CLOUDFLARE

LIVRE BLANC

Résilience du réseau et des services de Cloudflare

Sommaire

Vue d'ensemble

Internet repose sur des systèmes imparfaits, conçus pour privilégier avant tout la disponibilité. Les protocoles comme TCP et BGP s'appuient sur les principes fondamentaux des systèmes distribués, à savoir anticiper et prendre en compte les défaillances, et l'architecture d'Internet reflète cette réalité. Cependant, des points de défaillance subsistent et peuvent avoir un impact réel. Les opérateurs de réseaux doivent être en mesure de planifier les défaillances, de les détecter lorsqu'elles surviennent et d'en atténuer l'impact sur l'expérience des utilisateurs.

En raison du fonctionnement en temps réel de nombreuses applications sur Internet, les réseaux doivent non seulement couvrir une large part d'Internet, mais doivent également réagir aux défaillances et en atténuer l'impact en temps réel. Des temps d'arrêt de quelques minutes sont inacceptables : les clients s'attendent à ce qu'un incident soit résolu en quelques secondes seulement.

Cloudflare fournit des services d'infrastructure réseau essentiels, qui aident les entreprises à maîtriser leur sécurité et leurs communications sur Internet. Nous avons conçu notre réseau et les services qu'il fournit avec l'objectif d'atteindre un niveau inégalé d'excellence opérationnelle. Cloudflare traite en moyenne plus de 84 millions de requêtes HTTP et 61 millions de requêtes DNS par seconde, fournissant ses services à des millions de propriétés Internet et d'internautes.

Comment Cloudflare parvient-il à proposer des services fiables avec une telle ampleur, compte tenu de l'imprévisibilité d'Internet ?

La réponse réside dans l'architecture du réseau Cloudflare, qui intègre des fonctionnalités de résilience conçues pour s'exécuter de manière indépendante et résister à un large éventail de perturbations. Nos fonctionnalités de calcul, de connectivité réseau et de stockage, ainsi que nos processus opérationnels, sont conçus pour permettre à Cloudflare d'offrir une fiabilité comparable à la tonalité du réseau téléphonique traditionnel. Cloudflare fournit une véritable « tonalité cloud » pour les services de connectivité réseau et de sécurité dont dépendent les clients, quelles que soient les conditions d'Internet à un instant donné.

Ce livre blanc examine en détail les défis liés à l'exploitation d'applications et de services en temps réel sur Internet et explique pourquoi Cloudflare bénéficie d'un positionnement unique pour les relever.

Vivre dans un monde imparfait

Internet est un environnement imparfait. Néanmoins, les entreprises ont besoin de lui pour développer leurs activités et exploiter des structures permettant de connecter des utilisateurs, des données et des appareils distribués à des applications hébergées dans le cloud. Toute interruption des services peut avoir de graves conséquences. Au fil des ans, Cloudflare a documenté de nombreuses perturbations importantes des services Internet à travers le monde, causées par des accidents, des attaques DDoS ou des catastrophes naturelles et bien d'autres événements.

Internet est un réseau hétérogène, constitué de milliers de réseaux participants faiblement interconnectés, de tailles et de capacités très variables. Ces réseaux offrent différents niveaux de service ; certains proposent des services limités dans le cadre d'une démarche fondée sur la bonne volonté, tandis que d'autres opèrent dans le cadre des services commerciaux qu'ils fournissent. Grâce à des accords mutuels d'échange de trafic, que ce dernier soit ou non destiné à des hôtes présents sur les réseaux des opérateurs, Internet fonctionne comme un maillage mondial reposant sur la participation bienveillante de points d'échange Internet et de fournisseurs de services régionaux et locaux.

Toutefois, cette diversité introduit une certaine imprévisibilité. Le chemin emprunté par un paquet repose sur une succession de suppositions approximatives et de mécanismes de « meilleur effort » visant à assurer sa transmission. En l'absence de données en temps réel ou de modèles prédictifs fondés sur les conditions réelles du réseau à un instant donné, le prochain saut d'un paquet est généralement défini en fonction d'itinéraires par défaut ou du chemin présumé le plus court. Les décisions de routage ne tiennent jamais compte de l'état du service réseau. Les paquets sont donc souvent affectés par des dégradations graves des conditions d'acheminement :

- Au niveau le plus élémentaire, les réseaux peuvent subir des incidents temporaires et des baisses de performances susceptibles de réduire le débit et d'entraîner des pertes de paquets.
- La saturation des réseaux entraîne des encombrements qui dégradent les performances et l'expérience des utilisateurs.
- Outre ces types de ralentissements, qui peuvent survenir dans des conditions d'utilisation normales, un nombre croissant de perturbations intentionnelles sont imputables à des acteurs hostiles, qui cherchent à épuiser les ressources disponibles à des fins malveillantes.

Chez Cloudflare, notre mission est de contribuer à bâtir un Internet meilleur et, à cette fin, nous construisons une infrastructure permettant de rendre Internet plus rapide, plus fiable et plus sûr. Cette démarche est rendue possible par les services exécutés depuis et par l'intermédiaire de l'un des plus grands réseaux du monde, constitué de serveurs « bare metal » (sans virtualisation), d'une infrastructure backbone privée et d'une immense présence mondiale accessible en moins de 50 ms, en moyenne, par 95 % de la population mondiale.[1]

Les clients souhaitent souvent comprendre comment nous y parvenons. Comment Cloudflare parvient-il à proposer des services avec une telle ampleur, sans induire de compromis entre sécurité et performances, en offrant le niveau de fiabilité dont les entreprises ont besoin ? La réponse tient à un ensemble d'objectifs directeurs qui définissent la manière dont nous concevons notre infrastructure, afin qu'elle reste performante malgré les perturbations, qu'elles soient internes ou externes.

Comment l'architecture de Cloudflare garantit la résilience

De nombreuses entreprises priorisent l'amélioration de la disponibilité, en essayant d'accroître ou d'accélérer leur réactivité face aux défaillances, ce qui nécessite pour elles d'investir et de tester continuellement leurs capacités et processus de basculement. Bien que ces objectifs soient légitimes, Cloudflare adopte une approche différente : nos équipes d'ingénieurs spécialistes de la résilience déploient des efforts considérables pour réduire les scénarios nécessitant une intervention de reprise après sinistre.

L'ingénierie de la résilience de Cloudflare repose sur un principe simple : **comment concevoir une infrastructure essentielle capable de rester opérationnelle en partant du principe que les défaillances sont inévitables ?**

Lorsqu'une défaillance survient inévitablement, les services résilients de Cloudflare détectent et isolent celle-ci, afin qu'elle n'affecte pas la disponibilité des services. Les défaillances sont gérées « hors bande », à l'écart de la chaîne de mise en œuvre de nos services. Nous aspirons à proposer des services agnostiques aux défaillances sur l'ensemble de notre parc.

Pour comprendre les principes de la résilience, il est utile de définir, dans un premier temps, les concepts fondamentaux sur lesquels reposent les chemins de trafic mis en œuvre par Cloudflare, ainsi que les objectifs de conception des systèmes essentiels. Au niveau le plus abstrait, l'architecture de Cloudflare peut être divisée en deux segments, **le plan de contrôle et le plan de données**, chacun disposant d'une stratégie unique de résilience et de gestion des incidents.

Résilience du plan de contrôle

Le plan de contrôle fournit l'interface de gestion qui établit la source d'informations exactes pour la configuration des services de connectivité réseau et de sécurité dans l'environnement du client. Le plan de contrôle lui-même ne traite pas le trafic (ce qui est le rôle du plan de données). Il indique au plan de données quelles politiques appliquer et gère les configurations entre les différents datacenters.

Les services de plan de contrôle de Cloudflare sont généralement déployés selon une topographie plus traditionnelle et centralisée, sur trois datacenters indépendants, mais sont logiquement liés, dans une région principale (par exemple, les États-Unis). Ces trois datacenters sont répliqués avec une capacité équivalente dans une région secondaire (par exemple, l'UE). Les services du plan de contrôle sont conçus pour être résilients et garantir la continuité de la mise en œuvre des services en cas de défaillance d'un datacenter unique sur le site géographique principal. La défaillance de datacenters supplémentaires sur le site géographique principal déclencherait un basculement vers les datacenters de l'autre région (par exemple, en Europe, plutôt qu'aux États-Unis).

Conformément à sa logique de priorisation de la résilience à la reprise, Cloudflare continue à investir dans le renforcement de sa stratégie de résilience.

Par exemple :

- Nous utilisons de plus en plus fréquemment les deux régions du plan de contrôle dans une configuration active-active, qui permet d'augmenter à la fois notre capacité et notre réactivité, ainsi que notre tolérance aux défaillances. Par conséquent, nous pouvons résister à davantage de types de défaillances sans interruption de service ni besoin de basculement.
- Nous augmentons également la granularité du déplacement des services entre les différents sites du plan de contrôle, ce qui nous permet de répondre avec plus de précision aux incidents affectant une infrastructure locale.

Tests de chaos

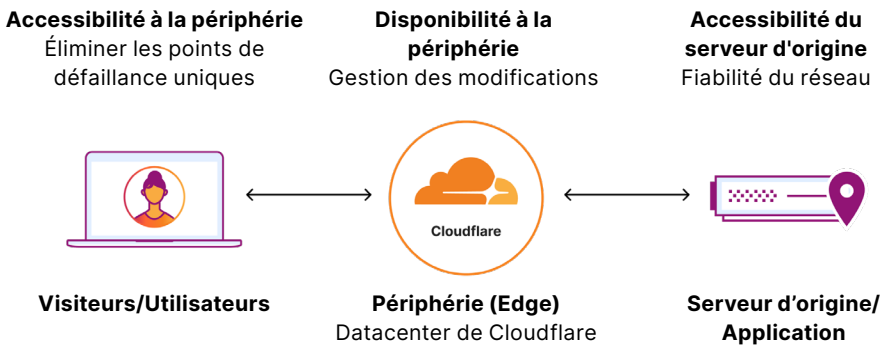
La résilience n'est pas une approche que l'on peut mettre en place, puis laisser de côté. Le « glissement » des systèmes, c'est-à-dire l'accumulation lente et souvent imperceptible de modifications susceptibles de dégrader les comportements souhaités et d'introduire des modes de défaillance imprévus, peut compromettre l'efficacité des programmes de résilience les plus robustes. Pour remédier proactivement à ce risque, Cloudflare réalise régulièrement des tests de chaos, en recherchant systématiquement les vulnérabilités potentielles liées à la dérive.

Résilience du plan de données

Le plan de données traite le trafic des clients de Cloudflare conformément aux politiques définies depuis le plan de contrôle. Bien que les services du plan de données reçoivent des instructions du plan de contrôle, leur fonctionnement ne dépend pas de lui. Toutes les politiques sont gérées depuis Quicksilver, notre référentiel clé-valeur distribué à l'échelle mondiale, garantissant que les services restent opérationnels avec une configuration connue et fiable en cas d'interruption des communications avec le plan de contrôle.

Anycast joue un rôle important dans la redondance des datacenters. Les datacenters de Cloudflare, présents dans plus de 330 villes, sont localement autonomes, mais également interchangeables, via la technologie Anycast et le protocole BGP. Chaque datacenter peut traiter n'importe quel service localement, sans dépendre des services exécutés dans un autre datacenter. Avec Anycast, chaque datacenter est redondant par rapport aux autres et, puisque chaque datacenter participe à Anycast, il n'est pas nécessaire de demander au client de basculer vers un autre datacenter, à une adresse IP différente.

Qu'il s'agisse d'un consommateur qui consulte un site web protégé par Cloudflare, d'un collaborateur qui accède à des applications connectées à Internet ou d'une agence qui se connecte à son réseau étendu (WAN), dans tous ces scénarios, le protocole BGP est utilisé pour rechercher le datacenter Anycast Cloudflare le plus proche. Si le datacenter préféré devenait indisponible, le protocole BGP basculerait automatiquement vers le datacenter Cloudflare le plus proche.



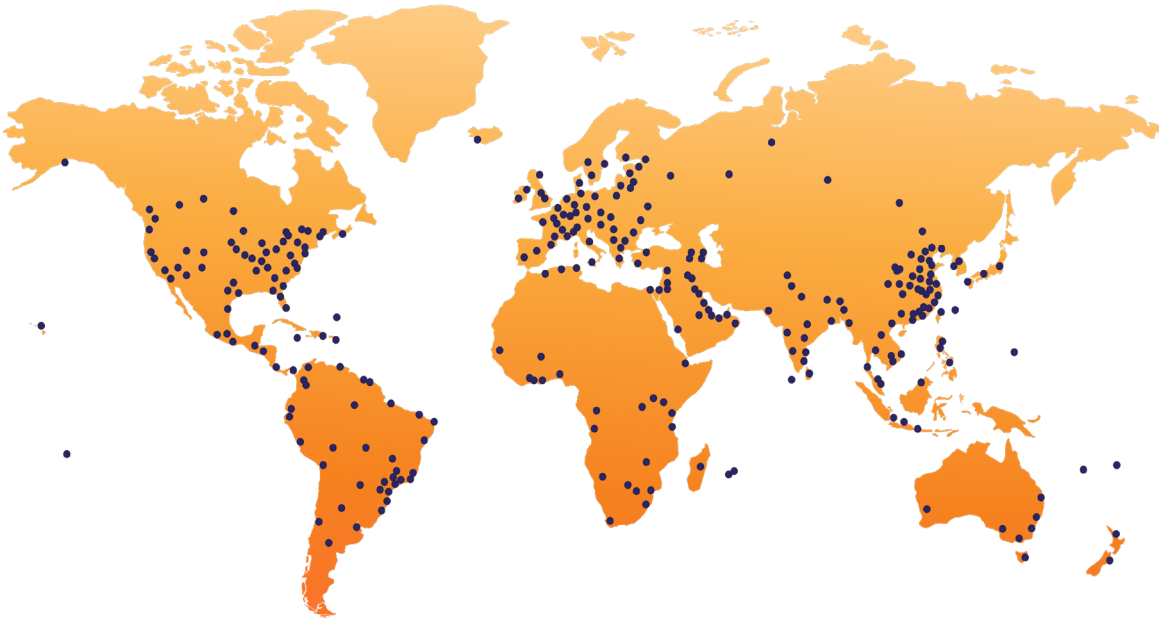
Pour assurer la résilience du plan de données, Cloudflare résout trois problèmes différents :

- Accessibilité à la périphérie : garantit que le trafic des utilisateurs finaux peut atteindre les datacenters et élimine les points de défaillance uniques au point d'entrée du trafic
- Disponibilité à la périphérie : préserve la qualité du code et la disponibilité des logiciels grâce à une gestion rigoureuse des modifications
- Accessibilité du serveur d'origine : routage adaptatif vers les applications des clients afin de garantir l'absence de pertes de données sur les chemins de trafic sortant

Accessibilité à la périphérie

L'accessibilité à la périphérie désigne la capacité des utilisateurs finaux à atteindre le réseau de Cloudflare. Il s'agit sans doute de l'aspect le plus important de la problématique de la résilience. En cas de défaillance d'un fournisseur d'accès Internet (FAI) ou d'un datacenter, l'accessibilité à la périphérie est réduite ou dégradée, ralentissant ou interdisant l'accès des utilisateurs aux ressources qu'ils souhaitent consulter sur Internet. Cloudflare répond de quatre manières essentielles aux problèmes d'accessibilité à la périphérie :

1. Réseau Anycast



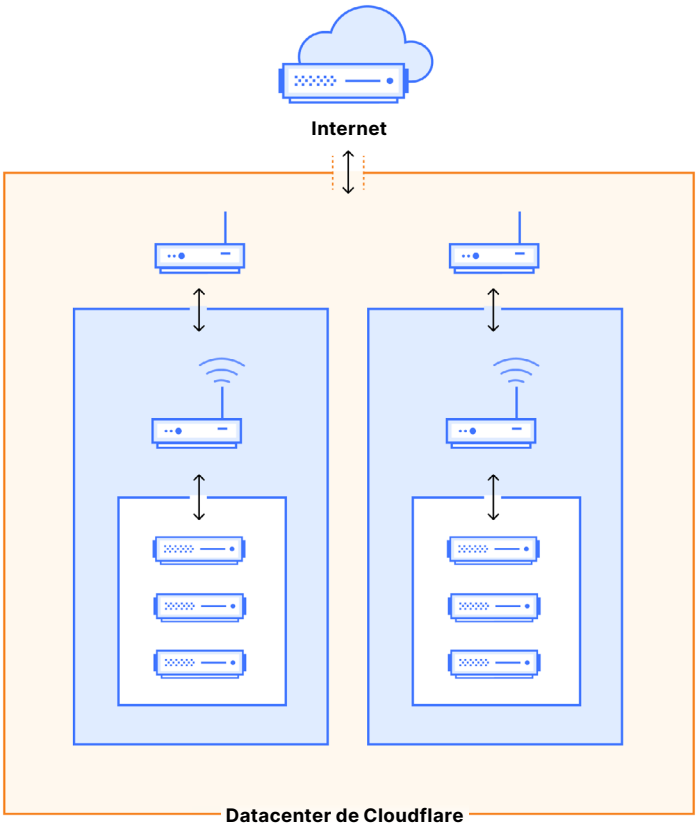
Notre architecture réseau, qui dépend fortement de la technologie Anycast, intègre des fonctionnalités d'amélioration des performances et de la résilience. Avec Anycast, le super-pouvoir qu'utilise l'ingénierie de Cloudflare, l'espace IP est annoncé partout : si l'un de nos points de présence (PoP, « Point of Presence ») est hors ligne, le trafic est simplement redirigé vers d'autres sites, au lieu d'être abandonné. La présence du réseau Cloudflare dans de nombreuses villes à travers le monde et son interconnexion avec les réseaux locaux nous permet de traiter le trafic client au plus près des utilisateurs. Ainsi, même en cas de déconnexion du transit d'un fournisseur d'accès Internet ou de défaillance d'un datacenter, l'acheminement du trafic n'est pas perturbé.

2. Chaque service Cloudflare s'exécute sur chaque site

En complément de la technologie Anycast, les datacenters Cloudflare sont conçus pour traiter le trafic localement, sans dépendre de chaînes de proxy vers d'autres ressources de calcul. Chaque machine exécute pratiquement tous les services ; ainsi, un datacenter peut être mis hors ligne sans perturber l'expérience des clients. Toutes les machines dans un datacenter sont interchangeables ; en effet, des centaines de machines exécutent le même service et peuvent prendre le relais en cas de défaillance d'une machine donnée.

3. Points de présence multi-colocalisation

La conception et la localisation des datacenters de Cloudflare reflètent les besoins de nos clients. Un réseau Anycast nous permet d'ajouter ou de supprimer des datacenters à notre convenance, mais nous devons continuellement surveiller les performances des clients. Nous avons adapté les topologies de nos datacenters afin d'assurer qu'une défaillance d'une section de capacité de calcul (ou « colocalisation ») ne perturbe pas le fonctionnement des autres. Ces datacenters (comportant plusieurs colocalisations) sont appelés « points de présence multi-colocalisation », ou sites MCP.



Ces sites séparent la connectivité Internet de la connectivité de calcul interne, permettant la mise hors ligne individuelle des colocalisations. Ainsi, même en cas d'incident affectant une colocalisation, l'ensemble du PoP d'une région peut rester en ligne, offrant une disponibilité et des performances supérieures aux clients. Ce type de datacenter élimine également les points de défaillance uniques grâce au déploiement d'équipements redondants au niveau de la couche connectée à Internet : en cas de défaillance d'un routeur (de périphérie) connecté à Internet, l'autre routeur de périphérie peut assurer le traitement du trafic afin de préserver le bon fonctionnement du site.

Ce modèle opérationnel aide les sites MCP à éviter les transferts de trafic, sauf en cas d'absolue nécessité, et augmente encore davantage la disponibilité pour les clients de Cloudflare.

4. Cloudflare Traffic Manager

Les datacenters MCP fonctionnent ensemble pour former le réseau Cloudflare au sens large. Ce réseau utilise la technologie Anycast afin de contribuer à assurer la transmission du trafic des clients. En plus d'Anycast, nous mettons en œuvre une gestion déterministe du trafic afin d'assurer que les requêtes de clients sont traitées par des sites qui sont en mesure de les traiter, avec les meilleures performances possibles. Ce système de gestion du trafic, appelé Traffic Manager, fonctionne en sondant continuellement le réseau de Cloudflare et en détournant automatiquement le trafic des datacenters dont les processeurs sont surchargés. Cette approche permet d'éviter les encombrements dans les datacenters présentant un trafic important ; au lieu de cela, le trafic est acheminé intelligemment vers un autre datacenter capable de le traiter.

Disponibilité à la périphérie

La disponibilité à la périphérie fait référence à la capacité de Cloudflare à traiter le trafic lorsqu'il arrive sur notre réseau. Lorsque des modifications apportées aux outils ou aux logiciels réseau entraînent des changements imprévus, la disponibilité peut être réduite et altérer l'expérience utilisateur. Afin d'éviter les incidents résultant d'une modification du code, Cloudflare a lourdement investi dans les mesures de contrôle du déploiement suivantes :

1. Entonnoir de déploiement

Lors du déploiement d'un logiciel, garantir la qualité du code exige tout d'abord de suivre et de limiter la capacité des développeurs et des clients à introduire des modifications dans l'écosystème. Cloudflare limite le nombre d'approches permettant à un utilisateur d'introduire des modifications dans notre infrastructure. Cela nous permet de surveiller précisément chaque modification et de nous assurer qu'elle fait l'objet d'une série de tests complète avant d'être déployée en production.

2. Gestion du périmètre d'impact des modifications

Cloudflare soutient également la disponibilité à la périphérie pendant le déploiement en limitant les déploiements aux datacenters de test ou aux groupes de test avant leur déploiement à grande échelle. C'est ce que nous appelons la « gestion du périmètre d'impact des modifications ».

Lorsque des modifications sont déployées sur le réseau, elles peuvent être mises en œuvre dans le monde entier en quelques minutes seulement. En limitant les modifications à un environnement de déploiement et en implémentant d'autres modifications en cascade, nous pouvons surveiller les effets d'une modification afin d'en évaluer les conséquences, prévues ou imprévues, avant qu'elle n'affecte des régions géographiques plus étendues ou des populations d'utilisateurs plus importantes.

Nous disposons de deux moyens pour limiter l'impact des modifications apportées au code :

- Limiter le nombre de sites qui reçoivent des modifications ; et
- Limiter le nombre d'utilisateurs qui reçoivent des modifications

En limitant le nombre de sites et de machines qui reçoivent les modifications, nous pouvons nous assurer que nous réalisons correctement les tests A/B du code sur un site unique, afin d'évaluer son intégrité avant de poursuivre. En limitant le nombre d'utilisateurs recevant des modifications, nous pouvons commencer par tester les correctifs sur des populations plus petites.

3. Déploiement fondé sur l'intégrité

Le déploiement fondé sur l'intégrité est un système qui évalue programmatiquement la pertinence d'une version en fonction d'indicateurs prédéfinis, puis produit une décision de validation ou de refus en fonction de l'impact potentiel. Cette série de vérifications automatisées permet non seulement d'empêcher le lancement d'une version préjudiciable, mais permet également d'annuler une version en cas de détection d'un impact dommageable.

Chaque produit et service déployé via Cloudflare doit comporter un objectif de niveau de service (SLO, Service Level Objective) réunissant à la fois un indicateur représentant l'intégrité du produit et une valeur cible en dessous de laquelle le produit serait considéré comme défaillant.

Les SLO comportent des degrés de consommation de budget d'erreur, c'est-à-dire des seuils de défaillance acceptables. Tout service dont les performances sont fondées sur l'intégrité fournit des SLO à un système automatisé dans le cadre de l'intégration d'une modification à déployer. Quelle que soit la portée du déploiement (offres gratuites, sous-ensemble de machines à Ashburn, etc.), le système automatisé :

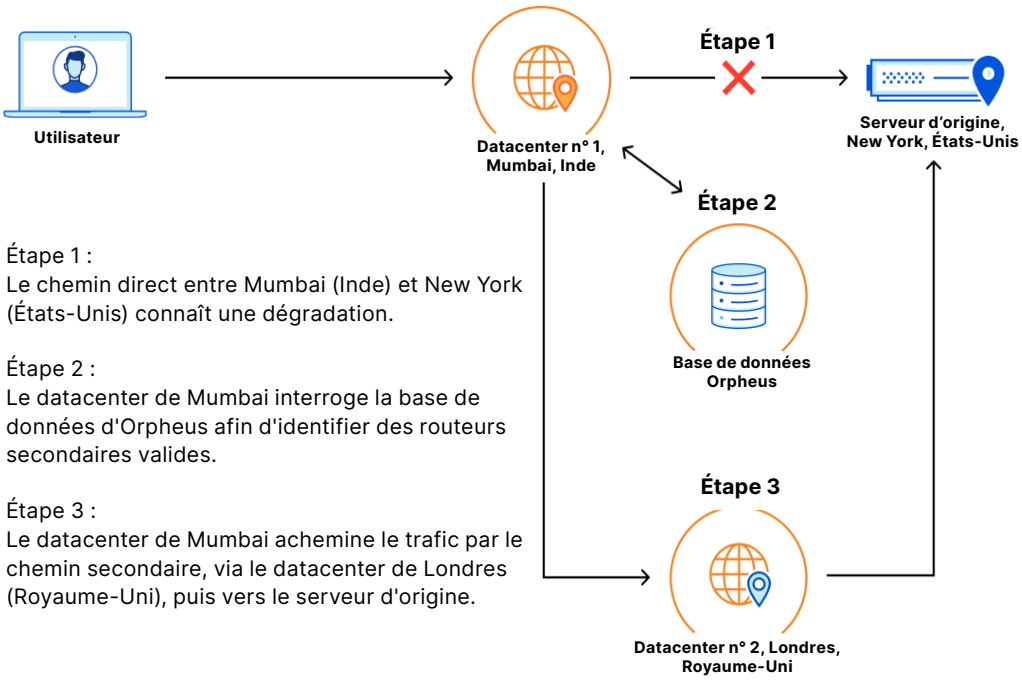
- Dans un premier temps, surveille le SLO du service pendant une période définie, afin d'assurer que l'intégrité ne chute pas sous le seuil établi.
- Si le SLO reste conforme à des plages acceptables pendant toute la durée de la période d'observation définie, le système fait automatiquement progresser l'ampleur du déploiement.
- Cependant, en cas de violation du SLO, le système interrompt automatiquement le déploiement et effectue une restauration, afin d'atténuer automatiquement les effets de la modification.

Ces étapes garantissent que l'intégrité du client n'est pas affectée par des déploiements de code et que la durée reste aussi courte que possible.

Accessibilité du serveur d'origine

L'accessibilité des serveurs d'origine fait référence à la capacité de Cloudflare à atteindre les destinations, qu'il s'agisse du serveur d'origine d'un client, d'un site SaaS ou de l'Internet public via Cloudflare Gateway. Le routage des requêtes vers leur destination est essentiel pour les utilisateurs qui accèdent au réseau de Cloudflare. Par exemple, Argo Smart Routing, l'outil de Cloudflare permettant d'optimiser les performances du réseau (notamment la valeur de temps jusqu'au premier octet), sonde continuellement le réseau de Cloudflare afin d'identifier le chemin le plus rapide vers les serveurs d'origine.

Orpheus, le pendant d'Argo, repose sur une philosophie similaire, mais sa fonction est différente. Orpheus a pour finalité d'établir des connexions fiables avec les serveurs d'origine. Orpheus examine spécifiquement les indicateurs qui déterminent la capacité de Cloudflare à atteindre les serveurs d'origine (par opposition au chemin le plus rapide vers un serveur d'origine) et identifie les chemins permettant de minimiser la perte de paquets sans affecter les performances dans un état stable. Ainsi, en cas d'incident, le trafic est automatiquement redirigé de manière à contourner les erreurs détectées.



Avant le lancement d'Orpheus en 2021, Cloudflare était en mesure d'acheminer avec succès 99,9 % du trafic vers les serveurs d'origine. Depuis la mise en œuvre d'Orpheus, notre capacité à acheminer le trafic vers les serveurs d'origine a progressé jusqu'à atteindre 99,99 %. Au cours de l'année à venir, nous allons étendre Orpheus afin de protéger davantage de types de trafic, d'agir sur davantage de scénarios de défaillance et de travailler plus rapidement, afin de réduire la durée des perturbations pour les utilisateurs.

Engagement envers la transparence opérationnelle

Même les réseaux les plus résilients et les plus innovants connaîtront des défaillances. Lorsqu'un incident se produit et affecte des clients, Cloudflare suit une procédure de réponse aux signalements d'incident comprenant une enquête approfondie, l'établissement de rapports interne et externe sur l'incident et, si nécessaire, des mises à jour concernant le traitement de l'incident pendant toute la durée de la perturbation.

Dans certains cas où les incidents ont entraîné ce type d'impact (ou donné naissance à une innovation), des analyses après incident sont publiées sur le blog de Cloudflare.

Conclusion

Le travail d'ingénierie sur lequel repose le réseau Cloudflare n'est pas des plus simples, mais c'est un travail que nous sommes fiers d'accomplir pour nos clients. La récompense réside dans la création d'une plateforme réseau qui soutient nos clients et l'ensemble de la communauté Internet.

En priorisant la résilience, pas uniquement comme une préoccupation technique, mais comme une philosophie opérationnelle fondamentale, nous faisons bien plus que renforcer nos défenses : nous bâtissons activement une entreprise qui est intrinsèquement prête pour l'avenir. Notre approche proactive consistant à tester et à adapter continuellement nos solutions nous permet d'évoluer avec fluidité, en nous adaptant aux exigences toujours changeantes de nos clients et au panorama dynamique d'Internet lui-même.

Nous sommes conscients que bon nombre d'informations présentées dans ce document s'articulent autour de concepts de connectivité réseau dont de nombreuses entreprises n'ont pas connaissance, car ils concernent l'architecture interne sur laquelle repose le fonctionnement d'un environnement de cloud mondial d'opérateur.

Si vous souhaitez bénéficier d'une séance d'information approfondie pour en savoir plus sur l'ingénierie de la résilience de Cloudflare, contactez votre représentant Cloudflare.

01 73 01 52 44 | enterprise@cloudflare.com | www.cloudflare.com/fr-fr/

RÉV. : BDES-8251.2025OCT28