oxibox

Documentation technique

Descriptif technique de la solution
Oxibox *Plug-and-Protect*

Version du 26.04.2024

Table des matières

I. Introduction

L'objectif de ce document est de définir les notions fondamentales et de décrire les aspects techniques et fonctionnels de la solution Oxibox « Plug-and-Protect ».

II. Définitions

1. Sauvegarde pérenne

Sauvegarde qui permet la conservation des données sur le long terme : semaines, mois, années selon les besoins.

2. Cyberrésilience

Capacité à assurer la continuité de l'activité et de la protection des données, même en cas de cyberattaque ou de catastrophe naturelle.

3. PRA

Un Plan de Reprise d'Activité (PRA) est un ensemble de procédures (techniques, organisationnelles, sécurité) qui permettent à une entreprise de prévoir par anticipation, les mécanismes pour reconstruire et remettre en route un système d'information en cas de sinistre important ou d'incident critique. En cas de sinistre, le PRA permet de reconstruire les serveurs en leur affectant les données répliquées et ainsi de redémarrer les applications sous quelques minutes ou quelques heures, suivant les solutions retenues. Il existe plusieurs niveaux de capacité de reprise, et le choix doit dépendre des besoins exprimés par l'entreprise.

4. Dépôts de sauvegarde

Les dépôts de sauvegarde rassemblent les données sauvegardées et sont stockés sur la cible de sauvegarde (appliance ou cloud). Il peut y avoir plusieurs dépôts par compte en fonction des déploiements. Ceux-ci sont séparés les uns des autres et les données de l'un ne peuvent pas être accédées via un autre dépôt.

5. Snapshots

Les snapshots sont stockés dans les dépôts de sauvegarde. Ils correspondent à une version de la sauvegarde. Quand l'agent a terminé une sauvegarde, un snapshot faisant référence à l'état de toutes les données de ce qui a été sauvegardé à cet instant T est créé dans le dépôt de sauvegarde. Les snapshots permettent de revenir à des versions passées de vos données.

6. Solution *Secure by design*

Un produit (comme Oxibox Plug-and-Protect) est dit « *secure by design* » si le risque et la sécurité sont intégrés lors de sa conception et tout au long de son cycle de vie. Son architecture est pensée pour être suffisamment robuste et garantir la sécurité et la confidentialité des données manipulées.

7. Sécurisation par défaut de la solution

En plus d'être *secure by design*, Oxibox Plug-and-Protect a été pensée pour être « *secure by default* ». Cela signifie que les paramètres de configuration par défaut sont les paramètres les plus sécurisés possibles. Ainsi, il n'est pas possible de créer par inadvertance une brèche de sécurité lors de son installation ou de son paramétrage.

8. Solution souveraine

Une solution est dite souveraine lorsque l'ensemble des traitements effectués (conception, développement, support client, vente) sont réalisés dans les limites du territoire national, par une entité de droit français et en application des lois et normes françaises.

9. Appliance

Équipement informatique dédié à la sauvegarde locale. Chez Oxibox, une appliance peut aussi externaliser vers le cloud public Oxibox ou vers une autre appliance Oxibox afin de respecter les recommandations de l'ANSSI (modèle 3-2-1-1).

Oxibox dispose de plusieurs appliances :

- Oxibox Mini

Un modèle pratique et esthétique pouvant être installé dans tous les environnements. Généralement adapté pour les petites entités dont le besoin en stockage n'est pas très élevé (de 1 à 4 To).

- Oxibox Compact

Un peu plus imposante que la Mini, l'Oxibox Compact permet d'augmenter considérablement la capacité de stockage (jusqu'à 66 To) et ce de manière évolutive en fonction du besoin. C'est un juste milieu entre une appliance de bureau compacte et un serveur de stockage dédié comme l'Oxibox Rack.

- Oxibox Fireproof

Oxibox Fireproof permet de répondre à des exigences opérationnelles particulières. En effet, ses propriétés ignifuge (30 minutes jusqu'à 850°C) et étanche (72h jusqu'à 3 mètres de profondeur) et son kit antivol permettent de protéger vos données des risques physiques : industriels, naturels, vol.
Les capacités de stockage sont extensibles jusqu'à 132 To.

- Oxibox Rack

L'Oxibox Rack est un serveur de stockage qui correspond parfaitement aux besoins de stockage de volumes importants (plusieurs Po) et peut s'intégrer dans une infrastructure existante. Les capacités du serveur sont adaptables à la commande ou lors du cycle de vie : stockage, carte(s) réseau(x) 10 Gbits/s, autochargeurs LTO...

III. Notions techniques

1. Processus de déduplication

La déduplication est un moyen efficace d'optimiser l'espace de stockage et les flux réseau en ignorant les données redondantes. La déduplication implémentée dans la solution Plug-and-Protect ne va donc ni transférer, ni stocker plusieurs fois les mêmes données grâce à une analyse réalisée directement à la source par l'agent de sauvegarde.

En ce qui concerne le mécanisme de déduplication, Oxibox va fragmenter chaque fichier analysé en blocs de taille égale. Une empreinte unique SHA-256 est générée pour chaque bloc, toutes les empreintes déjà stockées dans le dépôt sont référencées dans des fichiers d'indexation. Grâce à ce mécanisme, l'agent peut déterminer facilement si un bloc a déjà été stocké dans le dépôt de sauvegarde. Si tel est le cas, le bloc n'est pas pris en compte et l'agent de sauvegarde peut passer aux blocs suivants. Si la signature n'existe pas dans l'index, cela veut dire que les données contenues dans le bloc n'ont jamais été sauvegardées auparavant. Les données de ce bloc seront donc envoyées vers la cible de sauvegarde et stockées dans le dépôt de sauvegarde.

2. Sauvegarde dédupliquée

Oxibox utilise le principe de la sauvegarde dédupliquée. L'indexation des blocs de données permet de retrouver toutes les données qui composent un snapshot ou tout simplement de savoir si un bloc existe déjà dans le dépôt de sauvegarde.

L'agent de sauvegarde va commencer par analyser si une sauvegarde précédente existe et, si c'est le cas, va se baser sur celle-ci pour déterminer si un fichier est nouveau, a été supprimé ou si, selon plusieurs critères comme la date de dernière modification, il a été modifié.

Lorsqu'un fichier est nouveau ou a été modifié, l'agent va appliquer le processus de déduplication pour le sauvegarder.

L'accumulation de ces méthodes a plusieurs avantages :

- **Gain de temps**

Simplement en listant des métadonnées de fichiers et en se basant sur les références de la sauvegarde précédente, on peut déterminer si un fichier a besoin d'être analysé ou non. L'agent n'a donc même pas besoin de lire les données d'un fichier pour effectuer la sauvegarde d'un fichier déjà présent dans un autre snapshot.

De plus, le fait de n'envoyer que les blocs de données nécessaires permet aussi de gagner du temps en limitant l'utilisation du disque et du réseau.

- **Économie de ressources**

Ne pas stocker plusieurs fois les mêmes données permet de réduire la quantité de stockage nécessaire à la sauvegarde. Ne pas envoyer sur le réseau des données déjà stockées permet de réduire l'utilisation du réseau, ce qui peut s'avérer utile pour les connexions à débit limité par exemple.

- **Restauration rapide**

L'indexation des blocs de données permet de choisir n'importe quelle version de la sauvegarde sans aucun impact négatif sur le temps de restauration. En prenant l'exemple d'un dossier contenant plus ou moins le même nombre de fichiers et de même nature au cours du temps, il n'y aura donc quasiment aucune différence de temps entre restaurer la version de sauvegarde la plus récente ou une version bien plus ancienne.

Cette solution est donc plus efficace et plus fiable que d'autres méthodes comme la sauvegarde incrémentale ou la sauvegarde différentielle. En effet, ces deux autres méthodes ont les contraintes suivantes :

– La sauvegarde différentielle consiste à faire une sauvegarde complète, puis, pour chaque sauvegarde ultérieure, de sauvegarder toutes les différences par rapport à cette sauvegarde initiale. Chaque sauvegarde va donc re-sauvegarder des données déjà récupérées auparavant. De plus, cette méthode nécessite de refaire des sauvegardes complètes régulières, souvent appelées sauvegarde de consolidation, afin d'avoir un point de comparaison plus récent. Cette méthode est moins efficace, nécessite un besoin de stockage plus important et une quantité de données à transférer plus importante. Le temps nécessaire pour restaurer est moins long qu'une sauvegarde incrémentale, mais reste moins efficace que le sauvegarde dédupliquée.

– La sauvegarde incrémentale va analyser les fichiers pour ne transférer que les différences par rapport à la précédente sauvegarde. Elle est donc plus efficace que la sauvegarde différentielle au niveau du stockage et du transfert des données. Cependant, lors de la restauration, la sauvegarde incrémentale est moins efficace car il faut récupérer la sauvegarde initiale et appliquer dessus toutes les autres versions jusqu'à celle souhaitée. Si une seule version manque dans l'historique, cela

entraînera une perte de données car la chaîne constituant tout l'historique sera brisée.

3. Réplication

On parle de réplication de données si les mêmes données sont dupliquées sur plusieurs périphériques. La sauvegarde Oxibox propose des appliances pour avoir une sauvegarde locale ainsi que la possibilité de répliquer ces sauvegardes dans le cloud Oxibox.

4. Chiffrement à la source

Le chiffrement est un procédé qui consiste à convertir des données depuis un format lisible vers un format illisible à l'aide d'un secret, appelé clé de (dé)chiffrement. Le processus de chiffrement est donc réversible et permet d'assurer le principe de confidentialité.

La solution Oxibox chiffre les données à la source. Après une négociation avec la cible de sauvegarde, l'agent va obtenir une clé dérivée de la clé de chiffrement principale et va donc pouvoir chiffrer les données avant même leur transfert.

5. Chiffrement pendant le transit

Les données sont considérées comme étant en transit lorsqu'elles circulent entre des appareils, comme au sein de réseaux privés ou sur Internet. Les données sont plus exposées durant leur transit car il existe différents moyens selon le type de réseau de récupérer (« espionner ») ces informations. Le fait d'établir un canal chiffré entre les deux appareils qui veulent échanger des données est un des principes de base en cybersécurité. C'est le cas par exemple de la plupart des transferts lors d'une navigation sur Internet qui se fait donc généralement via HTTPS. Il existe d'autres méthodes de chiffrement en fonction des protocoles utilisés.

La solution Oxibox n'utilise que des protocoles chiffrés (SFTP ou HTTPS) pour le transfert des données. En sachant que les données sont en plus déjà chiffrées avant même leur transit sur le réseau, on peut donc parler de double-chiffrement pendant le transit.

6. Chiffrement de bout en bout

L'agent de sauvegarde de la solution Oxibox « Plug-and-Protect » chiffre à la source les données à sauvegarder. De plus, l'agent communique vers l'extérieur en utilisant le protocole sécurisé SFTP ou HTTPS qui chiffre également les données qu'il transmet. Ainsi, les données de sauvegarde manipulées par la solution Oxibox sont chiffrées de bout-en-

bout par l'agent et doublement chiffrées par le protocole sécurisé lors du transit sur le réseau. Les données sont stockées chiffrées dans le dépôt de sauvegarde.

7. *Air-Gapping*

L'*air-gapping* est une mesure de sécurité qui consiste à isoler un ordinateur ou un réseau en l'empêchant d'établir une connexion avec l'extérieur.

Dans la solution Oxibox, les sauvegardes sont séparées logiquement via un système de fichiers spécifique développé par Oxibox et qui filtre les opérations non autorisées. De plus, les agents font une négociation avec le serveur de sauvegarde pour obtenir un accès.

8. Immuabilité des sauvegardes

Une sauvegarde immuable est une sauvegarde qui ne peut absolument plus être modifiée. Le but d'une sauvegarde immuable est d'être inaltérable et de pouvoir être immédiatement déployée sur les serveurs de production en cas d'attaque de ransomware ou d'une autre forme de perte de données.

Grâce au système de fichiers filtrant développé par Oxibox, seules les opérations autorisées seront exécutées. Pour illustrer simplement, toutes les actions comme la modification ou la suppression ne peuvent se faire, car elles n'ont pas de raison d'exister dans le contexte d'une sauvegarde. Toutes ces actions sont regroupées dans des règles, construites pour permettre à l'agent de sauvegarde Oxibox d'opérer sainement.

9. Compatibilité POSIX et S3

POSIX (Portable Operating System Interface) est une norme destinée à la portabilité des applications, au niveau source, sur de nombreux systèmes.

S3 (Simple Storage Service) est un service de stockage d'objets définit par Amazon qui offre une capacité de mise à l'échelle, une disponibilité des données, une sécurité et des performances de pointe.

IV. Notions fonctionnelles

1. Redémarrage instantané de machines virtuelles

Notre technologie R2V permet un redémarrage instantané de machines virtuelles cross-hyperviseur. Grace à notre partenariat avec Airbus, nous disposons d'une CyberRange pour restaurer très rapidement l'environnement de travail sur une infrastructure sécurisée en attendant la remise en condition opérationnelle de son système d'information (SI).

2. Restauration granulaire

La restauration granulaire permet de sélectionner les données à restaurer et ce, peu importe leur format, leur structure ou leur taille. Ainsi, qu'il s'agisse d'un simple fichier, d'une machine virtuelle, d'une application stratégique, d'une base de données ou autres, la restauration granulaire d'Oxibox Plug-and-Protect se présente comme une solution rapide et efficace sur divers systèmes de stockage après un incident. Il est par exemple possible de restaurer un simple fichier contenu au sein d'un disque virtuel normalement associé à une machine virtuelle.

3. Sauvegardes dédupliquées multisources

Grâce à l'indexation des blocs de données, les différentes sources qui vont sauvegarder ont connaissance de la signature des blocs déjà existants dans le dépôt de sauvegarde. Comme ce ne sont que les signatures, les données des autres machines ne sont pas fuitées.

Lors des sauvegardes, l'agent se base donc sur cette indexation, comme décrit dans le processus de déduplication.

4. SLA

La SLA (pour Service Level Agreement – Convention de service) est le document qui spécifie les niveaux de service à fournir et le périmètre concerné. Ce document identifie la fourniture et le niveau de qualité requis en des termes objectifs et mesurables. Il est formel et constitue un document qui lie le client et le prestataire. Il doit permettre une définition flexible des prestations à fournir afin de pouvoir s'adapter aux évolutions inévitables des besoins et du périmètre couvert. Il doit constituer un outil de management du service. La Convention de Service permet aussi d'établir le coût annuel récurrent de la

prestation. Il existe différents niveaux de SLA chez Oxibox, allant de la SLA de Base (ne nécessitant aucun coût optionnel) à une SLA Premium.

5. Certification TIER III

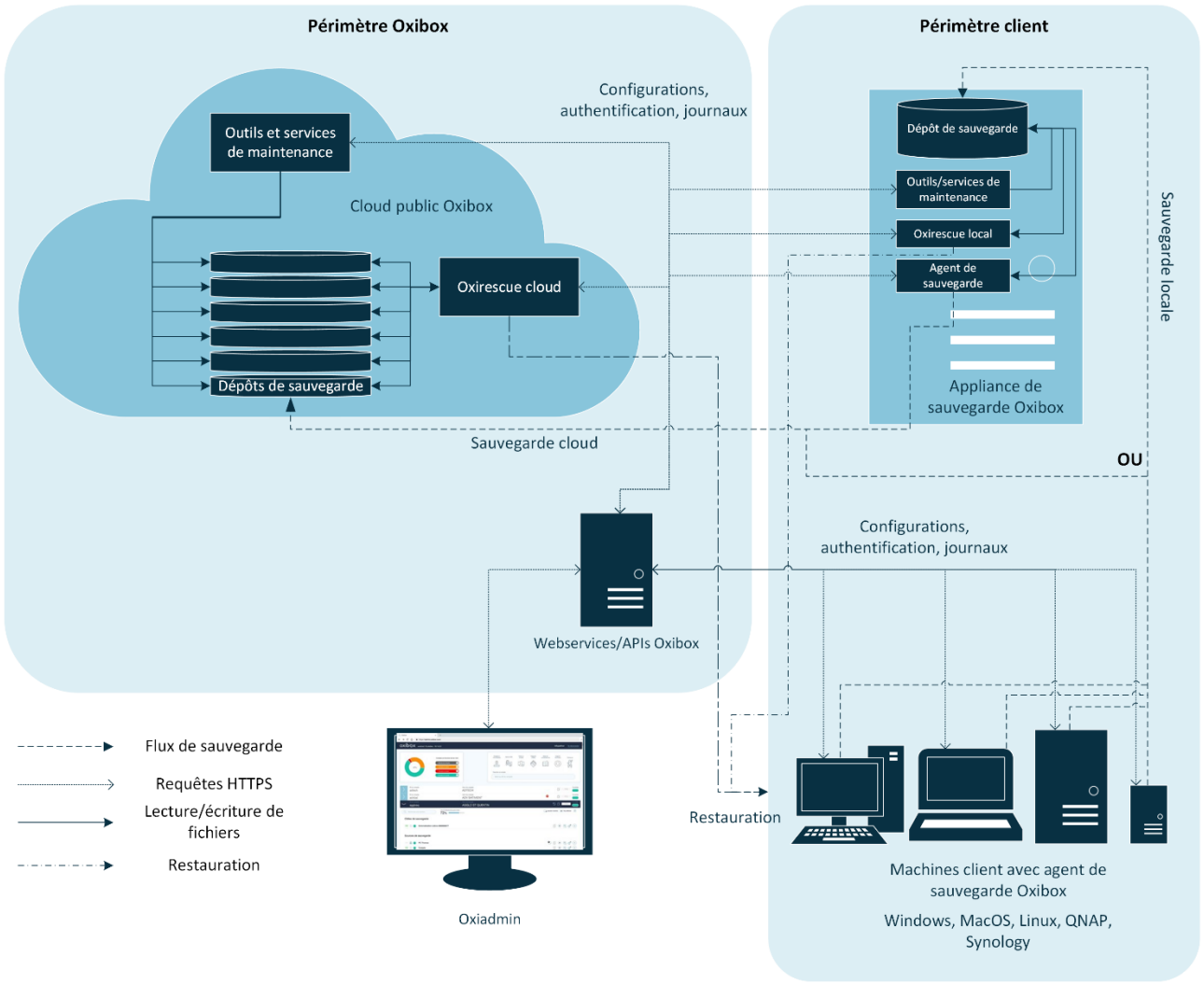
Ce type de certification n'est accordé qu'aux datacenters disposant de plusieurs circuits de distribution électrique et de refroidissement. De plus, tous les composants doivent être redondés et tout le matériel doit disposer d'une double alimentation. La disponibilité est de 99,982%.

Oxibox utilise deux datacenters certifiés TIER III, offrant ainsi à ses clients une excellente sécurisation de leurs données.

6. Certification HDS

La certification HDS est une obligation réglementaire qui s'adresse aux prestataires d'hébergement de données de santé à caractère personnel. Le prestataire d'hébergement francilien d'Oxibox est certifié HDS.

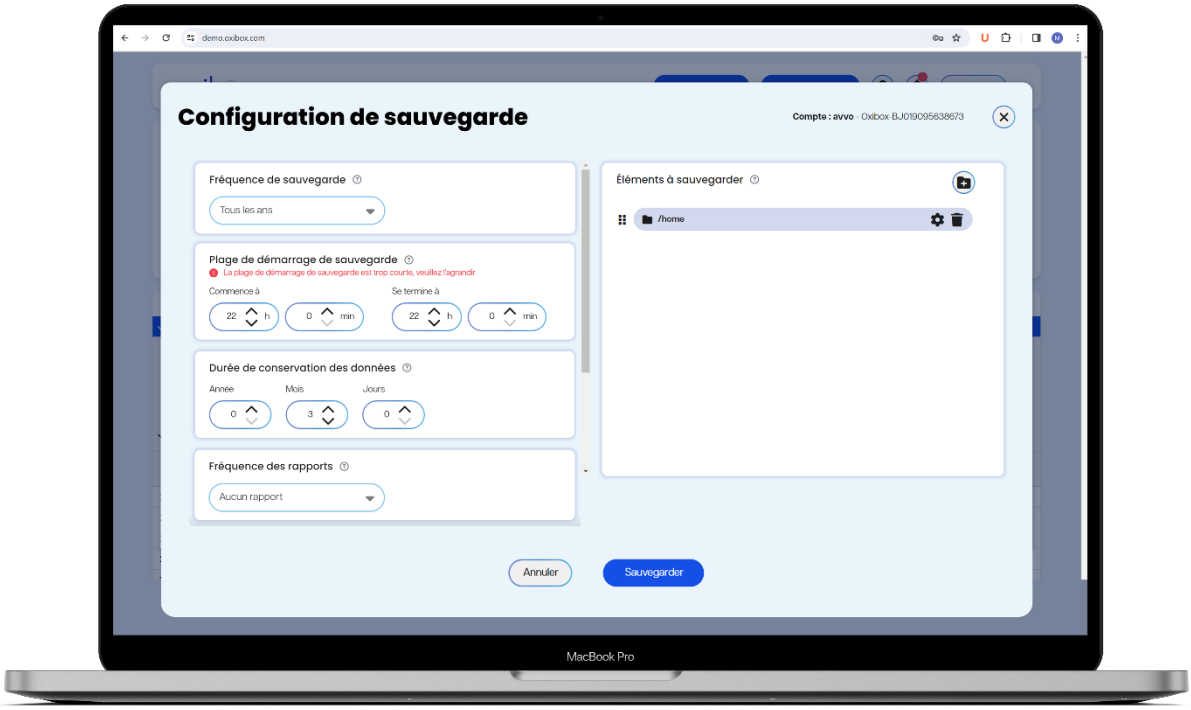
V. Fonctionnement général



La solution de sauvegarde Oxibox fonctionne par l'installation d'agents sur les machines à sauvegarder. Le fonctionnement est différent pour la sauvegarde de produits SaaS comme Microsoft 365.

Dans le cas d'une sauvegarde de machine, il faut installer l'agent Oxibox sur la machine en question via l'installeur dédié. Il faut ensuite enregistrer la machine pour la lier à un compte Oxibox.

Une fois que la machine est liée à un compte Oxibox, il est possible de configurer sa sauvegarde soit via une interface locale, disponible sur Windows et MacOS, soit via l'interface d'administration web Oxiadmin (Cf capture ci-dessous). Les agents réinstallés sur des machines qui ont déjà été configurées vont automatiquement récupérer la configuration précédemment enregistrée.



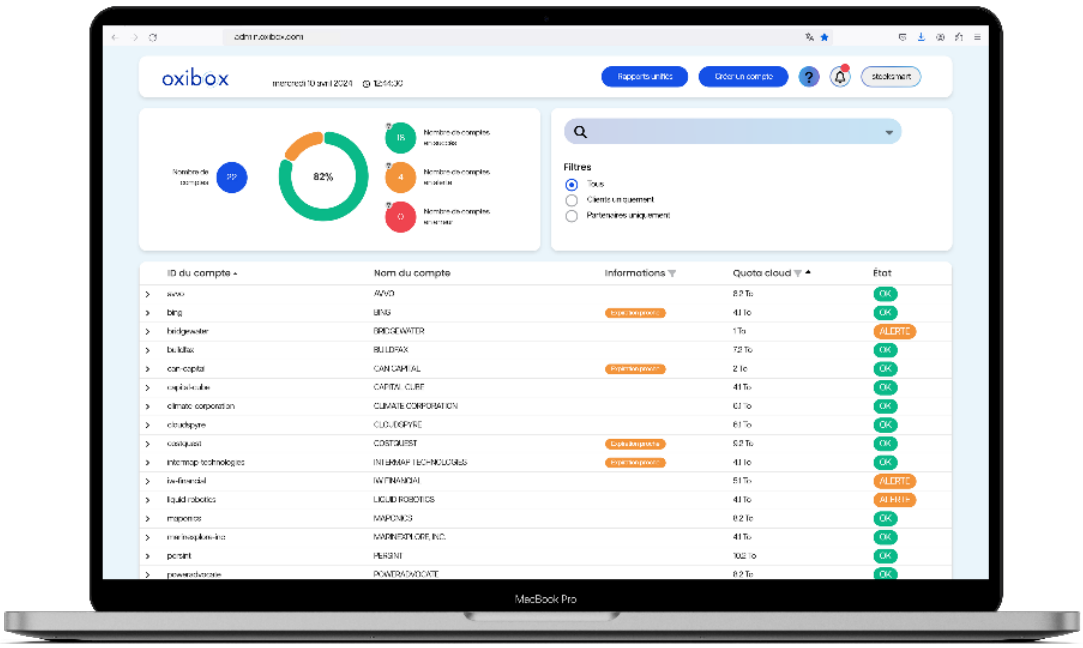
L'agent de sauvegarde va envoyer les données vers la cible configurée. Cela peut être une appliance ou directement le cloud public Oxibox. Dans les deux cas, le fonctionnement est similaire : l'agent se connecte à la cible de sauvegarde pour obtenir des accès, puis va commencer le transfert des données en appliquant le principe de la déduplication. Les flux sont chiffrés à la source et pendant le transit.

Sur la cible de sauvegarde, les données sont stockées dans des dépôts de sauvegarde. Plusieurs services automatiques vont interagir avec ces dépôts pour vérifier régulièrement leur intégrité et aussi pour nettoyer au fur et à mesure les données en fonction de la politique de rétention choisie.

La cible de sauvegarde héberge également les services de restauration Oxirescue, permettant soit via l'interface locale, soit via une interface web, d'accéder aux données souhaitées et de les restaurer dans la version choisie.

Dans le cas d'une appliance Oxibox, il est possible d'avoir une réplication vers le cloud public Oxibox afin d'augmenter le niveau de sécurité et de respecter la recommandation de l'ANSSI avec la sauvegarde 3-2-1-1. Dans ce cas, un agent de sauvegarde est également présent sur l'appliance et va lui-même répliquer les données dans le cloud public Oxibox. Cette réplication sera traitée de la même manière qu'une sauvegarde directe.

Tout le système de sauvegarde Oxibox est orchestré par différents services et APIs permettant d'automatiser les tâches, de permettre le suivi et la configuration à distance et en temps réel, ainsi que l'administration et la restauration en autonomie.



FIN DU DOCUMENT

38 boulevard Paul Cézanne,
78280 GUYANCOURT

contact@oxibox.com
+33 (0)1 30 54 45 79

www.oxibox.com