Pré-requis serveur applicatif PMB

Version document : 08/10/2018

La mise en œuvre de PMB nécessite à minima une machine sur laquelle sont installés un serveur Web (Apache, IIS) et un serveur de bases de données (Mysql).

Selon les besoins et l'environnement pré-existant, le serveur Web et le serveur de bases de données peuvent être installés sur des machines différentes.

- **Environnement matériel (Machine physique ou virtuelle)**
  - 1 serveur quadri-processeurs / RAM 8Go / DD 50Go

  Il s'agit là d'une valeur à adapter en fonction du volume de données et du trafic.

- **Espace disque requis (hors système)**
  - répertoire web pour l'installation du logiciel PMB (1Go)
  - répertoire de données mysql (10Go pour 100000 notices + 25% du volume des documents numériques indexables)
  - répertoire de stockage des documents numériques (fonction du volume de ceux-ci)
  - répertoire de travail permettant de réaliser les opérations de sauvegarde, montées de versions, ... (20Go)

- **Système d'exploitation**
  - Debian, Ubuntu, RedHat, CentOs, Mageia, ...
  - Windows toutes versions.

- **Serveur Web**
  - Apache 2.2 ou 2.4
  - IIS 7, IIS 8

- **Serveur de bases de données**
  - MySQL >= 5.5 et < 8.0 (ou équivalent MariaDB) avec moteur MyISAM

- **PHP**
  - Version 5.5 ou 5.6

  Sur Windows, une version 5.5 en 32 bits est nécessaire notamment pour installer l'extension php-yaz.

PMB Services – ZI de Mont sur Loir - Château du Loir – MONTVAL SUR LOIR - FRANCE
www.sigb.net ☎ +33(0)2 43 440 660 +33(0)2 43 444 132 pmb@sigb.net
SAS au capital de 103 000 € / RCS Le Mans : 478 151 772 / SIRET : 478 151 772 00033 / APE : 6202A

- **Activation des extensions PHP suivantes :**

  - php-apcu (optionnel, à partir de PMB5.0, pour mise en cache)
  - php-bz2
  - php-cas (optionnel, si mise en oeuvre authentification CAS)
  - php-curl
  - php-devel (optionnel, pour compilation des extensions php, notamment php-yaz)
  - php-dom (libxml >= 2.8)
  - php-fileinfo
  - php-gd
  - php-iconv
  - php-imagick (optionnel, pour visionneuse epub et génération de vignettes à partir de documents numériques)
  - php-intl
  - php-json
  - php-ldap (optionnel, pour interrogation LDAP)
  - php-mbstring
  - php-mysql
  - php-openssl
  - php-session
  - php-soap
  - php-sockets
  - php-sqlite3
  - php-xdiff
  - php-xml
  - php-xsl
  - php-yaz (optionnel, pour interrogation serveurs z3950)
  - php-zip

NB : Le nom des paquets et extensions peut changer selon les distributions.

- **Configuration de Php (fichier "php.ini") :**
  - date.timezone configuré (Europe/Paris par ex.)
  - display_errors = off
  - expose_php = off
  - max_execution_time >= 300
  - max_input_vars >= 50000
  - memory_limit >= 256M
  - post_max_size >= 64M
  - upload_max_filesize >= 64M (taille maximale d'un fichier téléchargé dans PMB)

- **Vérifications à effectuer si l'extension "suhosin" est installée :**
  - suhosin.request.max_vars (mini 2048)
  - suhosin.post.max_vars (mini 2048)

- **Configuration de Apache :**
  - Activation des modules rewrite et ssl

- **Configuration de MySQL (fichier "my.ini" ou "my.cnf")=** :
  - max_allowed_packet=16M (dans les sections [mysqld] et [mysqldump])
  - sql_mode = ''
  - character_set_server=utf8 (de préférence) ou latin1
  - collation_server=utf8_unicode_ci (de préférence) ou latin1_swedish_ci
  - default_storage_engine = MyISAM
  - open_files_limit >= 10000

- **Stockage des documents numériques :**

  Répertoire de stockage des documents numériques avec accès en écriture pour le serveur Web.

- **Indexation des documents numériques de type "pdf" :**

  Installation du paquet "poppler-utils" (exécutable pdftotext nécessaire pour l'indexation des pdf)

  NB : Le nom du paquet peut changer selon les distributions

- **Visionneuse epub :**

  Installation du paquet "poppler-utils" (exécutable pdftoppm nécessaire)

  NB : Le nom du paquet peut changer selon les distributions

- **Webdav :**

  Installation du paquet "perl-Image-ExifTool" (exécutable exiftool nécessaire)

  NB : Le nom du paquet peut changer selon les distributions

- **Communication et réseau :**

La gestion des relances et la diffusion d'information à partir du logiciel PMB se font par mail.

Ceci nécessite l'accès depuis le serveur Web à un **serveur SMTP**, et éventuellement un **compte de messagerie fonctionnel** (compte de la bibliothèque ou du centre de documentation).

Le logiciel PMB permet de récupérer des informations bibliographiques sur différents serveurs externes.

Pour ce faire plusieurs protocoles de communication sont utilisés, dont principalement z39.50 (sur tcp), OAI_PMH (sur http)

Chaque communication nécessite l'**ouverture** d'un **accès** depuis le serveur Web sur lequel est installé PMB.

Ci-après, voici un ensemble de serveurs souvent utilisés :

- protocole z39.50 :
url= z3950.bnf.fr / port= 2211
url= z3950.loc.gov / port= 7090
url= carmin.sudoc.abes.fr / port= 210

- protocole http/https :
url= http://oai.cairn.info
url= http://tel.archives-ouvertes.fr

Le logiciel permet éventuellement l'affichage de vignettes de couverture depuis Amazon.

Pour ce faire, le serveur Web doit pouvoir accéder à l'URL "http://images-eu.amazon.com"

Si l'accès du serveur vers l'extérieur est limité par un **proxy**, celui-ci devra être indiqué.

- **Accès au logiciel :**

Pour chaque installation, deux URLs (ou 2 Alias) sont à prévoir :

Une permettant l'accès à la partie publique du logiciel (destinée aux lecteurs),

la seconde à la partie gestion ou back-office (réservée aux documentalistes).

Pour des raisons de sécurité, l'accès à la partie gestion (Back-office) du logiciel doit être limité.

Nous préconisons de limiter cet accès avec la mise en place du protocole https et la présentation d'un certificat client installé dans les navigateurs et validé au niveau du serveur.

A défaut, il est au minimum nécessaire d'interdire l'accès à la partie gestion (Back-office) depuis Internet (accès sur un domaine local, limitation par adresses IP,...)

De même, nous recommandons vivement la mise en place du protocole https pour l'accès à la partie publique du logiciel.

La mise en place du protocole https nécessite un certificat SSL.

Si ce certificat doit faire partie d'une chaîne de certification reconnue, il doit être fourni.

- **Sauvegardes :**

  Les sauvegardes concernent la base de données et les répertoires de stockage des documents numériques et doivent être externalisées.

  Pour la base de données, la meilleure solution consiste à effectuer un « DUMP » de la base de données, qui pourra être restauré indépendamment de la plate forme d'accueil.

- **Récupération des lecteurs et authentification depuis un annuaire LDAP :**

  Depuis PMB, il est possible :

  - d'importer des lecteurs dans la base de données depuis un annuaire LDAP.
  - de synchroniser les informations concernant les lecteurs.

    (script appelé de façon manuelle ou automatique depuis le cron)
  - de vérifier l'authentification des lecteurs dans l'OPAC.

  L'import et la synchronisation des lecteurs nécessitent une connexion à l'annuaire LDAP, avec un utilisateur ayant les droits de lecture des données du LDAP.

  L'authentification se fait avec vérification des informations saisies dans l'OPAC (login+mot de passe) dans le LDAP.

  (Les mots de passe sont conservés dans le LDAP et ne sont pas stockés dans PMB).

  La communication avec le LDAP nécessite les informations suivantes :

  - Adresse du LDAP
  - Protocole utilisé (ldap ou ldaps)
  - basedn et structure des informations de lecteur stockées dans le LDAP
  - Utilisateur (LDAP) anonyme ou spécifique qui puisse se connecter et récupérer les informations des lecteurs.

- **Authentification automatique des lecteurs dans l'OPAC :**

  L'authentification automatique (SSO) dépend du système utilisé.

  Le principe général est de récupérer une information qui permette d'identifier le lecteur de façon automatique dans PMB.

  Systèmes pouvant être utilisés pour réaliser du SSO dans PMB :

  - NTLM, Kerberos
  - CAS, ADFS, Office365, GoogleApps, ...