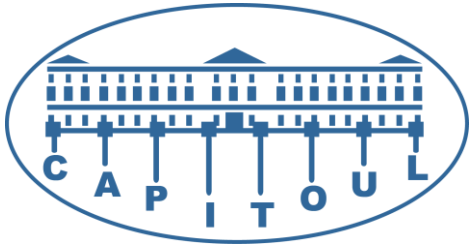
BITWARDEN(_RS)

Mathieu HENRICH MAUVEZIN
Administrateur Réseau et Système – Lycée Ozenne Toulouse
11/02/2021

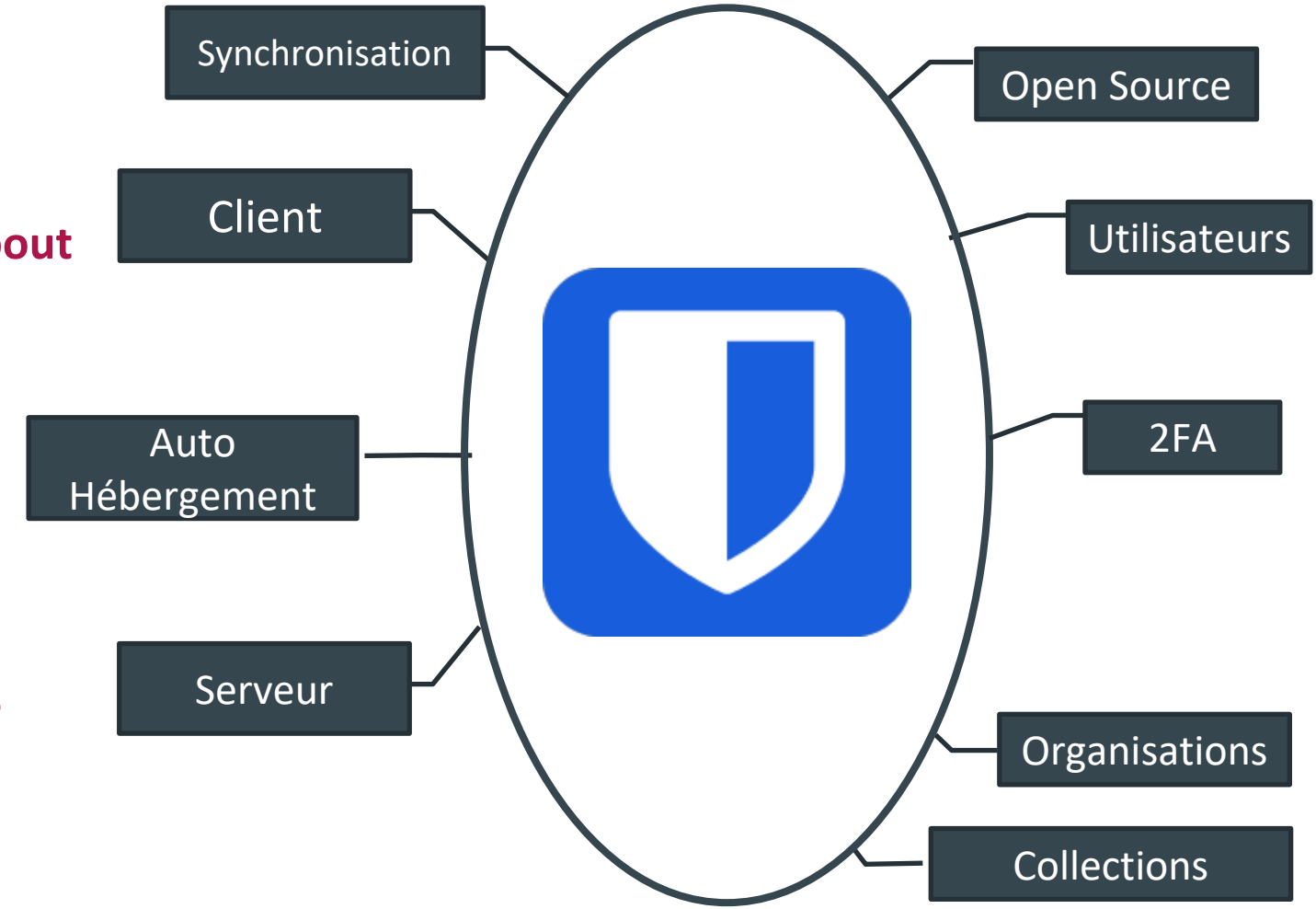


Lycée Ozenne
Toulouse

SOMMAIRE

C’est quoi Bitwarden ?

- **Gestionnaire de Mot de Passe**, Notes sécurisés, Cartes de crédits, identités
- Gestionnaire **partagé, chiffré de bout en bout (AES 256 bits)**
- Licence **Open Source**
- Peut être utilisé :
  - avec hébergement payant
  - **Auto Hébergement**
- Fonctionnement en mode **Client / Serveur**
- **Clients Multiplateformes**
- Créer en 2016 par Kyle Spearrin.



Bitwarden VS Bitwarden_RS

BITWARDEN (Standard)

- Version Officielle
- N'inclus pas la version Premium en Natif → Paiement d'un abonnement / Licence

BITWARDEN_RS (Premium)

- Version NON OFFICIELLE (pas sur les dépôts de Bitwarden)
- Codé en RUST (d'où son nom..) par Dani Garcia
- Active la fonctionnalité Premium sans frais
- Embarque un grand nombre de fonctionnalités de Bitwarden
- Les clients « classiques » sont entièrement compatibles
- Plus léger à héberger et à déployer

VOIR TABLEAU COMPARATIF DES FONCTIONS

Comparatif des fonctions

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

Lycée Ozenne Toulouse

FEATURES FOR BUSINESS	Free Organization	Teams	Enterprise	Bitwarden_RS
Base Users	2	1	1	1
Max Users	2	Unlimited	Unlimited	Unlimited
Max Collections	2	Unlimited	Unlimited	Unlimited
Access to all Bitwarden apps				
Item storage (Logins, Notes,…)	Unlimited	Unlimited	Unlimited	Unlimited
Sync all of your devices				
Shared Items	Unlimited	Unlimited	Unlimited	Unlimited
Secure Password Generator				
Encrypted file attachments		1 GB+ Personal // 1 GB+ for Org Items	1 GB+ Personal //1 GB+ for Org Items	NAN
Encrypted Export				
Premium Features	Upgrade Required			
Bitwarden Authenticator (TOTP)				
Two-step login	2FA	2FA, YubiKey, U2F, Duo	2FA, YubiKey, U2F, Duo	email, Duo, YubiKey, and FIDO U2F
Personal Emergency Access				**SelfHost - Création illimité**
Vault health reports				NAN
Event & audit logs				
User Groups				
API Access				
Directory Sync				
Login with SSO				
Enterprise policies				
Custom Management Role				
Priority support				
Cloud host				SelfHost
Self-host option				

Coût d'hébergement en Ligne

Grille Tarifs Hébergement en ligne – Professionnel – 07/02/2021

Free Organization	Teams Organization	Enterprise Organization
$0/month includes 2 users	**$3/month** per user	**$5/month** per user
Start storing and sharing secure passwords with a two-person organization.	Share private data safely with your coworkers, department, or entire organization.	Secure business secrets, enable enterprise policies, SSO authentication, and self-hosting.
The core features and sharing are 100% free. Upgrade anytime.	Includes Premium Features for all users. Explore our Teams plan free for 7 days.	Includes Premium and Teams Features for users. Explore our Enterprise plan free for 7 days.
Create Free Organization	Start Teams Free Trial	Start Enterprise Free Trial

Pricing shown is based on an annual subscription.

Auto Hébergement

Pourquoi Héberger son serveur Bitwarden ?

- Être **maitre de ses données** (RGPD …)
- Permet une **flexibilité d'utilisation** (Déploiement, Configurations,…)
- **Réductions des coûts d'exploitations** liée à un abonnement Professionnel (dans le cas de Bitwarden_RS)

Les Limites

- Vous êtes le seul **responsable de vos données**
- Vous devez gérer vous-même **l'intégrité et la sécurité de votre système**
- Mise en place de **sauvegardes et/ou duplication(s)**
- En bref : **un nouveau serveur** (parmi les nombreux autres) à **entretenir**

Hébergement - Spécifications Techniques

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Lycée Ozenne Toulouse

Types de système d'hébergement compatibles :

	Bitwarden Standard	Bitwarden_RS
Linux	✓	✗
MacOSX	✓	✗
Windows Server	✓	✗
Docker	✓	✓
Nas	✓	✓

Configuration minimale requise préconisé :

- Processor: x64, 2 GHz dual core
- Memory: 4 GB RAM (system memory)
- Storage: 25 GB
- Docker: Engine 19+ and Compose 1.24+

Hébergement

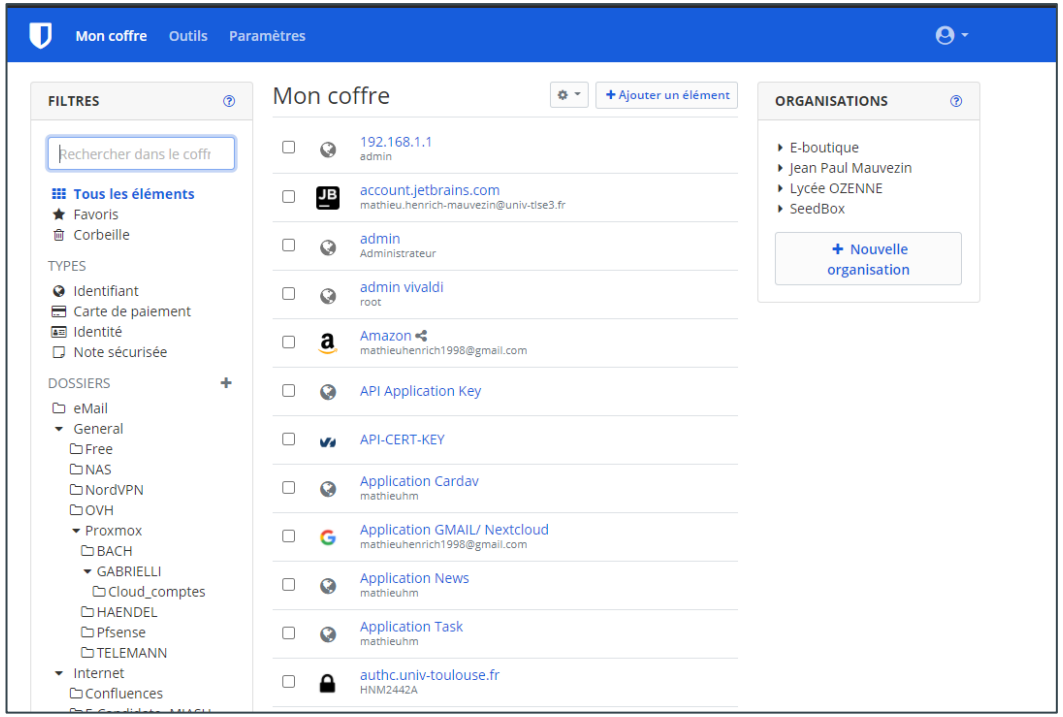
- Installation Sur Docker – Une grande simplicité

```
docker run -d --name Bitwarden_RS \
-e ADMIN_TOKEN=« Mot_de_Passe_Maitre » \
-v /bw-data/:/data/ \
-p 80:80 \
--restart always \
bitwardenrs/server:latest
```

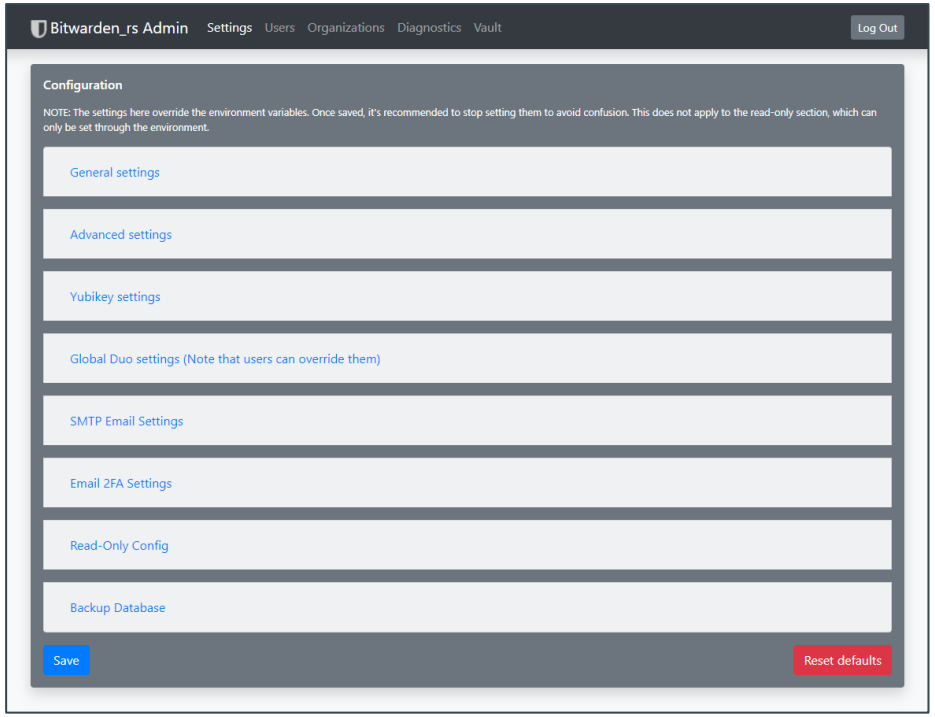
-v : Répertoire contenant les données
-p : le port utilisé pour le serveur Web
--restart always : garder la machine allumée

Hébergement

- Serveur avec deux interfaces de gestion
  - « Vault » : Données du coffre fort
  - Interface Administrateur (Configuration du serveur et des utilisateurs)



Interface WEB (vault) : utilisation du coffre fort



Interface WEB administration

Organisation des objets Bitwarden

- *Côté Professionnel*
- Bitwarden a une **structure propre** qui permet **d'organiser**, **sécuriser** et **partager tout ou partie** d'un coffre fort.

- **Structure élémentaire** :
  - Les Organisations
  - Les collections
  - Les groupes
  - Les politiques

Les Organisations

- Représentent des **entités** constituées **d'utilisateurs** qui souhaitent **partager des données**.
- Création **d'un nouveau coffre fort dédié** en **parallèle** de votre coffre fort **personnel.**

- Exemples d'organisations :
  - Cercle Familial
  - Une Equipe (Pole Administratif, Pole Maintenance,…)
  - Une Entreprise/Etablissement (UT1, Lycée Ozenne, ..)

- La définition d'une organisation doit être **déterminée** en fonction de l'**étendue** de cette dernière ainsi que des contrôles d'accès (utilisateurs).

  (Si très grande organisation, peut-être prévoir un découpage)

Les Collections

- Permettent de **structurer votre organisation**.
- **Similaires aux dossiers** utilisés dans votre coffre fort personnel.
- L'**accès** aux collections est établi par un **contrôle d'accès des utilisateurs.**
- **Tous les éléments du coffre (d'une organisation)** doivent être **stockés** dans au moins **une collection.**
- Une collection est **accessible à tous les utilisateurs autorisés à** cette dernière.

Les Groupes

- A utiliser en **complément** des **collections.**
- Permet **d'affiner les droits d'accès des utilisateurs.**
- Permet de **faciliter l'attribution des droits** sur un grand nombre d'utilisateurs.

Politiques d'organisation

- Définit les **règles de sécurité** liées au coffre fort de votre organisation.

Les règles disponibles :

- Exiger **l'authentification en deux étapes** pour les utilisateurs
- Définir des exigences **minimales pour la force du mot de passe maître**
- Définir les exigences minimales pour la **configuration du générateur de mot de passe**.(ex: plus de 8 caractères, caractères spéciaux, …)
- Exiger que les utilisateurs enregistrent des éléments du coffre dans une organisation en **retirant l'option de propriété individuelle**

CLIENTS

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Lycée Ozenne Toulouse

APPLICATIONS ✓

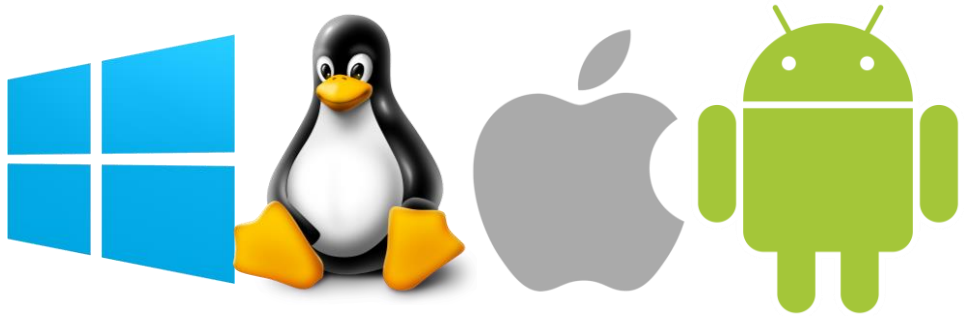
- Windows
- Linux
- OSX
- Android
- IOS
- Version CLI

EXTENSION NAVIGATEUR ✓

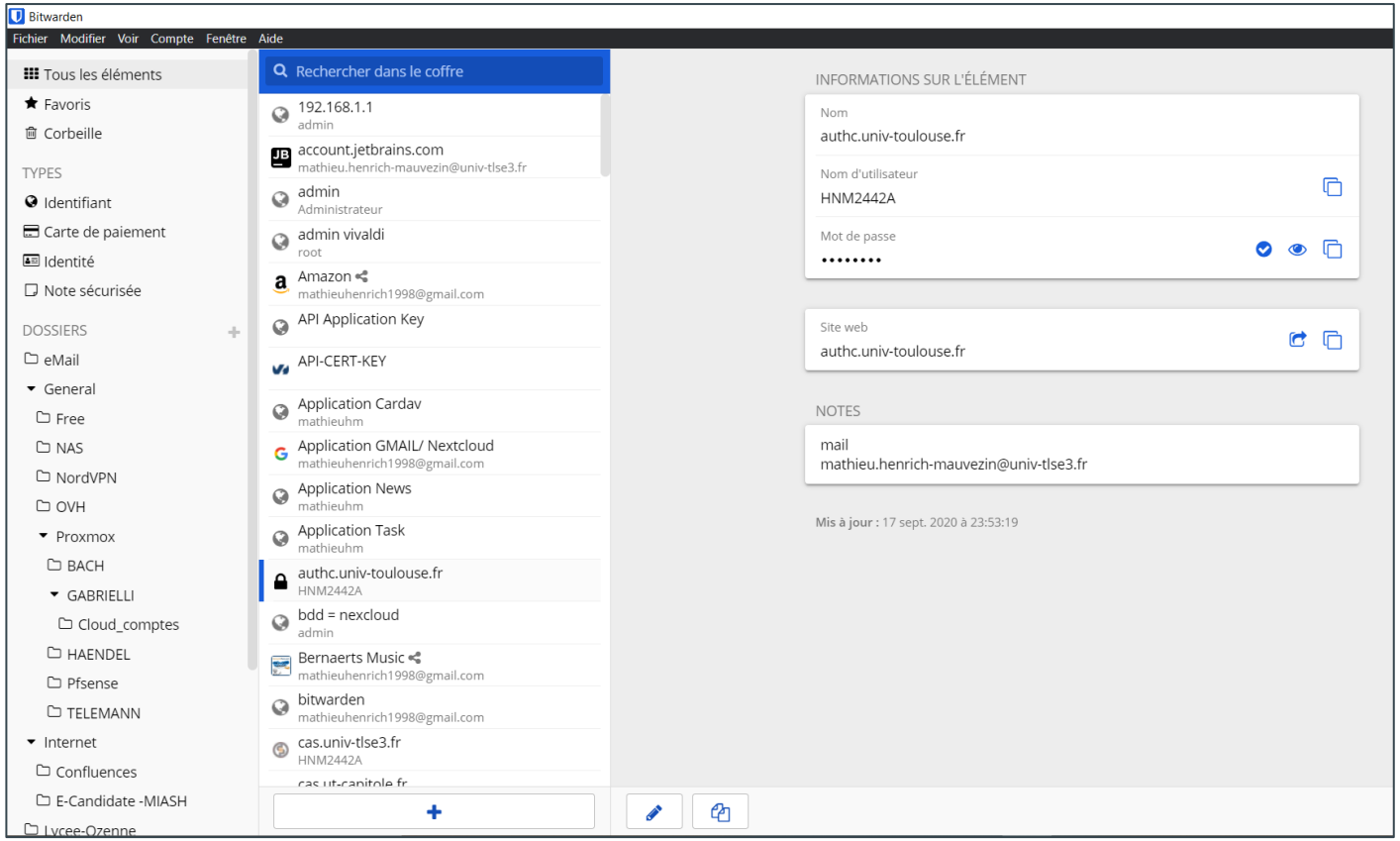
- Google Chrome
- Firefox
- Safari
- Vivaldi
- Edge
- Brave
- TOR Browser

Autocomplétions des formulaires Login/PW

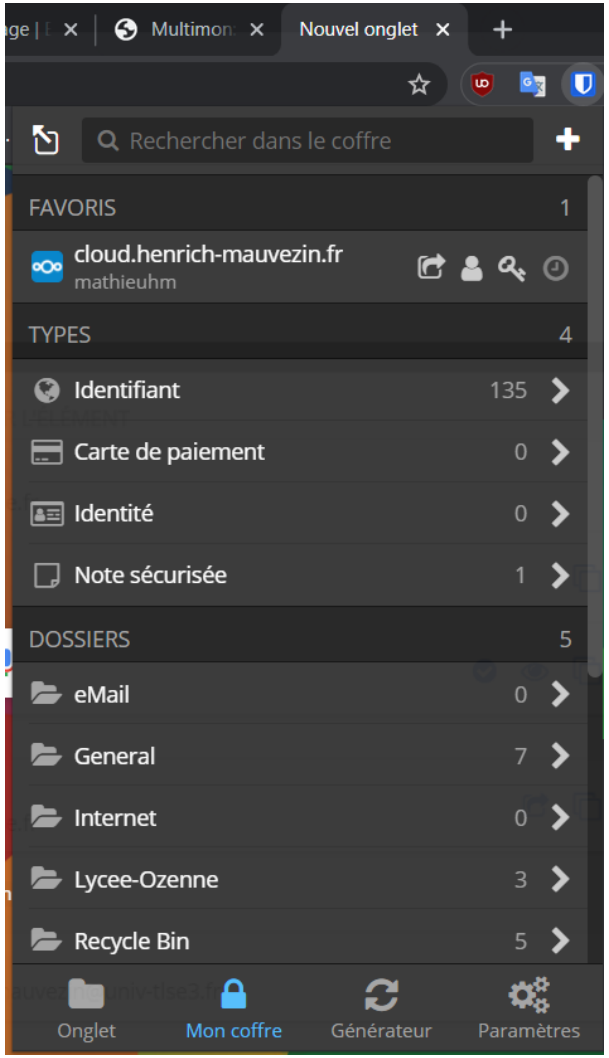
Génère un mot de passe et l'enregistre dans la base



CLIENTS – CAPTURES D'ECRANS



Application cliente Windows



Extension de Navigateur Chrome

CLIENTS – Stockage

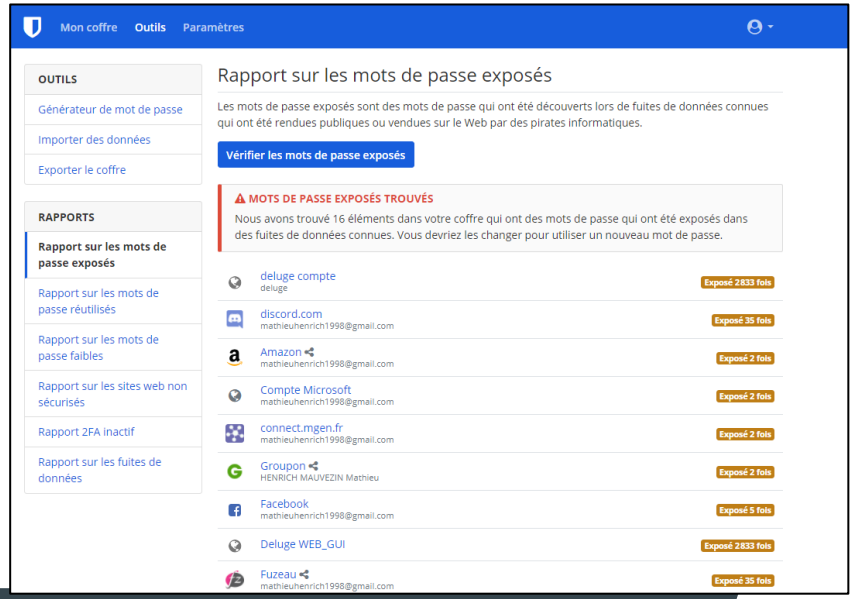
- L'ensemble des données du serveur sont **téléchargés par les clients** (synchronisation)
- Les datas stockés sur les clients sont **cryptées**
- Bases **décryptées lorsque on déverrouille l'application cliente**
- Serveur inaccessible → accès à son coffre fort (avant synchro)

```
"818eb5ee-00b2-400d-a5fa-b3fb7a16184c": {
    "id": "818eb5ee-00b2-400d-a5fa-b3fb7a16184c",
    "organizationId": null,
    "folderId": "5d36b0fa-e159-4b34-8cd5-d377f6ffd855",
    "userId": "525a8652-a885-4b48-b4a0-008d73e5c2b8",
    "edit": true,
    "viewPassword": true,
    "organizationUseTotp": true,
    "favorite": false,
    "revisionDate": "2021-01-18T18:25:58.034238Z",
    "type": 1,
    "name": "2.KNN7Amfbg1/zmFnT7/AKFA==|LWboC3vkBNzGE4iJ/0ZBew0Tot1GbOGFyOkOQFUXaQQ=|ECNP71apKKbDzu+42F4UAk7hzJbWfaEKGAQsSj/KIvg=",
    "notes": null,
    "collectionIds": [],
    "deletedDate": "2021-01-18T18:25:58.032324Z",
    "login": {
        "username": "2.lSTETYt0tD5qhfqAPD+RAw==|UM48mWnxjCcU6tqrdVnUsw==|VAtjorIrMaDcaFl7t+0cNFwRb2Ro/opUeO2iewK+zjM=",
        "password": "2.cMlGUtsXHP69twwtXpa9qA==|Coe1I6qsljeG7WuzCNkAIw==|rRdOtX0qe3sC/zohXeZMzFzYcI4/2dqsSpPCXQZB2F0=",
        "passwordRevisionDate": null,
        "totp": null
    },
    "attachments": []
},
"88746621-5e99-4a2f-96d5-7c700caebe32": {
```


Extrait fichier cryptés stocké sur la machine locale

Outils – Fonctions intéressantes

- **Générateurs** de mots de passe
- Rapport **des mots de passe exposés** lors d'une **fuite de données**
- Listes des **sites** Web **non sécurisés**
- Listes des **mots de passe réutilisés**
- Rapport sur **les mots de passe faibles**
- Rapport sur les sites contenant une double authentification



Utilisation dans l’environnement professionnel

- ATTENTION : (concerne la version de Bitwarden Standard)
- Il est possible grâce à **un connecteur, d’interfacer** les **comptes AD** avec Bitwarden.

- Espérons que cette fonction arrive sur la version RS…

- Questions qui se poses sur la communauté : Comment utiliser un Bitwarden personnel avec un Bitwarden professionnel ?

Migration vers Bitwarden

- Fonction d'importation des données d'un gestionnaire de mot de passe
- Listes outils compatibles

- 1Password (1pif)
- 1Password 6 & 7 Windows (.sv)
- 1Password 6 & 7 Mac (csv)
- Ascendo DataVault (csv)
- Avast Passwords (csv)
- Avira (json)
- BlackBerry Password Keeper (csv)
- Blur (csv)
- Brave (csv)
- **Chrome (csv)**
- Clipperz (html)
- Codebook (csv)
- **Dashlane (json)**
- Encryptr (csv)
- **Enpass (csv)**
- **Enpass (json)**
- **Firefox (csv)**
- F-Secure KEY (fsk)
- GNOME Passwords and Keys/Seahorse(json)
- **Kaspersky Password Manager (txt)**
- **KeePass 2 (xml)**
- **KeePassX (csv)**
- Keeper (csv)
- **LastPass (csv)**
- LogMeOnce (csv)
- Meldium (csv)
- mSecure (csv)
- Myki (csv)
- **Microsoft Edge (Chromium) (csv)**
- **Opera (csv)**
- Padlock (csv)
- Passbolt (csv)
- PassKeep (csv)
- Passman (json)
- Passpack (csv)
- Password Agent (csv)
- Password Boss (json)
- Password Dragon (xml)
- Password Safe (xml)
- PasswordWallet (txt)
- RememBear (csv)
- RoboForm (csv)
- SafeInCloud (xml)
- SaferPass (csv)
- SecureSafe (csv)
- SplashID (csv)
- Sticky Password (xml)
- True Key (csv)
- Universal Password Manager (csv)
- Vivaldi (csv)
- Yoti (csv)
- Zoho Vault (csv)

RESSOURCES

- Pour aller plus loin …

Installation – Configuration - Serveur

- Documentation Officielle de Bitwarden
- Dépôt GitHub Bitwarden_RS
- Docker Hub Bitwarden_RS
- Installation Bitwarden sur Nas Synology

Client

- Téléchargement des Clients
- Stockage des Data – Serveur et Clients
- Dépôt GitHub Application
- Dépôt GitHub Extension Navigateur

Les questions - Contact

- Contact

mathieu@henrich-mauvezin.fr
mathieu.henrich@lycee-ozenne.fr

Mathieu HENRICH MAUVEZIN