Note installations SAML2 et Passage à la Pafys v4.0.6

Ci-dessous les écarts à la documentation SOPRA pour le passage en v4.0.6

Auteur : Jérémy Fournier

Date : 15\09\2023

Version à installer : **LIV1219\_V406**

Pas à pas de l’installation à destination du Service Delivery (en RECETTE) :

Pour info on commence directement à l’étape 4 du guide Sopra.

**Prérequis :** Package SOPRA déposé dans /var/log/product/livraisons/ de relapv10197 et relapv101982. Les serveurs passifs seront mis à jour dans un second temps.

Les étape 5, 6 et 7 nécessite d’avoir les Users\Password de la base SEPARCT avec privilèges élevés.

*Les livrables MOE (fichiers de conf) sont dans /var/log/product/livraisons/Livrables\_MOE*

4. Préparation de l’environnement

Connexion en Admin à relapv10197 (batch) :

cd /var/log/product/livraisons/

gunzip –d LIV1219\_FFM\_Lot\_V406.tar

sudo tar -xvf LIV1219\_FFM\_Lot\_V406.tar

Connexion en Admin à relapv101982 (IHM) :

-> Même manip

5. Environnement Oracle ([relapv10197)](https://pam.swisslife.lan/SecretServer/app/#/secret/3293/general)

cd /var/log/product/livraisons/bdd/script

./maj\_bdd.sh SLF026\_FFMv4.0.3\_8tov4.0.6\_01.sql SEPARCT effi\_user EFFI\_PWD

6. Chargement du paramétrage en base de données - CSV ([relapv10197)](https://pam.swisslife.lan/SecretServer/app/#/secret/3293/general)

cd /var/log/product/livraisons/bdd/outilbd

gunzip ChargerBDCSV.tar.gz

sudo tar -xvf ChargerBDCSV.tar

cd /var/log/product/livraisons/bdd/outilbd/conf

*Le fichier ConfBD.properties est à remplir par le DBA*

*Remplacer les fichiers et log4j.properties par ceux fournis par la MOE*

Cd /var/log/product/livraisons/bdd/outilbd

sh ./ChargerBDCSV.sh /var/log/product/livraisons/bdd/parametrage

7. Chargement du paramétrage en base de données - MAE ([relapv10197)](https://pam.swisslife.lan/SecretServer/app/#/secret/3293/general)

cd /var/log/product/livraisons/bdd/script

./maj\_bdd.sh MAE-FFMv4.0.3.S.a.sql SEPARCT effi\_user effi\_pwd

8. IHM – Mise à jour de l‘environnement JBoss (relapv10182 IHM) :

Cd /product/exploitation/IHM/conf

*Remplacer les fichiers effihm.properties et effihm\_personnalisation.properties par ceux fournis par la MOE*

Cd /opt/rh/eap7/root/usr/share/wildfly/modules/ffm-saml

*Dans ce répertoire, supprimer le répertoire main/ existant et le remplacer par le répertoire main/ fourni par la MOE*

9 IHM - Déploiement du module sous JBoss (relapv10182 IHM) :

sudo systemctl stop *eap7-standalone.service*

*Atttendre quelques secondes*

sudo systemctl status eap7-standalone.service

*-> le service doit être arrêté*

*cp* /var/log/product/livraisons/as/effihm.ear /opt/rh/eap7/root/usr/share/wildfly/standalone/deployments/

(C’est un lien vers /product/wildfly/standalone/deployments)

sudo systemctl start eap7-ihm.service

*1iere validation MOE : Tester l’accès à* <https://rec-pafys.swisslife.fr/effihm/Welcome.do>

10. Direct Processing – Mise à jour de l’environnement JBoss (relapv10197 batch) :

Cd /usr/lib/systemd/system/

*Remplacer le fichiers eap7-standalone.service par celui fourni par la MOE*

Cd /product/exploitation/DP/conf/

*Remplacer le fichiers effdp.properties par celui fourni par la MOE*11. Direct Processing – Déploiement de l’application sous JBoss (relapv10197 batch)

sudo systemctl stop *eap7-standalone.service*

*Attendre quelques secondes*

sudo systemctl status *eap7-standalone.service*

*-> le service doit être arrêté*

*cp* /var/log/product/livraisons/as/paydp.ear /product/wildfly/standalone/deployments

*cp* /var/log/product/livraisons/as/mandp.ear /product/wildfly/standalone/deployments

sudo systemctl start *eap7-standalone.service*

sudo systemctl status *eap7-standalone.service*

*-> le service doit être démarré*

12. Batchs – Déploiement et configuration (relapv10197 batch)

tar -xvf /var/log/product/livraisons/batch/livBatch.tar

cp -Rv /var/log/product/livraisons/batch/BATCH/jar /product/exploitation/BATCH/

cp -Rv /var/log/product/livraisons/batch/BATCH/xsl /product/exploitation/BATCH/

- Les fichiers des répertoires jar et xsl sont à copier en annule et remplace dans le répertoire /product/exploitation/BATCH

*Les droits de lecture/exécution devront être accordés sur les shells du répertoire BATCH. Les droits de lecture devront être accordés sur le sous-répertoire param et sur son contenu. Les droits de lecture devront être accordés sur le sous-répertoire conf et sur son contenu.*

chmod –R 755 /product/exploitation/BATCH/

12.2.Batchs Base Archivage -> Pas d’installation de la base d’archivage.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*Fin de l’installation \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Annexe pour MOE, Configuration SAML2 : remarques générales

**Config du module saml2 : /product/jboss/wildfly/IHM/modules/ffm-saml/main (Attention ! : pour dev dans /opt/rh/eap7/root/usr/share/wildfly/modules/ffm-saml/main/properties)**

**Idp :**

-> Le but est obtenir les matricules des Salariés et Externes habilités au Groupe Active Directory à travers Azure Federation en tant qu’IDP. Certificats et Adresses Azure communiqués par Matthieu Lanoe.

Les métadatas :

[PAFYS - PROD (1).xml](https://slfr.sharepoint.com/:u:/r/sites/GRPS_DSI_DeptFonctionsCentrales/Documents%20partages/4-SI%20Finance/19%20-%20SEPA%20(FI05)/Passage%20en%20v406%20SAML2%20-%202023/PAFYS%20-%20PROD%20(1).xml?csf=1&web=1&e=KR8MBS)

[PAFYS - RE7 (2).xml](https://slfr.sharepoint.com/:u:/r/sites/GRPS_DSI_DeptFonctionsCentrales/Documents%20partages/4-SI%20Finance/19%20-%20SEPA%20(FI05)/Passage%20en%20v406%20SAML2%20-%202023/PAFYS%20-%20RE7%20(2).xml?csf=1&web=1&e=m24fe1)

**Intégration dans les fichiers de conf SOPRA :**

Attention, comme expliqué dans le guide SOPRA, supprimer les fins de lignes des certificats et clés avec notepad++ avant de les insérer dans le fichier properties saml. Il faut garder les ---- BEGIN CERTIF -------.

Pour l’idp remplir entityid, single\_sign\_on\_service avec l’entity id du metadata Azure fédération. Remplir la clé publique de la fédération Azure;

Pour le sp remplir entityid, assertion\_consumer\_service, single\_logout\_service avec l’URI de l’application (celle déclaré dans Azure fédération)

~~NB : Le certificat privée utilisé pour le SP est le Wildcard Swisslife valable pour tous les environnements. La clé publique du sp rattachée est aussi à renseigner.~~

**-> Les champs certificat du SP seront finalement laissés à vide !**

Pour info, au cas oû, voici les commande Openssl permettant d’obtenir un certificat auto-signé (validé avec la Pafys de Dev : permet le lancement de l’application).

Création d’une clé privée et d’un CSR

openssl req -sha256 -nodes -newkey rsa:2048 -keyout dtu-pafys.key -out dtu-pafys.swisslife.fr

Création d'un certificat public

openssl x509 -signkey dtu-pafys.key -in dtu-pafys.swisslife.fr -req -days 1095 -out dtu-pafys.swisslife.fr.public.crt

**effihm.properties**

**Dans /product/exploitation/IHM/conf/effihm.properties**

Après explication de SOPRA il faut commenter le paramètre #saml.response.attribute.login= . Si ce paramètre est laissé vide l’application plantera.

->on obtiendra en le laissant vide le comportement par défaut de FFM qui ira lire les Matricules dans l’attribut NameId (qui est situé en dehors des claims de la réponse saml2 de l’IDP)

**Configuration des options Java DP :**

Modifier dans le fichier de service /usr/lib/systemd/system/eap7-eff.service en Dev, en Recette et en Prod dans /usr/lib/systemd/system/eap7-standalone.service