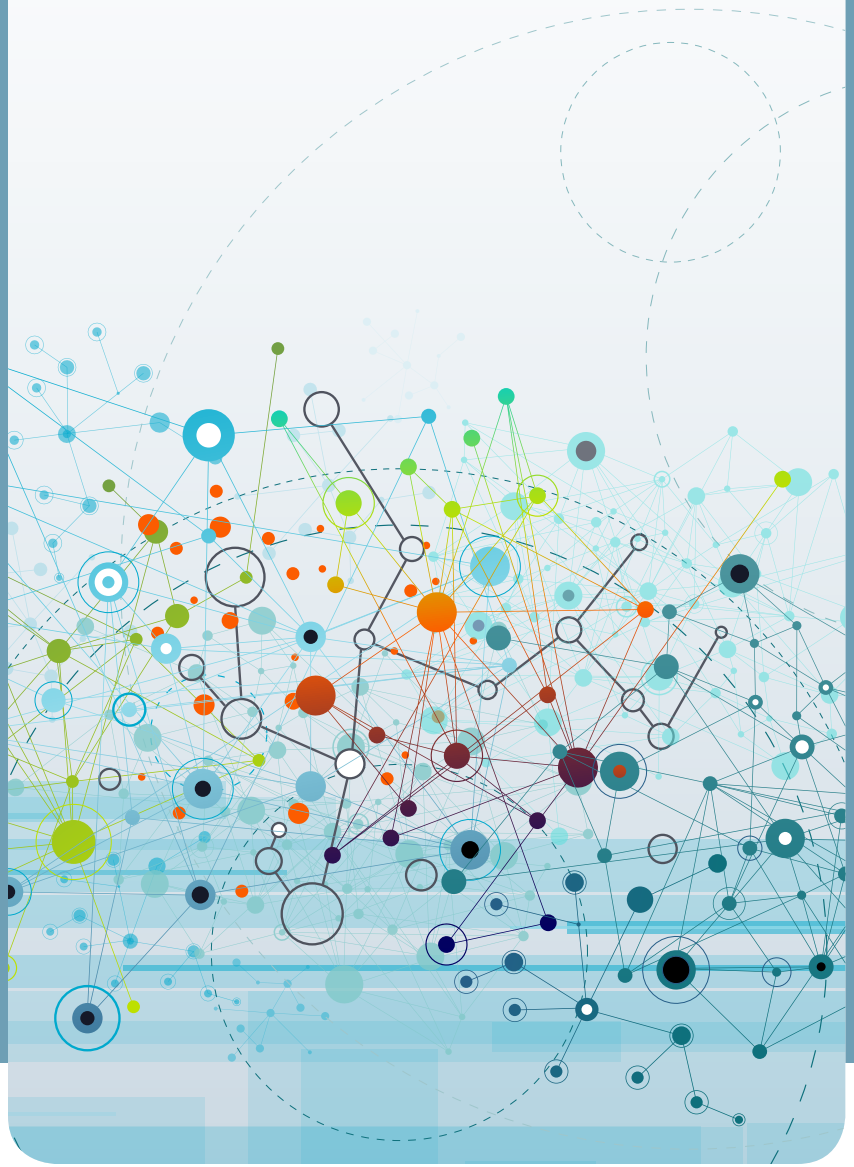
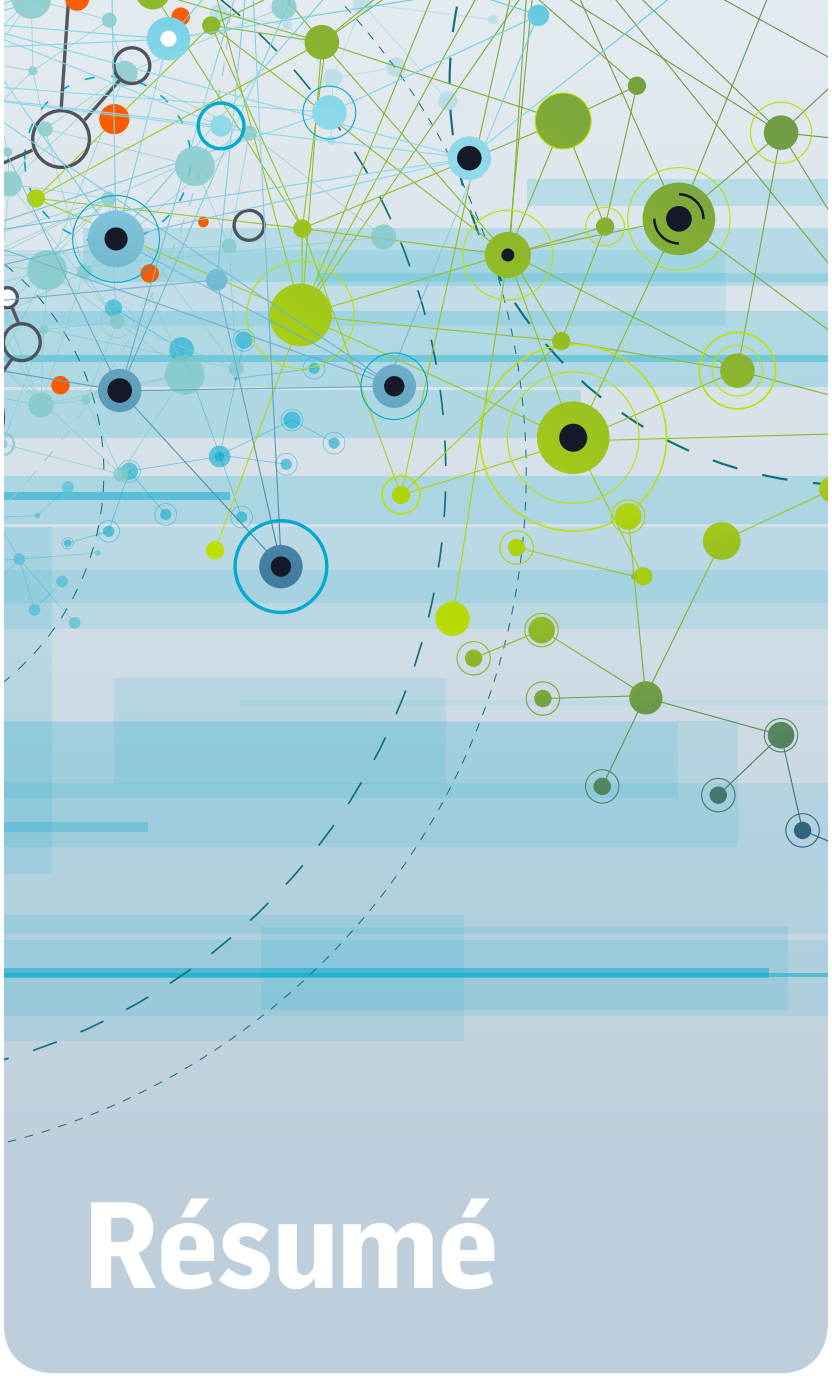


DOSSIER SPÉCIAL

Sécurité

PAR YANN SERRA

TechTarget Custom Media



Résumé

IBM COS consacre l'arrivée de solution de stockage distribuée qui dépassent les systèmes traditionnels (NAS) en performance tout en répondant à un besoin clé : celui de la sécurité. À la haute disponibilité des données, s'ajoutent trois garde-fous contre les failles de sécurité : dispersion, chiffrement et authentification pour lutter contre le vol de données.

IBM COS, un stockage sécurisé de classe gouvernementale

Mieux sécuriser les documents contre les incidents et les intrusions. Tel est l'un des avantages clés d'IBM Cloud Object Storage (COS), un nouveau système de stockage qui surpasse les systèmes de stockage traditionnels par son architecture massivement distribuée. « COS a été conçu pour répartir l'écriture des données sur plusieurs sites, qu'il s'agisse de salles informatiques ou de ressources en Cloud, typiquement celles de notre offre SoftLayer. L'information est de fait toujours disponible même lorsque des disques, des nœuds de stockage, voire un site entier, sont indisponibles. Non seulement, la solution est protégée contre les arrêts de service, mais elle est peut aussi se conformer à une classe d'usage gouvernementale puisqu'elle chiffre le contenu avec des clés internes », explique Philippe Ponti, expert technique d'IBM.

Issu du rachat en octobre 2015 de Cleversafe par IBM, COS est considéré par le cabinet IDC comme le leader du stockage objet et, ce, depuis deux ans. En exploitation depuis 2008, COS gère aujourd'hui plusieurs exaoctets de données dans le monde et a jusqu'ici engendré le dépôt de plus de 300 brevets technologiques. Les systèmes de stockage objet sont considérés par les analystes comme la succession logique des systèmes NAS. D'une part parce que leur ajout de nœuds en réseau ou en Cloud (plutôt que l'attachement direct de tiroirs disques sur un seul serveur), les rend bien plus extensibles. D'autre part, car ils fonctionnent avec des méthodes d'accès et des API qui permettent de mieux les intégrer aux applications modernes (mobile, Big Data, SaaS, GED, etc.).

LES DONNÉES TOUJOURS DISPONIBLES, MÊME EN CAS DE PANNE MAJEURE

En pratique, COS se compose de nœuds « Accesser » qui fragmentent d'abord les données en blocs (« slices » en anglais), puis les dispersent sur des « Slicestors », les nœuds de stockage à proprement parler. La dispersion est telle qu'il y a plus de blocs que nécessaires pour reconstruire un fichier. Ces blocs surnuméraires servent de copie de secours pour que l'information reste disponible même lorsque plusieurs Slicestors ne répondent plus. « Toute la puissance de la solution réside dans l'algorithme IDA de création et de répartition des blocs (dit Erasure Coding), qui fait en sorte qu'on puisse restaurer un fichier même si plusieurs blocs ont été altérés. Et, ce, quelque soit l'endroit où ils auront été altérés », indique Philippe Ponti. Il insiste sur l'apport de ce mécanisme par rapport aux solutions à déployer quand on utilise un NAS ou autre équipement de stockage : « avec COS, on assure la haute disponibilité de la donnée sans avoir besoin de mettre en œuvre un système de duplication complexe entre sites, ni avoir à gérer l'inertie d'un système de type RAID pour parer à la panne des disques », ajoute-t-il.

Il est à noter que les algorithmes d'Erasure Coding sont souvent proposés par l'industrie à la place du RAID classique, car ils réduisent la durée et le traitement nécessaires à la reconstruction des données. L'inconvénient potentiel de cette méthode est qu'elle pourrait s'avérer plus gourmande en puissance de calcul et qu'elle augmenterait la latence. « Il s'agit justement du défaut que les ingénieurs en charge du développement de COS sont parvenus à éviter en mettant au point leur algorithme AONT-RS (All Or Nothing Transform with Reed Solomon) avec l'objectif de fonctionner sur des nœuds au coût minimal », lance Philippe Ponti. Tous les nœuds utilisés dans COS - les Accessers, les Slicestors ainsi que le nœud de contrôle Manager CS - sont des serveurs x86 standards, fonctionnant sous le système d'exploitation ClevOS.

Dispersion, chiffrement et authentification contre les vols de données

DISPERSION, CHIFFREMENT ET AUTHENTIFICATION CONTRE LES VOLS DE DONNÉES

À la haute disponibilité des données, s'ajoutent trois garde-fous contre les failles de sécurité. D'abord, aucun disque ne contient assez de blocs pour restituer à lui seul un fichier. L'opérateur en charge de la solution peut même étendre la granularité de cette sécurité à l'échelle d'un Slicestor entier, voire à celle d'un site entier, ce qui évite aux matériels de représenter une faille de sécurité (vol de serveurs, par exemple). Ensuite, les accuser peuvent chiffrer eux-mêmes leurs blocs avec des clés de 128 à 256 bits, de sorte à empêcher qu'un programme ou qu'un intrus sur le réseau puisse les lire en outrepassant COS. Enfin, les sessions sont également chiffrés en TLS pour éviter qu'un espion à l'écoute du réseau ne puisse capter les données à la volée lors de leur enregistrement ou de leur lecture. L'interface d'administration de COS est à ce titre compatible avec les protocoles d'authentification d'accès classiques (les paires login/mot de passe d'Active Directory et autres OpenLDAP, Les paires de clés PKI, les services S3 Secret et Openstack Keystone, etc.).

« L'administrateur de la solution n'a pas lui-même accès aux contenus des fichiers stockés sur COS. Il a juste le droit de dimensionner la solution pour les besoins des utilisateurs en ajoutant plus ou moins de container, de nœuds Accessers pour ajuster les vitesses d'accès, et de nœuds Slicestors, pour ajuster la capacité disponible », conclut Philippe Ponti.