Installing Soffid using Docker

Guide to show the installation process os Soffid IAM using Docker

- Installing IAM Console
- Installing Sync server
- Upgrade syncserver proxy

Installing IAM Console

Guide to install IAM Console using Docker.

Prerequisites

- Docker
- 8GB RAM
- > 10GB disk space (50GB recomended)
- Supported database installed

Repositories

Soffid 3 uses the public Docker Hub: https://hub.docker.com/r/soffid/iam-console/

Soffid 4 uses the Google Cloud Artifact Registry, contact to Soffid when you need access to it.

Video Tutorial

https://www.youtube.com/embed/pEP76i7nX2M?rel=0

Installation

Soffid variables

To configure IAM console, the following environment variables can be set:

Variable	Description	Example

DB_URL	JDBC URL	jdbc:mariadb://dbcontainer/soffid jdbc:oracle:thin:@HOST:PORT:SID jdbc:oracle:thin:@//HOST:PORT/SERVICENAME
DB_USER	Database user	Soffid
DB_PASSWORD	Database password	5uper5ecret
JAVA_OPT	Java virtual machine options	-Xmx4096m
SECURE	(optional) Enables the Java Security Manager	true
SOFFID_TRUSTED_SCRIPTS	(optional) Allows you to use insecure classes. Available since console version 3.5.6	true false
HIDE_MENU	(optional) Allows you to hide the Console menu options. Available since console version 3.5.6	soffid.admin You can choose the proper option from the Console.yaml file.
AUTH_METHODS	(optional) Allows to force the authentication mechanisms. This configuration overrides the one configured in the authentication option of the Soffid console. Available since console version 3.5.6	Options SAML PASSWORD SAML PASSWORD
EXTERNAL_URL	(optional) Allows to override host name configuration when there are two Consoles. Available since console version 3.5.9.5	https://soffid.lab.internal.com
SECURE_SCRIPT	Available since console 3.6.72 and console 4.0.56. Allows to execute scripts with trusted and custom tructed clasess	true false (by default)
TRUSTED_CLASSES	Available since console 3.6.72 and console 4.0.56. Add new trusted classes (all package) separated by space	
SOFFID_DISABLE_GEOIP	Available since console version 4.0.67 This allows to disable the GeoIP service. It is useful when a Soffid instance does not have Internet access.	true false (by default)

Dababase tunning variables

Additional parameters to configure the database connections. Allows you to establish the min and the max of database connections:

Variable	Description	Example
DBPOOL_MIN_IDLE	The minimum number of connections should be kept in the pool at all times.	1 or 2
DBPOOL_MAX_IDLE	The maximum number of connections should be kept in the pool at all times.	between 10 and 15
DBPOOL_INITIAL	The connection number will be established when the connection pool is started.	3 or 4
DBPOOL_MAX	The maximum number of active connections that can be allocated. If no value is indicated, the default value is 30. The transaction fails if the maximum connections are reached within 30 seconds and no connection is released.	25

Volumes

The following volumes must be defined by default:

Volume	Usage
/opt/soffid/iam-console-4/logs	Console log files `/opt/soffid/iam-console-4/logs`
/opt/soffid/iam-console-4/index	Text search engine index files. It can be erased at any time. The engine will regenerate the search engine. `/opt/soffid/iam-console-4/index/`
/opt/soffid/iam-console-4/conf	Configuration files, including server.xml and tomee.xml files `/opt/soffid/iam-console-4/conf`

Docker commands

Here you have a sample command to start a docker container running IAM console, in this case the docker will be in a docker network, previously created. MariaDB docker is at the same network.

```
docker run -d \
  -e DB_URL=jdbc:mariadb://mariadb-service/soffid \
  -e DB_USER=soffid \
  -e DB_PASSWORD=soffid \
  --name=iam-console \
  --publish=8080:8080 \
  --network=soffidnet \
```

```
soffid/iam-console
```

To see console log files, execute:

```
docker logs -f iam-console
```

Ports

By default, the 8080 port will be exposed. When the TLS connection is going to be configured, add the tag --publish=443:443 to publish the TLS port.

Access to the Console

> When the console is created, the password for the user *admin* will be *changeit* and it will be valid for 24 hours.

> Now you can connect the Soffid Console http://localhost:8080/soffid/The first thing you must do is to change the admin user password.

> Next Step: Installing Sync server

Installing Sync server

Guide to install Sync server using Docker.

Prerequisites

Soffid IAM sync server requires the following requirements:

- Supported database installed
- Soffid Console Installed

Repositories

Soffid 3 uses the public Docker Hub: https://hub.docker.com/r/soffid/iam-console/

Soffid 4 uses the Google Cloud Artifact Registry, contact to Soffid when you need access to it.

Video Tutorial

Linux

https://www.youtube.com/embed/NHBvdzDWiWA

Installation

Install first Sync server

To configure the first IAM Sync server, the following environment variables can be set for the first server:

Variable	Description	Example
DB_URL	JDBC URL	jdbc:mariadb://dbcontainer/soffid
DB_USER	Database user	Soffid
DB_PASSWORD	Database password	5uper5ecret
SOFFID_HOSTNAME	The hostname used to access the sync server	syncserver01.soffid.com
SOFFID_PORT	TCP port used for incoming connections	760
SOFFID_MAIN	Set to yes for the first sync server, no for the next ones	**yes**

Additional parameters to configure the database connections. Allows you to establish the min and the max of database connections:

Variable	Description	Example
DBPOOL_MIN_IDLE	The minimum number of connections should be kept in the pool at all times.	1 or 2
DBPOOL_MAX_IDLE	The maximum number of connections should be kept in the pool at all times.	between 10 and 15
DBPOOL_INITIAL	The number of connections will be established when the connection pool is started.	3 or 4
DBPOOL_MAX	The maximum number of active connections that can be allocated. If no value is indicated, the default value is 30. The transaction fails if the maximum connections are reached within 30 seconds and no connection is released.	25
DBPOOL_MAX_IDLE_TIME	Number of seconds that a connection to a DB that is not in use is maintained. Available since Sync Server version 3.5.4.3	3600

Install next Sync servers

To configure the next sync servers, the following environment variables can be set:

Variable	Description	Example
SOFFID_SERVER	First sync server url	https://syncserver01.soffid.com:1760
SOFFID_USER	Soffid user to join the security domain. If you are working in a tenant, the user of the tenant.	admin
SOFFID_PASS	Soffid user password. If you are working in a tenant, the user password of the tenant.	changeit
SOFFID_HOSTNAME	The host name used to access to the sync server	syncserver.soffid.com
SOFFID_PORT	TCP port used for incomming connections	760
SOFFID_TENANT	Tenant name	master
SOFFID_MAIN	Set to yes for the first sync server, no for the next ones	**no**

Install Sync server in a private network

To configure a sync server in a private network, not directly accessible from the main sync server, the following environment variables can be set:

Variable	Description	Example
SOFFID_SERVER	First sync server url	https://syncserver01.soffid.com:1760
SOFFID_USER	Soffid user to join the security domain	admin
SOFFID_PASS	Soffid user password	changeit
SOFFID_HOSTNAME	The host name used to access to the sync server	syncserver.soffid.com
SOFFID_TENANT	Tenant name	master
SOFFID_MAIN	Set to yes for the first sync server, no for the next ones	**no**
SOFFID_REMOTE	Flag to enable cloud protocol	**yes**

You can use this configuration when the main sync server is located in the cloud.

The following volumes are defined by default

Volume	Usage
/opt/soffid/iam-sync/conf	Configuration files, including private keys and certificates

Command

Here you have a sample command to start a docker container running IAM sync server. Mind to specify the port number to expose the sync server docker to the outside world. It is not needed when using the cloud connectivity:

```
docker run -d \
  -e DB_URL=jdbc:mysql://mariadb-service/soffid \
  -e DB_USER=soffid \
  -e DB_PASSWORD=soffid \
  -e SOFFID_PORT=1760 \
  -e SOFFID_HOSTNAME=iam-sync.soffidnet \
  -e SOFFID_MAIN=yes \
  --name=iam-sync \
  --publish 1760:1760 \
  --network=soffidnet \
  soffid/iam-sync:latest
```

To see sync server log file, execute:

```
docker logs -f iam-sync
```

You can also view the log files inside the container. To do this, first enter the container, then you should find the log files in the **/var/log/soffid/** directory.

```
root@soffid:~# docker exec -it iam-sync /bin/bash
root@e1a90ff25d99:/# less /var/log/soffid/syncserver.log
```

> Now you can connect to the IAM console http://localhost:8080/soffid and chek if Console and Syncserver are connected.

Upgrade syncserver proxy

Step-by-step

To upgrade the version of the on-premise syncserver proxy, follow these steps:

1. Stop the syncserver container:

```
docker stop syncserver
```

2. Remove the container:

```
docker rm syncserver
```

3. Create a volume for the syncserver configuration:

```
docker volume create sync-conf
```

4. Create a file 'iam-sync-redeploy.sh' to hold the update script:

```
nano iam-sync-redeploy.sh
```

> Use your preferred text editor; `nano` is used here.

5. Copy the following script:

```
docker run -d \
  --name syncserver \
  -v sync-conf:/opt/soffid/iam-sync/conf \
  --restart always \
  --network=host \
  soffid/iam-sync:4.0.44
```

> Replace '4.0.44' with the desired version.

6. Save and exit the editor.

7. Run the script:

```
bash iam-sync-redeploy.sh
```

You should see a response like this:

