Water Data Project para Groots

Deployment - Runbook - Fase 1

[**Alcance**](#_gk6148zclt5t) **1**

[**Preparación del servidor**](#_c4qc5nm1h8ij) **1**

[Instalación de Docker](#_urbshxlzbi47) 1

[Healthcheck](#_n0p5inv9tovo) 2

[Python 3](#_m3bn4d95c3i4) 2

[**Instalación de KoBoToolbox**](#_79njv66wd626) **4**

[Healthcheck](#_d6ymxs62vron) 10

[**Troubleshooting**](#_lzv18zjmy4x5) **11**

[La instalación no se realiza por que no se puede generar el certificado TLS](#_n3yyjbhwz6p6) 11

[La aplicación no arranca y se queda esperando, solicitando 600 segundos más](#_bkffxjyix994) 13

[**Recomendaciones de Backup**](#_ipglma97gr7w) **14**

# Alcance

El término Runbook hace referencia a los pasos necesarios para llevar a cabo una tarea de manera expectable y reproducible en el tiempo.

El siguiente Runbook está diseñado para realizar:

* Instalación de KoBoToolbox utilizando el repositorio público puesto a disposición en Github

Para la elaboración de este documento de instrucciones se utilizó una máquina **Ubuntu Server 18.04.1 LTS**.

# Preparación del servidor

## Instalación de Docker

|  |
| --- |
| 1. sudo apt-get update |

|  |
| --- |
| 1. sudo apt-get install -y \   apt-transport-https \  ca-certificates \  curl \  gnupg-agent \  software-properties-common |

|  |
| --- |
| 1. curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add - |

|  |
| --- |
| 1. sudo apt-key fingerprint 0EBFCD88 |

Este paso es para revisar que el repo ha sido agregado correctamente

|  |
| --- |
| pub rsa4096 2017-02-22 [SCEA]  9DC8 5822 9FC7 DD38 854A E2D8 8D81 803C 0EBF CD88  uid [ unknown] Docker Release (CE deb) <docker@docker.com>  sub rsa4096 2017-02-22 [S] |

|  |
| --- |
| 1. sudo add-apt-repository \   "deb [arch=amd64] https://download.docker.com/linux/ubuntu \  $(lsb\_release -cs) \  stable" |

|  |
| --- |
| 1. sudo apt-get update |

|  |
| --- |
| 1. sudo apt-get install -y docker-ce docker-ce-cli containerd.io |

|  |
| --- |
| 1. sudo usermod -aG docker <YOUR\_USERS> |

<YOUR\_USERS> es el usuario que está realizando la instalación

|  |
| --- |
| 1. sudo apt install -y docker-compose |

|  |
| --- |
| 1. *Hacer logout y login nuevamente* |

### Healthcheck

|  |
| --- |
| 1. docker ps |

El resultado debe ser (si no existen containers):

|  |
| --- |
| CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES |

## Python 3

Usualmente en nuevas instalaciones de Linux, Python 3 ya viene instalado. Revisar primero:

|  |
| --- |
| 1. python3 --version |

Si el resultado es:

|  |
| --- |
| Python 3.7.9 |

o una versión mayor a Python 3.5, entonces se puede considerar a Python instalado

**Si Python no está instalado**

|  |
| --- |
| 1. sudo apt-get update |

|  |
| --- |
| 1. sudo apt-get install python3.7 |

Puede instalar una versión mayor a 3.5

Vuelva a revisar la versión de Python

|  |
| --- |
| 1. python3 --version |

Instalando Unzip

|  |
| --- |
| 1. apt-get install unzip |

### 

# Instalación de KoBoToolbox

**Descarga de los repositorios**

Se hará la descarga directa de los repositorios. Opcionalmente se puede usar una llave ssh para descargar sólo kobo-install, y ya con la llave en ~/.ssh el script realizará la acción `clone` de los otros dos repos (kobo-docker y nginx-certbot)

|  |
| --- |
| 1. Establezca la ruta base (path). Para efectos de este runbook::    1. Se usará al usuario llamado **kobo\_user**    2. Directorio de trabajo: **kobotoolbox**    3. Path: **/home/kobo\_user/kobotoolbox** 2. El usuario debe ser ***sudoer*** 3. Debe loguearse con el usuario: **kobo\_user** |

Kobo-install:

|  |
| --- |
| 1. cd **/home/kobo\_user/kobotoolbox** 2. curl -LJO https://github.com/kobotoolbox/kobo-install/archive/stable.zip |

|  |
| --- |
| 1. unzip kobo-install-stable.zip |

|  |
| --- |
| 1. mv kobo-install-stable kobo-install |

|  |
| --- |
| 1. mkdir zips 2. mv \*.zip ./zips |

**Ejecutar la instalación**

|  |
| --- |
| 1. cd ./kobo-install |

|  |
| --- |
| 1. python3 run.py -s |

Llene el Wizard a continuación:

Leyenda: <llenar>. Significa que se puede llenar el dato (por si no ha sido definido en el valor en corchetes “[ ]” )

|  |
| --- |
| ╔═══════════════════════════════════════════════════════════════╗  ║ Welcome to KoBoInstall! ║  ║ ║  ║ You are going to be asked some questions that will ║  ║ determine how to build the configuration of `KoBoToolBox`. ║  ║ ║  ║ Some questions already have default values (within brackets). ║  ║ Just press `enter` to accept the default value or enter `-` ║  ║ to remove previously entered value. ║  ║ Otherwise choose between choices or type your answer. ║  ╚═══════════════════════════════════════════════════════════════╝ |

|  |
| --- |
| Where do you want to install?  [**/home/kobo\_user/kobotoolbox/kobo-docker**]: <llenar> |

|  |
| --- |
| Please confirm path [**/home/kobo\_user/kobotoolbox/kobo-docker**]  1) Yes  2) No  [1]: <confirmar número> |

|  |
| --- |
| Do you want to see advanced options?  1) Yes  2) No  [1]: 1 |

|  |
| --- |
| What kind of installation do you need?  1) On your workstation  2) On a server  []: 2 |

|  |
| --- |
| Please choose which network interface you want to use?  enp0s3) 192.168.56.101 ---> <ejemplo>  other) Other  [enp0s3]: <especificar la interfaz de red correcta> |

|  |
| --- |
| Do you want to use separate servers for frontend and backend?  1) Yes  2) No  [2]:2 |

|  |
| --- |
| Public domain name [kobo.local]: <dominio principal, ej. mi-entidad.bo> |

|  |
| --- |
| KPI sub domain [kf]: kf |

|  |
| --- |
| KoBoCat sub domain [kc]:kc |

|  |
| --- |
| Enketo Express sub domain name [ee]:ee |

|  |
| --- |
| Do you want to use HTTPS?  1) Yes  2) No  []:1 |

|  |
| --- |
| ╔═══════════════════════════════════════════════════════  ║ Please note that certificates must be installed on a reverse-proxy ║  ║ or a load balancer. ║  ║ KoBoInstall can install one, if needed. ║  ╚═══════════════════════════════════════════════════════  Auto-install HTTPS certificates with Let's Encrypt?  1) Yes  2) No - Use my own reverse-proxy/load-balancer  []:<Escoja la opción que mejor se adapte> |

|  |
| --- |
| ╔════════════════════════════════════════════════╗  ║ Domain names must be publicly accessible. ║  ║ Otherwise Let's Encrypt won't be able to valid ║  ║ your certificates. ║  ╚════════════════════════════════════════════════╝  Email address for Let's Encrypt:<ingrese el correo electrónico> |

|  |
| --- |
| NOTA: Revise el manual “Deployment - Runbook + Support API – Fase 2” - sección “Certificados SSL” para una revisión a detalle de cómo instalar un certificado de LetsEncrypt o su propio certificado |

|  |
| --- |
| Please confirm [ <el correo electrónico>]  1) Yes  2) No  [1]: |

|  |
| --- |
| Internal port used by reverse proxy?  [8080]:<escoja el puerto correcto> |

|  |
| --- |
| SMTP server: <servidor de correo> |

|  |
| --- |
| SMTP port [25]: <puerto TLS> |

|  |
| --- |
| SMTP user: <usuario@correo.com> |

|  |
| --- |
| SMTP password: <password del correo> |

|  |
| --- |
| Use TLS?  1) True  2) False  [1]: |

|  |
| --- |
| From email address [support@nexion.com.bo]: <su e-mail> |

|  |
| --- |
| **Importante:** En las pruebas que se hicieron se tienen dos observaciones importantes:   1. Se debe usar un proveedor de correo que maneje TLS. Los proveedores que sólo manejan SSL no son compatibles con KoBoToolbox (kpi) y la creación de usuarios está resringida por dar errores al momento de la creación 2. Al usar una cuenta como Gmail, es posible que la misma sea bloqueada en caso que la infraestructura sea desplegada en un servicio de nube como Azure, AWS, otro. sin embargo Gmail sí funciona correctamente si la cuenta fue abierta en Bolivia y es usada en infraestructura de Bolivia. Datos de conexión en Gmail  * EMAIL\_HOST=smtp.gmail.com * EMAIL\_PORT=587 * EMAIL\_HOST\_USER=<usuario>@gmail.com * EMAIL\_HOST\_PASSWORD=<password> * EMAIL\_USE\_TLS=True |

|  |
| --- |
| Super user's username [super\_admin]: |

|  |
| --- |
| Super user's password [<su password para super\_admin>]: |

|  |
| --- |
| Docker Compose prefix? (leave empty for default): |

|  |
| --- |
| Staging mode?  1) Yes  2) No  [2]: |

|  |
| --- |
| KoBoCat PostgreSQL database name?  [kobocat]: |

|  |
| --- |
| KPI PostgreSQL database name?  [koboform]: |

|  |
| --- |
| PostgreSQL user's username?  [kobo]: <modificar si aplica, recomendado: mantener> |

|  |
| --- |
| PostgreSQL user's password?  [<password random>]: <ingresar el password si aplica> |

|  |
| --- |
| Do you want to tweak PostgreSQL settings?  1) Yes  2) No  [2]: <Sugerido 2, a menos que tengan claro qué se va a modificar en Postgres> |

|  |
| --- |
| MongoDB root's username?  [root]: <modificar si aplica, recomendado: mantener> |

|  |
| --- |
| MongoDB root's password?  [<password random>]: <ingresar el password si aplica> |

|  |
| --- |
| MongoDB user's username?  [kobo]: <modificar si aplica, recomendado: mantener> |

|  |
| --- |
| MongoDB user's password?  [<password random>]: <ingresar el password si aplica> |

|  |
| --- |
| Redis password?  [<password random>]: <ingresar el password si aplica> |

|  |
| --- |
| Do you want to expose backend container ports (`PostgreSQL`, `MongoDB`, `redis`) ?  1) Yes  2) No  [2]: <> |

|  |
| --- |
| Do you want to customize the application secret keys?  1) Yes  2) No  [2]: |

|  |
| --- |
| Do you want to use AWS S3 storage?  1) Yes  2) No  [2]: |

|  |
| --- |
| Google Analytics Identifier: <sólo si aplica> |

|  |
| --- |
| Google API Key: <sólo si aplica> |

|  |
| --- |
| Do you want to use Sentry?  1) Yes  2) No  [2]: <sólo si aplica> |

|  |
| --- |
| Do you want to tweak uWSGI settings?  1) Yes  2) No  [2]: <Sugerido 2, a menos que tengan claro qué se va a modificar en uWSGI> |

|  |
| --- |
| Do you want to activate backups?  1) Yes  2) No  [1]: 1 |

|  |
| --- |
| Do you want to activate backups?  1) Yes  2) No  [1]: 1 |

|  |
| --- |
| KoBoCat media backup schedule?  [0 0 \* \* 0]: 0 20 \* \* \* |

|  |
| --- |
| PostgreSQL backup schedule?  [0 2 \* \* 0]: 0 21 \* \* \*  En el ejemplo, cada día de cada mes de cada año a las 21:00. Se puede cambiar a cualquier valor que se ajuste a las necesidades de la entidad. |

|  |
| --- |
| MongoDB backup schedule?  [0 1 \* \* 0]: 0 22 \* \* \*  En el ejemplo, cada día de cada mes de cada año a las 22:00. Se puede cambiar a cualquier valor que se ajuste a las necesidades de la entidad. |

|  |
| --- |
| Redis backup schedule?  [0 3 \* \* 0]: 0 23 \* \* \*  En el ejemplo, cada día de cada mes de cada año a las 23:00. Se puede cambiar a cualquier valor que se ajuste a las necesidades de la entidad. |

|  |
| --- |
| Existing data found for kf.nexion-dev.tk,kc.nexion-dev.tk,ee.nexion-dev.tk. Continue and replace existing certificate? (y/N)  <N>  (este valor puede aparecer si ya se tienen certificados configurados) |

..........

╔════════════════════════════════╗

║ Ready ║

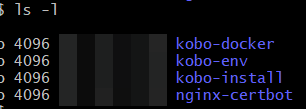
║ URL: https://kf.mi-entidad.bo/ ║

║ User: super\_admin ║

║ Password: <password de super\_admin>

╚════════════════════════════════╝

Si se realiza el listado de directorios (ls) se tiene este resultado



### Healthcheck

<https://kf.mi-entidad.bo/service_health/>

Resultado esperado:

|  |
| --- |
| OK KPI  Mongo: OK in 0.00382 seconds  Postgres: OK in 0.00606 seconds  Enketo [http://ee.mi-entidad.internal]: OK in 0.37 seconds  KoBoCAT [http://kc.mi-entidad.internal]: OK in 0.0392 seconds  ----BEGIN KOBOCAT RESPONSE----  OK  Mongo: OK in 0.000911 seconds  Postgres: OK in 0.0292 seconds  ---- END KOBOCAT RESPONSE ---- |

Al momento de navegar a:

* https://kf.mi-entidad.bo/

El resultado es:



# Troubleshooting

Síntoma:

|  |
| --- |
| La instalación no se realiza por que no se puede generar el certificado TLS |

**Posible Causa:** Es posible que tenga este mensaje, donde *nexion-dev.tk* es el dominio con el que se trabajó:

|  |
| --- |
| *### Downloading recommended TLS parameters ...*  *### Creating dummy certificate for kf.nexion-dev.tk,kc.nexion-dev.tk,ee.nexion-dev.tk ...*  *latest: Pulling from certbot/certbot*  *Digest: sha256:d650cb5dd297b5dc499b14767ebcb3ab4999d858637bd0d5c5f176be20521567*  *Status: Downloaded newer image for certbot/certbot:latest*  *Generating a RSA private key*  *................+++++*  *..................+++++*  *writing new private key to '/etc/letsencrypt/live/kf.nexion-dev.tk/privkey.pem'*  *-----*  *### Starting nginx ...*  *1.15-alpine: Pulling from library/nginx*  *Digest: sha256:57a226fb6ab6823027c0704a9346a890ffb0cacde06bc19bbc234c8720673555*  *Status: Downloaded newer image for nginx:1.15-alpine*  *### Deleting dummy certificate for kf.nexion-dev.tk,kc.nexion-dev.tk,ee.nexion-dev.tk ...*  *### Requesting Let's Encrypt certificate for kf.nexion-dev.tk,kc.nexion-dev.tk,ee.nexion-dev.tk ...*  *Saving debug log to /var/log/letsencrypt/letsencrypt.log*  *Plugins selected: Authenticator webroot, Installer None*  *Registering without email!*  *Obtaining a new certificate*  *Performing the following challenges:*  *http-01 challenge for ee.nexion-dev.tk*  *http-01 challenge for kc.nexion-dev.tk*  *http-01 challenge for kf.nexion-dev.tk*  *Using the webroot path /var/www/certbot for all unmatched domains.*  *Waiting for verification...*  *Challenge failed for domain ee.nexion-dev.tk*  *Challenge failed for domain kc.nexion-dev.tk*  *Challenge failed for domain kf.nexion-dev.tk*  *http-01 challenge for ee.nexion-dev.tk*  *http-01 challenge for kc.nexion-dev.tk*  *http-01 challenge for kf.nexion-dev.tk*  *Cleaning up challenges*  *Some challenges have failed.*  *IMPORTANT NOTES:*  *- The following errors were reported by the server:*  *Domain: ee.nexion-dev.tk*  *Type: connection*  *Detail: Fetching*  *http://ee.nexion-dev.tk/.well-known/acme-challenge/-WDxvEr5wU0lGoOPOeYcs2\_YZJ9zd1T24SLYhXGwZlg:*  *Timeout during connect (likely firewall problem)*  *Domain: kc.nexion-dev.tk*  *Type: connection*  *Detail: Fetching*  *http://kc.nexion-dev.tk/.well-known/acme-challenge/896lkmcJkY9YpO5pUpl72371jFW0z1RRvYGSorrd4E4:*  *Timeout during connect (likely firewall problem)*  *Domain: kf.nexion-dev.tk*  *Type: connection*  *Detail: Fetching*  *http://kf.nexion-dev.tk/.well-known/acme-challenge/BTW12mCBaj-4dmmmp\_ba\_XHxBXjYujHI5KfZbCYwruQ:*  *Timeout during connect (likely firewall problem)*  *To fix these errors, please make sure that your domain name was*  *entered correctly and the DNS A/AAAA record(s) for that domain*  *contain(s) the right IP address. Additionally, please check that*  *your computer has a publicly routable IP address and that no*  *firewalls are preventing the server from communicating with the*  *client. If you're using the webroot plugin, you should also verify*  *that you are serving files from the webroot path you provided.*  *- Your account credentials have been saved in your Certbot*  *configuration directory at /etc/letsencrypt. You should make a*  *secure backup of this folder now. This configuration directory will*  *also contain certificates and private keys obtained by Certbot so*  *making regular backups of this folder is ideal.*  *### Reloading nginx ...*  *2020/11/25 16:29:37 [emerg] 10#10: cannot load certificate "/etc/letsencrypt/live/kf.nexion-dev.tk/fullchain.pem": BIO\_new\_file() failed (SSL: error:02001002:system library:fopen:No such file or directory:fopen('/etc/letsencrypt/live/kf.nexion-dev.tk/fullchain.pem','r') error:2006D080:BIO routines:BIO\_new\_file:no such file)*  *nginx: [emerg] cannot load certificate "/etc/letsencrypt/live/kf.nexion-dev.tk/fullchain.pem": BIO\_new\_file() failed (SSL: error:02001002:system library:fopen:No such file or directory:fopen('/etc/letsencrypt/live/kf.nexion-dev.tk/fullchain.pem','r') error:2006D080:BIO routines:BIO\_new\_file:no such file)*  *An error has occurred* |

**Solución:** Se debe asegurar que el dominio configurado sea accesible

Usualmente esto es a través de la configuración de los registros DNS

--

Síntoma:

|  |
| --- |
| La aplicación no arranca y se queda esperando, solicitando 600 segundos más |

**Posible Causa:** Es posible que LetsEncrypt no esté funcionando correctamente debido a algún error interno

Solución:

* Revisar que los docker containers estén corriendo
* Por ejemplo en este caso el container nginxcertbox\_nginx\_1 no está corriendo

|  |
| --- |
| $ docker ps  CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES  e27b1e683e98 nginx:1.15-alpine "/bin/sh -c 'while :…" 2 hours ago Restarting (1) 45 seconds ago nginxcertbot\_nginx\_1  15e3f83a8922 certbot/certbot "/bin/sh -c 'trap ex…" 2 hours ago Up 2 hours 80/tcp, 443/tcp nginxcertbot\_certbot\_1  dffa63e85db8 nginx:1.19 "/docker-entrypoint.…" 2 hours ago Up 2 hours 0.0.0.0:8080->80/tcp kobofe\_nginx\_1  f08818536651 kobotoolbox/kobocat:2.020.44 "/sbin/my\_init" 2 hours ago Up 2 hours 8000-8001/tcp kobofe\_kobocat\_1  980f91e78884 kobotoolbox/kpi:2.020.30-hotfix-2450 "/bin/bash -c 'exec …" 2 hours ago Up 2 hours 8000/tcp kobofe\_kpi\_1  f3fc7903cec5 kobotoolbox/enketo-express-extra-widgets:2.3.10 "docker-entrypoint.s…" 2 hours ago Up 2 hours 8005/tcp kobofe\_enketo\_express\_1  cbe712f07491 mongo:3.4 "docker-entrypoint.s…" 2 hours ago Up 2 hours 27017/tcp kobobe\_mongo\_1  22aff885fc12 postgis/postgis:9.5-2.5 "docker-entrypoint.s…" 2 hours ago Up 2 hours 5432/tcp kobobe\_postgres\_1  ff7d047977c6 redis:3.2 "docker-entrypoint.s…" 2 hours ago Up 2 hours 6379/tcp kobobe\_redis\_cache\_1  f03bec5e2609 redis:3.2 "docker-entrypoint.s…" 2 hours ago Up 2 hours 6379/tcp kobobe\_redis\_main\_1 |

Específicamente el container se encuentra en estado Restarting. Debe revisar los logs de este container

|  |
| --- |
| e27b1e683e98 nginx:1.15-alpine "/bin/sh -c 'while :…" 2 hours ago Restarting (1) 45 seconds ago nginxcertbot\_nginx\_1 |

|  |
| --- |
| docker logs nginxcertbot\_nginx\_1 |

|  |
| --- |
| 2020/01/01 23:04:25 [emerg] 1#1: cannot load certificate "/etc/letsencrypt/live/kf.nexion-dev.tk/fullchain.pem": BIO\_new\_file() failed (SSL: error:02001002:system library:fopen:No such file or directory:fopen('/etc/letsencrypt/live/kf.nexion-dev.tk/fullchain.pem','r') error:2006D080:BIO routines:BIO\_new\_file:no such file)  nginx: [emerg] cannot load certificate "/etc/letsencrypt/live/kf.nexion-dev.tk/fullchain.pem": BIO\_new\_file() failed (SSL: error:02001002:system library:fopen:No such file or directory:fopen('/etc/letsencrypt/live/kf.nexion-dev.tk/fullchain.pem','r') error:2006D080:BIO routines:BIO\_new\_file:no such file) |

En este caso es posible que LetsEncrypt no haya podido comunicarse con el dominio. Para el ejemplo, el Registrar DNS no tenía configurados los NS del server en el que se hizo el despliegue. Una vez que se tiene configurado el NS del host DNS (on-premise o cloud) revisar que el container funcione correctamente ejecutando docker restart.

Si aún así el container se mantiene en estado *Restarting* , revise que:

* Los puertos 80 y 443 están habilitados en el firewall o grupo de seguridad.
* Su dominio se puede resolver por su DNS.
  + Puede usar el comando **dig** para verificar esta situación
* El dominio es público
* El correo proporcionado a Let’s Encrypt (en caso que haya usado esta opción) es válido

A pesar que esto esté correcto y aún el servicio no funcione, intente instalar nuevamente KoBotoolbox con la opción:

* python run.py -s

Y en la última opción escriba ***S*** :

|  |
| --- |
| Existing data found for kf.nexion-dev.tk,kc.nexion-dev.tk,ee.nexion-dev.tk. Continue and replace existing certificate? (y/N)  **<S>**  (este valor debería aparecer si ya se tiene la instalación realizada previamente) |

Este procedimiento hará que los registros se borren.

**IMPORTANTE: Sólo realice esta operación si está seguro que no va a perder información o configuraciones importantes. En todo caso asegúrese que realizó un backup previo.**

# Recomendaciones de Backup

KoBoToolbox ya contiene la opción de utilizar AWS S3 como repositorio de backups. Esto se indica en la documentación, en la sección “Backups”:

<https://github.com/kobotoolbox/kobo-docker#usage>

Sin embargo, si se decide optar por mantener los backups de forma local es importante que el personal técnico pueda considerar:

* Crear una tarea cron con un script bash que mueva periódicamente los backups a un repositorio en un lugar diferente a la máquina donde se encuentra la instalación.
* Crear un symlink en   
  **/home/kobo\_user/kobotoolbox/kobo-docker/backups**Y apuntar a una ubicación de disco que pueda ser manejada por fuera de la máquina donde se encuentra la instalación.
* Considerar el manejo de rotación de backups siguiendo una política de retención adecuada.