Coffre-fort numérique

Bertrand Wallrich, Frederic Beck

Coffre-fort numérique

Bertrand Wallrich
Laboratoire de Haute Sécurité
Inria Nancy Grand Est
615 rue du jardin botanique
54600 Villers-les-Nancy

Frédéric Beck
Laboratoire de Haute Sécurité
Inria Nancy Grand Est
615 rue du jardin botanique
54600 Villers-les-Nancy

Résumé

Les coffres forts numériques ont pour vocation de répondre à un problème auquel nous sommes de plus en plus souvent confrontés, à savoir travailler à plusieurs sur un même projet, un même code ou document, ou les mêmes données, et ce, de manière sécurisée sans pour autant nuire à la productivité. Ce problème est d'autant plus marqué lors de l'écriture ou la diffusion de documents sensibles, lors de collaboration avec des industriels, ou simplement lorsque l'on manipule des données pouvant porter atteinte à la vie privée.
Nous présentons ici une approche similaire aux coffres forts physiques, étendue au monde numérique. À l'image d'un coffre fort physique, un utilisateur doit "rentrer dans le coffre" afin de déverrouiller l'accès aux données pour lui-même et les autres utilisateurs du coffre. Ce coffre doit donc être auto-suffisant et contenir toutes les données ainsi que tout l'environnement de travail nécessaire pour manipuler ces données.

L'idée de base est de renforcer la sécurité des données en se basant sur la virtualisation et le chiffrement. Le premier utilisateur qui entre dans le coffre l'ouvre et rend les données accessibles à tous les utilisateurs du coffre; le dernier utilisateur qui quitte le coffre provoque sa fermeture et la fermeture de l'accès aux données. Quel que soit l'endroit où sont stockées les données, cela permet d'éviter tout accès indésirable ou fuite qui n'émanerait pas d'une action volontaire d'un utilisateur.

Mots-clefs

Sécurité, Confidentialité, Chiffrement, Virtualisation, Travail collaboratif

1 Introduction

Dans le contexte actuel, les usages du numériques sont de plus en plus répandus. Ce constat introduit de nouvelles problématiques et de nouvelles méthodologies de travail lorsqu'un groupe de personnes est amené à travailler en commun sur un même projet, tout en pouvant être dispersés géographiquement dans le monde, sur plusieurs fuseaux horaires, dans des entreprises ou organisations différentes.

Des solutions existent pour permettre à ces personnes de collaborer : gestionnaires de versions, forges logicielles, réseaux privés virtuels… Mais lorsque le sujet traité est sensible, implique l'utilisation de données hautement confidentielles, notamment si elles sont relatives à la vie privée des participants, ou simplement la rédaction et diffusion d'un document confidentiel, elles restent insuffisantes et n'adressent pas l'intégralité des contraintes inhérentes au projet.

Face à ce constat est née l'idée d'un coffre-fort numériques, qui ne serait pas limité à une solution de stockage sécurisé, mais inclurait en sus toutes les briques logicielles et outils nécessaires à la réalisation du projet. En faisant l'analogie avec un coffre fort physique, les utilisateurs devraient « ouvrir » le coffre

et y pénétrer afin d'y trouver son bureau et l'intégralité des outils nécessaires afin d'accomplir sa tâche. Le coffre reste ouvert tant que des utilisateurs y sont présents, la sortie du dernier utilisateur provoquant la fermeture automatique du coffre et la sécurisation des données contenues.

Dans cet article, nous positionnerons notre solution par rapport à l'existant, puis détaillerons notre solution ainsi que les choix techniques. Nous discuterons ensuite des considérations de sécurité avant de présenter les travaux futurs et de conclure.

2 Problématique et solutions existantes

2.1 Pourquoi un coffre-fort numérique ?

Le terme coffre-fort numérique est sans doute mal choisi, car il évoque le stockage, l'archivage, et non le travail sur des documents. Néanmoins, à l'instar de documents papier revêtus d'un besoins de confidentialité, il est nécessaire de pouvoir travailler sur des données confidentielles, les manipuler, avec un minimum de risque de divulgation.

Le besoin auquel nous avons tenté de répondre peut tenir en une phrase :

« Comment une équipe délocalisée peut travailler de manière collaborative sur un projet sensible ? »

C'est le besoin exprimé par exemple par des équipes projets de recherche Inria, lorsqu'ils ont de la confidentialité. Cela nous impose déjà les premières contraintes :

- Une équipe de personnes, donc des comptes et des droits à gérer.
- Délocalisé, donc via Internet.
- Générique : Il ne s'agit pas uniquement de gestion de document, ou de production de code. Mais essayer d'être le plus large possible.

2.2 Solution existantes

Avant tout développement d'une solution, il faut – paraît-il - s'assurer qu'elle n'en existe pas déjà.

Nous passerons les offres de coffres forts numériques grand publique proposé par divers établissements (banque, assurances, sociétés dédiées, …) dont l'objectif est celui de l'archivage de documents numérisés (fiche de paye, relevé bancaire, …). Ces offres ne présentent pas leur système de sécurité mis en place pour la confidentialité. Il est donc difficile d'évaluer leur robustesse. De plus, le travail sur ces données n'est pas satisfaisant, car il nécessite d'extraire la donnée du coffre, la modifier, puis la redéposer.

Les offres de «stockage dans le Cloud » sont déjà plus intéressantes, surtout celles qui précisent les mécanismes utilisés pour la confidentialité : Elles vantent le mérite du chiffrement des données sur leurs serveurs[1], l'évitement du Patriot Act[2] et la conformité CNIL[3] dans une localisation européenne[4], voir française, et plein d'autre éléments sur les noms des fichiers, les mots de passes, etc. Cependant, tant que le chiffrement ne se fera pas directement sur le poste utilisateur AVANT utilisation du service, avec une clef qui ne sort pas de ce poste (ou de la tête de l'utilisateur), l'hébergeur aura un accès, et devra donc avoir votre confiance la plus absolue.

Enfin, l'ensemble des logiciels présentent des fonctionnalités de sécurité qu'il convient d'étudier. En effet, une forge logiciel par exemple permet l'étanchéité des projets qu'elle héberge, de l'authentification, etc. cela ne peut-il pas suffire ?

1. https://www.google.com/intl/fr_fr/drive/
2. https://fr.wikipedia.org/wiki/USA_PATRIOT_Act
3. http://www.cnil.fr/
4. https://aws.amazon.com/fr/s3/

Enfin, quelques hébergeurs proposent des solutions plus clef en main[5] ou pas[6].

3 Notre approche

3.1 Choix et stratégie

Nous avons fixé quelques « vérités » de départ, permettant selon notre perception, de couvrir nos besoins. Ces choix arbitraires dictent la solution technique :

1. Le « coffre-fort » doit être accessible de tout Internet.
2. Le « coffre-fort » doit permettre une grande variété d'applications.
3. Une machine physique héberge un « coffre-fort » et un seul.
4. Tous les utilisateurs du « coffre-fort » ont tout accès aux données.
5. Lorsqu'il n'est pas utilisé, le « coffre-fort » doit être fermé.

3.2 Contraintes

Plusieurs contraintes sur le « coffre fort » apparaissent :

1. Un « coffre-fort » représente un projet sensible et un seul. Il ne doit être accédé que par une petite communauté d'utilisateurs qui ont à en connaître.
2. L'administration du « coffre-fort » doit être confié aux utilisateurs, les administrateurs systèmes ne devant plus avoir de droits sur les coffres.

3.3 Par rapport à l'existant

L'apport de cette solution se veut générique : Un coffre n'est pas lié ou dédié à une application, et les droits sur l'accès aux données n'est pas dépendante des possibilités de cette application. On déporte ainsi la problématique de la sécurité sur un niveau système et non plus sur l'applicatif.

Le second apport de la solution provient de ses deux états différents. Lorsque personne n'utilise le coffre, il est fermé, et donc dans un état de protection des données plus robuste que lorsqu'il est ouvert (les machines virtuelles sont suspendues, et les partitions de données chiffrées sont démontées).

3.4 Limites

Le « coffre-fort » a des limitations en terme de capacité et de performances. Certaines applications nécessitant du hardware spécifique (carte graphique), de la puissance de calcul élevé (clusters) ne pourront pas être intégrées dans un coffre.

4 Comment ça marche ?

4.1 Architecture logique

4.1.1 Vue générale

L'architecture générale d'un coffre fort numérique est présentée dans la Figure 1. On y retrouve les trois

5. https://casd.eu/
6. https://www.ovh.com/fr/cloud/

briques principales :

- les clients : potentiellement disséminés à travers le monde, un ordinateur avec un client VPN
- le stockage : une entité externe et indépendante au coffre, qui peut être hébergée n'importe où, et qui est capable d'exposer des volumes de stockage chiffrés via iSCSI
- le coffre en lui-même : un ou plusieurs hyperviseurs et services associés (serveur LDAP, passerelle VPN, forge logicielle, machines virtuelles de traitement...)

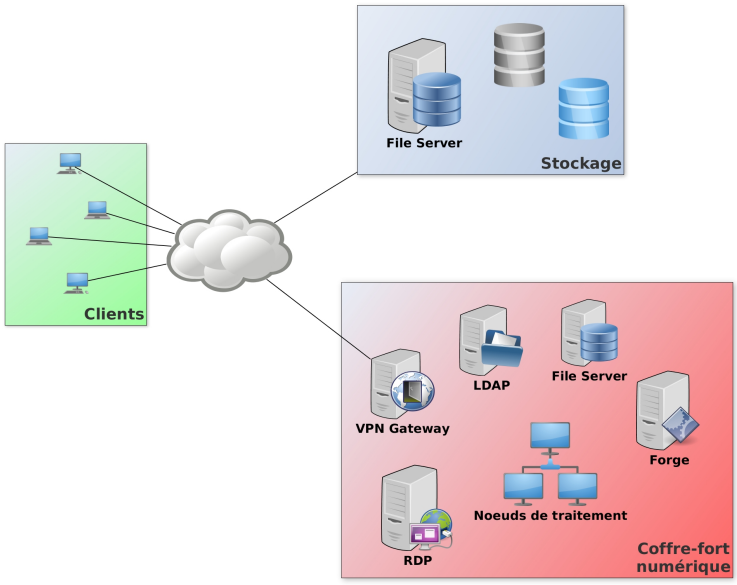

Figure 1: Architecture logique

L'accès au coffre se fait par le biais d'une connexion VPN, dont seule la passerelle est accessible et visible depuis Internet.

Dans le reste de l'article, nous considérons qu'un coffre est constitué d'un seul hyperviseur.

4.1.2 Services hébergés

Un coffre-fort numérique est composé d'un certain nombre de services mis à disposition des utilisateurs sous la forme de machines virtuelles. A minima, sont disponibles :

- une passerelle VPN permettant la connexion à distance
- un serveur LDAP afin de stocker les informations utilisateurs
- une machine de supervision dont le rôle est de centraliser les logs des différentes machines et services, qui peut être externalisée, appelée « monitor »
- un serveur d'accès au bureau à distance de type RDP
- une forge logicielle

Le coffre peut être personnalisé et inclure d'autres services et machines virtuelles (Wiki, base de données…). L'accès aux données via iSCSI et un serveur de fichiers de type NFS est assuré par l'hyperviseur lui-même de manière automatique et transparente pour l'utilisateur.

4.1.3 Etats

Un coffre-fort numérique peut être dans 3 états différents : fermé, ouvert, ou verrouillé.

Le coffre est dit « fermé » lorsque aucun utilisateur n'est connecté au VPN (la déconnexion du dernier utilisateur provoque la fermeture automatique du coffre), seuls les services nécessaires à son ouverture

sont actifs : une passerelle VPN, et un serveur LDAP. Les autres machines virtuelles sont toutes arrêtées, à l'exception de la machine de supervision. Dans cet état, les données contenues dans le coffre ne sont pas accessibles, même aux administrateurs de la solution, car l'hyperviseur ne voit que des blocs chiffrés exportés par le stockage via iSCSI.

Lorsque le premier utilisateur se connecte au coffre en initiant une connexion VPN, le coffre passe en mode « ouvert ». Dans cet état, le volume distant est monté, les données sont déchiffrées par l'hyperviseur avant d'être exportées vers les machines virtuelles via NFS. Toutes les machines virtuelles nécessaires au projet (forge logicielle, accès à distance via RDP, clusters de traitement/calcul…) sont démarrées et accèdent aux données via un montage NFS.

Lorsqu'un risque d'attaque ou d'intrusion est avéré (poste client compromis, identifiants volés...), un coffre peut être « verrouillé » par un membre du groupe de super utilisateurs ou administrateurs du coffre. Si le coffre était ouvert, il est fermé et les utilisateurs sont déconnectés. Une fois dans l'état verrouillé, le coffre ne peut plus être ouvert, et les données sont chiffrées et inaccessibles afin de garantir leur intégrité. Seuls les membres du groupe de super utilisateurs peuvent se connecter au coffre et accéder aux machines dites de service, telle que la machine monitor, afin d'analyser et résoudre le problème. Lorsque c'est le cas, un administrateur peut déverrouiller le coffre qui retourne alors dans l'état fermé et reprend un fonctionnement normal.

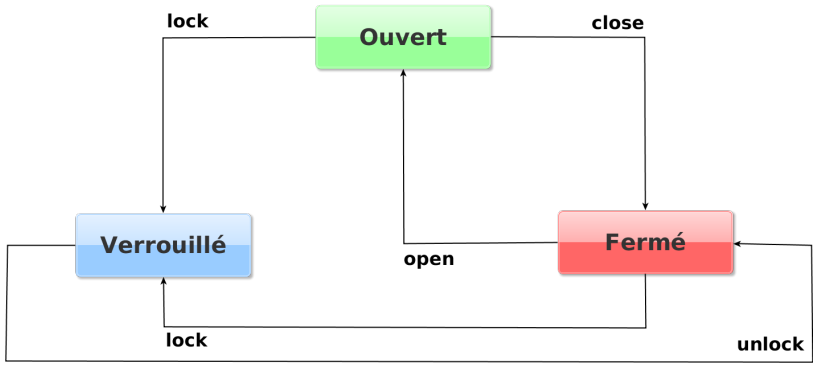

Figure 2: États d'un coffre

Les transitions entre ces différents états sont présentés dans la Figure 2.

4.1.4 Modes de fonctionnement

Un coffre peut fonctionner de 2 manières distinctes selon les besoins des projets. A tout moment, le coffre peut basculer d'un mode de fonctionnement à l'autre. Ces 2 modes sont directement liés aux choix technologiques présentés plus tard dans l'article.

Dans le mode dit « rapide », les machines virtuelles sont mises en pause. Elles ne sont pas a proprement dit stoppées, mais gelées, leur état étant stocké en RAM. La fermeture et réouverture du coffre est donc très rapide, mais l'état des machines virtuelles est perdu en cas de redémarrage de l'hyperviseur, et la sécurité de cette information ne peut être garantie à 100 %.

Dans le mode appelé « sûr », les machines virtuelles sont suspendues sur disque dans le volume crypté. Cela garantie la confidentialité et l'intégrité de l'état des machines virtuelles, ainsi que la reprise après redémarrage de l'hyperviseur, mais implique un délai plus long pour la fermeture et l'ouverture du coffre.

4.1.5 Tâches et traitements automatiques

Pour travailler sur les données contenues dans le coffre, il doit être dans un état ouvert afin que celles-ci soient accessibles. Cependant, cela peut rapidement devenir contraignant, voire impossible dans le cas de

traitement ou de tâches longues ou automatiques, ou si les volumes de données à traiter sont importants. Il est inconcevable de demander aux utilisateurs de garder leur machine cliente allumée, avec le VPN actif, d'autant plus que cela restreint énormément leur liberté de mouvement.

Pour permettre des traitements longs, sans rester connecté, un utilisateur peut programmer l'exécution d'une tâche. Cela implique que, même en cas de déconnexion de tous les utilisateurs, la fermeture du coffre est retardée jusqu'à la fin de la tâche programmée, ou de la durée associée choisie par l'utilisateur. A tout moment, l'utilisateur ou un administrateur peut annuler et supprimer cette tâche.

4.2 Choix techniques et implémentation

4.2.1 Accès au coffre

L'accès au coffre se fait via une passerelle OpenVPN reliée à un serveur LDAP interne au coffre. L'authentification des clients est détaillée dans la section 4.3.1. Ce serveur OpenVPN est configuré pour élever au maximum le niveau de sécurité, notamment en interdisant les communications directes entre les clients. Actuellement, la version 2.3.4 est déployée dans les coffres.

Une fois authentifié, un utilisateur peut, soit se connecter sur les machines virtuelles directement en SSH, soit avoir accès à un bureau distant via une connexion RDP.

Les restrictions d'accès et les limitations se font sur la base de groupes et ACLs LDAP, ainsi que de règles de pare-feux (voir section 5.1 pour plus de détails).

4.2.2 Virtualisation

Un coffre repose sur l'utilisation de la virtualisation et plus précisément un (ou plusieurs) hyperviseur(s) Xen, et des machines virtuelles en mode paravirtualisées.

L'utilisation d'un hyperviseur Xen permet l'accès à une machine virtuelle privilégiée, appelée « domaine 0 », qui permet de gérer les machines virtuelles et plus particulièrement leur accès aux fonctions réseau et leurs disques virtuels.

D'autre part, le cycle de vie d'une machine virtuelle Xen est parfaitement adaptée à un coffre et aux modes de fonctionnement (sûr ou rapide) souhaités.

Actuellement, la version 4.4 est utilisée.

4.2.3 Chiffrement et accès aux données

Les données du coffre sont stockées dans un volume chiffré par blocs de type AES256, sans utilisation de clé maître.

Ce chiffrement est réalisé via l'implémentation de référence de LUKS pour Linux, à savoir cryptsetup. Chaque utilisateur enregistré dans le serveur LDAP du coffre a une entrée dans l'entête LUKS du volume chiffré (ou slot), correspondant à l'heure actuelle à un hash de son mot de passe.

Ce volume de données peut être stocké n'importe où sur Internet, du moment que l'hyperviseur du coffre peut y accéder via iSCSI. En état fermé, l'hyperviseur ne voit que des blocs chiffrés. Une fois le coffre ouvert, le volume est déchiffré, monté, et mis à disposition des machines virtuelles via un serveur NFS.

Les droits dans ce volume sont gérés par les permissions Unix standards.

4.2.4 Communications et synchronisation internes

Afin d'assurer la communication entre les différentes briques logicielles d'un coffre (OpenVPN, hyperviseur Xen, cryptsetup...) et leur synchronisation, nous avons décidé d'utiliser RabbitMQ[7], une implémentation du protocole AMQP (pour Advanced Message Queuing Protocol), qui apporte une solution de messagerie entre applications, orientée message, avec utilisation de files d'attente. Une file est enregistrée auprès d'un serveur et un ou plusieurs consommateurs y sont associés.

7. https://www.rabbitmq.com/

Un serveur est déployé au niveau de l'hyperviseur Xen et plusieurs files sont répertoriées :

- « vpn » qui permet à OpenVPN de dialoguer et donner des ordres ou informations à l'hyperviseur, notamment lors de la procédure d'ouverture/fermeture d'un coffre ; les consommateurs sont donc déployés sur chaque hyperviseur du coffre
- « gateway » qui permet d'envoyer des ordres à la passerelle VPN, notamment en cas de verrouillage du coffre ; un seul consommateur est donc déployé au niveau de la passerelle VPN

Ce système a été dérivé pour permettre aux utilisateurs de programmer les tâches ou changer leur mot de passe, ou aux super utilisateurs d'administrer le coffre (ajout d'utilisateurs, verrouillage…) au travers de messages au format JSON, par exemple pour l'ajout d'une tâche :

```
{
    'command : 'task_add',
    'task_name' : nom/ID de la tâche,
    'task_user' : login,
    'task_expire' : durée
}
```

D'autre part, les consommateurs de ces différentes files sont chargés de maintenir des fichiers d'états décrivant l'état dans lequel se trouve le coffre, quelles sont les tâches actuellement programmées…

4.3 Fonctionnement détaillé

4.3.1 Authentification des clients

L'ouverture d'un coffre est conditionnée par l'authentification de l'utilisateur. Cette procédure est le résultat de la concaténation de plusieurs facteurs, et de plusieurs opérations séquentielles, à différents niveaux dans l'architecture globale d'un coffre : OpenVPN, LDAP et LUKS/cryptsetup.

Tout d'abord, le client doit s'authentifier au VPN en utilisant le profil fourni par un des administrateurs. Ce profil se base sur un certificat pour le coffre, un certificat utilisateur associé à la machine (et la clé privée correspondante) et un nom d'utilisateur et mot de passe, stockés dans un annuaire LDAP.

Une fois authentifié via le VPN et le compte LDAP, OpenVPN délègue une fonction d'authentification à cryptsetup : si l'utilisateur peut décrypter le volume de données, l'accès est validé, sinon l'authentification échoue.

Une fois la connexion VPN établie, l'utilisateur pourra accéder aux différents services et machines du coffre en utilisant les identifiants contenus dans l'annuaire LDAP et la clé privée associée à la clé publique enregistrée.

4.3.2 Ouverture

Au départ, le coffre est en mode fermé comme le montre la Figure 3.

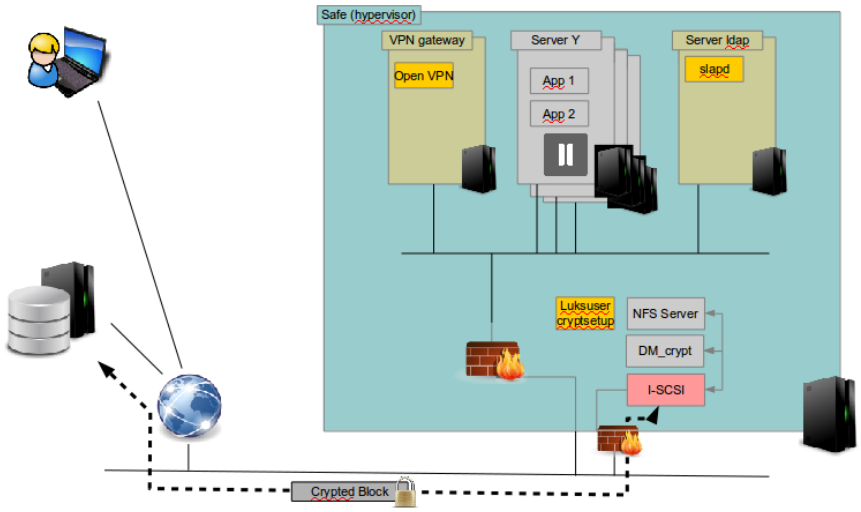

Figure 3: Coffre fermé

La connexion du premier utilisateur déclenche la procédure d'ouverture du coffre :

1. initiation d'une connexion avec la passerelle OpenVPN
2. authentification LDAP
3. envoi d'un hash du mot de passe à l'hyperviseur via RabbitMQ
4. déchiffrement et montage du volume de données
5. établissement de la connexion VPN
6. démarrage du serveur NFS dans l'hyperviseur et export du volume chiffré
7. réveil des machines virtuelles qui montent le volume NFS (si ce n'est pas déjà fait)
8. le coffre est ouvert

Une fois dans l'état ouvert, l'utilisateur peut accéder aux différentes machines et applications, ainsi qu'aux données, comme le montre la Firgure 4. Lorsque d'autres utilisateurs se connectent, la procédure précédente s'arrête à l'étape 5.

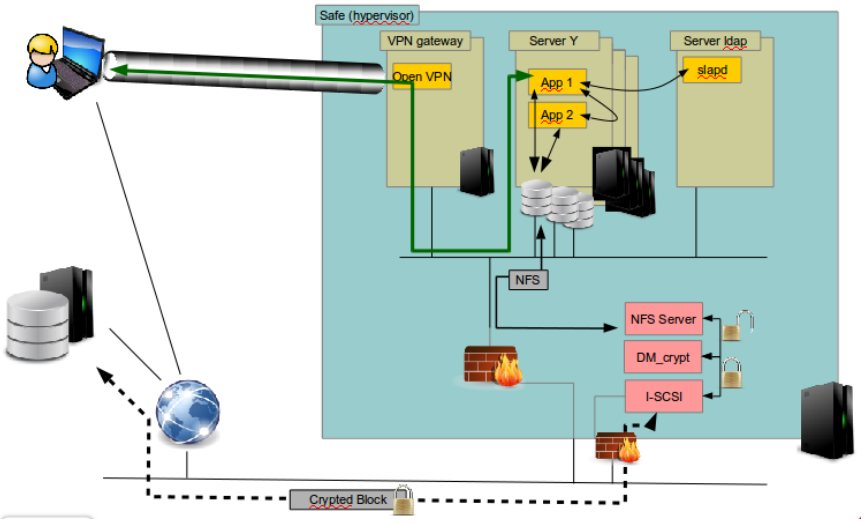

Figure 4: Coffre ouvert

4.3.3 Fermeture

Lors de la déconnexion du dernier utilisateur, la procédure de fermeture du coffre se déclenche :

1. les machines virtuelles sont mises en pause ou suspendues, à l'exception des machines de service (OpenVPN, LDAP et monitor)
2. le serveur NFS est arrêté dans l'hyperviseur
3. le volume distant est démonté

Le coffre revient dans l'état fermé présenté dans la Figure 3.

5 Considérations de sécurité

Les aspect sécurité de notre solution reposent sur une hypothèse : l'hyperviseur est considéré comme sûr.

En effet, l'hyperviseur est le centre névralgique de la solution, et sa compromission peut permettre de contourner les autres mesures mises en place : si un attaquant prend le contrôle de l'hyperviseur, il lui suffit d'attendre une ouverture pour avoir accès aux données, voire intercepter les clés de chiffrement. Dans la sécurisation de la solution, une attention toute particulière est donc portée à l'hyperviseur (accès par un réseau éthernet dédié, voire accès physique uniquement, un minimum de services, kernel hardening…).

5.1 A tout moment

Les données qui transitent entre un coffre et le stockage sont toujours des blocs chiffrés. Aucune clé ne reste en mémoire, sur une machine virtuelle ou l'hyperviseur. Les clés de déchiffrement sont générées à la volée par la passerelle VPN, mais jamais stockées. Cela permet d'externaliser sans risques le stockage.

Un parefeu est positionné au niveau de l'hyperviseur et le pont réseau par lequel transitent tous les paquets dans un coffre. Ce parefeu contient un ensemble de règles de base, dont le but est de limiter les échanges entre les machines virtuelles au strict minimum.

Un poste client peut provoquer un ouverture illicite du coffre, par exemple après enregistrement et rejeu d'une connexion via un keylogger, d'où la procédure de verrouillage du coffre.

5.2 Ouvert

Une machine virtuelle ou poste client compromis ne met pas en danger les clés de chiffrement, mais une fuite de données est possible.

Un utilisateur, par une action volontaire et délibérée peut extraire des données.

5.3 Fermé

Aucune clé de chiffrement n'est stockée, que ce soit en mémoire, dans le noyau ou sur disque .

Seule la passerelle VPN est accessible et attaquable depuis l'Internet.

Un administrateur ayant accès à l'hyperviseur ne peut ni monter le volume de stockage, ni accéder aux données.

6 Travaux futurs

6.1 Côté client

Le développement d'un client dédié est fortement envisagé. Plusieurs possibilités existent, et peuvent être complémentaires : client lourd logiciel ou appliance virtuelle, périphérique dédidé type Raspberry…

Un tel client pourrait, si besoin est, de mettre en place des VPNs de type site-to-site, afin d'intégrer au coffre du matériel spécifique (type SCADA ou GPU par exemple), afin de contourner une des limitations identifiées.

Enfin, la mise en place de mécanismes d'analyse de trafic (surveillance des fuites de données) ou d'activité (analyse du comportement des utilisateurs) permettrait de diminuer les risques de fuite de données ou de détecter une compromission d'un poste client.

6.2 Authentification

Les mécanismes d'authentification peuvent être renforcés, par l'utilisation de mots de passes à usage unique (OTP), et ainsi introduire dans la boucle un autre périphérique, tel qu'un téléphone portable sur lequel un code serait envoyé par SMS. En raison des limitations de la version actuelle d'OpenVPN, cela passe par le développement d'un client dédié (ou de la sortie de la version 2.5).

Différentes solutions sont actuellement à l'étude pour ne plus utiliser uniquement le hash du mot de passe en tant que clé de chiffrement LUKS.

La modification des schémas LDAP, voire de crypsetup sont également envisagés, pour permettre d'une part d'augmenter le nombre d'utilisateurs d'un coffre, et de lier un utilisateur à son numéro d'entrée dans l'entête cryptsetup, qui deviendrait un facteur d'authentification.

6.3 Côté hyperviseur

Des modifications et validations sont prévues pour permettre l'utilisation de plusieurs hyperviseurs dans un coffre, ainsi que plusieurs volumes de stockage, potentiellement chez plusieurs fournisseurs, et de limiter certains à de la lecture seule. Cela permettra en sus de mettre en place de nouvelles procédures de backup et de reprise sur crash (PRA).

Une solution pour renforcer la sécurité des clés de chiffrement serait l'utilisation de modules matériels de sécurité (HSM) pour stocker les clés en dehors du noyau. Des solutions à base de volumes chiffrés supplémentaires pour le stockage de ces clés sont également à l'étude.

Enfin, une exfiltration des logs et leur analyse est envisagée, afin de détecter au plus tôt les éventuels problèmes de fonctionnement ou intrusions.

7 Conclusion

Au delà du simple stockage de données en ligne dans le cloud, ou de l'hébergement de conteneurs ou de machines virtuelles, le coffre fort numérique permet un travail collaboratif sécurisé sur des données sensibles tout en garantissant leur confidentialité et leur intégrité.

Même si des pistes existent pour améliorer la solution, celle-ci permet déjà de répondre à un certain nombre de besoins, allant de la rédaction ou diffusion de documents, à l'exploitation de données sensibles ou le développement d'applications.