

Annonce de l'IBM z16 : Intelligence artificielle en temps réel pour le traitement à grande échelle des transactions et premier système du secteur résistant aux ordinateurs quantiques

- **L'IBM z16 intègre le processeur Telum d'IBM afin que les clients puissent réaliser l'inférence de modèles d'intelligence artificielle pour une meilleure compréhension en temps réel**
- **L'IBM z16 est le premier système du secteur résistant aux ordinateurs quantiques**

ARMONK, N.Y., le 5 avril 2022 : IBM (NYSE: [IBM](#)) a dévoilé aujourd'hui l'[IBM® z16™](#), le système de nouvelle génération d'IBM doté d'un accélérateur d'intelligence artificielle intégré à la puce, qui fournit une inférence optimisée en termes de latence. Cette innovation est conçue pour permettre aux clients [d'analyser à grande échelle les transactions en temps réel](#) pour les applications critiques telles que les cartes de crédit, les soins de santé et les transactions financières. S'appuyant sur le leadership historique d'IBM en matière de [sécurité](#), l'IBM z16 est également spécifiquement conçu pour aider à se protéger contre les menaces qui pourraient être utilisées dans un futur proche pour casser les technologies de chiffrement actuelles.

Les innovations d'IBM, notamment l'IBM z16, constituent l'épine dorsale technologique de l'économie mondiale depuis des décennies. Le mainframe IBM modernisé d'aujourd'hui est au cœur des environnements [Cloud hybride](#) et est apprécié par deux tiers des entreprises du classement Fortune 100, 45 des 50 premières banques mondiales, 8 des 10 premiers assureurs, 7 des 10 premiers détaillants mondiaux et 8 des 10 premiers opérateurs de télécommunications, en tant que plateforme hautement sécurisée pour l'exécution de leurs applications les plus critiques. Par exemple, selon une récente étude commandée par IBM et réalisée par Celent, intitulée « Operationalizing Fraud Prevention on IBM Z » (Opérationnalisation de la prévention des fraudes sur l'IBM Z), les IBM zSystems exécutent 70% des transactions mondiales, en valeur. [\[1\]](#)

« IBM est la référence en matière de traitement des transactions hautement sécurisées. Désormais, grâce aux innovations de l'IBM z16, nos clients peuvent accélérer leurs prises de décisions grâce à l'inférence de modèle là où se trouvent leurs données critiques », a déclaré Ric Lewis, SVP, IBM Systems. « Cela ouvre de nouvelles perspectives et change la donne pour nos clients et leurs secteurs d'activités en quête d'améliorations des expériences clients et de leurs résultats opérationnels. »

L'IA d'entreprise en temps réel va révolutionner les industries grâce à de nouveaux cas d'usages et de nouvelles applications

Les institutions financières du monde entier luttent contre les impacts des activités frauduleuses sur leurs revenus et leurs interactions avec les consommateurs. Selon une nouvelle étude d'IBM et Morning Consult intitulée « [Rapport IBM 2022 sur l'impact de la fraude financière mondiale](#) », la fraude liée aux cartes de crédit est le type de fraude le plus répandu chez les consommateurs des sept pays interrogés. En outre, les personnes sondées ont déclaré qu'elles pensaient que les banques et les réseaux de paiement devaient être les principaux responsables de la prévention de la fraude. Mais l'exécution de modèles d'IA par apprentissage profond à grande échelle et en temps réel n'a pas été possible jusqu'à maintenant en raison de problèmes de latence, c'est pourquoi les modèles de détection de la fraude ne sont exécutés à ce jour que sur moins de 10 % des transactions à fort volume - un nombre important de fraudes ne sont ainsi pas détectées.

L'IBM z16 associe de manière unique l'inférence de modèle d'intelligence artificielle, via son [processeur IBM Telum](#), au traitement hautement sécurisé et fiable des transactions à fort volume pour lequel IBM est réputé. Pour la première fois, les banques peuvent analyser la fraude lors de transactions à grande échelle : l'IBM z16 peut traiter 300 milliards de demandes d'inférence par jour avec une latence de seulement une milliseconde^[2]. Pour les consommateurs, cela pourrait signifier réduire le temps et l'énergie nécessaires pour gérer les transactions frauduleuses sur leur carte de crédit. Tant pour les commerçants que pour les émetteurs de cartes, cela pourrait vouloir dire une réduction des pertes de revenus, car les consommateurs pourraient éviter la frustration associée à des rejets de transactions qui pourraient les conduire à se tourner vers d'autres émetteurs de cartes pour de futures transactions.

D'autres menaces, notamment la fraude fiscale et le vol organisé dans le commerce de détail, sont des défis à maîtriser pour les gouvernements et les entreprises. Les paiements en temps réel et les méthodes de paiement alternatives telles que les crypto-monnaies mettent à l'épreuve les techniques traditionnelles de détection des fraudes. L'application des nouvelles capacités de l'IBM z16 à d'autres industries peut contribuer à créer de tous nouveaux cas d'usage, notamment :

- L'approbation de prêts : pour accélérer l'approbation des prêts aux entreprises ou aux particuliers.
- La compensation et le règlement : pour déterminer les transactions et/ou les opérations qui peuvent présenter un risque élevé avant le règlement.
- L'apprentissage fédéré pour le commerce de détail : pour mieux modéliser le risque de fraude et de vol.

Sécurisation des données avec le premier système résistant aux ordinateurs quantiques du secteur

Dans un environnement Cloud hybride comprenant des ressources en local et dans des Cloud publics, il est essentiel de se protéger contre les menaces actuelles et de se positionner contre les cybercriminels qui peuvent voler des données maintenant, pour les déchiffrer plus tard. S'appuyant sur les technologies d'IBM telles que la *Pervasive Encryption* (chiffrement systématique) et le *Confidential Computing* (informatique confidentielle), l'IBM z16 fait progresser la cyber-résilience d'un cran en protégeant les données contre les menaces futures qui pourraient évoluer avec les progrès de l'informatique quantique.

Premier système résistant aux ordinateurs quantiques du secteur^[3], l'IBM z16 repose sur la cryptographie par réseau euclidien, une approche permettant de construire des primitives de sécurité qui aident à protéger les données et les systèmes contre les menaces actuelles et futures. Grâce à la cryptographie résistante aux ordinateurs quantiques de l'IBM z16, les entreprises peuvent dès aujourd'hui préparer l'avenir de leurs applications et de leurs données.

Avec un processus d'initialisation sécurisé (ce qui signifie que les acteurs mal intentionnés ne peuvent pas injecter de logiciels malveillants dans le processus d'initialisation pour prendre le contrôle du système dès le démarrage), les clients de l'IBM z16 peuvent renforcer leur protocole de cyber-résilience et garder le contrôle de leur système. En outre, le module de sécurité matérielle Crypto Express 8S (CEX8S) offrira aux clients une technologie de chiffrement à la fois classique et résistante aux ordinateurs quantiques pour les aider à adresser leurs cas d'usages nécessitant la confidentialité, l'intégrité et la non-répudiation des informations. Le processus d'initialisation sécurisé et la cryptographie résistante aux ordinateurs quantiques de l'IBM z16 peuvent aider les clients à faire face aux futures menaces liées à l'informatique quantique, notamment les attaques de type « harvest now, decrypt later » (collecter maintenant, déchiffrer plus tard) qui peuvent conduire à l'extorsion, à la perte de propriété intellectuelle et à la divulgation d'autres données sensibles.

Modernisation pour le Cloud hybride

Au cours des trois dernières années, IBM a réalisé d'importants investissements dans le cadre de son engagement à adopter la technologie open-source sur la plateforme IBM zSystems et à établir une expérience

commune pour les développeurs dans le Cloud hybride. Ces solutions sont conçues pour aider nos clients à tirer parti de leurs investissements dans - et des points forts de - leur infrastructure informatique, de leurs applications et de leurs Clouds existants de manière transparente, tout en leur donnant la flexibilité d'exécuter, de concevoir, de gérer et de moderniser des applications « Cloud-natives » sur l'architecture de leur choix.

Les annonces récentes dans le cadre de cette démarche incluent :

- [**Stack de modernisation de l'IBM Z et du Cloud**](#) : pour aider les clients à accroître leur agilité et à accélérer leur transformation, y compris pour les projets développés avec les open-source du marché.
- [**Centre de modernisation de l'IBM Z et du Cloud**](#) : une porte d'entrée numérique vers une vaste gamme d'outils, de formations, de ressources, de partenaires de l'écosystème et d'expertise sectorielle d'IBM Consulting pour aider les clients IBM zSystem à accélérer la modernisation de leurs applications, données et processus dans une architecture Cloud hybride ouverte.
- [**Tarification sur mesure**](#) : une approche complète de type « Cloud à l'usage » qui est calculée en fonction des variations de consommation applicatives et des besoins métiers.
- [**Introduction d'Anaconda dans Linux on Z**](#) : un exemple d'introduction de modèles et bibliothèques en data science dans ces plateformes d'entreprise, offrant une expérience utilisateur homogène et transparente pour le data scientist où que ce soit dans les environnements du [**Cloud hybride**](#).
- [**Support rationalisé**](#) : un support à l'échelle ou industrialisé. IBM Technology Support Services offre aux clients IBM z16 un support clé en main pour les aider à prévoir et prévenir les interruptions non planifiées, ainsi que des services techniques qui accélèrent la façon dont les entreprises tirent parti des possibilités offertes par les environnements technologiques hybrides.

Avec l'IBM z16, IBM a utilisé une approche très collaborative qui est à l'écoute des attentes clients impliquant plusieurs centaines de personnes de plus de 70 clients, mode opératoire déjà lancé pour la conception des futurs systèmes mainframe IBM. L'IBM z16 sera disponible commercialement le 31 mai 2022. Pour en savoir

plus, veuillez consulter le [blog de Ross Mauri](#).

À propos d'IBM

IBM est un leader mondial du Cloud hybride et de l'IA, ainsi que des services aux entreprises, qui aide ses clients dans plus de 175 pays à capitaliser sur les connaissances issues de leurs données, à rationaliser leurs processus métier, à réduire leurs coûts et à acquérir un avantage concurrentiel dans leurs secteurs d'activité. Près de 3 800 entités gouvernementales et entreprises dans des domaines d'infrastructures critiques tels que les services financiers, les télécommunications et les soins de santé font confiance à la plateforme Cloud hybride d'IBM et à Red Hat OpenShift pour impacter leurs transformations numériques rapidement, efficacement et en toute sécurité. Les innovations révolutionnaires d'IBM en matière d'IA, d'informatique quantique, de solutions Cloud spécifiques à certains secteurs et de services aux entreprises offrent des options ouvertes et flexibles à nos clients. Tout cela est soutenu par l'engagement légendaire d'IBM en matière de confiance, de transparence, de responsabilité, d'inclusivité et de service.

Pour en savoir plus : www.ibm.com

Contacts presse :

Weber Shandwick pour IBM

IBM

Gaëlle Dussutour

Tél. : + 33 (0) 6 74 98 26 92

dusga@fr.ibm.com

Jennifer Tshidibi / Eric Chauvelot

Tél. : + 33 (0)6 13 94 26 58 / + 33 (0)6 21 64
28 68

ibmfrance@webershandwick.com

[1] « Opérationnalisation de la prévention des fraudes sur l'IBM Z », un rapport commandé par IBM et réalisé par Celent. Mars 2022.

[2] Avertissement : Les performances sont extrapolées à partir de tests internes d'IBM exécutant des opérations d'inférence locale dans une LPAR z16 avec 48 IFL et 128 Go de mémoire sur Ubuntu 20.04 (mode SMT) en utilisant un modèle synthétique de détection de fraude à la carte de crédit (<https://github.com/IBM/ai-on-z-fraud-detection>) exploitant l'accélérateur intégré pour l'IA de la puce Telum. Le benchmark a été exécuté avec 8 *threads* parallèles, chacun étant associé au premier cœur d'une puce différente. La commande `lscpu` a été utilisée pour identifier la topologie cœur-puce. Une taille de lot de 128 opérations d'inférence a été utilisée. Les résultats peuvent varier.

[3] Avertissement : Cité par un analyste tiers. L'IBM z16 avec la carte Crypto Express 8S fournit des API résistantes aux ordinateurs quantiques donnant accès à des algorithmes résistants aux ordinateurs quantiques qui ont été sélectionnés comme finalistes au cours du processus de normalisation PQC mené par le NIST. <https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3> submissions. La cryptographie résistante aux ordinateurs quantiques fait référence aux efforts déployés pour identifier les algorithmes résistants aux attaques des ordinateurs à la fois classiques et quantiques, afin de préserver la sécurité des informations même après la construction d'un ordinateur quantique à grande échelle. Source : <https://www.etsi.org/technologies/quantum-safecryptography>. Ces algorithmes sont utilisés pour garantir l'intégrité d'un certain nombre de programmes machines et de processus de démarrage. L'IBM z16 est le premier système de l'industrie à être protégé par une technologie résistante aux ordinateurs quantiques sur plusieurs couches de programmes machines.
