Lâchez les rênes, laissez-vous guider : installation facilitée et sécurisée d'eLabFTW

R Ferrere, J.-M Sibaud, H Valeins, S Sabatié, K Viaud, M Goillandeau, P Hortolland, Jean-Marc Sibaud

Poster ID

Lâchez les rênes, laissez-vous guider : installation facilitée et sécurisée d'eLabFTW

R. Ferrere [1], J.-M.Sibaud [2], H. Valeins [3], S. Sabatié [4],
K. Viaud [3], M. Goillandeau [5], P. Hortolland [6]

jres RENNES 2024

Introduction et présentation

Le CNRS, établissement de recherche à caractère pluridisciplinaire, a lancé en 2023 une offre de service pour la mise en place d'un Cahier de Laboratoire Electronique (CLE) basé sur le logiciel libre eLabFTW. Cette offre s'articule autour de deux solutions, une offre SaaS (Software as a Service) et **une offre On Premise (en local ou sur site)**. Dans ce poster nous allons vous **proposer un modèle d'accompagnement sur le déploiement et la configuration d'eLabFTW dans une unité de recherche**, en adéquation avec les consignes du CNRS.

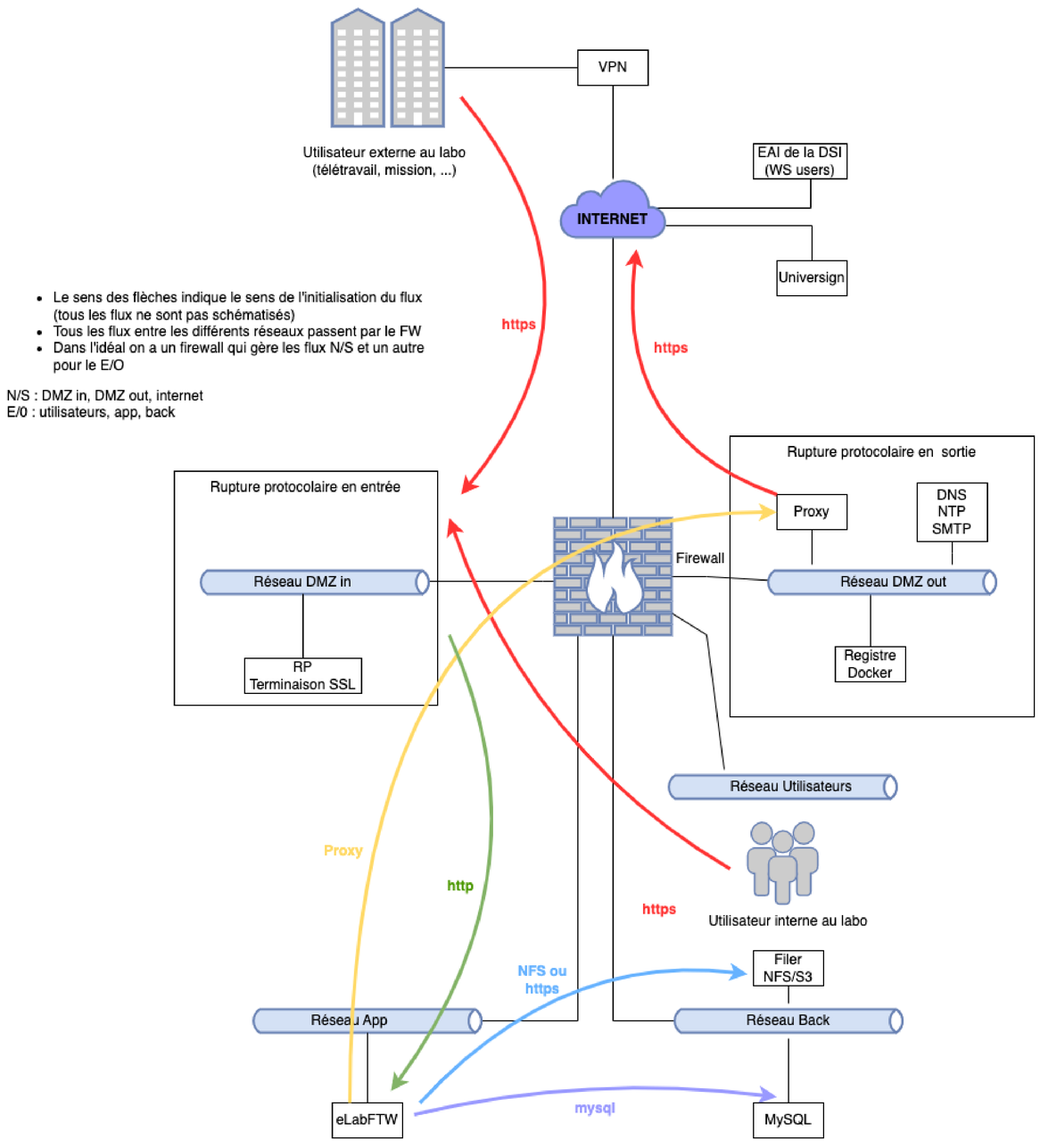
Principales actions d'exploitation

Une fois l'infrastructure installée cela fonctionne tout seul, et demande environ 1 heure de travail par mois. Il faut s'assurer de la mise en place de quelques actions pour l'exploitation, et être en mesure de faire face à un incident. Pour cela, se référer à l'article.

Quelles actions d'exploitation à mettre en place ?
- **La sauvegarde automatique** par Borgbackup, ou script et crontab.
- **Les mises à jour** de eLabFTW en lien avec la base de données MySQL.
- **La supervision avec les logs** de connexion et d'activité sur eLabFTW.

Pour effectuer une restauration **en cas de migration ou d'incident** :
- une procédure simple en 9 étapes !

Architecture sécurisée et adaptation périmétrique



☛ Au CNRS, la double authentification par Janus+ et clé USB FIDO2.

Installation sécurisée On Premise

Il s'agit de présenter **les différents composants, la méthodologie et les étapes utilisées** par le groupe de travail.

Les composants utilisés sont de plusieurs natures :

N°	Composants	Exigence
1	Pas d'accès depuis l'extérieur (via VPN et télétravail)	**Obligatoire**
2	Adresse IP externe pour appel Web Service	**Obligatoire**
3	Chiffrement des disques durs	**Obligatoire**
4	Chiffrement des sauvegardes	**Obligatoire**
5	Pare-feu d'infrastructure - segmenter les VM	**Obligatoire**
6	Présence d'un Reverse Proxy	Si possible
7	Utilisation d'une VM dédiée "Filer" - pièces jointes	Facultatif
8	Utilisation Proxy de Sortie "Squid" - flux sortant	Facultatif
9	Utilisation registre Docker dédié	Facultatif

- **le socle de base de virtualisation avec Docker**, et Proxmox (VM);
- **l'outil Docker Compose pour gérer les fichiers YAML** pour les services, les volumes de stockage;
- **les certificats** : la CA, le certificat serveur, le certificat client (4 étapes);
- **le service Filer pour stocker les fichiers** de façon persistante;
- le reverse proxy dans certains cas pour protéger des flux venant de l'extérieur.

☺ ☺ ☺ Notre cas pratique pour l'installation de l'infrastructure CLE en mode sécurisé en quelques étapes, tout en étant sur les machines virtuelles de eLabFTW et de MySQL:
- Sur la machine eLabFTW
  - ○ créer les répertoires pour les volumes persistants, les certificats
  - ○ créer le fichier docker-compose.yml pour l'installation de eLabFTW (en dernière version)
  - ○ lancer le conteneur eLabFTW : **docker-compose up -d**
- Sur la machine MySQL
  - ○ créer le fichier docker-compose.yml pour l'installation de MySQL
  - ○ installer et copier les certificats avant de lancer l'installation de MySQL
  - ○ ne pas oublier d'ajouter les informations dans le fichier (**pour les volumes et les certificats**)
  - ○ lancer le conteneur MySQL : **docker-compose up -d**
- Sur la machine eLabFTW
  - ○ initialiser la base de données eLabFTW :

docker exec -it elabftw bin/init db:install
- ○ **l'URL de l'application CLE est prête à être utilisée !** ☺ ☺ ☺

Résumé et Perspectives

Le cahier de laboratoire électronique (CLE) est appelé à s'imposer par sa facilité d'installation et d'exploitation en On Premise, et concerne de plus en plus d'EPST (INRAE, INSERM. . .). Cet outil satisfait toutes les contraintes de sécurité et devient accessible même pour des unités dites sensibles (ZRR).

Ce projet a été une véritable aventure humaine pour le groupe de travail des informaticiens du réseau RAISIN (Bordeaux) qui a réalisé une documentation et un article pour vous aider. Ce groupe de travail est prêt à aller plus loin comme par exemple sur une journée pratique JOSY ou JTECH, ou le développement d'un modèle pour une plus grande automatisation des certificats et des machines virtuelles avec PROXMOX.

Avec notre démarche nous avons constaté la présence d'une véritable bulle de confiance avec un environnement capable de protéger toutes les données car s'appuyant sur une conformité réglementaire et une cybersécurité renforcée.

RÉFÉRENCES

[1] CELIA - Centre Lasers Intenses et Applications - Univ. de Bordeaux - Domaine du Haut Carré - 43, rue Pierre Noailles - 33405 Talence, France
[2] UMR5295 I2M Institut de Mécanique et d'Ingénierie - Univ. Bordeaux - 351 cours de la libération - 33405 Talence Cedex
[3] UMR5536 CRMSB - Centre de Résonance Magnétique des Systèmes Biologiques - Univ. de Bordeaux - 146 Rue Léo Saignat - 33076 Bordeaux Cedex
[4] INRAE UR ETTIS - 50 Avenue de Verdun - Gazinet - 33610 Cestas
[5] UMR5293 IMN - Institut des Maladies Neurodégénératives - Univ. de Bordeaux - 146 rue léo Saignat - Centre Broca Nouvelle-Aquitaine - 33076 Bordeaux Cedex
[6] UMR529 LP2N - Laboratoire photonique, numérique et nanosciences - Institut d'Optique d'Aquitaine - Rue François Mitterrand - 33400 Talence Cedex

REMERCIEMENTS et PARTENAIRES

jres RENNES 2024
cnrs
INRAE

CONTACT

Jean-Marc Sibaud
UMR5295 – I2M
CNRS
jean-marc.sibaud@u-bordeaux.fr

GT CLE – RAISIN

https://raisin.pages.math.cnrs.fr/mkdocs/