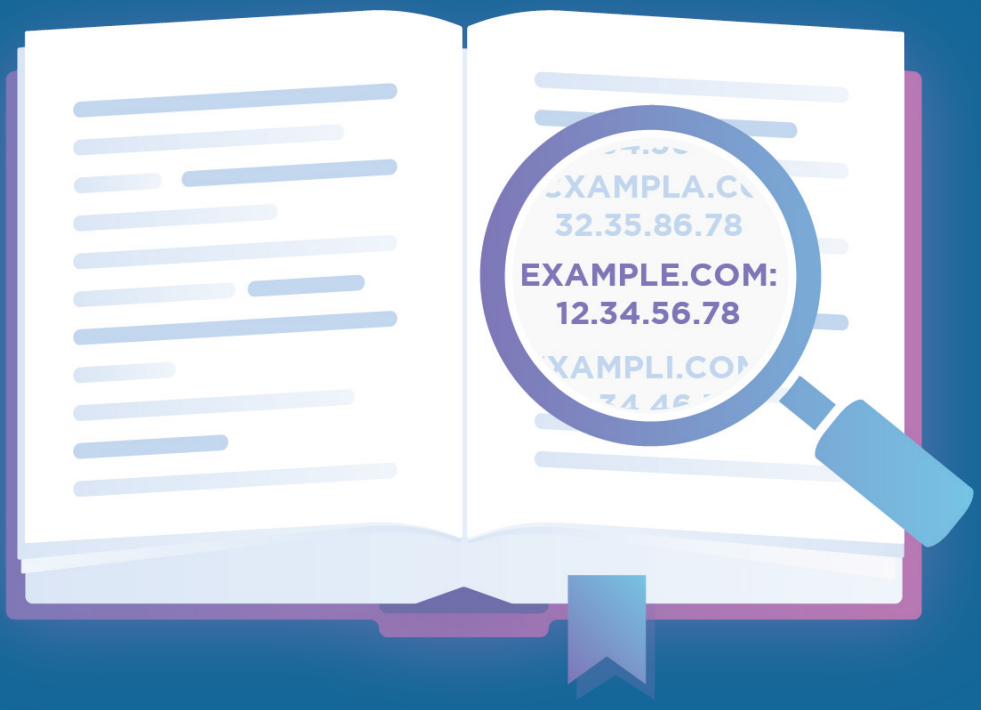
CLOUDFLARE®

Utiliser le DNS pour améliorer la navigation en ligne



+33 75 7 90 52 73 | enterprise@cloudflare.com | www.cloudflare.com/fr-fr/

I. Résumé

La rapidité de votre site web est celle de votre DNS, indépendamment de la structure du site ou de l'endroit où il est hébergé.

Lorsqu'il est utilisé et correctement configuré, le DNS peut améliorer considérablement la sécurité, les performances et la fiabilité d'une propriété Internet. Cependant, l'infrastructure DNS est très vulnérable à un large éventail de cyberattaques, de plus en plus courantes, qui peuvent dégrader les performances des serveurs DNS ou les mettre complètement hors service. Face à ces attaques, étant donné les attentes croissantes des utilisateurs en matière de performances et de disponibilité des sites web, il est risqué que le DNS soit un point de défaillance unique.

La sécurité, les performances et la fiabilité des sites nécessitent une sécurité DNS complète et une infrastructure DNS redondante optimisée pour les performances.

II. Sécurité DNS : un maillon faible de la cybersécurité en entreprise

L'infrastructure DNS utilisée aujourd'hui a été conçue dans les années 1980, lorsque l'accès à Internet était réservé aux organismes étatiques, aux scientifiques et aux militaires. Les architectes du système étaient préoccupés par la fiabilité et la fonctionnalité, et non par la sécurité.[1]

Tributaires de ce passé, les serveurs DNS d'aujourd'hui sont vulnérables à un large éventail d'attaques, notamment les attaques par usurpation d'identité, logiciels malveillants ou détournement de DNS ou DOS/DDoS. Ces attaques se produisent de plus en plus fréquemment et deviennent de plus en plus coûteuses. Selon le rapport mondial de l'IDC de 2019 sur les menaces DNS :

- 82 % des entreprises ont subi une attaque DNS ces deux dernières années
- Des augmentations importantes d'une année sur l'autre ont été signalées pour tous les types d'attaques, depuis les attaques de faible puissance jusqu'aux attaques volumétriques
- Le coût moyen par attaque a dépassé le million de dollars en 2019, soit une hausse de 49 % par rapport à l'année précédente [2]

Les attaques DNS sont souvent employées parallèlement à d'autres cyberattaques, souvent pour servir d'écran de fumée destiné à tromper le personnel de sécurité. Verizon estime que les attaques DNS sont impliquées dans environ un tiers des violations de données.[3]

Optimiser le DNS pour la sécurité

Étant donnée la grande diversité des menaces DNS, il convient, pour les contrer de manière efficace, d'adopter une stratégie multidimensionnelle qui comprend les éléments suivants :

- **Activez DNSSEC**, un ensemble de protocoles de sécurité qui vérifie les enregistrements DNS à l'aide de signatures cryptographiques. En s'assurant que la signature d'un site correspond à son enregistrement, les résolveurs de DNS peuvent authentifier le serveur d'origine des données envoyées depuis le serveur DNS et empêcher ainsi l'usurpation d'identité.

- **Utilisez des stratégies de limitation des attaques DDoS à plusieurs niveaux**, notamment en filtrant le trafic en appliquant la limitation de débit (rate limiting), en dressant une liste blanche et une liste noire d'adresses IP et en surveillant les connexions pour bloquer les requêtes malveillantes tout en autorisant le trafic légitime. En plus d'améliorer la sécurité, la limitation des attaques DDoS améliorera également la fiabilité et les performances en empêchant le trafic malveillant de submerger les serveurs DNS.

- **Mettez en place des pare-feux DNS** (filtrage DNS et blocage DNS) pour bloquer l'accès depuis des domaines malveillants connus.

- **Activez la journalisation DNS**. En plus de vous avertir si un pirate tente de s'introduire dans vos serveurs DNS, la journalisation DNS permet d'avoir une visibilité sur les problèmes de recherches DNS ou de mises à jour.

- **Imposez le HTTPS**. En obligeant les navigateurs à toujours charger les sites web en HTTPS, vous empêcherez l'usurpation de domaine en authentifiant chaque site avec un certificat SSL/TLS.

- **Maintenez les serveurs DNS à jour.** Les mises à jour comportent en général d'importants correctifs de sécurité.

III. Performances DNS : La lenteur des recherches DNS se traduit par une latence élevée

Lorsque les utilisateurs accèdent à un contenu sur internet, leurs appareils envoient une requête à un résolveur de DNS qui associe le nom de domaine du contenu et son adresse IP, puis renvoie la bonne adresse IP aux appareils. Chaque fois qu'un utilisateur accède à une nouvelle page dans son navigateur, il doit effectuer au moins une recherche DNS. De nombreuses pages chargent des contenus sur plusieurs domaines, ce qui nécessite plusieurs recherches. Ce processus s'appelle la résolution DNS. Le temps nécessaire pour résoudre chaque domaine demandé se cumule rapidement. L'optimisation de la vitesse de la résolution DNS est par conséquent essentielle pour obtenir une latence faible.

Tous les fournisseurs de services DNS n'ont pas optimisé la vitesse de résolution. Un fournisseur de services DNS lent peut mettre plus de 120 ms à résoudre chaque requête DNS.[4] Les fournisseurs de services DNS les plus rapides résoudront les requêtes en moins de 20 ms. Le DNS de Cloudflare, par exemple, résout les requêtes en moins de 12 ms en moyenne.[5]

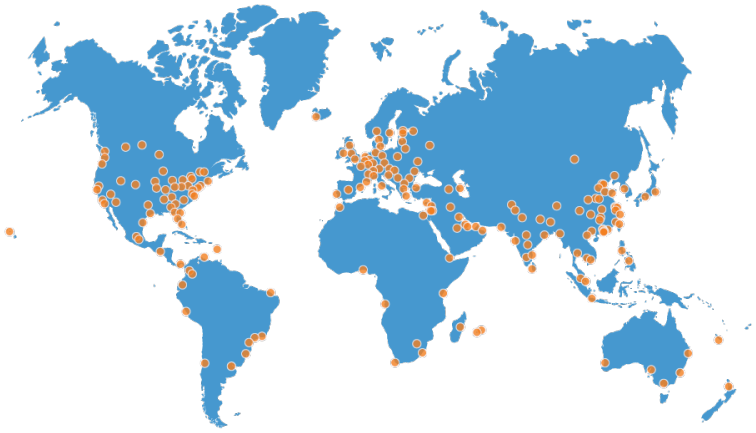
- Aujourd'hui, les internautes veulent que les contenus numériques se chargent instantanément. Même les plus petits désagréments peuvent avoir un impact négatif visible sur les taux d'engagement et de conversion.
- Une augmentation de seulement 100 à 400 ms de la latence d'un site a un impact mesurable sur le comportement des consommateurs[6]
- Le taux de conversion baisse de 7 % pour une seule seconde supplémentaire de temps de chargement[7]
- Environ la moitié des utilisateurs d'appareils mobiles souhaitent que les applications répondent en moins de deux secondes[8]
- Google utilise la vitesse de chargement des pages comme critère de classement des résultats de recherche sur ordinateur et sur les appareils mobiles[9]

Optimiser le DNS pour améliorer les performances

Voici quelques conseils qui vous permettront d'obtenir de bonnes performances dans un marché où chaque milliseconde compte.

- **Utilisez le routage mondial basé sur la géolocalisation**. Chaque fois qu'une requête d'un utilisateur parcourt une distance géographique de 160 km pour obtenir des ressources numériques, cela représente environ 0,82 ms de latence, [10], il est donc important de géo-orienter les visiteurs vers l'infrastructure DNS située près du lieu où ils se trouvent.
- **Déterminez le TTL optimal**. Le TTL (Time To Live) contrôle indirectement la mise en cache du résolveur DNS. Un TTL bas peut dégrader les performances, mais peut faciliter l'équilibrage de charge basé sur le DNS. Un TTL élevé améliore les performances, mais peut diriger les utilisateurs vers un serveur mis en cache et ayant été depuis mis hors service. Étant donné le grand nombre de variables en jeu, il n'existe aucun paramétrage optimal universel pour le TTL.
- **Utilisez anycast.** Cherchez un fournisseur de services DNS Anycast, ce qui permet à plusieurs serveurs de noms DNS distribués à l'échelle mondiale d'annoncer la même adresse IP. Anycast améliore la vitesse de résolution DNS et fournit également une protection par basculement DNS parfaite.

Déplacez votre DNS vers la périphérie du réseau



11 ms
Vitesse moyenne de résolution DNS

<5 seconds
for worldwide DNS propagation

IV. Fiabilité DNS : la redondance empêche les temps d'arrêt

Si les problèmes de latence ne sont pas traités, votre site web, dans le pire des cas, peut devenir inaccessible. Le coût des temps d'arrêt est élevé et en constante augmentation. En 2010, le coût moyen par minute de panne dans un centre de données était de 5 617 $ US. En 2016, ce montant s'élevait à à 8 851 $ US.[11]

Dans la mesure où la fiabilité du DNS a un impact direct et important sur les résultats des entreprises, toute entreprise doit tendre vers un taux de disponibilité de 100 %. Bien que cet objectif puisse paraître ambitieux, il est atteignable si ces dernières adoptent une stratégie à facettes multiples axée sur la redondance.

Optimiser le DNS pour accroître la fiabilité

La performance et la fiabilité vont de pair : elles forment un ensemble indissociable. Les unes ne peuvent pas exister sans l'autre. Toutes les mesures que vous prenez pour améliorer la fiabilité amélioreront également les performances. Par exemple, l'utilisation de deux fournisseurs de services DNS améliore les temps de chargement des pages, car la résolution des serveurs de noms se fera par défaut avec le fournisseur de services DNS le plus rapide.

- **Fournisseurs de services DNS doubles (principal/secondaire)**. Dans une configuration DNS à fournisseur unique, tous les utilisateurs reçoivent les réponses de l'ensemble des serveurs de noms de ce fournisseur, ce qui rend les sites vulnérables aux pannes du fournisseur. L'ajout d'un deuxième fournisseur de services DNS a pour effet de doubler le nombre de serveurs de noms disponibles pour ces domaines. Si le fournisseur faisant autorité n'est pas disponible, le trafic des requêtes est automatiquement acheminé vers les serveurs de noms de secours.
- **DNS basé sur le cloud**. Peu d'entreprises ont les ressources et l'expertise internes nécessaires pour gérer leurs propres serveurs DNS. L'externalisation vers un fournisseur de services DNS basé sur le cloud permet d'améliorer les performances, la fiabilité et la sécurité, de minimaliser les coûts et de permettre aux techniciens informatiques de l'entreprise de se consacrer à des projets internes.
- **Segmentation du serveur de noms**. Certains fournisseurs de services DNS regroupent plusieurs de leurs clients, voire tous, dans le même enregistrement de serveur de noms. Si un client subit une attaque DDoS, tous ses « voisins » sont gravement impactés. Assurez-vous que votre fournisseur de services DNS segmente son réseau afin que seul un petit nombre de clients partagent des enregistrements de serveur de noms.
- **Un très grand réseau mondial de nœuds DNS**. Le réseau DNS de votre fournisseur doit inclure un grand nombre de nœuds DNS répartis dans le monde entier. Ainsi, si un nœud tombe en panne, le trafic peut être acheminé vers l'un des nœuds restants. Un réseau mondial permet également le géo-guidage qui a pour effet d'améliorer les performances.
- **Équilibrage de charge mondial et local** . En plus de veiller à ce qu'aucun serveur ne soit surchargé, si un serveur vient à tomber en panne, un équilibreur de charge redirige le trafic vers les serveurs restants.

V. Conclusion

Dans le marché numérique actuel en perpétuelle évolution, quelques millisecondes de temps de chargement peuvent améliorer ou détériorer la navigation de vos utilisateurs et leur taux de conversion. Les performances et la fiabilité des sites web dépendent de la vitesse de résolution DNS, mais les serveurs DNS sont extrêmement vulnérables à un large éventail de cyberattaques. Afin de diposer d'une infrastructure DNS sécurisée hautement performante avec une disponibilité de 100 %, il est important se doter d'un dispositif complet garantissant la sécurité, la fiabilité et les performances du site de l'entreprise.

VI. Ce que peut vous apporter Cloudflare

Cloudflare propose un service DNS d'entreprise faisant autorité qui s'appuie sur de nombreuses bonnes pratiques. Ce dernier offre le temps de réponse le plus rapide du marché, une redondance inégalée et une sécurité avancée avec sa protection contre les attaques DDoS et son DNSSEC intégré. Pour en savoir plus et discuter avec un membre de notre équipe, rendez-vous sur www.cloudflare.com/dns/.

Notes de fin

1. ICANN, « DNSSEC - De quoi s'agit-il et pourquoi est-ce important ? » https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-fr . Consulté le 27 janvier 2020.
2. IDC, « Rapport mondial sur les menaces DNS 2019 », https://www.efficientip.com/resources/idc-dns-threat-report-2019/. Consulté le 26 janvier 2020.
3. Global Cyber Alliance, « The Economic Value of DNS Security », https://www.globalcyberalliance.org/wp-content/uploads/Economic-Value-of-DNS-Security-GCA-2019.pdf. Consulté le 27 janvier 2020.
4. Mann, Bill. « The Best DNS Servers for Speed and Privacy in 2019. » Blokt, https://blokt.com/guides/best-dns-servers. Consulté le 27 janvier 2020.
5. « DNS Performance Analytics and Comparison. »https://www.dnsperf.com/. Consulté le 23 juillet 2019.
6. Brutlag, Jake. « Speed Matters », Google AI Blog, https://ai.googleblog.com/2009/06/speed-matters.html. Consulté le 27 janvier 2020.
7. Rodman, Tedd. « Marketing & Web Performance: How Site Speed Impacts Metrics », Yotta, https://www.yottaa.com/marketing-web-performance-101-how-site-speed-impacts-your-metrics. Consulté le 27 janvier 2020.
8. Dimensional Research. « Failing to Meet Mobile App User Expectations: A Mobile App User Survey »,https://techbeacon.com/sites/default/files/gated_asset/mobile-app-user-survey-failing-meet-user-expectations.pdf. Consulté le 27 janvier 2020.
9. « Using page speed in mobile search ranking », Google Webmaster Central Blog, https://webmasters.googleblog.com/2018/01/using-page-speed-in-mobile-search.html. Consulté le 27 janvier 2020.
10. Sherman, Fraser. « Network Latency Milliseconds Per Mile », Techwalla, https://www.techwalla.com/articles/network-latency-milliseconds-per-mile/ Consulté le 27 janvier 2020.
11. Priceonomics Data Studio. « Quantifying the Staggering Cost of IT Outages », https://priceonomics.com/quantifying-the-staggering-cost-of-it-outages/. Consulté le 27 janvier 2020.