

Table des matières

■ Installation de syspass	2
1.1 Installation des paquets	2
1.2 Installation des dépendances php.....	3
1.3 Ajout d'un certificat.....	3
1.3.1 Génération d'un certificat auto-signé	3
1.4 Attribution des droits adéquats sur le dossier apache	4
1.5 Configuration d'Apache.....	4
1.6 Configuration de la base de données.....	4
1.7 Redémarrage des services.....	5
1.8 Redirection des ports NAT.....	5
1.9 Première connexion	6
■ Import/Export d'une sauvegarde de la base de mot de passe	8
2.1 Import d'une sauvegarde de la base de données	8
2.2 Export d'une sauvegarde de la base de données.....	8
■ Sauvegarde totale de l'application.....	8
3.1 Import d'une sauvegarde de l'application	8
3.2 Export d'une sauvegarde de l'application.....	8
■ Import / Export des entrées	8
4.1 Import des comptes	9
4.2 Export des comptes	9
■ Modification du logo	9
5.1 Icône présente sur les pages	9
5.2 Logo d'entrée	10
5.2.2 Modification de la taille de l'image	10
■ Masquage du pied de page et de la version de l'application.....	10
6.1 Modification du pied de page	11
6.2 Suppression du nom et de la version de l'application	11
■ Modification des couleurs	12
7.1 Modification de la couleur de fond de la balise de navigation	12
7.2 Changement de couleur des arrière-plans.....	12
■ Configuration de la partie LDAP	12
8.1 Recherche des groupes sur un client LDAP	13
8.2 Import de compte LDAP	13
■ Transfert/Export des logs	13

9.1	Transfert des logs	13
9.2	Export des logs	13
■	Journalisation des actions	14
■	Gestion des certificats SSL/TLS.....	15
11.1	Génération du certificat et de la clé privée (en auto signé).....	15
11.2	Changement du certificat.....	16
11.3	Protection de la clé privée.....	16
11.3.1	Utilisation d'un fichier de configuration.....	16
■	Consulter l'état de l'espace disque	17
■	Le Master Password	17
13.1	Parade contre un Master password partagée : le Master password temporaire.....	17

■ Installation de syspass

1.1 Installation des paquets

On suppose que l'installation se fait sur une Ubuntu 18.04 server.

```
apt install locales apache2 libapache2-mod-php7.2 php-pear php7.2 php7.2-cgi php7.2-cli \
php7.2-common php7.2-fpm php7.2-gd php7.2-json php7.2-mysql php7.2-readline \
php7.2-curl php7.2-intl php7.2-ldap php7.2-xml php-pear-http libmcrypt-dev libreadline-dev \
php7.2-dev php-mbstring php-xdebug mariadb-server git
```

On installe le plugin pour le chiffrement des entrées de mot de passe avec l'utilitaire PHP pecl via la commande :

```
pecl install mcrypt-1.0.2
```

Lors de la demande de préfix libmcrypt prefix, taper entrée.

```
root@secu_server:~# pecl install mcrypt-1.0.2
WARNING: channel "pecl.php.net" has updated its protocols, use "pecl channel-upd
ate pecl.php.net" to update
downloading mcrypt-1.0.2.tgz ...
Starting to download mcrypt-1.0.2.tgz (33,698 bytes)
.....done: 33,698 bytes
6 source files, building
running: phpize
Configuring for:
PHP Api Version:      20170718
Zend Module Api No:   20170718
Zend Extension Api No: 320170718
libmcrypt prefix? [autodetect] : ■
```

Puis exécuter cette dernière commande pour que le module mcrypt de php soit pris en compte :

```
echo "extension=mcrypt.so" >> /etc/php/7.2/cli/php.ini
```

Désormais, l'application peut se télécharger et être extrait dans le dossier du serveur Apache. On y télécharge le contenu de l'application syspass :

```
cd /var/www/html/  
git clone https://github.com/nuxsmin/sysPass  
mv sysPass syspass
```

1.2 Installation des dépendances php

Puis à la racine de syspass, il est nécessaire de télécharger composer : un gestionnaire de dépendances de paquets pour PHP.

```
cd /var/www/html/syspass  
wget https://getcomposer.org/installer
```

Puis de l'exécuter dans le répertoire syspass pour qu'il installe les bonnes dépendances :

```
mv installer composer-setup.php  
  
php composer-setup.php  
php composer.phar install --no-dev
```

1.3 Ajout d'un certificat

Afin d'obtenir une connexion sécurisée HTTPS, il faut utiliser un certificat.

Dans le cas où l'administrateur n'a pas de certificat voici la procédure ci-dessous pour en générer un qui soit auto-signé.

1.3.1 Génération d'un certificat auto-signé

```
cd /tmp
```

```
openssl req -x509 -out localhost.crt -keyout localhost.key -newkey rsa:2048 -nodes -sha256 -subj  
'/CN=localhost' -extensions EXT -config <(\n  
  printf "[dn]\nCN=localhost\n[req]\ndistinguished_name =  
dn\n[EXT]\nsubjectAltName=DNS:localhost\nkeyUsage=digitalSignature\nextendedKeyUsage=serv  
erAuth")
```

Les paramètres en jaune sont au choix de l'utilisateur.

Puis on convertit le certificat généré au format pem :

```
openssl x509 -outform PEM -in localhost.crt -out localhost.pem
```

1.4 Attribution des droits adéquats sur le dossier apache

Des droits spécifiques doivent être mis en place dans le dossier `/var/www/html/syspass/app` :

```
cd /var/www/html/syspass/app
chmod 750 config/ backup/
chown www-data backup/ config/ cache/
chgrp www-data config/ cache/
```

1.5 Configuration d'Apache

En premier lieu dans `/etc/apache2/apache2.conf` il faut exécuter la commande suivante pour qu'Apache lance une instance sur Syspass :

```
nano /etc/apache2/apache2.conf
```

Pour ajouter un certificat (dans l'exemple ci-dessous `localhost.pem`). Voici les commandes ci-dessous :

```
cp localhost.pem /etc/ssl/certs/
cp localhost.key /etc/ssl/private/
rm /tmp/localhost.pem /tmp/localhost.key /tmp/localhost.crt
```

Puis configurer apache pour qu'il le prenne en compte :

```
cd /etc/apache2/sites-available
nano 000-default.conf
```

Dans `000-default.conf` indiquer le chemin du répertoire syspass à la directive `DocumentRoot` :

```
DocumentRoot /var/www/html/syspass
```

Dans `default-ssl.conf` indiquer le chemins des certificats et la racine de syspass :

```
DocumentRoot /var/www/html/syspass
SSLCertificateFile /etc/ssl/certs/localhost.pem
SSLCertificateKeyFile /etc/ssl/private/localhost.key
```

```
a2ensite 000-default.conf default-ssl.conf
```

1.6 Configuration de la base de données

Pour pouvoir utiliser syspass, il est nécessaire de créer une base de données dédiée à l'application. MariaDB un gestionnaire de base de donnée sera utilisé dans notre cas.

MariaDB a déjà été installé (cf. 1.1), il faut désormais lancer une session MariaDB.

```
mariadb -u root -p
```

Y rentrer ces commandes :

```
# MariaDB [(none)]> create database syspass;  
# MariaDB [(none)]> grant all privileges on syspass.* to spadmin@localhost identified by "Strong  
Password";  
# MariaDB [(none)]> flush privileges;  
# MariaDB [(none)]> quit;
```

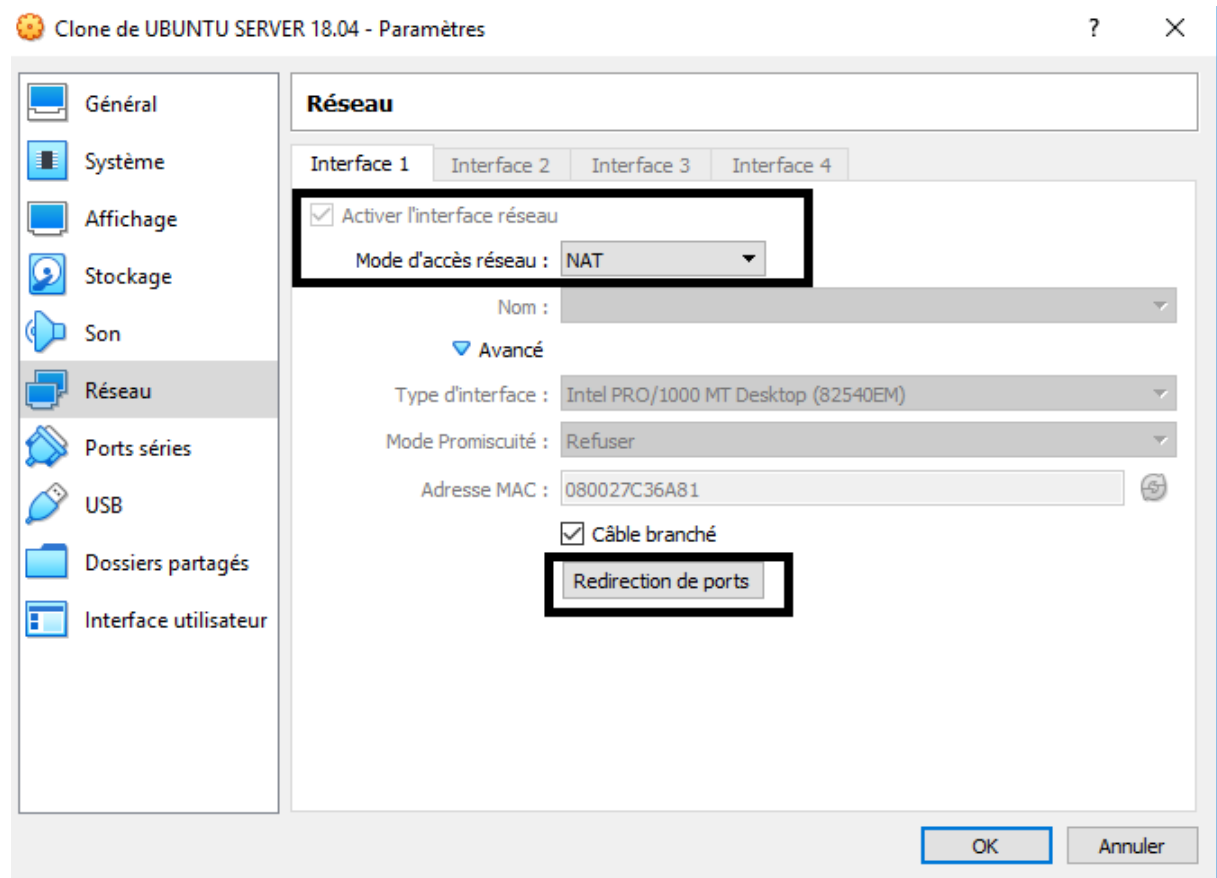
1.7 Redémarrage des services

Afin que toutes les opérations précédentes il faut redémarrer les services:

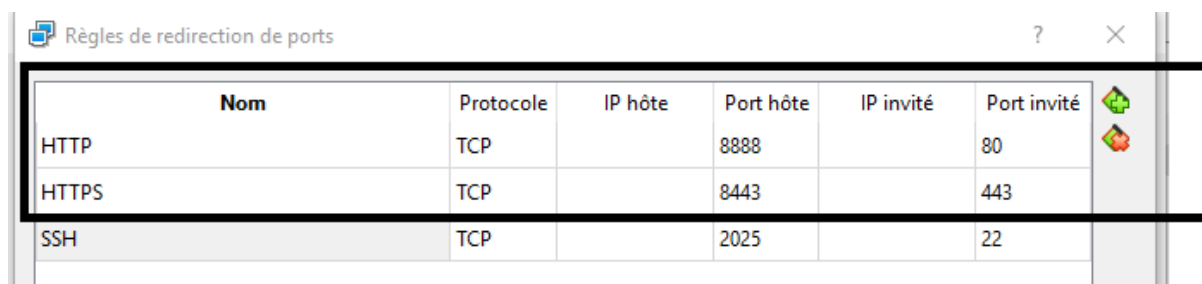
```
service apache2 restart  
service mariadb restart  
service php7.2-fpm restart
```

1.8 Redirection des ports NAT

Sur virtual box il est nécessaire bien mettre le mode d'accès réseau en NAT et de faire une redirection des ports 80 et 443 (ports associés à HTTPS).



Dans notre cas le port 80 est associé au port 8888 et le port 443 au port 8443.



Nom	Protocole	IP hôte	Port hôte	IP invité	Port invité
HTTP	TCP		8888		80
HTTPS	TCP		8443		443
SSH	TCP		2025		22

1.9 Première connexion

L'url d'accès est de la forme suivante :

`https://IP_ADDRESS_OR_HOSTNAME:{8888, 8443}`

On arrive sur la première page de pré-installation. On renseigne le mot de passe du compte administrateur, le mot de passe maître et les informations concernant la base de données (vue précédemment).

Il est nécessaire de cocher hosting mode.

Installation 3.1-RC4

sysPass Admin

sysPass admin user

Password

Master Password

Master Password

Password (repeat)

DB Configuration (MySQL)

DB access user

DB access password

sysPass database name

sysPass database server

General

Language

Hosting Mode ☐

INSTALL

A cocher

■ Import/Export d'une sauvegarde de la base de mot de passe

2.1 Import d'une sauvegarde de la base de données

L'import d'une base de données (fichiers .sql) s'effectue en ligne de commandes (avec la commande MySQL source pour l'import) :

```
mariadb -u root -p
source chemin_du_script ;
exit ;
```

2.2 Export d'une sauvegarde de la base de données

L'export de la base de mot de passe se fait tout simplement sur l'interface Web dans la partie Configuration / Sauvegarde. Le format de la base est en tar.gz.



■ Sauvegarde totale de l'application

Il est aussi possible de sauvegarder et de restaurer toute l'application ce qui comprend tout l'environnement (application/configuration et la base de données de mot de passe).

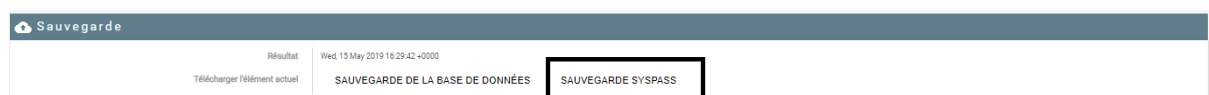
3.1 Import d'une sauvegarde de l'application

Récupérer l'archive contenant la sauvegarde de l'application et exécuter les commandes suivantes :

```
service apache2 stop
cd /var/www/html
rm -rf *
mkdir /var/www/html/syspass
cd syspass
tar -xzf archive.tar.gz /var/www/html/syspass
rm archive.tar.gz
service apache2 start
```

3.2 Export d'une sauvegarde de l'application

Pour exporter la base, tout comme la sauvegarde de la base de donnée il suffit de revenir sur la partie sauvegarde et de cliquer sur le bouton « Sauvegarde Syspass »



Une archive au format .tar.gz sera téléchargée.

■ Import / Export des entrées

Les comptes (entrées contenant les mots de passes et autres informations associées) peuvent être importés et exportés.

4.1 Import des comptes

L'import peut se faire au format XML/CSV dans la partie import des comptes :

The screenshot shows the 'Importer CSV/XML' section of the SysPass web interface. At the top, there is a navigation bar with tabs: GÉNÉRALE, COMPTES, WIKI, LDAP, COURRIEL, CHIFFREMENT, SAUVEGARDE, IMPORTER COMPTES (active), and INFORMATION. Below the navigation bar, the 'Importer CSV/XML' section is active. It contains two dropdown menus: 'Utilisateur par Défaut' set to 'sysPass Admin' and 'Groupe par Défaut' set to 'Admins'. Below these is a large dashed box with a green upload icon. To the right of this box are two circular icons: a blue one with a left arrow and a green one with a right arrow. Below this section are two other sections: 'XML' and 'CSV'. The 'XML' section has two input fields: 'Importer un Mot de Passe' and 'Mot de Passe Maître', both with a right arrow icon. The 'CSV' section has a 'Délimiteur CSV' field with a dropdown menu set to ';'. At the bottom right of the interface are three circular icons: a blue one with a left arrow, a green one with a right arrow, and a green one with a play icon.

4.2 Export des comptes

A l'aide d'un mot de passe propre à un utilisateur, il est possible aussi d'exporter des comptes au format XML dans la partie sauvegarde, et la rubrique XML :

The screenshot shows the 'Sauvegarde' section of the SysPass web interface. At the top, there is a navigation bar with tabs: GÉNÉRALE, COMPTES, WIKI, LDAP, COURRIEL, CHIFFREMENT, SAUVEGARDE (active), IMPORTER COMPTES, and INFORMATION. Below the navigation bar, the 'Sauvegarde' section is active. It contains a 'Résultat' field with the text 'Sauvegarde de la base de données' and a 'Télécharger l'élément actuel' button. Below this is a section titled 'Exporter les comptes'. It contains a 'Résultat' field with the text 'XML SYSPASS' and a 'Télécharger l'élément actuel' button. Below this are two input fields: 'Mot de Passe d'exportation' and 'Mot de Passe d'exportation (confirmer)', both with a right arrow icon. At the bottom right of the interface are three circular icons: a blue one with a left arrow, a green one with a right arrow, and a green one with a play icon.

Modification du logo

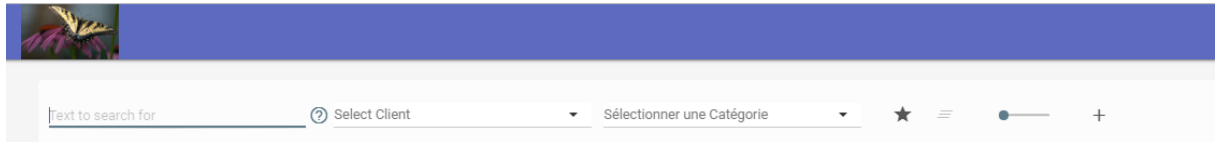
5.1 Icône présente sur les pages

Pour remplacer l'icône présente sur les pages exécuter les commandes suivantes . Dans notre cas l'icône va être remplacé par un papillon:

```
service apache2 stop
cd /var/www/html/syspass/public/images/
cp logo_icon.png logo_icon.png.bkp
rm logo_icon.png

# import sur une clé usb déjà montée
cp /mnt/papillon.jpg .
```

```
mv papillon.jpg logo_icon.png
cp logo_full_nobg_outline_color.png logo_full_nobg_outline_color.png.bkp
rm logo_full_nobg_outline_color.png
cp logo_icon.png logo_full_nobg_outline_color.png
```



5.2 Logo d'entrée

5.2.1 Changement de l'image

La transformation du logo d'entrée en papillon se fait via les commandes ci-dessous :

```
service apache2 stop
cd /var/www/html/syspass/public/images/
cp logo_full_nobg_outline.png logo_full_nobg_outline.png.bkp
rm logo_full_nobg_outline.png
cp logo_icon.png logo_full_nobg_outline.png
service apache2 start
```

5.2.2 Modification de la taille de l'image

Pour avoir une taille adéquate du logo d'entrée il faut modifier dans `var/www/html/syspass/app/modules/web/themes/material-blue/css/style.min.css` le sélecteur `css background size` à 30%.

```
.....
#box-pub-noheader { background: transparent url(public/images/logo_full_nobg_outline.png) no-
repeat top center; background-size: 30% auto; width: 40em; min-height: 20em; margin: 0 auto; }
.....
```

Après la modification, redémarrer le service apache, et recharger le cache du navigateur.



Masquage du pied de page et de la version de l'application

Pour modifier le contenu du footer, il suffit de modifier la page `app/modules/web/themes/material-blue/views/_partials/footer.inc` avec les commandes ci-dessous sur le serveur. Puis après modification il est nécessaire de redémarrer le service Apache :

```
# sauvegarde de footer.inc
cp app/modules/web/themes/material-blue/views/_partials/footer.inc
app/modules/web/themes/material-blue/views/_partials/footer.inc.bkp

#Modification du footer
nano app/modules/web/themes/material-blue/views/_partials/footer.inc
```

#redémarrage d'Apache 2 Service apache2 restart
--

6.1 Modification du pied de page

Le nom de l'admin peut être modifié sur cette zone (la balise div footer-left).

```
<div id="footer-left" class="footer-parts">
    <?php if ($_getvar('loadApp') === true && $_getvar('ctx_userName')): ?>
        <div id="session">
            <span id="user-info">
                <?php
                /** @var IconInterface $ctx_userType */
                $ctx_userType = $_getvar('ctx_userType');

                if ($ctx_userType): ?>
                    <i id="user-type-footer"
                    class="material-icons"> <?php echo $ctx_userType->getIcon();?> </i>
                    <span for="user-type-footer"
                    class="mdl-tooltip mdl-tooltip--top"><?php echo $ctx_userType-
                    >getTitle();?></span>
                    <?php else: ?>
                        <i class="material-icons">face</i>
                    <?php endif; ?>
                    <span id="user-name-footer"><?php echo $_getvar('ctx_userName');?></span>
                    <span for="user-name-footer"
                    class="mdl-tooltip mdl-tooltip--top">
                        <?php printf('%s : %s', __('Group'), $_getvar('ctx_userGroup')); ?> </span>
                    </span>
                </div>
            <?php endif; ?>
        </div>
    </div>
```

Contenu du div footer-left

Le contenu en rouge est à changer.

6.2 Suppression du nom et de la version de l'application

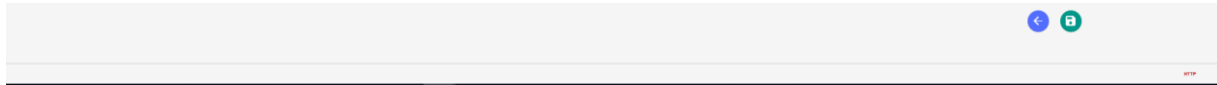
Pour supprimer le nom de l'application et de sa version sur cette portion de code (la balise `div project`), il suffit de commenter ou de supprimer le contenu en rouge :

[illegible]

```
</div>
```

Contenu du div projet

Après modification, le contenu du footer indésirable a été omis.



Contenu vide du footer

A noter qu'il y a aussi la balise <title> aussi à modifier.

Modification des couleurs

Pour changer les couleurs, il faut modifier ou rajouter des sélecteurs CSS.

7.1 Modification de la couleur de fond de la balise de navigation

Rajouter à la fin du fichier /var/www/html/syspass/app/modules/web/themes/material-blue/css/material.min.css le code CSS suivant :

```
a#btn-1{background-color: #141b4d} a#btn-4{background-color: #141b4d} a#btn-5001{background-color: #141b4d} a#btn-5002{background-color: #141b4d} a#btn-5003{background-color: #141b4d} a#btn-1101{background-color: #141b4d} a#btn-config{background-color: #141b4d} a#notifications{background-color: #141b4d} button#users-menu-lower-right{background-color: #141b4d} .mdl-layout__header-row{background-color: #141b4d} .login{background-color: white} .logout{background-color: white} .main{background-color: white}
```

A noter que la couleur violette est #141b4d .

7.2 Changement de couleur des arrière-plans

Outre l'opération précédente (7.1) il est nécessaire de modifier les sélecteurs ci-dessous dans /var/www/html/syspass/app/modules/web/themes/material-blue/css/styles.min.css :

```
body.login,body.logout,body.userpassreset { background: #607d8b; }  
.....  
body.login footer, body.logout footer, body.userpassreset footer { background: #78909C; }
```

Par ces valeurs :

```
body.login,body.logout,body.userpassreset{background:white;}  
.....  
body.login footer,body.logout footer,body.userpassreset footer{background:white;}
```

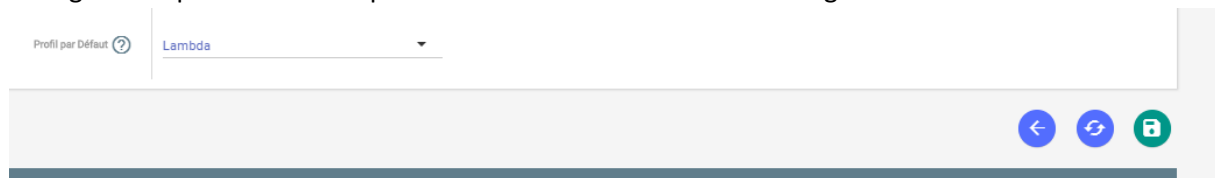
Ensuite il est nécessaire de redémarrer le service Apache et de recharger le cache du navigateur.

Configuration de la partie LDAP

8.1 Recherche des groupes sur un client LDAP

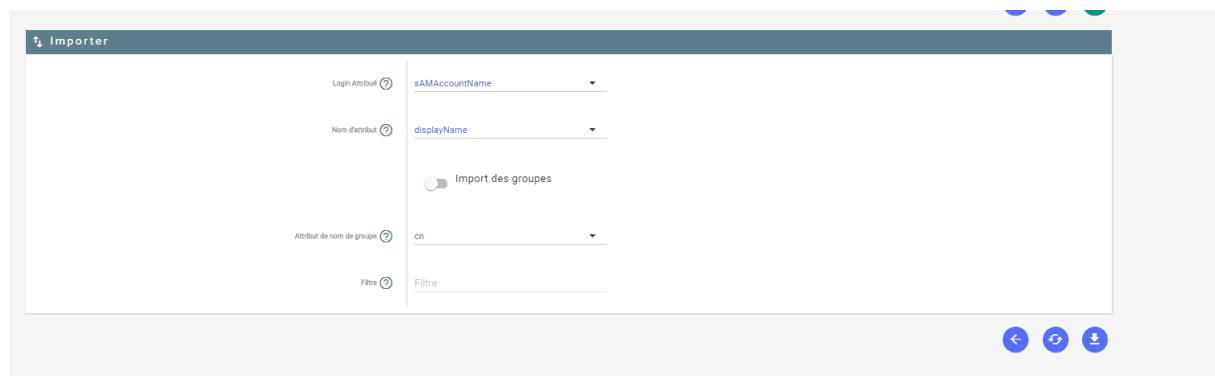
La configuration de LDAP se fait à partir de l'interface Web dans la partie Configuration / LDAP.

Par la suite, il faut vérifier la configuration avec le bouton de synchronisation, et sauvegarder la configuration pour la rendre opérationnelle avec le bouton de sauvegarde.



8.2 Import de compte LDAP

Pour importer les comptes LDAP il suffit sur la même page de remplir les informations suivantes et de les importer avec le bouton d'import :



Normalement, les nouveaux comptes sont présents dans la partie utilisateurs.

Désormais un user appartenant à cette liste pourra se loguer via LDAP sur l'application.

■ Transfert/Export des logs

9.1 Transfert des logs

Pour le transfert des logs, il suffit de consulter dans configuration/Générale la partie « Evènements ». Le panneau de configuration concernant le protocole RSYSLOG s'y trouve :

1. Cocher « Activer le journal des évènements »
2. Cocher « Activer Syslog Distant »
3. Mettre l'adresse IP du collecteur de log dans le champ Serveur

9.2 Export des logs

L'export des logs se fait dans la partie configuration/information où il faut télécharger SysPass.log. Ce fichier contient l'ensemble des logs de l'application.

GÉNÉRALE

COMPTES

WIKI

LDAP

COURRIEL

CHIFFREMENT

SAUVEGARDE

IMPORTER COMPTES

INFORMATION

Information sur l'Application

Version de sysPass

3.1-RC2 (310.19043001)
Config: 310.19043001
App: 310.19043001
DB: 310.19043001

Base de données

SERVER_VERSION : 5.5.5-10.1.38-MariaDB-0ubuntu0.18.04.2
CLIENT_VERSION : mysqlnd 5.0.12-dev - 20150407 - S18: 359f1daa22d608524295e1bd773aceff11e6579 8
SERVER_INFO : Uptime: 2216 Threads: 1 Questions: 1485 Slow queries: 0 Opens: 110 Flush tables: 1 Open tables: 54 Queries per second avg: 0.641
CONNECTION_STATUS : Localhost via UNIX socket
Nom: syspass@localhost
Version: 7.2.17-0ubuntu0.18.04.1
Extensions: Core, date, libxml, openssl, pcre, zlib, filter, hash, Reflection, SPL, sodium, session, standard, apache2handler, mysqlnd, PDO, xml, calendar, ctype, curl, dom, mbstring, fileinfo, ftp, gd, gettext, iconv, intl, json, ldap, exif, mysqli, pdo, mysql, Phar, posix, propro, raphf, readline, shmop, SimpleXML, sockets, sysvmsg, sysvsem, sysvshm, tokenizer, wddx, xmlreader, xmlwriter, xsl, http, Zend OPcache, xdebug
Unavailable extensions:
Mémoire Utilisée: 4096 KB
Utilisateur: www-data
Download rate: 43 MB/s
OP Cache
num_cached_scripts : 382
num_cached_keys : 715
max_cached_keys : 16229
hits : 21640
start_time : 1558092615
last_restart_time : 0
oom_restarts : 0
hash_restarts : 0
manual_restarts : 0
misses : 384
blacklist_misses : 0
blacklist_miss_ratio : 0
opcache_hit_rate : 98.236447511805

PHP

Apache/2.4.29 (Ubuntu)
Wed, 15 May 2019 14:57:49 +0000

Configuration de Sauvegarde

[DOWNLOAD JSON](#)

Langage

fr_FR.utf8

Session Chiffrée

Non

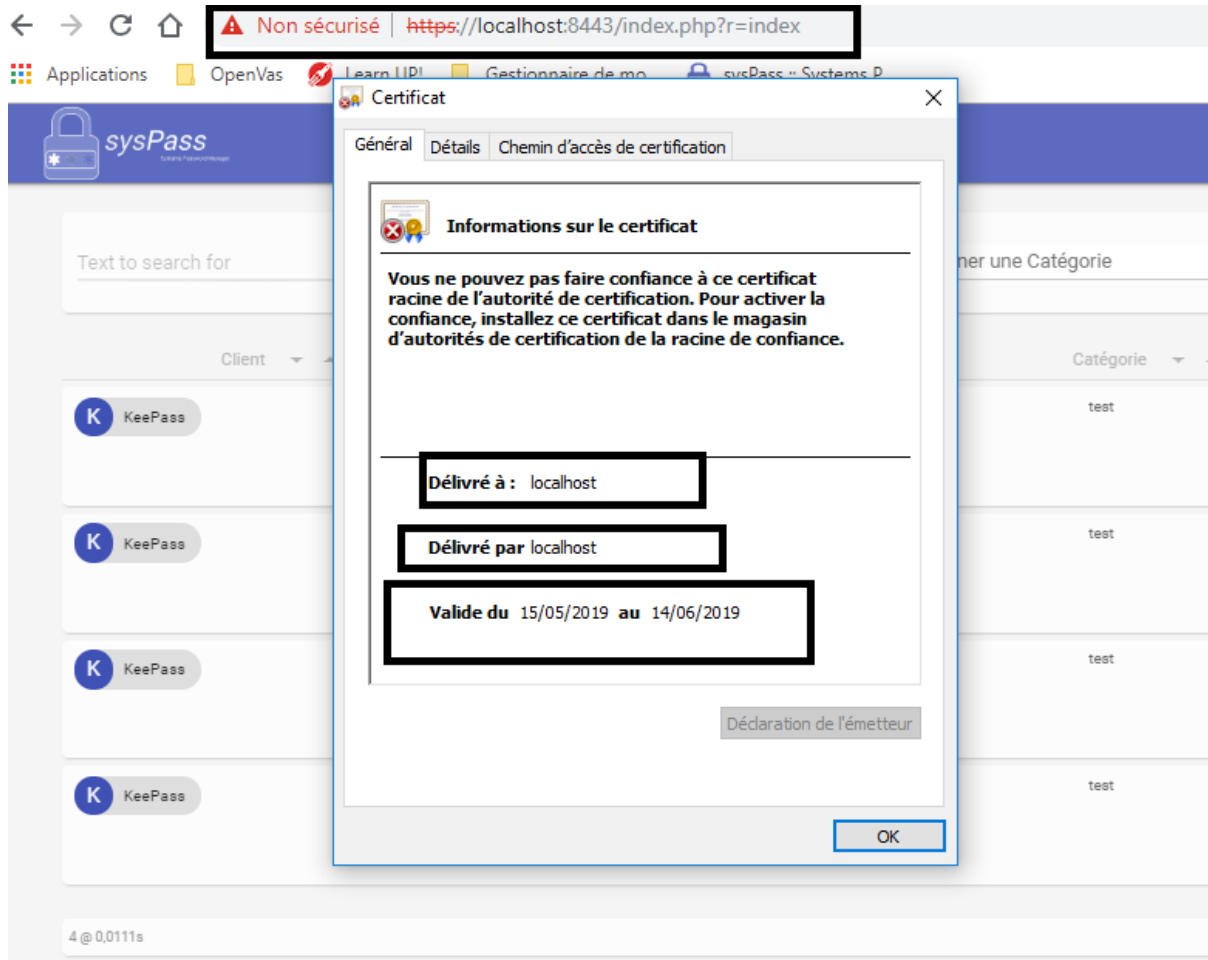
Plugins Change

[Log file](#)
[DOWNLOAD SYSPASS.LOG](#)

Journalisation des actions

Pour journaliser des actions d'un certain type il suffit tout simplement de retourner sur Configuration/Général. Ensuite, dans la liste déroulante Evénement, il est possible d'indiquer à l'application les actions que nous voulons capturer :

Gestion des certificats SSL/TLS



L'url d'accès au site en HTTPS est `https://@IP_HOSTNAME`

Sur ce cas, le certificat, et la clé privée ont été générés sur OpenSSL.

En ce qui concerne la signature du certificat, celui a été autosigné par OpenSSL .

Le format du certificat est en .pem (enveloppe x509) et la clé au format .key .

11.1 Génération du certificat et de la clé privée (en auto signé)

Afin de générer un certificat, il est nécessaire au préalable de générer une bi-clé asymétrique RSA.

```
openssl genrsa -des3 -out localhost.key 1024
```

Une passphrase permettant le déchiffrement de cette clé sera demandée.

Par la suite la demande de signature du certificat est demandée :

```
openssl req -new -key localhost.key -out localhost.csr
```

Ensuite, la génération du certificat auto-signé peut se faire via cette commande :

```
openssl x509 -req -days 365 -in localhost.csr -signkey localhost.key -out localhost.crt
```

Une conversion au format PEM du certificat se fait, ceci afin d'améliorer sa compatibilité avec Apache2 :

```
openssl x509 -outform PEM -in localhost.crt -out localhost.pem
```

11.2 Changement du certificat

Le certificat est placé dans /etc/ssl/certs, pour le changer il y a plusieurs étapes :

1. Désactiver le module SSL par l'instruction `a2dismod ssl` et le service Apache2.
2. Désactiver le service Apache 2 par les instructions :
 - a. `service apache2 reload`
 - b. `service apache2 stop`
3. Copier le nouveau certificat dans /etc/ssl/certs
4. Vérifier que le fichier de configuration Apache2 gérant le service SSL/TLS utilise bien ces 4 directives (dans notre cas le fichier de configuration est /etc/apache2/site-available/default-ssl.conf) :
 - a. `LoadModule ssl_module modules/mod_ssl.so` (à placer avant la directive `<IfModule mod_ssl.c>`)
 - b. `SSLEngine on`
 - c. `SSLCertificateFile /etc/ssl/certs/'nom du certificat'.pem`
 - d. `SSLCertificateKeyFile /etc/ssl/private/'nom de la clé privée'.key`
5. Démarrer Apache2 par `service Apache2 start` et activer le module SSL par `a2enmod ssl`

11.3 Protection de la clé privée

Rappelons que la clé privée a été chiffré à l'aide d'un mot de passe. Afin d'en empêcher son vol par un attaquant ayant eu accès au serveur.

Par conséquent, lors du démarrage d'Apache, celui-ci aura besoin de ce mot de passe pour déchiffrer la clé privée et donc initier des connexions SSL/TLS.

Le mot de passe associé à la clé privée peut être indiqué de deux manières :

11.3.1 Utilisation d'un fichier de configuration

1. Créer le script suivant (nommé `passphrase-file.sh`):

```
#!/bin/sh
echo "Mot_de_passe_de_la_clé_privée";
```

2. Placer ce fichier dans /etc/apache2/ et le rendre exécutable avec la commande `chmod +x passphrase-file.sh`
3. Ajouter dans /etc/apache2/apache2.conf la directive suivante :

```
SSLPassPhraseDialog exec:/etc/apache2/passphrase-file.sh
```

4. Redémarrer Apache2

■ Consulter l'état de l'espace disque

Utiliser directement sur le serveur la commande suivante :

```
df -h /var/www/html/syspass
```

■ Le Master Password

Un mot de passe maître est exigé lors de l'installation de Syspass. Il permet de chiffrer/déchiffrer la base de mots de passe. Il est possible de le modifier. Mais ceci est à faire avec minutie, car en cas de perte, il n'y a pas de possibilité de récupération de la base de mot de passe sans celui-ci.

Par la suite ce master password sera demandé dans plusieurs cas :

- Lors d'une authentification d'un utilisateur après un changement du master password ;
- A la première connexion d'un utilisateur ;
- Pour importer une base de mots de passe (au format XML) contenant un ancien master password ;

13.1 Parade contre un Master password partagée : le Master password temporaire

Ce mot de passe est une donnée critique, sa connaissance doit être restreint à un nombre limité de personnes.

Pour pallier à ce problème de sécurité, Syspass délivre des masters passwords temporaires qui permettront à des nouveaux utilisateurs de se loguer.

Ainsi, un administrateur pourra fournir ce master password temporaire (d'une durée paramétrable) à de nouveaux utilisateurs.

L'application peut aussi se charger de l'envoyer par email directement aux personnes concernés.