

Le Cloud d'IBM offre des services de cryptographie résistante aux ordinateurs quantiques et de chiffrement hyperprotégé pour aider à sécuriser les données à l'ère de l'hybride

IBM associe son leadership dans le Cloud hybride à son expertise dans le quantique et la sécurité pour rester à la pointe dans le domaine de la cybersécurité quantique

ARMONK, N.Y., 30 novembre 2020 : IBM (NYSE: [IBM](#)) a annoncé aujourd'hui une série de services et de technologies Cloud conçus pour aider les clients à maintenir le plus haut niveau de protection disponible en matière de chiffrement des clés de cryptographie afin de contribuer à protéger les données existantes dans le Cloud^[1] et de se préparer aux menaces futures qui pourraient évoluer avec les progrès de l'informatique quantique. La compagnie propose désormais des solutions de cryptographie résistante aux ordinateurs quantiques pour la gestion des clés et des applications transactionnelles dans IBM Cloud[®], inventées par les chercheurs d'IBM Research, ce qui en fait l'approche de cryptographie résistante aux ordinateurs quantiques la plus complète du secteur disponible actuellement pour la sécurisation des données.

Les nouvelles capacités comprennent :

Des solutions de cryptographie résistante aux ordinateurs quantiques : Grâce à l'utilisation de normes ouvertes et de technologies open source, ces solutions améliorent les normes utilisées pour la transmission de données entre les entreprises et le Cloud, ce qui contribue à sécuriser les données en utilisant un algorithme résistant aux ordinateurs quantiques.

Des services étendus de chiffrement hyperprotégé dans IBM Cloud (IBM Cloud Hyper Protect Crypto Services) : De nouvelles capacités sont disponibles pour améliorer la confidentialité des données dans les applications Cloud - où les données envoyées sur le réseau vers les applications Cloud et les éléments de données sensibles tels que les numéros de carte de crédit sont stockés dans une base de données qui peut être chiffrée au niveau de l'application - soutenues par le plus haut niveau de protection de chiffrement de clé de cryptographie du secteur à travers la capacité "Keep Your Own Key" (KYOK).

*« Alors que notre dépendance aux données s'accroît à l'ère du Cloud hybride et que les capacités de l'informatique quantique progressent, le besoin de confidentialité des données devient encore plus critique. IBM propose aujourd'hui une approche de chiffrement résistant aux ordinateurs quantiques la plus complète pour sécuriser les données disponibles actuellement et pour aider les entreprises à protéger leurs données existantes et à se prémunir contre les menaces futures », a **déclaré Hillery Hunter, Vice President and Chief Technology Officer, IBM Cloud** . « La sécurité et la conformité restent au cœur d'IBM Cloud, car nous continuons à investir dans le calcul de confiance et dans nos capacités de chiffrement de pointe pour aider les entreprises de toutes sortes - en particulier celles des secteurs hautement réglementés - à sécuriser leurs données ».*

Se préparer aux menaces des ordinateurs quantiques grâce aux développements de nouveaux algorithmes de chiffrement

Alors que l'informatique quantique vise à résoudre des problèmes complexes que même les superordinateurs les plus puissants du monde ne peuvent pas résoudre, les futurs ordinateurs quantiques tolérants aux pannes

pourraient présenter des risques potentiels, comme la capacité de casser rapidement les algorithmes de chiffrement et d'accéder à des données sensibles. Pour atténuer ces risques, IBM a élaboré un programme stratégique clair pour contribuer à protéger la sécurité à long terme de ses plateformes et services. Ce programme comprend la recherche, le développement et la standardisation d'algorithmes de cryptographie résistant aux ordinateurs quantiques comme outils de base open source tels que CRYSTALS et OpenQuantumSafe. Cela comprend également la gouvernance, les outils et la technologie nécessaires pour aider les clients à s'engager sur cette voie conduisant à un avenir plus sûr.

Aujourd'hui, comme prochaine étape de ce programme, IBM apporte ses [capacités de chiffrement de pointe](#), développées par les spécialistes du domaine chez IBM Research, pour aider ses clients à adopter une approche de cryptographie résistante aux ordinateurs quantiques pour leurs données en transit dans le Cloud d'IBM. Ces capacités sont conçues pour aider les entreprises à se préparer aux menaces futures et peuvent être utiles contre les attaques dans lesquelles des acteurs malveillants récoltent aujourd'hui des données chiffrées dans l'intention de les déchiffrer plus tard, au fur et à mesure des progrès de l'informatique quantique.

IBM Key Protect, un service basé sur le Cloud qui assure la gestion du cycle de vie des clés de chiffrement utilisées dans les services IBM Cloud ou les applications client, a maintenant introduit la possibilité d'utiliser une connexion TLS (Transport Layer Security) basée sur la cryptographie résistante aux ordinateurs quantiques en aidant à protéger les données pendant la gestion du cycle de vie des clés.

IBM Cloud introduit également des capacités pour s'affranchir des risques liés aux ordinateurs quantiques afin de faciliter les applications transactionnelles. Lorsque des applications conteneurisées « Cloud natives » s'exécutent sur Red Hat® OpenShift® sur IBM Cloud ou IBM Cloud Kubernetes Services, des connexions TLS sécurisées peuvent favoriser les applications transactionnelles avec des solutions de cryptographie résistante aux ordinateurs quantiques pendant le transit des données et protéger contre les violations potentielles.

Protéger les données sensibles avec les services de chiffrement hyperprotégé dans IBM Cloud (IBM Cloud Hyper Protect Crypto Services)

Les entreprises doivent également atténuer les risques liés aux menaces externes et internes, ainsi que veiller au respect de la réglementation.

Aujourd'hui, IBM Cloud offre également de nouvelles capacités pour aider à sécuriser les applications transactionnelles et les données sensibles en utilisant les services [IBM Cloud Hyper Protect Crypto Services](#), qui offrent le plus haut niveau de protection en matière de chiffrement des clés de cryptographie en fournissant aux clients la capacité "Keep Your Own Key" (KYOK). Conçu sur du matériel certifié FIPS-140-2 niveau 4 - le plus haut niveau de sécurité offert par tout fournisseur de Cloud du secteur pour les modules de cryptographie^[2] -, ce service permet aux clients d'avoir le contrôle exclusif de leurs clefs de chiffrement, et donc le contrôle sur les données et les applications protégées par celle-ci.

Conçus pour les applications transactionnelles nécessitant un chiffrement plus avancé, les clients d'IBM Cloud peuvent garder leurs clés privées sécurisées dans le module de sécurité de l'infrastructure Cloud tout en déchargeant la connexion TLS vers les services de chiffrement IBM Cloud Hyper Protect Crypto Services pour aider à établir une connexion sécurisée avec le serveur web. Ils peuvent également réaliser un chiffrement des données sensibles au niveau de l'application, comme par exemple un numéro de carte de crédit, avant qu'elles

ne soient stockées dans un système de base de données.

Continuer à répondre aux exigences des clients et des secteurs hautement réglementés en matière de sécurité

IBM a investi dans les technologies de calcul de confiance depuis plus de dix ans et propose aujourd'hui des solutions de calcul de confiance prêtes à l'emploi pour aider ses clients à protéger leurs données, applications et processus.

Fidèle à son engagement en matière de sécurité et de conformité, IBM continue de collaborer avec ses pairs du secteur pour faire progresser les initiatives de standardisation. Par exemple, les meilleures pratiques de sécurité sur IBM Cloud sont désormais disponibles en tant que référence pour servir de fondation pour IBM Cloud pour le Centre pour la Sécurité d'Internet ([CIS : Center for Internet Security](#)) et les équipes de cryptographie d'IBM Research sont des contributeurs essentiels aux algorithmes QSC qui sont présélectionnés dans le National Institute of Standards and Technology (NIST).

IBM, le logo IBM et IBM Cloud sont des marques commerciales ou des marques déposées d'IBM Corp. aux États-Unis et/ou dans d'autres pays.

Red Hat® et OpenShift® sont des marques commerciales ou des marques déposées de Red Hat, Inc. ou de ses filiales aux États-Unis et dans d'autres pays.

À propos d'IBM Cloud

Pour en savoir plus : <https://www.ibm.com/fr-fr/cloud>

Based on IBM Hyper Protect Crypto Service, the only service in the industry built on FIPS 140-2 Level 4-certified hardware. FIPS 140-2 Security Level 4 provides the highest level of security defined in this standard. At this security level, the physical security mechanisms provide a comprehensive envelope of protection around the cryptographic module with the intent of detecting and responding to all unauthorized attempts at physical access.

Encryption keys and cryptographic operations are protected with highest level certified HSM - with Hyper Protect Crypto services: FIPS 140-2 Level 4.

Contacts presse :

IBM

Gaëlle Dussutour

Tél. : + 33 (0) 6 74 98 26 92

dusga@fr.ibm.com

Weber Shandwick pour IBM

Robin Legros / Eric Chauvelot

Tél. : + 33 (0)6 68 04 57 83 / +33 (0)6 21 64 28 48

ibmfrance@webershandwick.com
