header not implemented	<a href="#">More info</a>
cookies	true	0	No cookies detected	
contribute	true	0	Contribute.json isn't required on websites that don't belong to Mozilla	
cross-origin-resource-sharing	true	0	Public content is visible via cross-origin resource sharing (CORS) Access-Control-Allow-Origin header	
public-key-pinning	true	0	HTTP Public Key Pinning (HPKP) header not implemented	
redirection	true	0	Initial redirection is to HTTPS on same host, final destination is HTTPS	
referrer-policy	true	0	Referer-Policy header not implemented	
subresource-integrity	true	0	Subresource Integrity (SRI) not implemented, but all scripts are loaded from a similar origin	
x-content-type-options	true	0	X-Content-Type-Options header set to "nosniff"	
x-frame-options	true	0	X-Frame-Options (XFO) header set to SAMEORIGIN or DENY	
x-xss-protection	false	-10	X-XSS-Protection header not implemented	<a href="#">More info</a>

canary-deploy

## Descripció

Es coneix com a *canary* a la tècnica per donar accés a un grup d'usuaris a un desplegament alternatiu al productiu emprant la mateixa URL per tal de poder-hi fer validacions abans de obrir-ho al públic general.

En el cas concret de l'Ajuntament consistirà en l'accés a l'entorn de desenvolupament a través de la URL productiva per tal que la web pugui ser validada.

Aquesta tècnica permet publicacions més robustes i ràpides especialment útil quan s'han de fer dins finestres de temps ajustades.

Aquest accés quedarà restringit a personal de l'Ajuntament. La manera d'accedir-hi serà mitjançant una *cookie* de tal manera que si a la petició hi és present es podrà consultar el nou entorn. Aquesta *cookie* es donarà només a aquelles persones que hagin de veure aquest nou entorn.

Aquesta tècnica s'empra el moment de publicar una nova web o en la substitució d'una existent, en general les correccions sobre una web existent no necessiten aquesta validació addicional.

## Fluxes de treball

## Publicació de web de nova creació

En una web de nova creació es tindrà l'entorn de dev- i quan s'acosti la publicació serà necessari també el nou-.

Serà l'entorn nou- que al moment de validació prèvi a la publicació es posarà com a canary quedant accessible a la URL final per la gent que tingui la cookie habilitada.

En aquest cas si no es té la cookie la URL productiva no serà accessible ja que no hi ha una web prèvia.

Al moment de la publicació es promocionaria la canary a la web productiva cosa que faria que la cookie deixés de ser necessària per accedir a la web.

Com que ja s'hauria validat la web, l'únic canvi és fer innecessària la cookie, el qual triga segons en ser aplicat.

## Publicació de web que en substitueix una altra

En el cas d'una web que en substitueix una altra tindrem una web dev- on s'ha fet el desenvolupament, la nou- preparada per substituir la productiva i la productiva que serà substituïda en la publicació. Eventualment es podria tenir un altre entorn de dev per l'antiga productiva en cas que s'hi hagin fet un manteniment paral·lel a la creació de la nova web.

La web nou- seria posada en mode canary i passaria a tenir la mateixa URL que la web productiva però només accessible si es té la cookie.

Un cop validat al moment de la publicació el desplegament del canary seria intercanviat per el productiu i el productiu quedaria amb una URL old-. L'únic que introdueix el canary es que es força un intercanvi de frontal en les publicacions quan es substitueix una web. La old quedaria preparat per ser arxivat i donat de baixa.

## Interacció amb CI/CD

La publicació amb canary es independent del CI/CD. Els canvis amb CI/CD es fan a cada entorn ja sigui dev-, nou- o productiu.

Si s'ha d'aplicar un canvi a un entorn productiu aquest segueix el flux habitual, fer-se a dev primer, després mesclar a master i desplegar a producció o bé directament desplegant a master i per tant producció si es un hotfix. En aquestes correccions no hi cap intercanvi d'entorns darrera de la URL productiva.

## Procediments

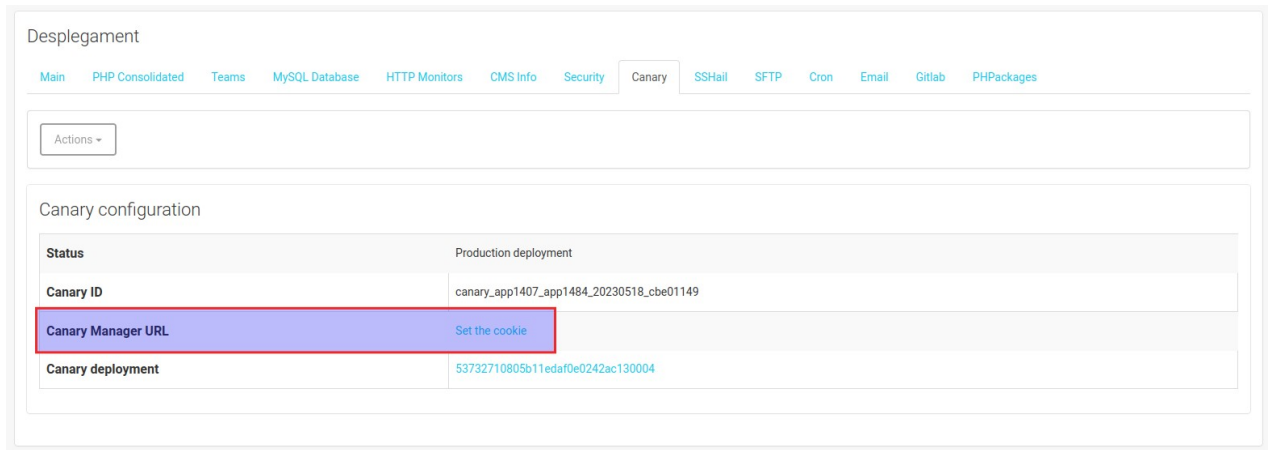
### Alta, eliminació o pas a producció

Per tal de sol.licitar la creació d'un canary, la seva eliminació o el pas a producció s'haurà de fer via tiquet de JIRA.

## Accedir a una versió canary

Una vegada APSL ha donat d'alta un entorn com a canary es pot accedir a Sygox tant al desplegament que és productiu com al que és desenvolupament per tal de fixar la cookie.

Clicarem a "set the cookie" i posteriorment a la nova pàgina clicarem a "Afegeix".



Desplegament

Main PHP Consolidated Teams MySQL Database HTTP Monitors CMS Info Security **Canary** SSHail SFTP Cron Email Gitlab PHPackages

Actions -

Canary configuration

Status	Production deployment
Canary ID	canary_app1407_app1484_20230518_cbe01149
Canary Manager URL	Set the cookie
Canary deployment	53732710805b11edaf0e0242ac130004

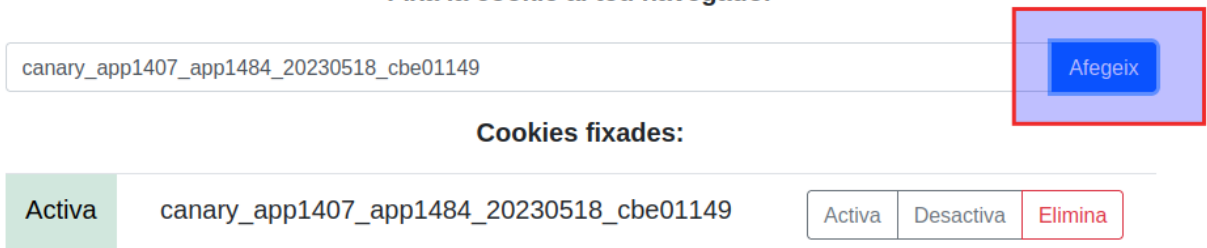
## AjBCN Canary Manager

ajuntament.barcelona.cat

Eina per gestionar les cookies dels canary deploy al teu navegador.

Aquesta eina serveix per fixar o eliminar cookies que habiliten l'accés a versions canary d'una aplicació. El seu ús només és per personal de l'Ajuntament de Barcelona que necessita accedir a versions de webs que encara no han estat publicades.

### Fixa la cookie al teu navegador



canary\_app1407\_app1484\_20230518\_cbe01149

Afegeix

Cookies fixades:

Activa	canary_app1407_app1484_20230518_cbe01149	Activa	Desactiva	Elimina
--------	--	--------	-----------	---------

Si volem desactivar la cookie o eliminar-la seguirem el mateix procediment.

Mentre una aplicació estigui fixada com a canary, la cookie tindrà efecte quan estigui activa.

Secció orientada als administradors de Sygox els quals fan operacions avançades com desplegaments de codi i manteniment de la propia eina

## Actualitzar-codi-de-l'aplicació

Per tal d'actualitzar el codi hem de fer el següent.

S'ha de tenir en compte l'ordre ja que `front` , `worker` i `seq-generator` depenen del `core` . Així doncs, el `core` és l'últim a apagar.

Accedir al servidor `sygox` . Si hi ha canvis al `core` o al `worker` s'haurà de fer un pull primer.

Fem els builds per minimitzar el downtime:

```
cd /srv/sysgov2-core
make build

cd /srv/sysgov2-worker
make build

cd /srv/sysgov2-front # Si no hi ha canvis de front no fer aquest build
make build
```

Aturam els serveis:

```
cd /srv/sysgov2-front
make stop

cd /srv/sysgov2-worker
make stop

cd /srv/sygox-seq-generator
make stop

cd /srv/sysgov2-core
make stop
```

Tornam a aixecar el servei:

```
cd /srv/sysgov2-core
make up

cd /srv/sygox-seq-generator
make up

cd /srv/sysgov2-worker
```

```
make up

cd /srv/sysgov2-front
make up
```

## Preparació-Sygox-CLI

Sygox disposa d'una CLI que ataca la seva API. D'aquesta manera és poden automatitzar algunes accions fàcilment.

La idea del Sygox és que tant la CLI com el client web senzillament són consumidors de l'API del backend.

La CLI està configurada a l'usuari root del servidor intern-sygox (on hi ha el sygox). Es poden emprar les comandes `sygox-cli` i `sygox-shell` un cop canviat a l'usuari root dins del servidor.

Si per altra banda ho volem configurar en local podem fer-ho així:

Haurem de clonar el repositori de [git@gitlab.apsl.net:AjuntamentBarcelona/sygox-cli.git](https://gitlab.apsl.net:AjuntamentBarcelona/sygox-cli.git). Si s'ha seguit la posada a punt de l'entorn de desenvolupament ja ho tindrem a `ARREL_SYGOX/sygox/tools/sygox-cli`.

Copiam el fitxer `sysgov-client.env.example` a `prod.env` i ajustam les variables d'entorn `SYGOX_HOST` / `SYGOX_SERVER_SECRET`.

```
cp sysgov-client.env.example prod.env

vim prod.env

# i ajustam:

SYGOX_HOST=https://web:ajuntament@sygox.dtibcn.cat
SYGOX_SERVER_SECRET=Posam-el-mateix-secret-que-hi-ha-al-servidor
SYGOX_EXECUTE_JOBS=True # Si es deixa a false només es fa dry runs
```

Després afegim les següents línies al nostre `~/.bash_aliases` ajustant `ARREL_SYGOX/sygox/tools/sygox-cli`.

```
alias sygox-cli='docker-compose -f ARREL_SYGOX/sygox/tools/sygox-cli/docker-
compose.remote.yaml run --env-file ARREL_SYGOX/sygox/tools/sygox-cli/prod.env
--rm client sygox'
alias sygox-shell='docker-compose -f ARREL_SYGOX/sygox/tools/sygox-
```

```
cli/docker-compose.remote.yaml run --env-file ARREL_SYGOX/sygox/tools/sygox-  
cli/prod.env --rm client sygox-shell'
```

Comprovam que funciona llistant les aplicacions:

```
sygox-cli application list
```

També podem provar de llistar els desplegaments de l'última aplicació de la llista (per exemple)

```
sygox-cli deployment list --application_id $(sygox-cli application list |  
tail -2 | awk '{print $2}' | head -1)
```

Donar-d'alta-un-rol-d'usuari

Els rols són agrupacions de permisos sobre recursos.

Un cop definit completament el rol es pot assignar a altres usuaris i ja inclourà totes les polítiques afegides el primer cop.

Aquí es descriu l'alta dels rols `admin` i `_g_dti_technician`.

## Rol d'administrador

Per crear el rol d'usuari administrador:

```
INSERT INTO roles ("role") VALUES ('admin');  
  
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES  
( 'admin', 'create', '*', true);  
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES  
( 'admin', 'create', '*:*', true);  
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES  
( 'admin', 'create', '*:*:*', true);  
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES  
( 'admin', 'create', '*:*:*:*', true);  
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES  
( 'admin', 'create', '*:*:*:*:*', true);  
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES  
( 'admin', 'create', '*:*:*:*:*:*', true);  
  
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES  
( 'admin', 'retrieve', '*', true);
```

```

INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('admin', 'retrieve', '*:*', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('admin', 'retrieve', '*:*:*', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('admin', 'retrieve', '*:*:*:*', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('admin', 'retrieve', '*:*:*:*:*', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('admin', 'retrieve', '*:*:*:*:*:*', true);

INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('admin', 'update', '*', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('admin', 'update', '*:*', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('admin', 'update', '*:*:*', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('admin', 'update', '*:*:*:*', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('admin', 'update', '*:*:*:*:*', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('admin', 'update', '*:*:*:*:*:*', true);

INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('admin', 'delete', '*', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('admin', 'delete', '*:*', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('admin', 'delete', '*:*:*', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('admin', 'delete', '*:*:*:*', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('admin', 'delete', '*:*:*:*:*', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('admin', 'delete', '*:*:*:*:*:*', true);

INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('admin', 'execute', '*', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('admin', 'execute', '*:*', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('admin', 'execute', '*:*:*', true);

```

```

INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('admin', 'execute', '*:*:*:*', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('admin', 'execute', '*:*:*:*:*', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('admin', 'execute', '*:*:*:*:*:*', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('admin', 'execute', '*:*:*:*:*:*:*', true);

```

## Tècnic de la DTI

Per crear el rol de tècnic de la DTI:

```

INSERT INTO roles ("role") VALUES ('_g_dti_technician');

-- Llistar totes les applications i deployments
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('_g_dti_technician', 'retrieve', 'application:*', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('_g_dti_technician', 'retrieve', 'application:*:deployment:*', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('_g_dti_technician', 'retrieve', 'application:*:deployment:*:entry:*',
true);

-- Storages de plugins de només lectura
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('_g_dti_technician', 'retrieve',
'application:*:deployment:*:storage:php_consolidated_php_params:*', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('_g_dti_technician', 'retrieve',
'application:*:deployment:*:storage:php_consolidated_docker_services:*',
true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('_g_dti_technician', 'retrieve',
'application:*:deployment:*:storage:http_monitoring_monitors:*', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('_g_dti_technician', 'retrieve',
'application:*:deployment:*:storage:php_consolidated_cron:*', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('_g_dti_technician', 'retrieve',
'application:*:deployment:*:storage:cms_info:*', true);

-- Gestió de bases de dades (lectura i creació, però no esborrat)
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('_g_dti_technician', 'execute',
'application:*:deployment:*:action:db_manager_mysql_database:add_MySQL_databa
se', true);

```

```

INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('g_dti_technician', 'retrieve',
'application*:deployment*:storage:db_manager_mysql_servers:*', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('g_dti_technician', 'create',
'application*:deployment*:storage:db_manager_mysql_databases', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('g_dti_technician', 'retrieve',
'application*:deployment*:storage:db_manager_mysql_databases:*', true);

-- Gestió de bases de dades (DB info)
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('g_dti_technician', 'create',
'application*:deployment*:storage:db_manager_db_info', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('g_dti_technician', 'execute',
'application*:deployment*:action:db_manager_mysql_database:update_db_info',
true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('g_dti_technician', 'retrieve',
'application*:deployment*:storage:db_manager_db_info:*', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('g_dti_technician', 'update',
'application*:deployment*:storage:db_manager_db_info:*', true);

-- SSHail (lectura, creació, esborrat i lectura de contrasenyes)
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('g_dti_technician', 'execute',
'application*:deployment*:action:php_c10d_sshail:add_user_SSHail', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('g_dti_technician', 'execute',
'application*:deployment*:action:php_c10d_sshail:remove_user_SSHail',
true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('g_dti_technician', 'execute',
'application*:deployment*:action:php_c10d_sshail:edit_user_SSHail', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('g_dti_technician', 'execute',
'application*:deployment*:action:php_c10d_sshail:add_sporadic_SSHail',
true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('g_dti_technician', 'create',
'application*:deployment*:storage:php_consolidated_sshail_users', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('g_dti_technician', 'delete',
'application*:deployment*:storage:php_consolidated_sshail_users:*', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('g_dti_technician', 'retrieve',
'application*:deployment*:storage:php_consolidated_sshail_users:*', true);

```

```

INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('_g_dti_technician', 'update',
'application*:deployment*:storage:php_consolidated_sshail_users:*', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('_g_dti_technician', 'retrieve',
'application*:deployment*:unmask_passwords:php_consolidated_sshail_users',
true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('_g_dti_technician', 'retrieve',
'application*:deployment*:list_all_users:php_consolidated_sshail_users',
true);

-- sFTP (lectura, creació, esborrat i lectura de contrasenyes)
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('_g_dti_technician', 'execute',
'application*:deployment*:action:php_c10d_sftp:add_user_sFTP', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('_g_dti_technician', 'execute',
'application*:deployment*:action:php_c10d_sftp:add_sporadic_user_sFTP',
true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('_g_dti_technician', 'execute',
'application*:deployment*:action:php_c10d_sftp:remove_user_sFTP', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('_g_dti_technician', 'create',
'application*:deployment*:storage:php_consolidated_sftp_users', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('_g_dti_technician', 'delete',
'application*:deployment*:storage:php_consolidated_sftp_users:*', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('_g_dti_technician', 'retrieve',
'application*:deployment*:storage:php_consolidated_sftp_users:*', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('_g_dti_technician', 'retrieve',
'application*:deployment*:unmask_passwords:php_consolidated_sftp_users',
true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('_g_dti_technician', 'delete',
'application*:deployment*:storage:php_consolidated_sftp_users', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('_g_dti_technician', 'retrieve',
'application*:deployment*:list_all_users:php_consolidated_sftp_users',
true);

-- email (lectura, creació, esborrat)
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('_g_dti_technician', 'retrieve', 'application*:deployment*:entry:php-
consolidated-email', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES

```

```

('g_dti_technician', 'create',
'application*:deployment*:storage:php_consolidated_email', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('g_dti_technician', 'execute',
'application*:deployment*:action:php_c10d_email:set_email_configuration',
true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('g_dti_technician', 'execute',
'application*:deployment*:action:php_c10d_email:remove_email_configuration'
, true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('g_dti_technician', 'retrieve',
'application*:deployment*:storage:php_consolidated_email:*', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('g_dti_technician', 'delete',
'application*:deployment*:storage:php_consolidated_email:*', true);

-- equips
INSERT INTO role_policies ("role", "action", "resource") VALUES
('g_dti_technician', 'create', 'platform:team'); -- Permis per crear equips
INSERT INTO role_policies ("role", "action", "resource") VALUES
('g_dti_technician', 'create', 'application:<app-id-team>:deployment'); --
Per crear deployments a l'app d'Equips (substituir app id)
INSERT INTO role_policies ("role", "action", "resource") VALUES
('g_dti_technician', 'execute',
'application*:deployment*:action:sygox_teams_deployment_member_manager:assi
gn_member'); -- Per crear membres dins un equip
INSERT INTO role_policies ("role", "action", "resource") VALUES
('g_dti_technician', 'execute',
'application*:deployment*:action:sygox_teams_deployment_member_manager:refu
se_member'); -- Per eliminar un membre d'un equip
INSERT INTO role_policies ("role", "action", "resource") VALUES
('g_dti_technician', 'execute',
'application*:deployment*:action:sygox_teams:assign_team'); -- Per assignar
equips a desplegaments
INSERT INTO role_policies ("role", "action", "resource") VALUES
('g_dti_technician', 'execute',
'application*:deployment*:action:sygox_teams:refuse_team'); -- Per
desassignar equips de deployments
INSERT INTO role_policies ("role", "action", "resource") VALUES
('g_dti_technician', 'execute',
'application*:deployment*:action:member_manager:edit_role');
INSERT INTO role_policies ("role", "action", "resource") VALUES
('g_dti_technician', 'create',
'application*:deployment*:storage:team_deployments'); -- Per crear storages
team_deployments
INSERT INTO role_policies ("role", "action", "resource") VALUES
('g_dti_technician', 'create',
'application*:deployment*:storage:team_members'); -- Per crear storages

```

```

team_members
INSERT INTO role_policies ("role", "action", "resource") VALUES
('_g_dti_technician', 'retrieve',
'application:*:deployment:*:storage:team_deployments:*'); -- Per obtenir
storages team_deployments
INSERT INTO role_policies ("role", "action", "resource") VALUES
('_g_dti_technician', 'retrieve',
'application:*:deployment:*:storage:team_members:*'); -- Per obtenir storages
team_members
INSERT INTO role_policies ("role", "action", "resource") VALUES
('_g_dti_technician', 'delete',
'application:*:deployment:*:storage:team_members:*'); -- Per eliminar membres
d'un equip
INSERT INTO role_policies ("role", "action", "resource") VALUES
('_g_dti_technician', 'delete',
'application:*:deployment:*:storage:team_deployments:*'); -- Per desassignar
equips de deployments
INSERT INTO role_policies ("role", "action", "resource") VALUES
('_g_dti_technician', 'update',
'application:*:deployment:*:storage:team_members:*'); -- Per editar rols de
membres d'equip

-- phpackages (creació de credencials d'usuaris i de projecte)
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('_g_dti_technician', 'create',
'application:*:deployment:*:storage:phpackages_users', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('_g_dti_technician', 'create',
'application:*:deployment:*:storage:phpackages_project', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('_g_dti_technician', 'execute',
'application:*:deployment:*:action:phpackages:create_project_credencials',
true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('_g_dti_technician', 'execute',
'application:*:deployment:*:action:phpackages:create_user_credencials',
true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('_g_dti_technician', 'retrieve',
'application:*:deployment:*:storage:phpackages_users:*', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('_g_dti_technician', 'retrieve',
'application:*:deployment:*:storage:phpackages_project:*', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('_g_dti_technician', 'retrieve',
'application:*:deployment:*:unmask_passwords:phpackages_users', true);

-- gitlab (creació de repositoris i usuaris)

```

```

INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('g_dti_technician', 'create', 'application*:deployment*:storage:git',
true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('g_dti_technician', 'update', 'application*:deployment*:storage:git:*',
true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('g_dti_technician', 'execute',
'application*:deployment*:action:git_manager:assign_team_members_to_gitlab'
, true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('g_dti_technician', 'execute',
'application*:deployment*:action:git_manager:assign_to_existent_git_project'
, true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('g_dti_technician', 'execute',
'application*:deployment*:action:git_manager:create_git_project', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('g_dti_technician', 'execute',
'application*:deployment*:action:git_manager:configure_gitlab_deploy_key',
true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('g_dti_technician', 'retrieve', 'application*:deployment*:storage:git:*',
true);

-- CMS Info
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('g_dti_technician', 'retrieve',
'application*:deployment*:storage:php_consolidated_cms_info:*', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('g_dti_technician', 'create',
'application*:deployment*:storage:php_consolidated_cms_info', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('g_dti_technician', 'update',
'application*:deployment*:storage:php_consolidated_cms_info:*', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('g_dti_technician', 'execute',
'application*:deployment*:action:php_c10d_cms_info:update_checklist',
true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('g_dti_technician', 'execute',
'application*:deployment*:action:php_c10d_cms_info:update_only_cms_info',
true);

-- Trivy
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('g_dti_technician', 'execute',
'application*:deployment*:action:php_c10d_security:trivy_scan', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES

```

```

('g_dti_technician', 'create',
'application*:deployment*:storage:php_consolidated_security_trivy', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('g_dti_technician', 'retrieve',
'application*:deployment*:storage:php_consolidated_security_trivy:*',
true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('g_dti_technician', 'update',
'application*:deployment*:storage:php_consolidated_security_trivy:*',
true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('g_dti_technician', 'delete',
'application*:deployment*:storage:php_consolidated_security_trivy:*',
true);

-- Sygox redirector
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('g_dti_technician', 'execute',
'application*:deployment*:action:campaign_redirector_manager:add_campaign_r
edirection', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('g_dti_technician', 'execute',
'application*:deployment*:action:campaign_redirector_manager:edit_campaign_
redirection', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('g_dti_technician', 'execute',
'application*:deployment*:action:campaign_redirector_manager:remove_campaig
n_redirection', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('g_dti_technician', 'create',
'application*:deployment*:storage:campaign_redirections', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('g_dti_technician', 'retrieve',
'application*:deployment*:storage:campaign_redirections:*', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('g_dti_technician', 'update',
'application*:deployment*:storage:campaign_redirections:*', true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('g_dti_technician', 'delete',
'application*:deployment*:storage:campaign_redirections:*', true);

-- EC2 Docker Apps
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('g_dti_technician', 'execute',
'application*:deployment*:action:ec2_docker_app_manager:start_server',
true);
INSERT INTO role_policies ("role", "action", "resource", "allowance") VALUES
('g_dti_technician', 'execute',

```

```
'application*:deployment*:action:ec2_docker_app_manager:stop_server',  
true);
```

## Altres permissos d'exemple

Aquí hi ha un llistat d'altres permissos a mode d'exemple per si s'han de canviar `app_id` i `deployment_id` pels IDs de l'aplicació i desplegament adients.

```
/** Admin */  
  
insert into user_roles ("role", "username") values ('admin', 'admin');  
  
/** Normal user with all needed permissions for a php-consolidated platform  
***/  
  
/* role and user */  
insert into roles ("role") values ('_u_user');  
insert into user_roles ("role", "username") values ('_u_user', 'user');  
  
/* application */  
insert into role_policies ("role", "action", "resource", "allowance")  
values ('_u_user', 'create', 'application', true);  
  
insert into role_policies ("role", "action", "resource", "allowance")  
values ('_u_user', 'retrieve', 'application:app_id', true);  
  
insert into role_policies ("role", "action", "resource", "allowance")  
values ('_u_user', 'update', 'application:app_id', true);  
  
insert into role_policies ("role", "action", "resource", "allowance")  
values ('_u_user', 'delete', 'application:app_id', true);  
  
/* deployment */  
insert into role_policies ("role", "action", "resource", "allowance")  
values ('_u_user', 'create', 'application:app_id:deployment', true);  
  
insert into role_policies ("role", "action", "resource", "allowance")  
values ('_u_user', 'retrieve', 'application:app_id:deployment:dep_id', true);  
  
insert into role_policies ("role", "action", "resource", "allowance")  
values ('_u_user', 'update', 'application:app_id:deployment:dep_id', true);  
  
insert into role_policies ("role", "action", "resource", "allowance")  
values ('_u_user', 'delete', 'application:app_id:deployment:dep_id', true);  
  
/* entries (tabs) */  
insert into role_policies ("role", "action", "resource", "allowance")  
values ('_u_user', 'retrieve',
```

```

'application:app_id:deployment:dep_id:entry:deployment-main', true);

insert into role_policies ("role", "action", "resource", "allowance")
values ('_u_user', 'retrieve',
'application:app_id:deployment:dep_id:entry:php-consolidated', true);

insert into role_policies ("role", "action", "resource", "allowance")
values ('_u_user', 'retrieve',
'application:app_id:deployment:dep_id:entry:php-consolidated-cron', true);

insert into role_policies ("role", "action", "resource", "allowance")
values ('_u_user', 'retrieve',
'application:app_id:deployment:dep_id:entry:php-consolidated-email', true);

insert into role_policies ("role", "action", "resource", "allowance")
values ('_u_user', 'retrieve',
'application:app_id:deployment:dep_id:entry:php-consolidated-sshail', true);

insert into role_policies ("role", "action", "resource", "allowance")
values ('_u_user', 'retrieve',
'application:app_id:deployment:dep_id:entry:deployment-php-consolidated-
sftp', true);

/* actions (in buttons) */
insert into role_policies ("role", "action", "resource", "allowance")
values ('_u_user', 'execute',
'application:app_id:deployment:dep_id:action:deployment_actions:update_deploy
ment_info', true);

insert into role_policies ("role", "action", "resource", "allowance")
values ('_u_user', 'execute',
'application:app_id:deployment:dep_id:action:deployment_actions:delete_deploy
ment_main', true);

insert into role_policies ("role", "action", "resource", "allowance")
values ('_u_user', 'execute',
'application:app_id:deployment:dep_id:action:deployment_job:update_job_info',
true);

insert into role_policies ("role", "action", "resource", "allowance")
values ('_u_user', 'execute',
'application:app_id:deployment:dep_id:action:php_c10d_params:set_php_params',
true);

insert into role_policies ("role", "action", "resource", "allowance")
values ('_u_user', 'execute',
'application:app_id:deployment:dep_id:action:php_c10d_params:remove_php_param
s', true);

```

```
insert into role_policies ("role", "action", "resource", "allowance")
values ('_u_user', 'execute',
'application:app_id:deployment:dep_id:action:php_c10d_salt:create_deployment'
, true);

insert into role_policies ("role", "action", "resource", "allowance")
values ('_u_user', 'execute',
'application:app_id:deployment:dep_id:action:php_c10d_salt:edit_deployment',
true);

insert into role_policies ("role", "action", "resource", "allowance")
values ('_u_user', 'execute',
'application:app_id:deployment:dep_id:action:php_c10d_salt:force_salt_apply',
true);

insert into role_policies ("role", "action", "resource", "allowance")
values ('_u_user', 'execute',
'application:app_id:deployment:dep_id:action:php_c10d_salt:enable_deployment'
, true);

insert into role_policies ("role", "action", "resource", "allowance")
values ('_u_user', 'execute',
'application:app_id:deployment:dep_id:action:php_c10d_salt:disable_deployment'
, true);

insert into role_policies ("role", "action", "resource", "allowance")
values ('_u_user', 'execute',
'application:app_id:deployment:dep_id:action:php_c10d_salt:delete_deployment'
, true);

insert into role_policies ("role", "action", "resource", "allowance")
values ('_u_user', 'execute',
'application:app_id:deployment:dep_id:action:php_c10d_salt:archive_deployment'
, true);

insert into role_policies ("role", "action", "resource", "allowance")
values ('_u_user', 'execute',
'application:app_id:deployment:dep_id:action:db_manager_mysql_database:add_My
SQL_database', true);

insert into role_policies ("role", "action", "resource", "allowance")
values ('_u_user', 'execute',
'application:app_id:deployment:dep_id:action:db_manager_mysql_database:remove
_MySQL_database', true);

insert into role_policies ("role", "action", "resource", "allowance")
values ('_u_user', 'execute',
'application:app_id:deployment:dep_id:action:php_c10d_cron:add_cron', true);
```

```
insert into role_policies ("role", "action", "resource", "allowance")
values ('_u_user', 'execute',
'application:app_id:deployment:dep_id:action:php_c10d_cron:remove_cron',
true);

insert into role_policies ("role", "action", "resource", "allowance")
values ('_u_user', 'execute',
'application:app_id:deployment:dep_id:action:php_c10d_email:set_email_configuration', true);

insert into role_policies ("role", "action", "resource", "allowance")
values ('_u_user', 'execute',
'application:app_id:deployment:dep_id:action:php_c10d_email:remove_email_configuration', true);

insert into role_policies ("role", "action", "resource", "allowance")
values ('_u_user', 'execute',
'application:app_id:deployment:dep_id:action:php_c10d_sftp:add_user_sFTP',
true);

insert into role_policies ("role", "action", "resource", "allowance")
values ('_u_user', 'execute',
'application:app_id:deployment:dep_id:action:php_c10d_sftp:remove_user_sFTP',
true);

insert into role_policies ("role", "action", "resource", "allowance")
values ('_u_user', 'execute',
'application:app_id:deployment:dep_id:action:php_c10d_sshail:add_user_SSHail',
true);

insert into role_policies ("role", "action", "resource", "allowance")
values ('_u_user', 'execute',
'application:app_id:deployment:dep_id:action:php_c10d_sshail:remove_user_SSHail',
true);

/* storage (create rows for each plugins) */
insert into role_policies ("role", "action", "resource", "allowance")
values ('_u_user', 'create',
'application:app_id:deployment:dep_id:storage:php_consolidated_params',
true);

insert into role_policies ("role", "action", "resource", "allowance")
values ('_u_user', 'create',
'application:app_id:deployment:dep_id:storage:db_manager_mysql_databases',
true);

insert into role_policies ("role", "action", "resource", "allowance")
values ('_u_user', 'create',
'application:app_id:deployment:dep_id:storage:php_consolidated_cron', true);
```

```

insert into role_policies ("role", "action", "resource", "allowance")
values ('_u_user', 'create',
'application:app_id:deployment:dep_id:storage:php_consolidated_email', true);

insert into role_policies ("role", "action", "resource", "allowance")
values ('_u_user', 'create',
'application:app_id:deployment:dep_id:storage:php_consolidated_sftp_users',
true);

insert into role_policies ("role", "action", "resource", "allowance")
values ('_u_user', 'create',
'application:app_id:deployment:dep_id:storage:php_consolidated_sshail_users',
true);

```

Donar-d'alta-usuari-a-l'aplicació

## Descripció

Aquest procediment mostra com es fa la creació d'usuaris administradors. Per crear un usuari d'aplicació s'ha d'empregar la [documentació següent](#).

L'alta de l'usuari es fa al panell d'AWS Cognito. Es troba al compte APSL subcompte sygox.

Comptes: <https://ajbcn-isoc.signin.aws.amazon.com/console>

Panell d'usuaris Congnito: [https://eu-west-1.console.aws.amazon.com/cognito/v2/idp/user-pools/eu-west-1\\_3oc1wjft/users?region=eu-west-1](https://eu-west-1.console.aws.amazon.com/cognito/v2/idp/user-pools/eu-west-1_3oc1wjft/users?region=eu-west-1)

Triam administrar usuaris "Create User" i omplim les dades del nou usuari i ho cream.

Camp	Dades
Username	Fem nom.cognom.matricula on matricula es pot fer amb Python amb <code>dni = "87654321A" i print(dni\[-1\].lower() + dni\[-7:-1\])</code>
Temporary Password	En general un d'aleatoria amb pwgen o apg
Email	El correu electrònic de l'usuari (marcar-lo com a verificat)

**Create user**

**Username (Required)**  
example.user.a123456

Send an invitation to this new user?  
 SMS (default)  Email

**Temporary password**  
●●●●●●●●●●●●●●●●

**Phone Number**

Mark phone number as verified?

**Email**  
usuari@example.com

Mark email as verified?

Create user

## Assignar usuaris a rols i grups

Per assignar els usuaris a un rol o grup específic, es pot fer via sygox:

<https://gitlab.dtibcn.cat/ajbcn-isoc/ajbcn-isoc-wiki/-/wikis/Gesti%C3%B3-d'equips-de-Sygox>

## Permisos\_OLD (Ja no es fa via base de dades).

Finalment caldrà assignar permisos a l'usuari creat per tal que pugui dur a terme les accions pertinents.

Tots els usuaris han de tenir assignat el rol `\_u_nom.cognom.x123456` on `nom.cognom.x123456` ha de coincidir amb el que s'ha creat a Cognito.

Per tant hauréu d'afegir al següent a la base de dades.

```
INSERT INTO roles (role) VALUES ('_u_example.user.a123456');  
INSERT INTO user_roles (role, username) VALUES ('_u_example.user.a123456',  
'example.user.a123456');
```

Si és un tècnic de la DTI l'afegirem al grup de tècnics de la DTI.

```
INSERT INTO user_roles (role, username) VALUES ('_g_dti_technician',
'example.user.a123456');
```

Per altra banda si és un admin l'afegirem al grup d'admins:

```
INSERT INTO user_roles (role, username) VALUES ('admin',
'example.user.a123456');
```

## Accedir-al-PostgreSQL-de-producció

Hem d'accedir per ssh a la màquina on tinguem desplegat el projecte. Per accedir a la màquina de Sygox s'haurà de fer a través del bastió. Es pot fer:

```
ajbssh sygox
```

Cal configurar prèviament l' `ajbssh` per executar aquesta comanda. El procediment es troba [aquí](#).

Posteriorment, ens situam al directori `/srv/sysgov2-core` i executam la comanda `make psql`.

Això ens treurà una terminal de PostgreSQL de l'entorn de producció.

```
cd /srv/sysgov2-core
make psql
```

## Modificació-de-camps-tipus-JSON-a-BD

Degut al dinamisme de l'aplicació es comú que algun cap pugui ser emprat per un plugin i guardat a BD però que aquest no aparegui a la interfície gràfica.

Per això aquí es descriu com manipular directament els camps JSON del PostgreSQL.

En l'exemple s'afegeixen paràmetres PHP a un desplegament.

```
UPDATE storage SET data = jsonb(data) || jsonb_build_object(
  'ini_overrides',
  json_build_array(
    jsonb_object(
      '{"kind", "php_admin_value", "param", "memory_limit", "value",
"256M"}'
    ), jsonb_object(
```

```

        '{"kind", "php_admin_value", "param", "max_input_vars", "value",
"2000"}'
    ), jsonb_object(
        '{"kind", "php_admin_value", "param", "max_execution_time", "value",
"300"}'
    )
)
)
)
WHERE
namespace = 'php_consolidated_php_params' AND
deployment_id = 'dddddddddddddddddddddddddddddddd';

```

En l'exemple afegim a la columna data (tipus json) una clau anomenada `ini_overrides` que conté una llista de jsons.

Si ja existeix la clau `ini_overrides` i en volguessin afegir el més còmode es duplicar en la nostra consulta els ja existents ja que aquest update sobreescriu tot la clau `ini_overrides`.

### Modificar-els-fils-de-PHP-per-a-una-aplicació

En cas que no s'hagi creat encara el namespace de `php_consolidated_php_params` caldrà fer un insert:

```

INSERT INTO storage (deployment_id, namespace, data)
VALUES
('<deployment_id>', 'php_consolidated_php_params',
jsonb_object('{{"max_children", "<nombre-de-fils>"}}'));

```

Si ja existeix el namespace, s'haurà de fer de la següent manera:

```

UPDATE storage SET data = jsonb(data) || jsonb_build_object('max_children',
'<nombre-de-fils>') WHERE namespace = 'php_consolidated_php_params' AND
deployment_id = '<deployment_id>';

```

### Afegir-un-servei-docker-associat-a-una-aplicació

Hi poden haver aplicacions PHP que necessiten serveis puntuals. En general aquests serveis s'han d'evitar. En cas d'haver d'implementar el servei es pot donar d'alta mitjançant un `docker`.

Per afegir un servei amb exposició de ports i muntatge d'un directori hem d'inserir el servei a la BD de sygox. En l'exemple és un solr amb dos ports (el Sygox força que

siguin interns a 127.0.0.1) i el muntatge d'un volum. Per l'elecció de port se seguirà el següent patró:

5<num\_app>X, on X és el número de servei docker associat a l'aplicació.

Per exemple, l'aplicació 0435 amb un servei solr hi posaria el port 54350 (zero final en cas que sigui el primer servei).

```
BEGIN;
INSERT INTO storage (deployment_id, namespace, data)
VALUES (
  'DDDDDDDDDDDDDDDDDDDDDDDDDDDDDD',
  'php_consolidated_docker_services',
  json_build_object(
    'service_name', 'solr',
    'image', 'solr:5',
    'ports', json_build_array(
      '8983:8983',
      '8079:8079'
    ),
    'volumes', json_build_array(
      './film_data:/opt/solr/server/solr/film'
    )
  )
);

SELECT * from storage
WHERE deployment_id = 'DDDDDDDDDDDDDDDDDDDDDDDDDDDDDD'
AND namespace = 'php_consolidated_docker_services'
COMMIT;
```

Un cop afegit a la BD anam al desplegament, `PHP Consolidated` i executam l'acció `Force Salt Apply`.

Finalment haurem d'accedir com a `root` al servidor d'aplicacions. Anar al directori `/var/www/apps/appXXXX/docker-services/appXXXX` i fer un `docker-compose up -d`.

### Exposar-un-servei-docker-al-port-80-(HAproxy)

Si volem que un docker assignat a una app tingui accés a fora (via port 80), s'haurà de configurar

```
BEGIN;
UPDATE storage SET data = jsonb(data) || jsonb_build_object(
```

```

    'haproxy_expose',
    json_build_array(
      jsonb_object(
        '{"type", "http", "local_port", "ppppp", "host",
"xxxxxxxxxxxxxxxxxxxxxxxxxxxx", "path", "/"}'
      )
    )
  )
)
WHERE
  namespace = 'php_consolidated_docker_services' AND
  deployment_id = 'dddddddddddddddddddddddddddddd';
COMMIT;

```

Un cop afegit a la BD anam al desplegament, `PHP Consolidated` i executam l'acció `Force Salt Apply`.

## Debug-de-Sygox-en-producció

En algunes ocasions ens trobem que les tasques que iniciem des del Sygox no s'inicien. Hi podria haver diversos motius, que intentarem repassar a continuació a mode de validacions que cal fer per tal de depurar el servei.

### El salt daemon està actiu?

Entrar al servidor `salt.dtibcn.cat` i comprovar si el daemon que se'n ocupa de comprovar si hi ha tasques noves enviades des del sygox està up.

```

cd /opt/sygox-salt
sudo make ps

docker-compose -f docker-compose.prod.yml ps

```

Name	Command	State
Ports		
-----		
-----		
sygox-salt-api-redis 6379/tcp	docker-entrypoint.sh redis ...	Up
sygox-salt_caddy_1 0.0.0.0:443->443/tcp, 0.0.0.0:80->80/tcp	/sbin/tini caddy --conf /e ...	Up
sygox-salt_sygox-salt-api_1	entrypoint.sh start	Up
sygox-salt_sygox-salt-daemon_1	entrypoint.sh start	Up

Els serveis haurien d'estar UP. Si no ho estan:



I revisam que el pillar de l'aplicació estigui actualitzat. Si ho està, podem fer un `Force salt apply` des de Sygox o bé llançar la recepta des del servidor:

```
sudo salt appserver-php-static-<id-server> state.sls php-server test=True
```

I comprovar que els canvis s'apliquen.

## Comprovar els logs de cada component del Sygox

Haurem de comprovar els logs dels components de Sygox. Sobretot del `core` i del `worker`. Entrem a la màquina `sygox.dtibcn.cat`:

```
cd /srv/sysgov2-worker/ # o cd /srv/sysgov2-core/ per al core
sudo docker-compose -f docker-compose.prod.yml logs -f -tail=1000
```

## Extreure llistat d'ids d'aplicació consolidada i URL dels deployments

```
SELECT COALESCE(data->'consolidated_app_name', private_data->'consolidated_app_name'), data->'mainUrl' FROM deployments;
```

## Gestió d'equips de Sygox per operadors APSL

Per entendre el sistema d'equips a nivell global es recomana llegir el document [Gestió d'equips de Sygox](#).

## Assignació de permisos a gestor d'equips

El rol `_g_dti_techician` ja té els permisos necessaris per poder gestionar la creació d'equips, crear membres o esborrar-los i assignar equips a desplegaments o desassignar-los. En tot cas, en algun moment donat, ens pot interessar crear de nou els permisos per algun altre rol o regenerar-los de nou. A continuació es llisten els `insert` a base de dades necessari per tal que un rol tingui els privilegis per gestionar equips:

```
INSERT INTO role_policies (role, action, resource) VALUES
('_g_dti_techician', 'create', 'platform:team'); -- Permís per crear equips
INSERT INTO role_policies (role, action, resource) VALUES
('_g_dti_techician', 'create', 'application:<app-id-team>:deployment'); --
Per crear deployments a l'app d'Equips (substituir app id)
INSERT INTO role_policies (role, action, resource) VALUES
('_g_dti_techician', 'execute',
'application:*.deployment:*.action:team_manager:assign_member'); -- Per crear
membres dins un equip
INSERT INTO role_policies (role, action, resource) VALUES
```

```

('g_dti_technician', 'execute',
'application*:deployment*:action:team_manager:refuse_member'); -- Per
eliminar un membre d'un equip
INSERT INTO role_policies (role, action, resource) VALUES
('g_dti_technician', 'execute',
'application*:deployment*:action:php_c10d_teams:assign_team'); -- Per
assignar equips a desplegaments
INSERT INTO role_policies (role, action, resource) VALUES
('g_dti_technician', 'execute',
'application*:deployment*:action:php_c10d_teams:refuse_team'); -- Per
desassignar equips de deployments
INSERT INTO role_policies (role, action, resource) VALUES
('g_dti_technician', 'create',
'application*:deployment*:storage:team_deployments'); -- Per crear storages
team_deployments
INSERT INTO role_policies (role, action, resource) VALUES
('g_dti_technician', 'create',
'application*:deployment*:storage:team_members'); -- Per crear storages
team_members
INSERT INTO role_policies (role, action, resource) VALUES
('g_dti_technician', 'retrieve',
'application*:deployment*:storage:team_deployments:*'); -- Per obtenir
storages team_deployments
INSERT INTO role_policies (role, action, resource) VALUES
('g_dti_technician', 'retrieve',
'application*:deployment*:storage:team_members:*'); -- Per obtenir storages
team_members
INSERT INTO role_policies (role, action, resource) VALUES
('g_dti_technician', 'delete',
'application*:deployment*:storage:team_members:*'); -- Per eliminar membres
d'un equip
INSERT INTO role_policies (role, action, resource) VALUES
('g_dti_technician', 'delete',
'application*:deployment*:storage:team_deployments:*'); -- Per desassignar
equips de deployments

-- per llistar tots els membres de tots els equips assignats
INSERT INTO role_policies (role, action, resource) VALUES
('g_dti_technician', 'retrieve',
'application*:deployment*:list_all_users:php_consolidated_sftp_users');
INSERT INTO role_policies (role, action, resource) VALUES
('g_dti_technician', 'retrieve',
'application*:deployment*:list_all_users:php_consolidated_sshail_users');

```

Esborrar-desplegament-de-la-BD-de-Sygox

En cas que s'hagi creat malament un desplegament pot ser convenient esborrar-lo de la BD.

Aquesta tasca s'ha de fer amb molta cura i sempre assegurant amb el responsable tècnic del projecte que l'esborrat s'ha de fer i es l'única via per des-encallar el tema.

Un cas típic on pot haver-se de fer es amb un desplegament que s'ha quedat a mig crear per una fallada a una API com ara el sygox-seq-generator. El desplegament no s'ha completat però alhora ja ha reservat la `mainUrl` i no deixa crear-lo de nou.

En cas de voler fer l'esborrar haurem d'entrar a la BD de Sygox i executar el següent (canivat `abcde123456789abcde` per el `deployment_id` corresponent.):

```
BEGIN;

DELETE FROM jobs_results WHERE result_id IN (
    SELECT result_id FROM jobs_results
    LEFT JOIN jobs ON jobs.job_id = jobs_results.job_id
    WHERE jobs.deployment_id = 'abcde123456789abcde'
);

DELETE FROM jobs WHERE jobs.deployment_id = 'abcde123456789abcde';

DELETE FROM deployments WHERE deployment_id = 'abcde123456789abcde';

COMMIT;
```

## Desplegament-dels-SSHail

SSHail és el servei que gestiona la creació de contenidors dockers on poder-hi fer SSH per tal d'aïllar de forma lògica el codi de les aplicacions dels servidors consolidats.

D'aquesta manera un desenvolupador pot fer SSH al servidor d'aplicacions i només tenir accés al directori (i subdirectoris) on es troba l'aplicació.

El desplegamentde SSHail es compona de dues parts diferenciades.

## Build i publicació de les imatges

El servidor de salt s'encarrega de fer el `build` de cada una de les imatges de SSHail. Posteriorment, les publica al [registry de l'Ajuntament](#).

Per fer executar la recepta, caldrà que al salt màster executem:

```
salt-call --local state.sls php-server.sshail.build-images test=True
```

```
salt-call --local state.sls php-server.sshail.build-images
```

Com que el nombre d'imatges és gran podria ser que el Gitlab retornés error 429 per excés de peticions. En tal cas, s'haurà d'eliminar el ban (no posar cap IP a cap whitelist, ja que és necessari que hi hagi rate limits). S'accedés al servidor de gitlab com a usuari administrador:

```
root@gitlab:# /opt/gitlab/embedded/bin/redis-cli -s /var/opt/gitlab/redis/redis /var/opt/gitlab/redis/redis.socket> del cache:gitlab:rack::attack:allow2ban:ban:<IP>
```

S'haurà de canviar la IP per la de sortida a Internet que tengui el Salt.

Aquesta recepta s'encarrega de comprovar que existeix el fitxer d'autenticació de docker, situat a `~/.docker/config.json` (en aquest cas, usuari root). Les credencials es poden trobar al [Vaultier d'APSL](#) i és el token amb permisos de lectura i escriptura. El fitxer d'autenticació codifica en base 64. Aquesta part substitueix haver de fer manualment `docker login`.

Una vegada comprovada l'autenticació, fa el build de cada una de les imatges i posteriorment les publica al registry. Aquesta part només s'ha de fer un cop cada vegada que hi ha canvis en les imatges de SSHail i no caldrà fer-la més.

Per forçar que els servidors consolidats descarreguin les imatges SSHail haurem d'executar:

```
salt '*php-*' state.sls php-server.sshail.pull-images test=True
salt '*php-*' state.sls php-server.sshail.pull-images
```

És necessari també que al fitxer `/srv/pillar/top.sls` hi hagi el `minion_id` del salt màster per a que tengui accés al pillar `/srv/pillar/php-server/common.sls`, on hi ha la següent informació necessària:

```
sshail:
  registry:
    host: 'registry-gitlab.dtibcn.cat'
    group: ajbcn-isoc
    project: sshail-images
    login_rw: '<token-base-64>'
    login_r: '<token-base-64>'
  ubuntu_versions:
    - '20.04'
```

Les versions d'Ubuntu serveixen per indicar amb quines imatges base s'ha de fer el build del SSHail minimal. A dia d'avui es creen només amb les version 20.04, malgrat que al registry es mantenen les 16.04, que ja no poden ser construïdes de nou per problemes de dependències.

## Configuració del SSHail a cada appserver

L'altra part del procés és la recepta genèrica de SSHail que s'executa sempre que a Sygox hi ha canvis d'aquest plugin. Aquesta recepta comprova i instal·la el paquet SSHail i genera el fitxer `/etc/sshail/sshails.yml` on hi ha la informació necessària per generar els SSHail. Una vegada l'usuari faci una petició a l'endpoint del SSHail del seu usuari es farà `pull` de la imatge en cas de no ser-hi present al servidor i l'iniciaria amb els paràmetres adients.

La recepta encarregada d'aquesta part valida també l'autenticació contra el registry. En aquest cas és amb l'usuari `sshail` i usa un token només amb permisos de lectura.

Més informació al procediment [Gestió d'usuaris SSHail i sFTP en desplegaments PHP Consolidats](#).

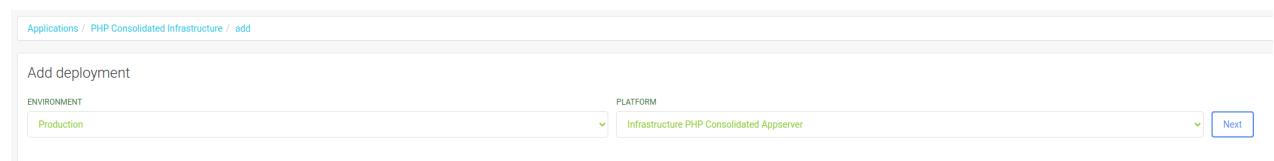
### Afegir-un-nou-servidor-d'aplicacions-a-Sygox

Aquest procediment explica els passos a seguir per afegir un nou servidor d'aplicacions a Sygox i poder-hi crear aplicacions.

Abans de res, s'haurà hagut de crear el servidor mitjançant [el procediment corresponent](#). A continuació, seguim els següents passos per donar-lo d'alta a Sygox.

1. Accedim a [Sygox](#).
2. Busquem l'aplicació [PHP Consolidated Infrastructure](#)
3. Cliquem per crear una nova aplicació i emplenem els camps de la següent manera:

Cal posar que és entorn productiu i que es tracta del tipus `Infrastructure PHP Consolidated Appserver`



Applications / PHP Consolidated Infrastructure / add

Add deployment

ENVIRONMENT: Production

PLATFORM: Infrastructure PHP Consolidated Appserver

Next

Li assignem la url, la criticitat i el dia de sortida a producció (pot esser el mateix que es dona d'alta)

Valors d'exemple:

- url: `c10d://php-c10d-static-06.aws.dtibcn.cat`

Additional information

Basic information

MAIN APPLICATION URL\*

c10d://php-c10d-static-03.aws.dtibcn.cat

Additional application URLs

CRITICITY

Criticality type

High

ESTIMATED RELEASE DATE

dd/mm/aaaa

NEXT

Emplenem els camps tècnics. Malgrat que surti com a opcional, posar també el DNS del bastió SSHail. Si el nou servidor serà el que s'usarà a partir d'ara per crear-hi les aplicacions cal posar-lo com a `default`

Valors d'exemple:

- name: php-c10d-static-06
- endpoint: php-c10d-static-06.aws.dtibcn.cat
- minion id: php-c10d-static-06
- friendly name: PHP c10d Static 06 (AWS)
- DNS SSHail bastion: sshail-bastion.aws.dtibcn.cat

Additional information

Appserver

NAME\*

eg. appserver-php-static-01

php-c10d-static-03

ENDPOINT\*

eg. appserver-php-static-01 (endpoint with dtibcn.cat)

php-c10d-static-03.aws.dtibcn.cat

MINION ID\*

eg. appserver-php-static-01

php-c10d-static-03

FRIENDLY NAME\*

eg. Appserver PHP Static 01

PHP c10d Static 03 (AWS)

SSHAIL BASTION

DNS SSHail bastion (Optional)

sshail-bastion.aws.dtibcn.cat

ELIGIBLE\*

Is this server eligible when creating new deployments?

yes

DEFAULT\*

Is the default to use?

no

PREVIOUS NEXT

Finalment, posem a quin proveïdor està donat d'alta. Les noves altes ja estan a AWS

Additional information

Provider

Amazon Web Services

Amazon Web Services

ACCOUNT ID

ajbcn-issoc

REGION

eu-west-1

PREVIOUS NEXT

## Sygox-en-mode-lectura

Hi ha ocasions en què cal operar el servidor de Salt o el mateix de Sygox i necessitem que no hi hagi execucions de salt ni aplicacions de configuracions a servidors. Aquest procediment explica com fer-ho. La dinàmica és simple, i es configura mitjançant la creació de fitxers.

## Sygox en mode manteniment

El mode manteniment de Sygox guarda tots els canvis i el persistor desa el pillar però l'aplicació de la recepta és amb `test=True`. Això fa que no apliqui cap canvi al servidor, però obtinguem en canvi quin hauria estat el resultat de la seva aplicació.

Per tal d'activar el mode manteniment:

```
cd sygox-salt/sygox-salt-locks
mv maintenance.disabled maintenance.enabled
```

Per deshabilitar-lo:

```
mv maintenance.enabled maintenance.disabled
```

## Sygox deshabilitat

El mode de deshabilitació de Sygox també persisteix els canvis en els pillars del servidor de SaltStack, però a diferència del mode manteniment no executa el Salt, ni tant sols, en el mode test. Aquest mode és útil si no volem interaccionar amb SaltStack.

Per tal d'activar aquest mode:

```
cd sygox-salt/sygox-salt-locks
mv skip-salt.disabled skip-salt.enabled
```

Per deshabilitar-lo:

```
mv skip-salt.enabled skip-salt.disabled
```

## Canviar-l'aplicació-a-la-que-pertany-un-desplegament-a-Sygox

Aquest procediment descriu com canviar l'aplicació a la que pertany un desplegament, ja que es pot donar el cas que per coherència s'hagi de moure un desplegament. També pot ser que s'hagi creat per error a l'aplicació on no tocava.

## Canviar l'application ID

Primer de tot caldrà [accedir al postgres](#). Un cop dins, haurem de canviar l'ID de l'aplicació pel nou:

```
BEGIN;

SELECT * FROM deployments WHERE deployment_id = '<deployment-id>'; -- per
comprovar

UPDATE deployments SET application_id = '<new-app-id>' WHERE deployment_id =
'<deployment-id>';

SELECT * FROM deployments WHERE deployment_id = '<deployment-id>'; --
comprovem que està tot correcte i fem commit

COMMIT;
```

## Canviar els permisos

En segon lloc, caldrà canviar els permisos associats, ja que es construeixen en base a l'app id i el deployment id:

```
BEGIN;

select * from role_policies where resource like 'application:<old-app-
id>:deployment:<deployment-id>%'; -- comprovem que existeixen permisos amb
l'app id equivocat

UPDATE role_policies SET resource = REPLACE(resource, '<old-app-id>', '<new-
app-id>') WHERE resource LIKE 'application:<old-app-id>:deployment:
<deployment-id>%';

select * from role_policies where resource like 'application:<old-app-
id>:deployment:<deployment-id>%'; -- comprovem que ja no hi ha permisos
equivocats

COMMIT;
```

### salt-validator-debug

El salt-validator és una recepta que utilitza el plugin de redireccions de campanya de Sygox per tal de validar que una configuració d'Nginx és correcte abans d'aplicar cap canvi. A vegades pot donar error, la majoria d'elles per configuració incorrecte. Però hi ha uns outputs tan llargs que és complicat saber què passa amb els logs de Sygox. Per això, la depuració manual és important.

## Build de la imatge

Primer de tot, podem fer el build. Des del servidor de salt:

```
docker build -t salt-validator /srv/salt/salt-validator/files
```

## Execució del verificador

```
docker run --rm --hostname http-front-pub-01-a --env SITE=www.barcelona.cat -  
-env JOB_ID_NEXT_REDIR=d1e1407aae9511ecaf700242ac130004 --  
volume=/srv/salt:/srv/salt:ro --volume=/srv/pillar:/srv/pillar:ro salt-  
validator validate-front
```

Haurem de substituir `JOB_ID_NEXT_REDIR` pel valor del job id que hagi llançat la tasca.

## Verificacions des de dins el contenidor

Si fins aquí no ens és suficient, es pot entrar dins el contenidor i fer el procés manualment per tenir més control dels outputs

```
docker run -it --entrypoint /bin/bash --hostname http-front-pub-01-a --env  
SITE=www.barcelona.cat --env  
JOB_ID_NEXT_REDIR=d1e1407aae9511ecaf700242ac130004 --  
volume=/srv/salt:/srv/salt:ro --volume=/srv/pillar:/srv/pillar:ro salt-  
validator
```

Un cop dins, podem executar les receptes

```
salt-call state.sls http-frontend pillar="{ 'apply_sites':  
['www.barcelona.cat'], 'apply_telegraf': False, 'inside_docker': True}" --  
log-level=critical
```

Una vegada veiem què passa, podem arreglar-ho i tornar a llançar la tasca des de Sygox.

Si això no ha anat bé es poden mirar diversos aspectes a dins el contenidor.

Un test de l'nginx:

```
nginx -t
```

Consultar els logs de l'nginx:

```
cat /var/log/nginx/error.log
```

O un mateix output de la recepta que només s'executa a dins el contenidor:

```
-----
  ID: output-nginx-log
Function: cmd.run
  Name: cat /var/log/nginx/error.log
  Result: True
  Comment: Command "cat /var/log/nginx/error.log" run
  Started: 11:21:43.113075
  Duration: 18.004 ms
  Changes:
    -----
    pid:
      117
    retcode:
      0
    stderr:
    stdout:
      2022/09/20 11:21:36 [info] 70#70: Using 32768KiB of shared
memory for nchan in /etc/nginx/nginx.conf:72
      2022/09/20 11:21:37 [info] 73#73: Using 32768KiB of shared
memory for nchan in /etc/nginx/nginx.conf:72
      2022/09/20 11:21:38 [info] 75#75: Using 32768KiB of shared
memory for nchan in /etc/nginx/nginx.conf:72
      2022/09/20 11:21:42 [info] 116#116: Using 32768KiB of
shared memory for nchan in /etc/nginx/nginx.conf:72
```

[[[esborrar-vinculaci0-repositori-aplicacio-php-consolidada-a-repositori-gitlab]]]

## Sygox-canviar-versio-per-defecte-PHP

Quan sorgeixen versions noves de PHP s'han de donar d'alta a la plataforma.

A banda del [suport a nivell que s'hagi d'implementar al Salt](#) també s'ha de posar disponible al Sygox.

1. Editarem el fitxer `sygox-php-consolidated/sygox_php_c10d/php_version.yaml` per afegir la nova versió de PHP al desplegable i fixar la versió per defecte:

```
---
title: "PHP Version"
type: object
properties:

  phpVersion:
    title: "Version"
```

```
description: "Specify the application PHP version"
type: string
default: "8.2"
enum:
  - "5.6"
  - "7.1"
  - "7.2"
  - "7.4"
  - "8.0"
  - "8.1"
  - "8.2"
enumNames:
  - "PHP 5.6"
  - "PHP 7.1"
  - "PHP 7.2"
  - "PHP 7.4"
  - "PHP 8.0"
  - "PHP 8.1"
  - "PHP 8.2"
```

required:

- phpVersion

2. També editarem el fitxer `sygox-php-`

`consolidated/sygox_php_c10d/edit_deployment.yaml` seguint els mateixos criteris que l'anter

3. Finalment editarem `sygox-php-`

`consolidated/sygox_php_c10d_sshail/parameters.py` on s'estableix la relació entre els frameworks i la versió de drush, com també el nom de les imatges.

```
sshail_images = [  
    'ajb-php5.6-drush8:16.04',  
    'ajb-php5.6-drush8:20.04',  
    'ajb-php7.1-drush8:16.04',  
    'ajb-php7.1-drush8:20.04',  
    'ajb-php7.2-drush8:16.04',  
    'ajb-php7.2-drush8:20.04',  
    'ajb-php7.4-drush8:16.04',  
    'ajb-php7.4-drush8:20.04',  
    'ajb-php7.2-drush10:16.04',  
    'ajb-php7.2-drush10:20.04',  
    'ajb-php7.4-drush10:16.04',  
    'ajb-php7.4-drush10:20.04',  
    'ajb-php8.0-drush10:20.04',  
    'ajb-php8.1-drush10:20.04',  
    'ajb-php8.2-drush10:20.04',  
]
```

```

sshail_images_names = [
    'ajb-php5.6-drush8:16.04 (deprecated)',
    'ajb-php5.6-drush8:20.04',
    'ajb-php7.1-drush8:16.04 (deprecated)',
    'ajb-php7.1-drush8:20.04',
    'ajb-php7.2-drush8:16.04 (deprecated)',
    'ajb-php7.2-drush8:20.04',
    'ajb-php7.4-drush8:16.04 (deprecated)',
    'ajb-php7.4-drush8:20.04',
    'ajb-php7.2-drush10:16.04 (deprecated)',
    'ajb-php7.2-drush10:20.04',
    'ajb-php7.4-drush10:16.04 (deprecated)',
    'ajb-php7.4-drush10:20.04',
    'ajb-php8.0-drush10:20.04',
    'ajb-php8.1-drush10:20.04',
    'ajb-php8.2-drush10:20.04',
]

default_image_tag = '20.04'

framework_image_sshail = {
    'wordpress': 'drush8',
    'drupal_7': 'drush8',
    'drupal_less_8.4': 'drush8',
    'drupal_equal_greater_8.4': 'drush10',
    'drupal_9': 'drush10',
    'other': 'drush8',
}

```

4. Caldrà fer una *merge request* de la branca on es desenvolupi cap a la branca `develop` i assignar-la al responsable. Posteriorment es farà *merge* a `master` i es podrà [desplegar](#).

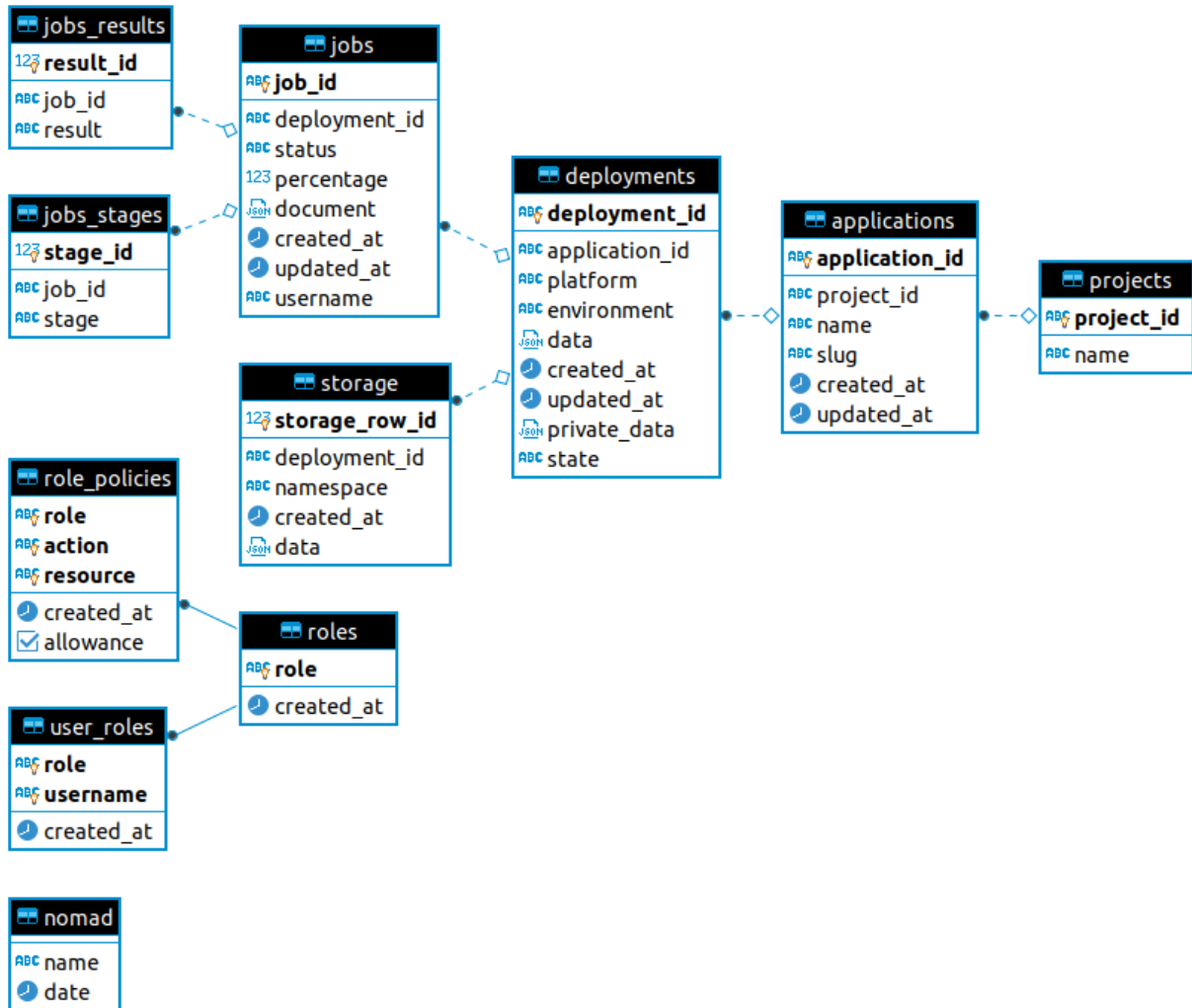
## Sygox Manual de Desenvolupament

Secció orientada als desenvolupadors de Sygox, els quals n'amplien les seves funcionalitats.

### Model-de-dades

Generat amb DBeaver el 28-04-2020.

- La taula `projects` actualment no s'utilitza.
- No hi ha taula d'usuaris ja que els proporciona AWS Cognito. Per això els `username` no són FKs.
- La taula `nomad` es per les migracions.



## Entorn-de-desenvolupament-local

Aquí descrivim com fer el setup de l'entorn local emprant docker + docker-compose per desenvolupar amb Sygox.

## Aixecar entorn local

### Descarregar els repositoris

Per defecte, el mínim per tenir un entorn per desenvolupar és: `sygox-seq-generator`, `sysgov2-core`, `sysgov2-worker` i `sysgov2-front`. Posteriorment es baixaran els plugins que siguin necessaris per desenvolupar, ja que no cal tenir-los tots en local.

A continuació es descriu com muntar tot el projecte.

Les URL dels repositoris i plugins són:

Base

- <https://gitlab.apsl.net/AjuntamentBarcelona/sysgov2-front>
- <https://gitlab.apsl.net/AjuntamentBarcelona/sysgov2-core>

- <https://gitlab.apsl.net/AjuntamentBarcelona/sysgov2-worker>
- <https://gitlab.apsl.net/AjuntamentBarcelona/sygox-common>
- <https://gitlab.apsl.net/AjuntamentBarcelona/sygox-seq-generator>

## Plugins

- <https://gitlab.apsl.net/AjuntamentBarcelona/sygox-php-consolidated>
- <https://gitlab.apsl.net/AjuntamentBarcelona/sygox-salt>
- <https://gitlab.apsl.net/AjuntamentBarcelona/sygox-db-manager-mysql>
- <https://gitlab.apsl.net/AjuntamentBarcelona/sygox-http-monitoring>
- <https://gitlab.apsl.net/AjuntamentBarcelona/sygox-teams>
- <https://gitlab.apsl.net/AjuntamentBarcelona/sygox-phpackages>
- <https://gitlab.apsl.net/AjuntamentBarcelona/sygox-redirector>

## Tools

- <https://gitlab.apsl.net/AjuntamentBarcelona/sygox-cli>

```
cd <alla-on-tenguis-els-projectes>

mkdir sygox
mkdir sygox/plugins
mkdir sygox/tools

cd sygox
git clone git@gitlab.apsl.net:AjuntamentBarcelona/sysgov2-core.git
git clone git@gitlab.apsl.net:AjuntamentBarcelona/sysgov2-front.git
git clone git@gitlab.apsl.net:AjuntamentBarcelona/sysgov2-worker.git
git clone git@gitlab.apsl.net:AjuntamentBarcelona/sygox-common.git
git clone git@gitlab.apsl.net:AjuntamentBarcelona/sygox-seq-generator.git

cd plugins
git clone git@gitlab.apsl.net:AjuntamentBarcelona/sygox-php-consolidated.git
git clone git@gitlab.apsl.net:AjuntamentBarcelona/sygox-salt.git
git clone git@gitlab.apsl.net:AjuntamentBarcelona/sygox-db-manager-mysql.git
git clone git@gitlab.apsl.net:AjuntamentBarcelona/sygox-http-monitoring.git
git clone git@gitlab.apsl.net:AjuntamentBarcelona/sygox-teams.git
git clone git@gitlab.apsl.net:AjuntamentBarcelona/sygox-redirector.git
git clone git@gitlab.apsl.net:AjuntamentBarcelona/sygox-phpackages.git

cd ../tools
git clone git@gitlab.apsl.net:AjuntamentBarcelona/sygox-cli.git
```

## Configuració de variables d'entorn

Una vegada tinguem els entorns haurem de configurar les variables d'entorn.

Cada repositori té els fitxers `<servei>.env-example` cal crear el fitxer `<servei>.env` i editar els valors com correspongui. Als README.md de cada projecte hi haurà detalls de cada un.

Pot ser útil configurar la variable d'entorn `EXECUTOR_BACKEND=local` al `sysgov-core.env` de forma que els jobs s'executen sempre al moment sense emprar cues, és a dir, no falta arrencar el `sysgov2-worker`.

## Aixecar el projecte

Un cop configurat cal aixecar el projecte.

El primer servei a aixecar és el `core`, ja que els altres s'hi connecten. Serà necessari carregar un [dump de producció anonimitzat](#).

```
user@apsl:~/sysgov/sysgov2-core$ git checkout develop
user@apsl:~/sysgov/sysgov2-core$ make configure
user@apsl:~/sysgov/sysgov2-core$ make build
user@apsl:~/sysgov/sysgov2-core$ docker-compose up -d postgres
user@apsl:~/sysgov/sysgov2-core$ docker-compose exec -T postgres psql -U
usygox -d sygoxdb < sygox-reduced-dump.sql
```

```
user@apsl:~/sysgov/sygox-seq-generator$ git checkout develop
user@apsl:~/sysgov/sygox-seq-generator$ make build
user@apsl:~/sysgov/sygox-seq-generator$ cp docker-compose.override.yml-
example docker-compose.override.yml
user@apsl:~/sysgov/sygox-seq-generator$ make initdb
```

```
user@apsl:~/sysgov/sysgov2-worker$ git checkout develop
user@apsl:~/sysgov/sysgov2-worker$ make build
```

```
user@apsl:~/sysgov/sysgov2-front$ git checkout develop
user@apsl:~/sysgov/sysgov2-front$ make build
```

Després podem aixecar el `core`, `front`, `seq-generator` i `worker` amb l'script `sygox-tmux.sh` present al `sygox-common`.

```
user@apsl:~/sysgov$ cp sygox-common/sygox-tmux.sh .
user@apsl:~/sysgov$ ./sygox-tmux.sh
```

**Nota:** Si al aixecar algun servei dona error de que no troba alguna xarxa, s'ha d'aixecar el servei amb `docker-compose up --force-recreate`.

Per accedir al Sygox local caldrà anar a <http://localhost:3000> amb usuari `demo` i contrasenya `demoDEMO1234`.

Per a depurar codi, per exemple, al `sysgov2-core`, podem fer un docker attach `<container_id>` tal i com s'especifica a <https://stackoverflow.com/a/40449862>. El detach es fa amb `CTRL-p CTRL-q`. Per fer-ho més fàcil, es pot emprar `make attach`. A l'arxiu `sysgov-core.env` convé incrementar el `GUNICORN_TIMEOUT` per a que no es mori el worker mentre depuram el codi.

## Permisos d'administrador

Si en haver carregat el dump dona problemes de rols (podria ser si és un dump reduït) caldrà crear el rol administrador i assignar-hi l'usuari `demo`. Penseu que a producció l'usuari `demo` no existeix. En tot cas, si s'utilitza el dump anonimitzat i reduït que hi ha al repositori del core no hauria de caldre.

```
user@aps1:~/sysgov/sysgov2-core$ make psql
```

```
INSERT INTO public.roles (role, created_at) VALUES ('_u_demo', '2018-11-19
15:50:57.085606');
INSERT INTO public.user_roles (role, username, created_at) VALUES ('_u_demo',
'demo', '2021-06-10 15:20:22.335308');
INSERT INTO public.user_roles (role, username, created_at) VALUES ('admin',
'demo', '2021-06-10 15:22:14.888919');
```

## Desenvolupament de plugins

Per fixar tots els plugins caldrà que completem els fitxers del `core` i `worker` anomenats `requirements/plugins.txt` amb el següent contingut. Per defecte ja venen emplenats, però podem fixar la branca `develop` per l'entorn local:

```
git+ssh://git@gitlab.aps1.net/AjuntamentBarcelona/sygox-php-
consolidated.git@develop#egg=sygox-php-c10d
git+ssh://git@gitlab.aps1.net/AjuntamentBarcelona/sygox-db-manager-
mysql.git@develop#egg=sygox-db-manager-mysql
git+ssh://git@gitlab.aps1.net/AjuntamentBarcelona/sygox-http-
monitoring.git@develop#egg=sygox-http-monitoring
git+ssh://git@gitlab.aps1.net/AjuntamentBarcelona/sygox-
teams.git@develop#egg=sygox-teams
git+ssh://git@gitlab.aps1.net/AjuntamentBarcelona/sygox-
git.git@develop#egg=sygox-git
git+ssh://git@gitlab.aps1.net/AjuntamentBarcelona/sygox-
phpackages.git@develop#egg=sygox-phpackages
```

```
git+ssh://git@gitlab.apsl.net/AjuntamentBarcelona/sygox-
redirector.git@develop#egg=sygox-redirector
```

Per agilitzar el desenvolupament de plugins pot ser convenient crear un `docker-compose.override.yml` a partir del `-example` ajustant els path perquè apuntin al directoris. Això s'hauria de fer tant al `core` com al `worker`. D'aquesta manera no cal fer el build cada vegada que es modifiqui un plugin i és suficient aturant i aixecant el contenidor. Així, a més, si volem desenvolupar part d'un plugin agafarem el codi que tenim a la nostra màquina.

```
user@apsl:~/sysgov/sysgov2-core$ cp docker-compose.override.yml-example
docker-compose.override.yml
user@apsl:~/sysgov/sysgov2-core$ cd ../sysgov2-worker
user@apsl:~/sysgov/sysgov2-worker$ cp docker-compose.override.yml-example
docker-compose.override.yml
```

Posteriorment caldrà canviar `YOUR_CODE_DIR` per la ruta correcta del sistema de fitxers.

## Saltstack local

Fins aquí hauria d'anar tot bé tret de que els jobs de deployment fallaran ja que no tenim un Salt configurat per fer realment els deploys. Si ho necessitam, podem tenir un entorn de salt de proves.

Per això instal·lam `vagrant` i `virtualbox`.

```
apt install vagrant virtualbox virtualbox-dkms
```

Anam al directori del `sygox-salt`, preparam variables d'entorn i obtenim les receptes salt.

```
cd sygox/plugins/sygox-salt

cp sygox-salt-api.env-example sygox-salt-api.env
cp sygox-salt-daemon.env-example sygox-salt-daemon.env

git clone git@gitlab.apsl.net:isocbcn/salt-master.git

vagrant up
```

Per integrar el salt local amb el Sygox podem trobar al tiquet <https://projectes.apsl.net/issues/101325> les passes per configurar-ho.

Dump-de-la-base-de-dades-de-dev

En algunes circumstàncies ens interessarà fer feina amb les dades de l'entorn de dev. En aquest cas, primer haurem d'accedir al servidor `sygox-dev.dtibcn.cat`:

```
cd /srv/sysgov2-core
sudo docker-compose exec postgres pg_dump -U usygox -Fp sygoxdb > ~/sygox-dev.sql
```

Aquest dump serà en format de text pla. Posteriorment, al nostre entorn local de desenvolupament hi haurem de bolcar aquest dump. Ho podem fer de dues formes. Cal que la base de dades de `sygoxdb` no estigui creada, llavors:

```
docker-compose exec -T postgres psql -U usygox -d sygoxdb < sygox-dev.sql
```

Una altra opció és esborrar tot el directori `pgdata` i iniciar els contenidors amb el dump dins la carpeta `initdb.d` del repositori `sysgov2-core`.

Cal tenir en compte que si el dump és per usar en un entorn de desenvolupament local s'han d'anonimitzar les dades seguint el procediment [Anonimitzar dump de Sygox](#)

## Flux-de-feina

Tots els repositoris tenen tres branques:

- `develop`
- `pre`
- `master`

Tots els desenvolupaments nous es realitzaran a partir de la branca de `develop`, és a dir, crearem una branca nova a partir de `develop` amb la següent nomenclatura: `<descripció>`.

Un cop acabat el desenvolupament passarem els canvis d'aquesta branca a `develop` per poder testejar en local.

LA la branca de `pre` passaran el canvis de `develop` per poder-los validar en un entorn estable (staging). Els commits a aquesta branca desplegarà el canvis automàticament a l'entorn de Staging.

A `master` només passaran els canvis que han de ser desplegats a producció. Aquests canvis passen directament de la branca de `pre`.

## Autenticació-a-l'entorn-de-desenvolupament-de-Sygox

L'aplicació empra Cognito per autenticació d'usuaris, s'usarà un usuari genèric per els entorns de develop/pre

- usuari: `demo`
- password: `demoDEMO1234`

Podem configurar aquestes dades al subcompte d'APSL en AWS.

Implementació-dels-permisos-de-Sygox

## Conceptes

Els sistema de permisos està implementat mitjançant un role-based access control (rbac) format per:

- Noms d'usuari. S'obtenen de AWS Cognito.
- Rols. Es defineixen a la taula roles.
- Rols d'usuari. Relació de noms d'usuari i rols definit a la taula user\_roles.
- Acció: Crear, recuperar, actualitzar, eliminar o executar (CRUDE).
- Recurs: Especifica un component del sistema: aplicació, desplegament, menu, etc.
- Polítiques. indica si un rol pot executar o no una acció sobre un recurs. Es defineixen a la taula role\_policies.

## Recursos

Els recursos son una versió molt simplificada de les expressions regulars. Només permeten els següents caràcters:

- Lletres → `[a-z,A-Z]`
- Nombres → `[0-9]`
- `-`
- `_`
- `:` S'empra com a delimitador.
- `*` S'empra com "tot fins al següent delimitador".

A més, cada `*` es substitueix per `[^:]*`, és a dir, tot fins al següent delimitador `:`. La implementació és al fitxer `sysgov/core/resources.py`.

## Funcionament de polítiques

Per conveni, s'ha decidit que els recursos s'especifiquin de forma jeràrquica, de forma que sigui fàcil donar permisos a tot o a una dada concreta d'una acció, d'un plugin, d'un deployment d'una aplicació.

L'estructura genèrica és: `component:id_component:subcomponent:id_subcomponent:etc` .

Més concretament: `application:app_id:deployment:dep_id:type:plugin:namespace:id` .

Exemples de polítiques (rol, acció, recurs):

- El rol `admin` pot executar tot  
`admin execute *:?:*:?:?:?:?:?:?:?:*`
- El rol `user` pot crear aplicacions:  
`user create application`
- El rol `user` pot consultar un deployment concret:  
`user retrieve`  
`application:686d7c30bf8c11eaad530242ac1d0003:deployment:8442fe6cbf8c11ea9a190242ac1d0003`
- El rol `user` pot actualitzar qualsevol cosa de un deployment concret:  
`user update`  
`application:cd059ac683c811ea8e3b0242ac190003:deployment:2c7bc2a8936c11eea8610242ac190003:*`
- El rol `user` pot eliminar un SSHail user concret (el de id 50):  
`user delete`  
`application:cd059ac683c811ea8e3b0242ac190003:deployment:2c7bc2a8936c11eea8610242ac190003:storage:php_consolidated_sshail_users:50`

Per veure més exemples en format SQL, veure a [Donar d'alta un rol d'usuari](#)

## Detalls d'implementació

### Core

El core proveeix endpoints REST ( `sysgov/core/views/permissions.py` ) i mètodes Python ( `sysgoc/core/use_cases/permissions.py` ) per poder fer les comprovacions necessàries de permisos.

Internament, quan es reb una petició HTTP “només” es carreguen de la base de dades a memòria les polítiques de tots els rols de l'usuari de la petició. El match d'una política i les expressions regulars es fa a nivell de Python, concretament amb la llibreria Balrog.

### Common (RestInteractor)

La classe `RestInteractor` ( `sygox_common/libs/interactors/rest_interactor.py` ) ofereix mètodes Python per a que els plugins puguin fer les consultes necessàries de permisos a l'API del core:

- `def is_allowed(self, action, resource)`
- `def are_allowed(self, policies)`
- `def create_user_policies(self, policies)`

## Plugins

Cada plugin és responsable d'implementar la seva lògica de comprovacions i creacions de permisos (polítiques) que necessiti mitjançant el RestInteractor. Per a més detalls veure l'apartat Desenvolupament de plugins.

### Llibreries-de-Sygox

Com podem veure a la secció d'arquitectura, el sistema està compost per un conjunt de subsistemes: core, worker, generator, etc. El codi font d'aquests subsistemes es troba al gitlab d'APSL (veure la secció d'entorns de desenvolupament).

Els més importants i que s'han de destacar són els següents.

### Common

Common és la llibreria que conté codi compartit entre `core` i `worker`.

- **Interactor:** És la llibreria que usa el worker per comunicar-se amb el core (un client API). Aquest conté un conjunt de funcionalitats requerides pel desenvolupament dels plugins.
- **Menus:** Component que implementa com representar les dades dels plugins.
- **Plugins:** Els plugins que es troben a la llibreria common són genèrics i fan referència al core de l'aplicatiu: els Deployments. El plugin de tipus `deployment` implementa les següents opcions:
  - **Update:** `[update_deployment_info]`: Aquesta acció utilitza el `rest_interactor` (API) per recollir la informació del deployment a editar i crea un job (via `rest_interactor`) per actualitzar el deployment. Un cop creades les tasques actualitza el seu propi estat.

```
self._task_in_progress()
if action == 'update_deployment_info':
    self.action_update_deployment(job_id)
self._task_finished()
```

- **Delete:** `[delete_deployment_main]`: És l'encarregada de generar un job (via `rest_interactor`) per eliminar el deployment en si mateix (soft deleted: marca l'estat com a deleted).

```
self._task_in_progress()
if action == 'delete_deployment_main':
    self.action_delete_deployment(job_id)
self._task_finished()
```

- **Data:** Conjunt de funcionalitats pel tractament de dades.
- **Variables:** Definició de variables comuns entre el core i worker/plugins.

## Plugins

Conjunt de llibreries que agrupen funcionalitat per a realitzar accions sobre deployments. Tots els plugins utilitzen la llibreria common com a mecanisme de comunicació amb el core. A mode d'exemple, hi ha el plugin `Sygox_php_c10d`, de cabdal importància en l'entorn de Sygox.

`Sygox_php_c10d` és plugin orientat a desplegar aplicatius PHP en servidors consolidats, és a dir, amb una estructura i un procediment clarament definit. Aquest plugin s'ha pres de referència per la implementació d'un conjunt de funcionalitats del `core` a mode d'exemple per la resta de plugins.

Concretament aquest plugin implementa les accions:

- Create [`create_deployment`]:
- Apply [`force_salt_apply`]:
- Edit [`edit_deployment`]:

i alhora disposa d'una pre-implementació de les accions:

- Enable [`enable_deployment`]:
- Disable [`disable_deployment`]:
- Delete [`delete_deployment`]:

Així mateix també té pre-implementada la validació de les accions anteriors.

Per a més informació sobre el desenvolupament, veure [Desenvolupament de plugins](#).

## Generator

**#TODO**

### Desenvolupament-de-plugins

El sistema de plugins està implementat emprant [Stevedore](#).

Cada plugin que es desitgi crear ha de contenir un arxiu `setup.py` en el què es defineixin els entrypoints necessaris per al funcionament del plugin. Depenent del tipus de plugin s'haurà implementar un entrypoint o un altre.

### Plugins tipus "Action"

Els plugins de tipus `Action` són els encarregats de proveir de nova funcionalitat a la UI. De moment, aquestes noves funcionalitats estan destinades a un deployment en concret.

El desenvolupament mínim per implementar un plugin de tipus `Action` és implementar una classe amb els mètodes següents:

- `def is_suitable(self, tags, app_id, deployment_id, storage_id=None)`  
En base als seus paràmetres ha de decidir si es mostrarà a la UI o no.
- `def get_actions(self, namespace, app_id, deployment_id)`  
Ha de retornar un llistat de strings que indiquen les accions que aporta aquest plugin tenint en compte que pot dependre dels permisos que tingui l'usuari per l'aplicació i/o deployment.
- `def execute_action(self, action, job_id)`  
Mètode encarregat d'executar les accions del job associat. Convé coimprobar si es tenen els permisos necessaris

Existeixen també una sèrie de mètodes opcionals:

- `def setup(self)`  
Per si fa falta inicialitzar qualsevol cosa.
- `def teardown(self)`  
Per si fa falta tancar o eliminar algun recurs. Aquest mètode s'executarà sempre, fins i tot si es produeix alguna excepció.
- `def handle_exception(self, e)`  
Només s'executarà quan es produeixi una excepció.

Per tant, el cicle d'execució de l'acció seria el següent:

1. `setup` (opcional)
2. `execute_action`
3. `handle_exception` (opcional)
4. `teardown` (opcional)

Una vegada desenvolupat el plugin, haurem de generar el `setup.py` corresponent i implementar l'entrypoint "`sysgov.actions`". De tal manera que quedi com:

```
setup(
    # ...
    entry_points={
        'sysgov.actions': [
            'plugin_name = path.to.file:ClassName'
        ]
    }
)
```

En qualsevol cas, a l'hora d'implementar un nou plugin el més senzill és mirar un del mateix tipus dels que ja hi ha implementats.

## Plugins tipus "Action" per deployments

Els plugins de tipus action que s'empren per fer deployments tenen alguns requeriments especials més.

- `def get_all_actions(self)`  
Ha de retornar un llistat de strings que indiquen les accions que aporta aquest plugin sense tenir en compte permisos.
- `def get_job_creation_resources(self, namespace, app_id, deployment_id)`  
Ha de retornar un llistat de recursos de permisos (expressions regulars) que són necessaris tenir abans de que el job de crear el deployment s'executi. Per exemple:  
`application:1234:deployment:5678:action:php_c10d_salt:create_deployment`

## Plugins tipus "Schema"

Els plugins de tipus Schema són els encarregats d'afegir formularis als diferents Wizards que té l'aplicació.

El desenvolupament d'un plugin de tipus "Schema" ha de ser a través d'una classe que implementi els següents mètodes:

- `def is_suitable(self, _tags, app_id=None, deployment_id=None, storage_id=None)`  
En base als seus paràmetres ha de decidir si es apte o no.
- `def get_schemas(self)`  
Aquest mètode ha de retornar el llistat de schemas disponibles per al plugin en qüestió.
- `def get_schema_definition(self, schema)`  
Aquest mètode rep el nom d'un schema i ha de retornar la definició per a aquest schema (JSON del YAML).
- `def get_schema_priority(self, schema)`  
Aquest mètode ha de retornar un nombre indicant la prioritat del schema donat. Quan més petit sigui el nombre, més prioritat tindrà.
- `def get_schema_ui(self, schema)`  
Aquest mètode ha de retornar el schema ui del schema donat.

Un cop desenvolupat el plugin haurem generar un `setup.py` a l'igual que els plugins de tipus "Action". El `setup.py` ha de quedar de la següent manera:

```
setup(  
    # ...  
    entry_points={  
        'sysgov.schemas': [  
            'plugin_name = path.to.file:ClassName',  
            'plugin_name_2 = path.to.file:ClassName2
```

```
]
}
)
```

## Plugins tipus “Menu”

Aquest tipus de plugins són capaços d'injectar nous menús a la interfície d'usuari. El plugin ha d'implementar els següents mètodes:

- `def is_suitable(self, tags, app_id, deployment_id, storage_id=None)`  
En base als seus paràmetres ha de decidir si es apte o no.
- `-def get_menus(self)`  
Ha de retornar un llistat de menús. Per exemple, [“menu:deployment”, ...]

El `setup.py` ha de ser com el següent:

```
setup(
    # ...
    entry_points={
        'sysgov.menus': [
            'namespace = path.to.file:ClassName'
        ]
    }
)
```

## Plugins tipus “Entry”

Aquests plugins són capaços d'afegir nous "entries" o "tabs" a un menú existent. Per a això la classe ha d'incloure els següents mètodes:

- `def is_suitable(self, tags, app_id, deployment_id, storage_id=None)`  
En base als seus paràmetres ha de decidir si es apte o no. Convé tenir en compte els permisos de l'usuari per mostrar només els tabs que pot emprar.
- `def get_entries(self)`  
Retornarà un llistat dels entries que proporciona el plugin. Exemple: [“entry:php-consolidated-sshail”, ...]
- `def get_entry_title(self, entry)`  
Aquest mètode retornarà el nom de l'entry que se li passi com a paràmetre.
- `def get_priority(self, entry)`  
Aquest mètode retornarà un enter representant la prioritat del "entry" dins de menú. Quan més petit sigui el nombre, més prioritat tindrà.

El `setup.py` ha de ser com el següent:

```

setup(
    # ...
    entry_points={
        'sysgov.entries': [
            'namespace = path.to.file:ClassName'
        ]
    }
)

```

## Plugins tipus “Widget”

Aquests plugins són capaços d'injectar widgets a un "entry" en concret. Per a això, la classe haurà d'implementar els següents mètodes:

- `def is_suitable(self, tags, app_id, deployment_id, storage_id=None)`  
En base als seus paràmetres ha de decidir si es apte o no. Convé tenir en compte els permisos de l'usuari per mostrar només els widgets que pot emprar.
- `def get_widget(self, application_id, deployment_id, username, is_admin)`  
Aquest mètode tindrà ha de retornar l'estructura de dades corresponent al widget que es vulgui representar.

El `setup.py` ha de ser com el següent:

```

setup(
    # ...
    entry_points={
        'sysgov.widgets': [
            'namespace = path.to.file:ClassName'
        ]
    }
)

```

## Plugins tipus “Platform”

Aquests plugins seran capaços d'injectar noves plataformes en el desplegable de platforms. Per aconseguir un plugin així haurem de definir una classe amb els següents mètodes:

- `def get_platforms(self)`  
Aquest mètode ha de retornar un llistat amb les plataformes (text human-readable) que es vol injectar.

El `setup.py` ha de ser com el següent:

```
setup(  
    # ...  
    entry_points={  
        'sysgov.platforms': [  
            'namespace = path.to.file:ClassName'  
        ]  
    }  
)
```

## Plugins multiparadigma

En més d'una ocasió ens trobem que un connector necessita afegir tant una acció com un schema. No hi ha cap problema, simplement afegirem dos entypoints al setup.py, un per a l'acció i un altre per al schema. El setup.py resultant hauria de ser una cosa semblant a:

```
setup(  
    # ...  
    entry_points={  
        'sysgov.platforms': [  
            'namespace = path.to.file:ClassName'  
        ],  
        'sysgov.actions': [  
            'namespace = path.to.file:ClassName'  
        ]  
    }  
)
```

## Instal·lació de plugins

Per instal·lar aquests nous connectors cal seguir els següents passos:

Afegir el nou plugin en els requirements del projecte CORE.

```
$ pip install -r requirements.txt.
```

## Enllaços-útils-pel-desenvolupament-de-Sygox

- Live demo de JSON Schema amb ReactJS: <https://rjsf-team.github.io/react-jsonschema-form/>