

À mesure que les CIO adoptent le multicloud, ces derniers doivent veiller à ce que leur réseau soit modernisé afin d'assurer l'agilité, la flexibilité, l'élasticité et la sécurité requises par les services cloud distribués.

Modernisation du réseau : répondre au besoin de services cloud distribués et sécurisés

Septembre 2022

Rédigé par : Brad Casemore et Ghassan Abdo

Introduction

Véritables moteurs de l'entreprise numérique, les applications se révèlent de plus en plus distribuées dans l'ensemble des environnements cloud et de périphérie. Les DSI et les CXO (directeurs de l'expérience client) font face au défi visant à garantir des services réseau simplifiés, cohérents, extensibles et hautement automatisés, aptes à assurer une sécurité robuste à un panorama cloud distribué et apparemment infini d'applications et d'utilisateurs. On peut s'interroger sur la façon dont les entreprises peuvent atteindre ces objectifs en considérant un environnement multicloud difficile nécessitant une approche moderne de la mise en réseau vers et sur les clouds publics, les datacenters sur site, les environnements de périphérie et les installations de colocalisation.

Ce rapport explore la manière dont les architectures réseau et les services réseau cloud définis par logiciel (qui découplent l'innovation logicielle et la vélocité des fonctionnalités de l'infrastructure physique sous-jacente) aident les entreprises à atteindre leurs ambitions en termes de flexibilité, d'agilité et de performances au sein de ce nouvel environnement.

Tendances principales

Si le réseau reste invisible aux utilisateurs (en particulier lorsqu'il fait son travail correctement), il reste impératif à la réussite de l'entreprise numérique. En fait, compte tenu des attentes numériques d'applications et de services toujours actifs (non interrompus par la dégradation des performances ou les pannes), le réseau se révèle plus important que jamais, d'autant plus lorsqu'il étend ses ramifications partout où il peut faire la différence. Les applications et les données dépendent des mérites du réseau, et réussissent ou échouent en conséquence.

EN BREF

STATISTIQUES ESSENTIELLES

Dans l'étude CloudPulse conduite par IDC en octobre 2021, seules 24 % des personnes interrogées dans les entreprises ont mentionné qu'elles comptaient se concentrer sur un environnement à cloud unique ces deux prochaines années, tandis que 76 % d'entre elles ont signalé qu'elles entendaient suivre les variations des environnements multicloud.

Le cloud a complètement redéfini les architectures et les infrastructures (de même que le modèle opérationnel) associées à la mise en réseau des datacenters. En outre, le multicloud renforce un besoin de transformation qui s'étend à l'ensemble des environnements WAN et de périphérie. S'il est vrai que le réseau était défini par logiciel dans le datacenter sur site et même dans le modèle WAN (sous forme de SD-WAN), l'essor des environnements hybrides et multicloud implique que le besoin de mesures d'automatisation, de contrôle et de sécurité intelligentes et basées sur des politiques doit devenir omniprésent pour répondre aux exigences de l'ère du cloud. Dans l'étude mondiale conduite par IDC et consacrée au SD-WAN, les personnes interrogées ont massivement mentionné que l'adoption des modèles SaaS et IaaS, de même que les stratégies multicloud de leurs entreprises, allaient prendre de plus en plus d'importance à l'égard des choix en matière de technologie WAN.

En fait, à mesure que les applications gagnent en importance sur le plan de l'activité et deviennent de plus en plus distribuées, sur plusieurs clouds et environnements de périphérie, un besoin opérationnel se fait sentir pour des services réseau simplifiés, cohérents, extensibles et hautement automatisés, aptes à assurer une sécurité robuste à un panorama cloud distribué et apparemment infini d'applications et d'utilisateurs. De plus, les entreprises font face à de nouvelles exigences en matière de routage rapide, fiable et sécurisé du trafic, capables de proposer des points d'entrée et des accès directs pratiques vers et depuis les clouds afin d'atténuer la latence, de renforcer la disponibilité et d'améliorer l'expérience numérique des utilisateurs.

IDC trouve que les entreprises en marche vers le cloud adoptent en masse les stratégies informatiques multicloud. Dans l'étude *CloudPulse* conduite par IDC en octobre 2021, seules 24 % des personnes interrogées dans les entreprises ont mentionné qu'elles comptaient se concentrer sur un environnement à cloud unique ces deux prochaines années, tandis que 76 % d'entre elles ont signalé qu'elles entendaient suivre les variations des environnements multicloud. Près de 50 % des personnes interrogées ont indiqué qu'elles aimeraient disposer d'un environnement multicloud facilitant la migration des charges de travail et des données ou duquel une application donnée pourrait s'exécuter en toute fluidité sur différents clouds. En outre, dans l'étude *Future of Digital Infrastructure 2022 Global Sentiment* conduite en 2022 par IDC et consacrée à l'avenir de l'infrastructure numérique, 77 % des personnes interrogées dans les entreprises ont convenu que le besoin d'interconnexions entre clouds publics, installations de colocalisation et sites de campus/de périphérie transforme les conceptions réseau et pousse les entreprises à travailler avec de nouveaux partenaires d'interconnexion.

Au sein de ce paysage, les motivations spécifiques en faveur du multicloud varient. Certaines entreprises signalent que différentes applications ou différents scénarios d'utilisation conviennent à différents clouds, tandis que d'autres déclarent passer expressément par plusieurs fournisseurs pour atténuer le risque d'aliénation à un fournisseur. D'autres encore rapportent avoir commencé leur parcours cloud avec un seul fournisseur IaaS, avant de s'étendre à d'autres pour des raisons architecturales. L'adoption du multicloud est parfois stimulée par une nouvelle application nécessitant des capacités uniquement disponibles chez un

Le cloud a complètement redéfini les architectures et les infrastructures (de même que le modèle opérationnel) associées à la mise en réseau des datacenters.

fournisseur de cloud différent et parfois, différentes équipes et différents services (travaillant en parallèle) sélectionnent différents fournisseurs IaaS, de manière parfaitement indépendante. De plus, certaines entreprises adoptent des stratégies multicloud pour disposer d'un moyen d'action en matière de tarification et de négociation avec leur fournisseur IaaS principal.

Indépendamment de la raison, à mesure que les entreprises exécutent leur stratégie cloud et multicloud, elles découvrent invariablement que la modernisation de l'infrastructure informatique s'avère à la fois hautement nécessaire et extrêmement difficile. Si les infrastructures de calcul et de stockage se sont largement alignées sur les architectures définies par logiciel et les services cloud, le réseau est resté bien trop souvent à la traîne, n'étant pas aussi agile ou orienté service que les autres éléments d'infrastructure.

Les DSI comprennent désormais, à un degré sans précédent, les mérites universels des architectures réseau et des services réseau cloud définis par logiciel, qui découplent l'innovation logicielle et la vitesse des fonctionnalités de l'infrastructure physique sous-jacente. Le découplage de l'aspect matériel et logiciel permet non seulement aux entreprises de proposer des services réseau agiles, mais aussi d'atténuer les contraintes sur la chaîne logistique en bénéficiant de la flexibilité liée au fait de disposer de plusieurs options physiques. Cette capacité est illustrée par le cas des fonctions virtualisées ou conteneurisées qui s'exécutent sur les plateformes physiques standard du secteur et l'utilisation de plans de contrôle et de gestion abstraits exécutés sur un substrat de plan de données, standardisé et basé sur des équipements physiques, prenant en charge les exigences associées aux services cloud à la demande.

Quoi qu'il en soit, IDC continue à estimer que de nombreux DSI négligent ou sous-évaluent la modernisation du réseau comme une nécessité à leur adoption du multicloud, pour découvrir tardivement (et souvent à un coût considérable) que cette modernisation est indispensable à la réussite du multicloud. Pendant ce temps, les entreprises qui ont rencontré ces problèmes (ou qui se sont penchées bien à l'avance sur ces considérations) reconnaissent le besoin d'une transformation réseau omniprésente.

L'avènement de l'architecture native cloud pour les applications, reposant sur des conteneurs et des microservices, accélérera le passage à la modernisation du réseau, en exposant davantage les limitations des approches rigides, définies par équipements physiques et faisant l'objet d'une surallocation, en matière de proposition de services réseau et de sécurité vitaux. Dans les environnements natifs du cloud, le réseau doit l'être tout autant que les applications qu'il soutient, afin de proposer le choix et la personnalisation des services, une échelle élastique, une programmabilité extensive et des intégrations basées sur API aux outils associés.

Un réseau cloud et multicloud doit être en adéquation étroite avec les besoins de l'application, afin de réagir à la vitesse de l'activité numérique. Au moment où un nombre croissant d'applications migrent vers le cloud, le réseau doit adhérer aux principes de ce dernier. Les architectures, les infrastructures et les méthodes opérationnelles traditionnelles ne disposent pas de l'agilité, de la flexibilité et des autres attributs cloud essentiels à l'ère du cloud. Elles se montrent trop fragiles, trop manuelles, trop lentes et trop sujettes aux erreurs pour rester en phase avec une activité numérique continue. L'architecture et l'infrastructure ne se révèlent pas uniquement obsolètes et complexes, incapables de prendre en charge le besoin de vitesse exigé par les entreprises numériques, elles ne parviennent pas non plus à fournir la sécurité requise, avec un

ensemble d'infrastructure de sécurité fragmenté ne générant que des goulets d'étranglement inefficaces et incomplets.

Comme les points précédents l'attestent, la nécessité d'une modernisation réseau axée sur le cloud s'avère claire et convaincante. Plus encore, la modernisation propose un éventail considérable d'avantages tangibles qui se répercutent de façon positive sur le service fourni et la réussite de l'entreprise.

Avantages

Un réseau multicloud à la fois bien défini (via la collaboration organisationnelle) et bien mis en œuvre peut proposer toute une gamme de possibilités en phase avec le cloud :

- » **Performances à la demande.** Tout comme le cloud, un réseau multicloud doit être à la demande, c'est-à-dire provisionné, déployé et disponible selon les besoins.
- » **Échelle élastique.** Tout comme les ressources cloud évoluent automatiquement selon les besoins, un réseau multicloud doit pouvoir le faire de manière similaire, conformément aux exigences des charges de travail cloud dynamiques.
- » **Agilité et vitesse.** Les infrastructures réseau traditionnelles et les pratiques opérationnelles qui les accompagnent sont désormais connues pour leur manque d'agilité. Un réseau multicloud, qui prend nécessairement en charge les charges de travail cloud distribuées, doit être agile et capable de fonctionner à la vitesse de l'activité numérique.
- » **Flexibilité et choix.** S'il s'agit toujours d'attributs désirables, la flexibilité et le choix sont devenus de plus en plus importants pour les acheteurs d'équipements informatiques des entreprises, dans le sillage de la pandémie de COVID-19 et des perturbations de la chaîne logistique qui en ont résulté. La flexibilité et le choix accordent aux entreprises la liberté d'agir rapidement et d'innover selon leurs propres conditions, afin de les aider à atteindre leurs objectifs opérationnels, comme une proposition de service plus rapide et une amélioration continue des services proposés.
- » **Sécurité cloud Zero Trust.** Grâce à une sécurité Zero Trust (c-à-d. à vérification systématique) complète et omniprésente, les équipes informatiques d'une entreprise peuvent s'assurer que les applications et les utilisateurs distribués sont protégés de manière proactive contre les menaces susceptibles de mettre en danger la disponibilité des services et l'expérience numérique.
- » **Observabilité omniprésente et en temps réel pour un processus de dépannage/résolution des problèmes plus rapides et des NetOps proactives.** Les entreprises poursuivant un modèle multicloud rencontrent souvent un ensemble de défis en termes de visibilité, notamment une visibilité intermittente ou partielle sur les différents clouds et toute une gamme d'angles morts. Pour accélérer le processus de dépannage/résolution et aider l'équipe des opérations informatiques à adopter une approche plus proactive de la disponibilité et des performances, les réseaux multicloud doivent disposer d'une visibilité et d'une observabilité omniprésentes et en temps réel. Cet aspect permet également de s'assurer que l'agilité n'est pas obtenue au détriment du contrôle.

- » **Réduction de coûts.** Intelligemment résilient et automatisé, un réseau cloud moderne doit, en définitive, faire en sorte que les perturbations et les pannes soient minimisées, que les opérations soient plus efficaces et productives, que les coûts matériels soient réduits et que les applications et les services n'aient pas attendre la disponibilité de l'infrastructure et des opérateurs réseau pour provisionner, configurer et prendre en charge manuellement les architectures et les infrastructures traditionnelles, définies par équipements physiques.

Cloudflare

Cloudflare a répondu au besoin de mise en réseau cloud et multicloud moderne par un ensemble croissant de services réseau, mais aussi de services pour applications et de services de sécurité, élargissant à la fois son applicabilité aux scénarios d'utilisation et son ubiquité géographique.

Le réseau Cloudflare couvre 275 villes à travers le monde et se connecte directement à 11 000 autres réseaux, notamment ceux d'éminents FAI, services cloud et sociétés privées, afin de permettre à une entreprise de tirer parti de données en temps réel sur l'ensemble de son réseau et d'améliorer les performances pour ses clients. Conçu pour prévenir les vastes attaques DDoS volumétriques, il présente une capacité réseau périphérique de 155 Tb/s et achemine les réponses à 95 % de la population mondiale connectée à Internet en 50 ms ou moins.

Les services commerciaux de Cloudflare peuvent être classés dans quatre catégories principales (les services pour applications, les services réseau, les services pour développeurs et les services de sécurité Zero Trust), toutes sous-tendues par l'infrastructure réseau de Cloudflare et ses produits pour développeurs.

Les services proposés par Cloudflare en matière d'amélioration de la sécurité et des performances des applications sont les suivants :

- » **Amélioration des performances des applications :** mise en cache/CDN, (Anycast) DNS, équilibrage de charge, transmission et diffusion vidéo (Cloudflare Stream), optimisation de contenu web (redimensionnement d'images, priorisation HTTP/2 et optimisation complète de pages), optimisation mobile (SDK mobile) et optimisation WAN.
- » **Amélioration de la sécurité des applications :** DNSSEC, protection anti-DDoS des couches 3/4, SSL/TLS, gestion des robots logiciels, protection contre les attaques DDoS de la couche 7, pare-feu d'applications Web (WAF), sécurité IdO, limitation du débit et sécurité du périmètre, pare-feu DNS et API/Page Shield (solution lancée en 2021).

Cloudflare One, la dernière plateforme de Cloudflare, prend en charge une architecture SASE unifiée. Elle se compose des éléments suivants :

- » Une plateforme SSE composable prenant en charge l'accès sécurisé, la sécurité du SaaS, la sécurité des e-mails, la passerelle Internet, l'isolation de navigateur et la prévention de perte de données.

- » Une offre de réseau en tant que service (Network-as-a-Service, NaaS) constituée de Magic WAN, Magic Firewall et Magic Transit.

Les services réseau de Cloudflare comprennent un pare-feu en tant que service (Firewall-as-a-Service, FaaS), une protection anti-DDoS des couches 3 et 4 basée sur proxy inverse, le WAN en tant que service (WAN-as-a-Service, WANaaS) et la solution Network Interconnect (interconnexion réseau), afin de permettre à la fois la connectivité aux adresses IP publiques et privées entre les datacenters, les bureaux régionaux et les sites des partenaires.

Les services d'amélioration des performances/de la sécurité et les services réseau proposés par Cloudflare reposent sur la solution de routage intelligent de l'entreprise. La solution de routage intelligent achemine le trafic autour du réseau, pour une latence réduite et une fiabilité accrue. La mise en cache par niveau intelligente, qui fait également partie de l'offre Argo, tire parti des mêmes données sur les performances et le routage afin de chercher de manière dynamique une origine pour les datacenters de haut niveau.

Basée sur une architecture sans serveur isolée, la plateforme Workers de Cloudflare est la suite pour développeurs phare du fournisseur. Grâce à Cloudflare Workers, les développeurs peuvent créer des applications sans serveur capables d'évoluer, sans devoir consacrer de temps et d'efforts à l'infrastructure ou aux opérations.

L'entreprise assure des services allant de la mise en œuvre à l'intégration, en passant par le support et le conseil. Elle dispose de centres d'assistance disponibles 24 h/24, 7 j/7, répartis sur les différents fuseaux horaires et implantés dans les lieux suivants : San Francisco, Austin, Kirkland, Londres, Lisbonne, Munich et Singapour, ainsi qu'au Japon. Les clients du portail en libre-service bénéficient d'une assistance par e-mail (offres gratuite, Pro et Business) et par chat (offre Business uniquement). La satisfaction client est mesurée à l'aide d'enquêtes envoyées après la fermeture des tickets de support.

Le modèle de commercialisation de Cloudflare est principalement axé sur le contact direct avec le client, bien que l'entreprise réalise également des ventes via ses partenaires le cas échéant. Elle segmente généralement ses clients en quatre catégories (clients stratégiques, clients de terrain, milieu de gamme et PME) et met en adéquation ses ressources de ventes/commercialisation avec les besoins uniques en matière de proposition, de sécurité et d'infrastructure informatique de ces segments. L'initiative Bandwidth Alliance de Cloudflare met en valeur l'approche de l'entreprise à l'égard de la collaboration avec d'autres fournisseurs de cloud dans l'optique de développer sa clientèle. Cloudflare se concentre particulièrement sur l'extension de ses partenariats OEM, comme ceux déjà conclus avec IBM, Rackspace et Aquila. Le fournisseur collabore avec les principaux fournisseurs de cloud, fournisseurs de colocalisation et opérateurs mondiaux (dont la majorité sont situés aux Amériques) afin d'étendre sa capacité et d'améliorer l'interconnectivité de ses clients. Il s'est également engagé dans diverses initiatives en faveur du développement durable, comme la conception d'un Internet vert et la réduction des émissions, bien qu'aucun objectif tangible ne soit actuellement disponible.

Défis

Cloudflare a connu une forte croissance depuis son OPI, mais l'entreprise fait face à plusieurs défis :

- » Elle doit améliorer ses services de diffusion de médias et en élargir la portée. Considérant l'impact toujours plus important du trafic vidéo sur Internet, Cloudflare devra mieux se positionner dans ce segment et proposer des services de diffusion de médias avancés, incluant notamment une protection du contenu, comme un système de gestion des droits numériques.
- » Cloudflare a développé avec succès son réseau et sa capacité ces dernières années, mais elle doit accroître la sensibilisation sur la manière dont ces développements ont renforcé les performances et la fiabilité de ses services de diffusion vidéo et dont l'entreprise prévoit de continuer à poursuivre cet objectif d'investissement dans les années à venir.
- » L'entreprise peut bénéficier d'une expansion de son activité intermédiaire afin de compléter ses efforts de vente directe. Une approche programmatique de la gestion des partenaires générera de nouvelles opportunités de croissance pour Cloudflare.
- » Cloudflare développe son activité à un rythme rapide. Elle doit investir dans la quantité et la qualité adéquates de ressources pour pérenniser sa réussite et maintenir sa dynamique.

Conclusion

Convenablement comprise, la transformation numérique s'est traduite par une importance accrue de l'activité numérique. Les applications, en particulier celles qui facilitent les interactions efficaces avec les utilisateurs, constituent le moteur des entreprises numériques. Ceci dit, les applications dépendent d'un « système nerveux numérique » prenant la forme d'un réseau moderne, capable de proposer des services de sécurité et des services réseau robustes et évolutifs sur un paysage de plus en plus complexe et distribué.

Pour les raisons explorées dans ce rapport, les entreprises de tous les secteurs et de toutes les régions géographiques reconnaissent de plus en plus que les réseaux ne peuvent demeurer en l'état dans le contexte actuel de transformation de l'infrastructure numérique. Si Cloudflare peut continuer à développer son catalogue en phase avec les évolutions des exigences des clients, IDC pense que la société pourra jouer un rôle précieux en aidant les entreprises à moderniser leurs architectures réseau, leur infrastructure et leurs modèles opérationnels afin de répondre aux besoins d'agilité numérique, de flexibilité, de performances, de fiabilité, d'échelle et de sécurité omniprésente.

À propos des analystes



Brad Casemore, vice-président Recherche chargé des datacenters et des réseaux multicloud

Brad Casemore occupe le poste de vice-président Recherche chargé des datacenters et des réseaux multicloud (Research Vice President, Datacenter and Multicloud Networks) chez IDC. Il couvre les équipements réseau physiques et logiciels des datacenters, ainsi que les services réseau IaaS proposés via le cloud et les technologies connexes, notamment les logiciels et les services de mise en réseau hybrides et multicloud, ainsi que les réseaux de transit. M. Casemore travaille également en étroite collaboration avec les analystes des pôles Réseaux d'entreprise, Serveurs, Stockage, Cloud et Sécurité d'IDC afin d'évaluer l'impact de l'informatique émergente, ainsi que de l'infrastructure convergente et hyperconvergente.



Ghassan Abdo, vice-président Recherche chargé des télécommunications mondiales, de la virtualisation et du réseau CDN

Occupant le poste de vice-président Recherche chargé des télécommunications mondiales, de la virtualisation et du réseau CDN, M. Abdo couvre l'évolution de l'écosystème cloud des télécommunications, ainsi que les services de mise en réseau virtualisés et émergents pour entreprises. Ses domaines de prédilection comprennent le SD-WAN et les services gérés pour fournisseurs de services, les services émergents de mise en réseau virtuelle basée sur la virtualisation des fonctions réseau (Network Function Virtualization, NFV) et les autres services WAN gérés.

MESSAGE DU SPONSOR

Plus d'informations sur Cloudflare

Cloudflare a développé une plateforme cloud mondiale offrant un vaste éventail de services. Cette dernière permet de mieux sécuriser les organisations, d'améliorer les performances de leurs applications et d'éliminer la complexité et les coûts liés à la gestion de chaque élément physique d'un réseau. Cette plateforme sert de plan de contrôle unifié, facile à utiliser et évolutif permettant d'assurer la sécurité, les performances et la fiabilité de l'ensemble des applications sur site, hybrides, cloud et SaaS (Software-as-a-Service, logiciel en tant que service).

Détail essentiel, chaque datacenter composant le réseau mondial de Cloudflare (qui s'étend sur plus de 275 villes à travers le monde) peut assurer chacun de ces services. La latence susceptible de compliquer la mise en œuvre de solutions cloud s'en trouve donc réduite. Rationalisez votre pile réseau, accélérez votre transformation et armez votre réseau pour la suite.

Pour en savoir plus, rendez-vous sur <https://www.cloudflare.com/fr-fr/cloudflare-one/>.



Le contenu de ce rapport a été adapté d'un rapport de recherche IDC existant publié sur www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, Massachusetts 02494,
États-Unis
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com

Cette publication a été produite par IDC Custom Solutions. Les opinions, les analyses et les résultats de l'étude présentés dans ce document sont tirés d'études et d'analyses plus détaillées conduites et publiées en toute indépendance par IDC, sauf lorsqu'il est fait mention d'un sponsoring spécifique. IDC Custom Solutions publie du contenu d'IDC sous divers formats susceptibles d'être diffusés par différentes sociétés. Une licence de diffusion du contenu d'IDC accordée à un titulaire ne signifie pas qu'IDC approuve celui-ci ou formule un avis à son égard.

Publication externe des données et informations d'IDC – toute information d'IDC destinée à être utilisée dans le cadre de publicités, de communiqués de presse ou de supports promotionnels doit préalablement faire l'objet du consentement écrit du vice-président ou du directeur du bureau local d'IDC concerné. Un projet du document proposé doit accompagner une telle demande. IDC se réserve le droit de refuser l'approbation de toute utilisation externe, quelle qu'en soit la raison.

Copyright 2022 IDC. Toute reproduction sans autorisation écrite est strictement interdite.