Advanced Users Guide

Version 4.0.5-247-gea63ed2b

Lybero developement team

2019-11-13

Version : 4.0.5-247-gea63ed2b

Summary

1 Introduction

1.1 Sécurité

CryptnDrive de Lybero.net est un logiciel serveur web permettant le stockage, le partage et le transfert de fichiers et de textes de manière chiffrée sans aucune installation de logiciels sur les machines des utilisateurs.

Il est utilisable de plusieurs manières : en s'enregistrant sur notre instance de démonstration https://drive.lybero.net où nous ne garantissons le stockage de l'information que pendant 1 mois, via une instance que Lybero.net installe et administre pour votre compte, ou bien via une instance installée par une autre organisation (la votre par exemple).

L'ensemble des chiffrements est fait de bout en bout, via un chiffrement fait en javascript dans le navigateur pour les informations. Les informations sont stockées dans une base de données mongodb. Le serveur web central est extrèmement passif, il reçoit des informations et les stocke, assure la synchronisation des informations avec les navigateurs des clients et l'envoie des notifications. Il n'a aucune fonction de traitement des informations.

L'authentification est faite de manière flexible, ou bien de manière autonome ou bien via oauth2 (Google, . . .). Les clés publiques sont stockées sur le serveur de fichiers, les clés privées sont stockées chiffrées avec la phrase de passe des utilisateurs et ne sont déchiffrées que dans les navigateurs.

Chaque dépôt de fichiers est chiffré avec une clé AES256 spécifique. La clé AES est elle-même chiffrée avec la clé publique de chaque utilisateur ayant accès au partage.

Le partage d'un dépôt de fichiers donc son transfert peuvent se faire entre des personnes enregistrées dans le système, ou pas encore enregistrée, ou bien avec un groupe de recouvrement que nous appelons groupe à quorum.

Lorsqu'un partage d'un dépôt de fichiers est fait avec un groupe à quorum, les membres du groupe à quorum ne peuvent pas accéder au dépôt de fichiers. Par contre, ils peuvent inviter des tiers (enregistrés ou pas). Si un tiers invité accepte l'invitation et si un quorum (par exemple 3 sur 5) accepte son accès, l'invité pourra accéder au dépôt de fichiers. Il y a donc séparation stricte (cryptographique) entre l'autorisation d'accès et l'accès à l'information. A aucun moment, un membre du quorum (que nous appelons administrateur de secrets) ne peut accéder à l'information déchiffrée, et tant que le quorum ne l'a pas accepté, le demandeur ne peut pas non plus accéder à l'information (elle reste chiffrée). Ce mécanisme offre à la fois sécurité par le nombre et flexibilité pour les organisations. Il permet de reproduire cryptographiquement les procédures fonctionnelles d'accès à l'information.

Ce manuel est décomposé en 3 parties principales :

- Le manuel utilisateur
- Le manuel d'installation
- Des éléments sur les algorithmes utilisés.

2 Utilisation avancée

2.1 Recouvrement à quorum

Nous allons maintenant utiliser un groupe d'administrateurs de secrets à quorum pour opérer un recouvrement par un tiers.

2.1.1 Configuration d'un Quorum

Tout d'abord, nous ajoutons un groupe à quorum en partage sur un coffre. Pour cela, l'administrateur doit ajouter le groupe à quorum via le menu d'administration (Administration > Quorums).

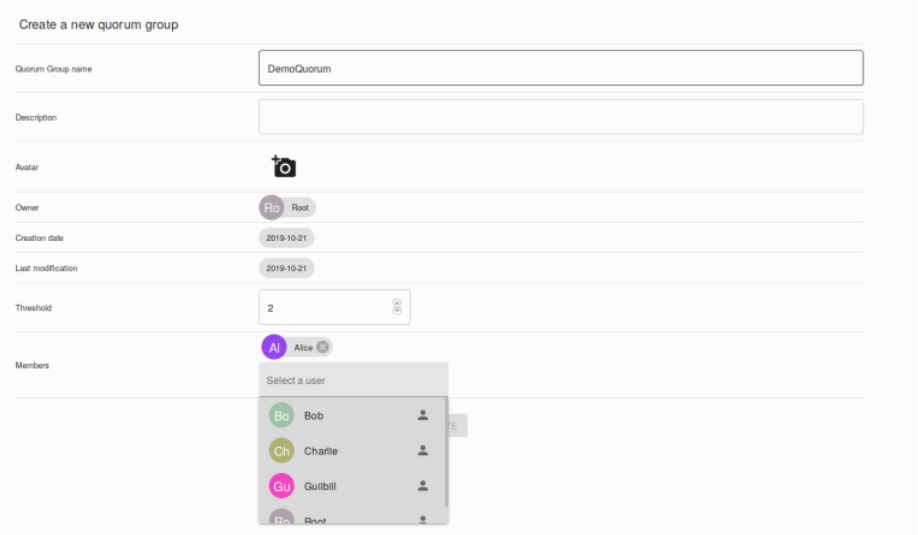


Figure 1: Ajout d'un groupe à Quorum

L'administrateur doit indiquer le nom du groupe, éventuellement une description, le seuil du quorum, et les membres du quorum. Pour finaliser le groupe à quorum il faut que chaque membre du groupe se connecte 2 fois. Dans notre cas, nous ajoutons Alice, Bob et Charlie dans un groupe à quorum avec un seuil de 2.

Une fois le groupe à quorum créé, il faut indiquer dans la configuration du répertoire de coffres concerné que l'on veut utiliser ce quorum. Pour cela, dans les paramètres du répertoire de coffres (root par exemple), ajouter au groupe souhaité (All groups par exemple) le groupe à quorum comme Service de recouvrement.

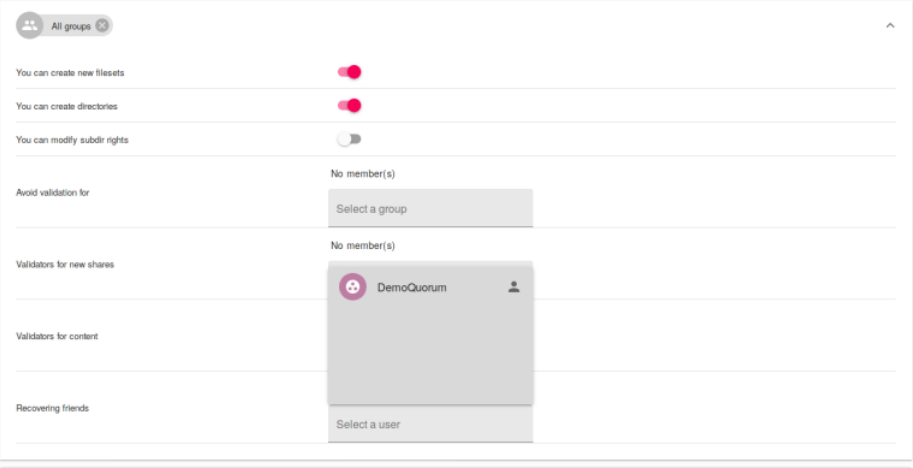


Figure 2: Configuration du groupe à quorum

Une fois cette configuration faites, tous les coffres qui seront créés dans le répertoire de coffre root ou ses sous répertoires de coffres bénéficieront du mécanisme de recouvrement par quorum.

2.1.2 *Création d'un coffre avec mécanisme de recouvrement par Quorum*

Maintenant que nous avons configuré le recouvrement par le groupe à Quorum composé d'Alice, Bob et Charlie, un utilisateur lambda peut créer un coffre qui bénéficiera du recouvrement pas quorum. L'utilisateur Delta créé un coffre et y dépose un fichier. Dans les partages du dépôt, nous pouvons voir le groupe à quorum.

Figure 3: Le quorum est présent dans les partages

Notons que les membres du Quorum, si on ne leur a pas partagé le coffre, peuvent le voir en grisé sur leur interface, mais ne peuvent pas le déchiffrer.

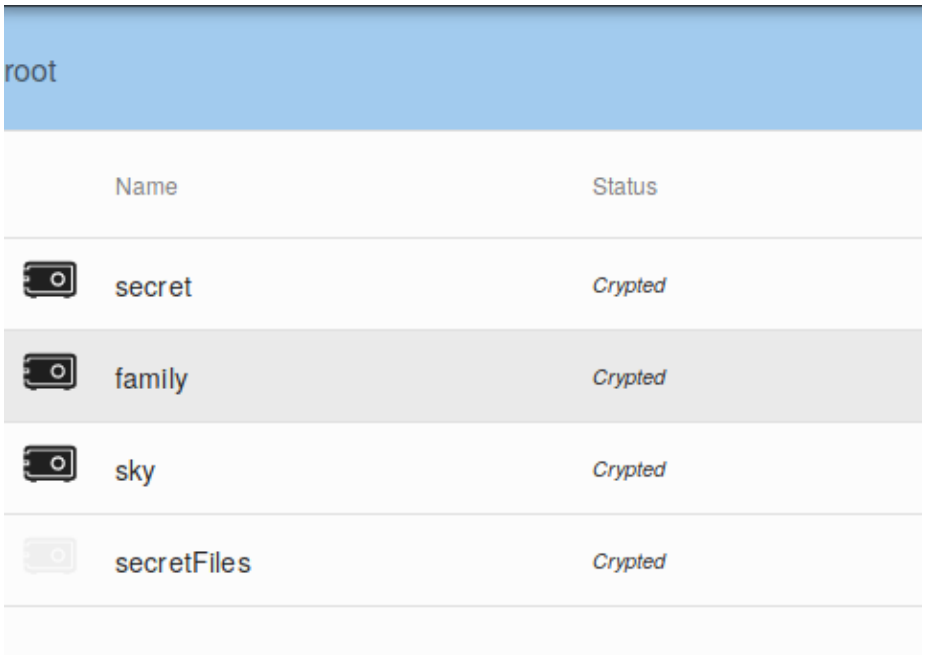


Figure 4: Vue du coffre par le quorum

2.1.3 Procédure de recouvrement

Un membre du quorum peut inviter un utilisateur à accéder au coffre. Pour cela elle peut accéder au partages du coffre en question (elle ne peut toujours pas le déchiffrer), et ajouter l'utilistateur de son choix.

Une notification indique alors aux membres du quorum qu'une demande de recouvrement a été faite.

Ils peuvent alors accepter ou refuser. Lorsque le nombre de membres du quorum ayant accepté le recouvrement est supérieur ou égal au seuil du quorum, alors, le recouvrement est effectif et l'utilistateur a accés au coffre.

Il faut bien comprendre que ce mécanisme est cryptographique. Le groupe à quorum a une clé publique, mais pas de clé privée. Lorsque c@a.net a demandé à accéder au coffre, la clé AES256 du dépôt chiffrée par la clé publique du groupe à quorum a été sur-chiffrée par la clé publique de c@a.net.

Au dernier déchiffrement partiel du membre du quorum, la clé AES256 du dépôt est restée chiffrée par la clé publique de c@a.net. c@a.net a récupéré cette

Figure 5: Partage du coffre

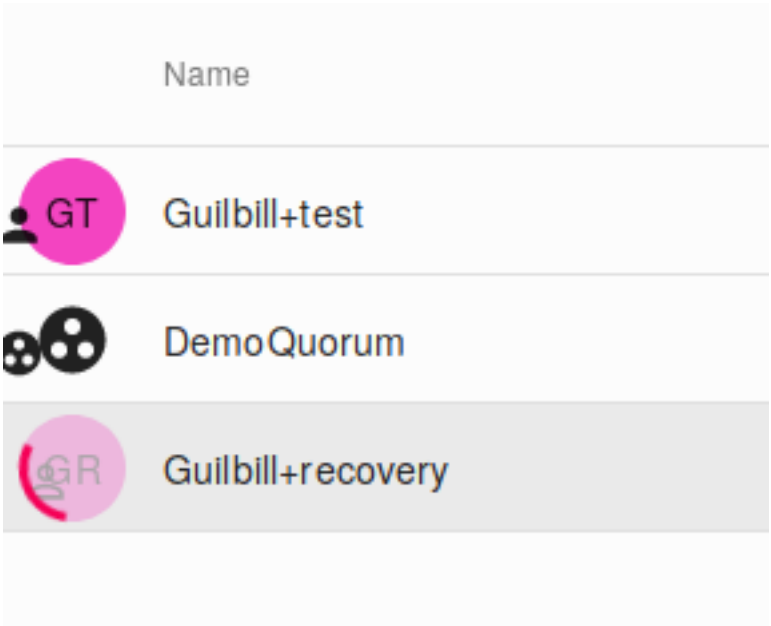


Figure 6: Recouvrement en attente

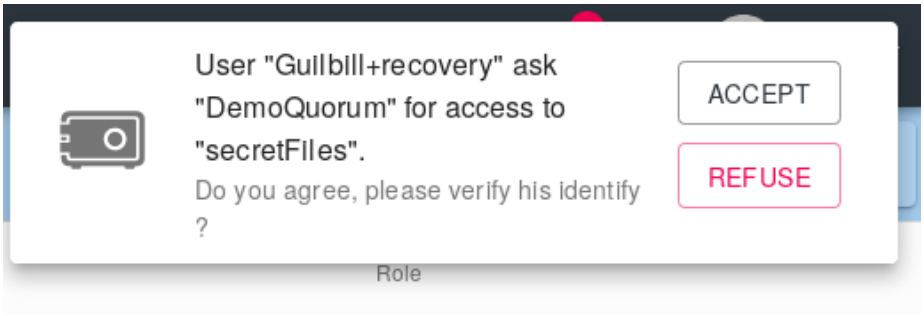


Figure 7: Demande d'accès à un dépôt

valeur puis l'a déchiffrée avec sa clé privée. Il a alors eu accès à la clé AES256 du dépôt et donc au dépôt.

La séparation entre l'autorisation d'accès par le groupe à quorum et l'accès au dépôt est cryptographique. C'est une propriété très précieuse de notre système. Elle permet à un groupe de personnes non expertes de mener les opérations de recouvrement qui sont habituellement confiées à des experts techniques, qui fonctionnellement ne sont pas forcément les mieux à mêmes de mener ces opérations.

2.2 Droits des répertoires de coffres et validations

Le mécanisme de répertoires de coffres permet de mettre en place une gestion plus fine des possibilités des utilisateurs. Chaque répertoire de coffre peut être paramétré de sorte à coller au plus près des besoins.

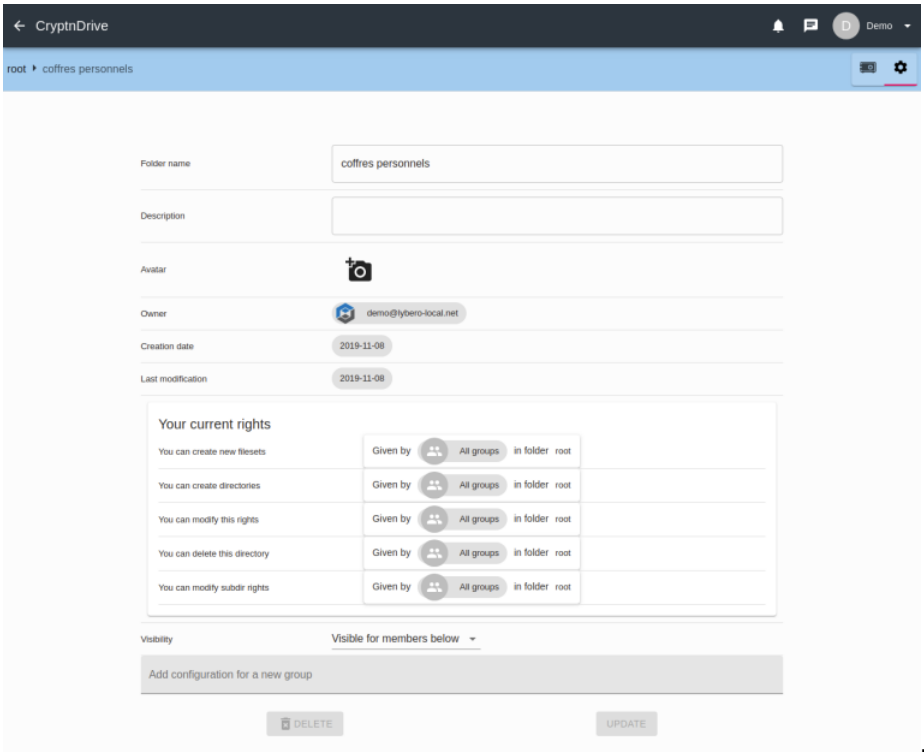
2.2.1 Modification des droits des répertoires de coffres

L'édition des droits des répertoires peut-être particulièrement épineuse, c'est pourquoi nous vous conseillons de ne pas donner la possibilité à tous les utilisateurs de modifier les droits des répertoires de coffres. Préférez déléguer cette tâche à un groupe d'utilisateurs expérimentés et conscient de leurs actions.

L'attribution des droits sur les répertoires se fait sur la base de la conjonction de l'appartenance à un groupe et du répertoire sur le quel les droits sont modifiés. Il n'est pas possible par exemple de modifier les droits d'un et un seul utilisateur.

Pour se faire, entrez dans un répertoire de coffres et allez dans ses paramètres ( ).

Vous voici alors devant la fenêtre de configuration de ce répertoire de coffres.



Afin de modifier les droits de ce répertoire, intéressons-nous aux deux derniers éléments des propriétés.

La visibilité vous permet de définir si ce répertoire est visible pour :

- Les groupes pour les quels vous aller appliquer une configuration
- Personne si celui-ci est vide et tout ceux qui sont en partage d'un coffre contenu dans ce répertoire.

L'ajout d'une configuration pour un nouveau groupe permet d'appliquer des règles pour des groupes en particulier.

Il y a au moins un groupe existant sans modification de votre part, le groupe 

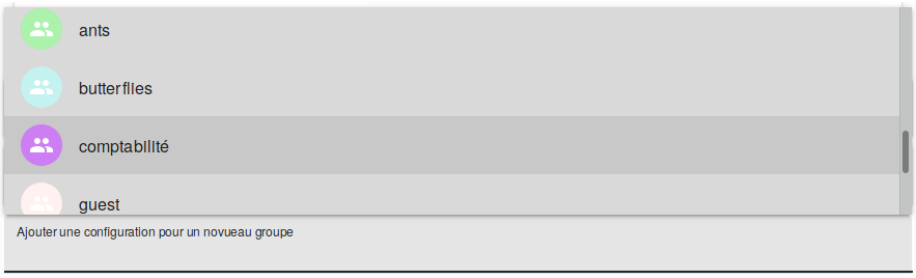
(tous les groupes) qui regroupe donc tous les groupes. Le fonctionnement des droits est celui-ci : vous jouissez du droit le plus haut. Si vous faites partie d'un groupe 

, que la configuration du groupe 

ne vous donne pas le droit de créer de coffre et que la config-

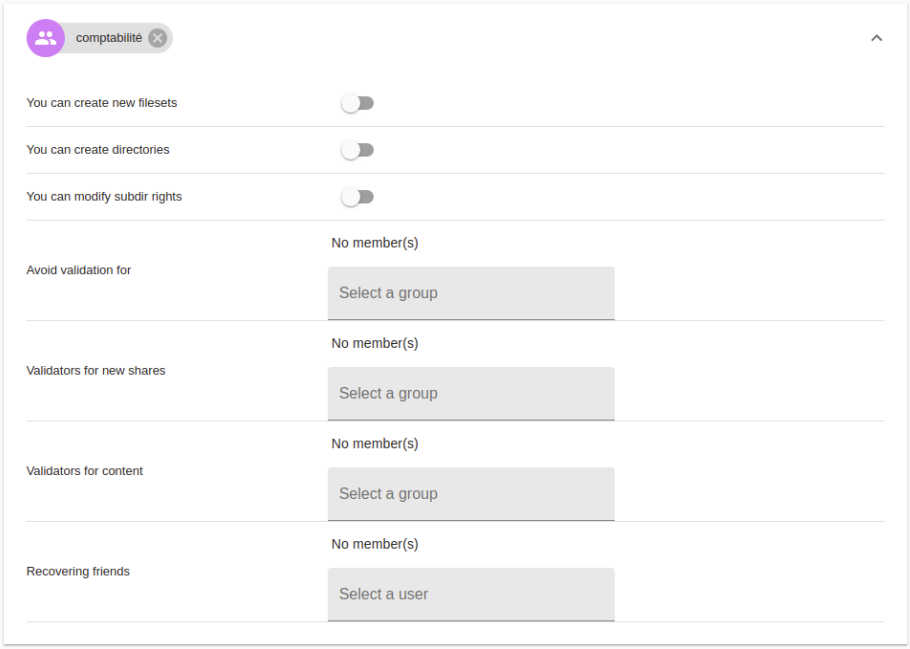
uration de ce groupe  vous donne cette possibilité, vous avez alors le droit de créer des coffres. C'est une notion importante à comprendre pour vous en sortir dans l'attribution des droits. Ceci vous permet d'appliquer des droits très restrictifs pour le groupe  et affiner pour chaque groupe ensuite.

L'attribution des droits est somme-toute assez simple, cliquez dans la zone "Ajouter une configuration pour un nouveau groupe" puis sélectionnez le groupe pour le quel vous souhaitez appliquer une configuration dans la liste des groupes disponibles.



vous verrez alors le groupe apparaître dans la liste des configurations.

Cliquez sur le bouton de déploiement de la section  et vous verrez apparaître la fenêtre de configuration du groupe.



Vous pourrez, dans l'ordre :

- Donner ou refuser le droit à ce groupe de de créer des coffres,
- donner ou refuser le droit à ce groupe de créer des répertoires de coffres,
- donner ou refuser le droit à ce groupe de modifier les droits des sous-répertoires.
- définir un ou des groupes exempts de validation de partage,
- définir le groupe responsable de la validation de partages,
- définir le groupe en charge de la validation de contenu,
- définir le groupe en charge du recouvrement.

Une fois votre configuration effectuée, n'avez plus qu'à cliquer sur le bouton "Mise à jour".

2.2.2 Les validations

Il y a donc, dans Crypt n Drive, deux systèmes de validation :

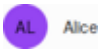
- La validation de contenu
  - Chaque fichier partagé par un membre d'un groupe soumis à la validation de fichiers devra être validé par un groupe de tiers décidé à l'avance, avant sa mise à disposition dans un coffre.
- La validation de partage
  - Chaque invité externe à l'application verra son identité validée, non plus par l'invitant, mais par un groupe de tiers décidé à l'avance.

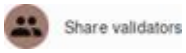
Pour assurer la bonne marche de ces systèmes nous vous conseillons de créer au moins deux groupes, différents du groupe à quorum vu précédemment. Un groupe pour la validation des fichiers et un groupe pour la validation des nouveaux partages.

2.2.2.1 Validation de contenus

Prenons le cas suivant: Il y a :

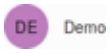
- Le groupe de validation de contenus 

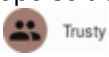
  - Dans ce groupe se trouve 

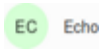
- Le groupe de validation de partages 

  - Dans ce groupe se trouve 

- Le groupe comptabilité 

  - Dans ce groupe se trouve 

- Le groupe Trusty 

  - Dans ce groupe se trouve 

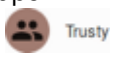
- Et enfin 

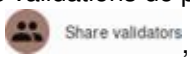
Avec le compte administrateur, nous créons un répertoire de coffres “test validation”. je vais ajouter une configuration dans ce répertoire pour le groupe 

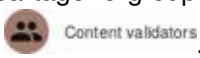
Rendons nous donc dans les propriétés du répertoire, puis dans le champs pour ajouter une nouvelle configuration et sélectionnons le groupe 

.

Donnons d’abord le droit de créer des coffres, puis celui de créer des sous-répertoires. Afin de ne pas risquer de faire voler en éclat la configuration, interdisons au groupe 

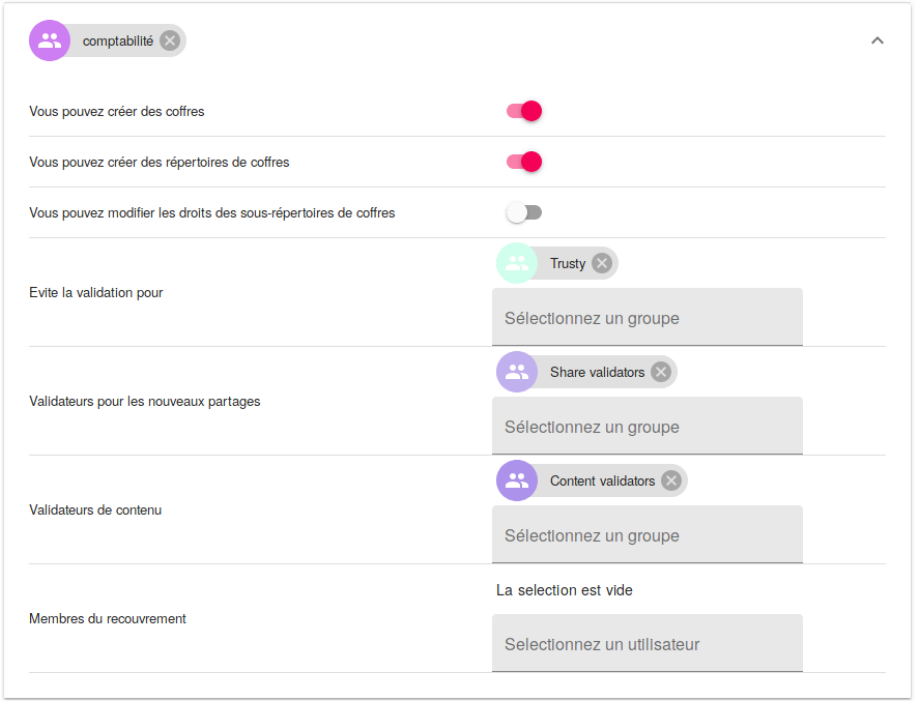
de modifier les droits des sous-répertoires. Ensuite, le groupe 

évitera les validations de partage. Nous placerons en validateurs de partage le groupe 

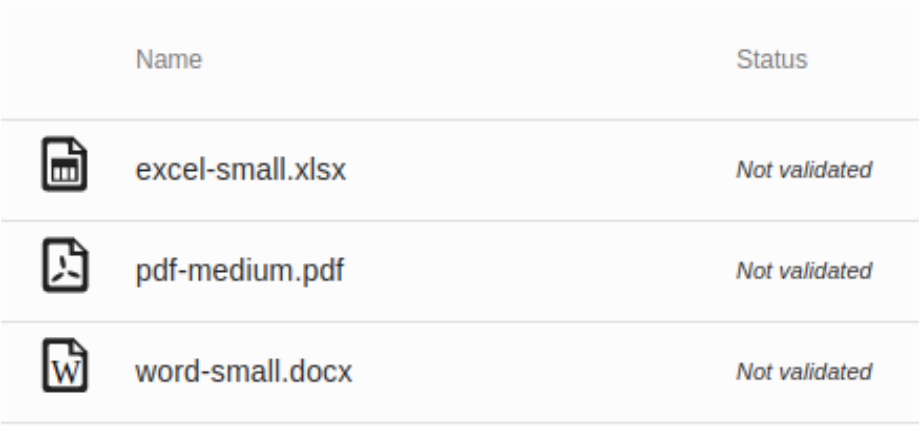
, puis en validateurs de contenus le groupe 

.

Ce qui nous donne cette configuration :



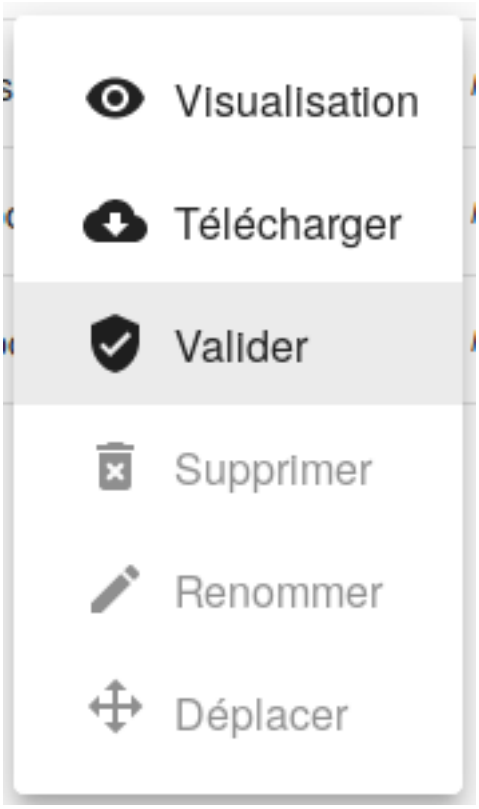
Nous mettons à jours les paramètres et nous connectons avec DE Demo et voyons l'apparition du nouveau répertoire test validations. Nous créons alors dans ce répertoire le coffre testV. Déposons maintenant quelques fichiers. Les fichiers sont dans un état "non validés"comme l'on peut le voir sur cet écran :



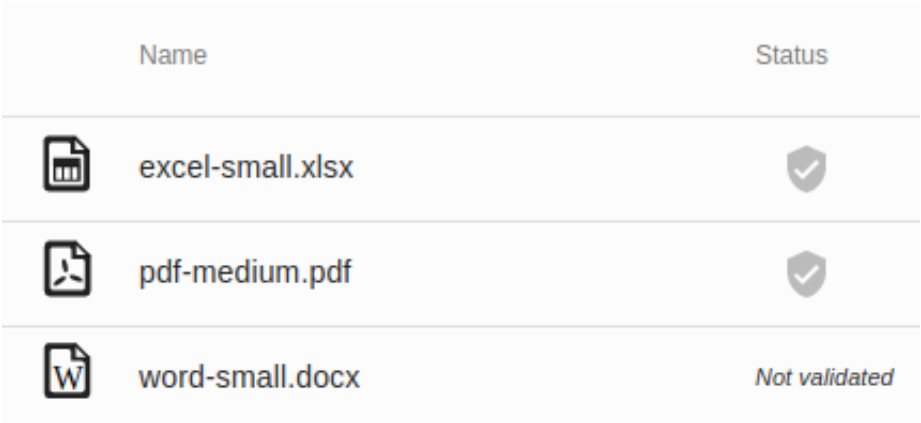
Ces fichiers ont besoin d'être validés par le groupe de validation de contenus à

savoir Content validators.

AL Alice se connecte donc (en temps que membre du groupe de validation de contenus), pénètre dans le coffre “testV” et s’aperçoit que 3 fichiers attendent une validation. un clic droit sur un fichier offre une nouvelle option à AL Alice, celle de valider le fichier :



Elle peut donc visualiser et/ou télécharger le fichier, s’assurer du contenu et valider ou non le fichier. Validons donc les deux premiers mais pas le dernier pour s’apercevoir que le statut des deux fichiers validés a changé pour le statu validé représenté par cette icône :

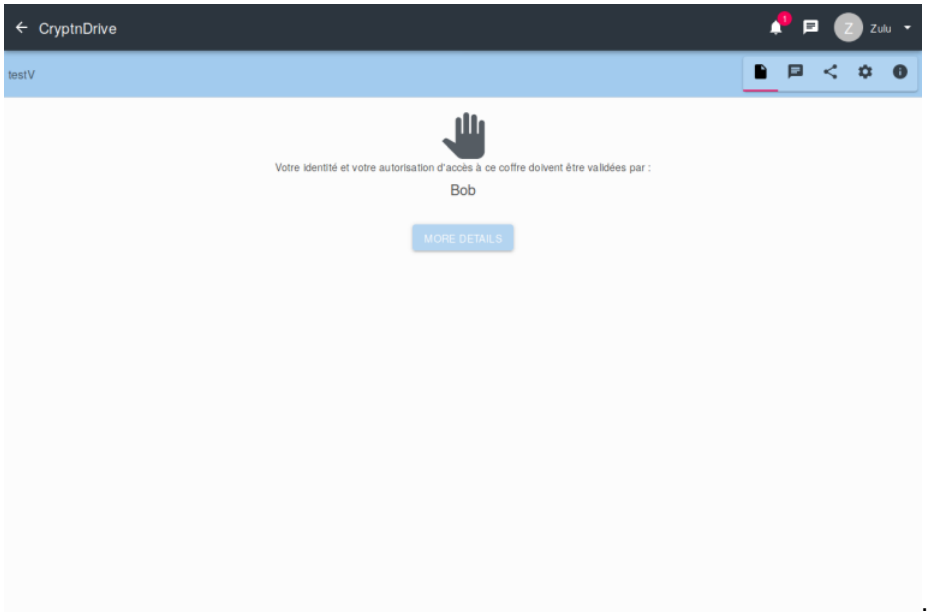


AL Alice peut maintenant demander à DE Demo de modifier ou supprimer son fichier non validé.

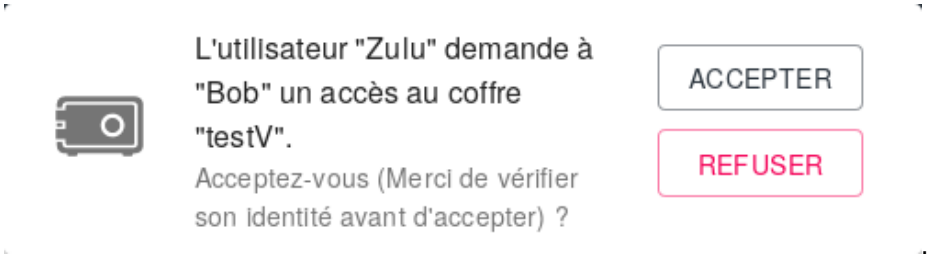
Demo souhaite maintenant partager ce coffre avec un tiers, essayons d'inviter CH Charlie, en utilisant l'onglet des partages. (notons au passage la présence de AL Alice et BO Bob dans la liste des partages en qualité de respectivement "validateur de contenu" et "validateur"). Ajoutons donc CH Charlie et connectons-nous avec lui.

CH Charlie voit bien le répertoire et nous pouvons rentrer dans le coffre. Voir et télécharger les fichiers. Rien de plus normal puisque CH Charlie fait partie du groupe Trusty qui évite la validation de partage. Si nous répétons l'opération avec un tiers hors de ce groupe, voyons ce qui se passe, invitons donc ZU Zulu.

Une fois connecté avec ZU Zulu en ayant cliqué sur le lien par mail, ZU Zulu arrive directement dans le coffre et voit cet écran :



C'est donc à BO Bob qui fait partie du groupe Share validators de valider le partage. Il se connecte, voit l'alerte dans la barre du haut



Maintenant, ZU Zulu voit bien le coffre, avec uniquement deux fichiers validés.

Une subtilité subsiste pour la configuration. Si vous ne spécifiez qu'un groupe qui "évite la validation" sans ajouter de groupe de validation de partage ni de validation de contenu, les seuls membres à qui les coffres de ce répertoire peuvent être partagés seront les utilisateurs de ce groupe. C'est une autre façon de permettre à l'administrateur de contrôler le partage.# Conclusion

2.3 conclusion

CryptnDrive de Lybero.net permet à la fois la sécurité des données et des transferts dans une organisation avec une facilité d'utilisation maximale et en

même temps une capacité pour l'organisation de maitriser totalement le système (mise à disposition des codes sources, gestion des serveurs utilisés, utilisation de groupe à quorum pour les recouvrements).

Si vous avez des suggestions de tous ordres sur le logiciel ou sur cette documentation, n'hésitez pas à nous en faire part à contact@lybero.net .