

Soldes : les précautions que doivent prendre les e-commerçants

Les soldes de début d'année sont synonymes de pic d'activité pour les e-commerçants, et ce pic devrait se prolonger jusqu'au 21 février. Pour s'assurer une bonne saison, les e-commerçants doivent se préparer. Un dysfonctionnement - qu'il s'agisse de l'indisponibilité des services ou un ralentissement général - engendrera une diminution du chiffre d'affaires mais aussi une insatisfaction des consommateurs. Infrastructure, sécurité, tout doit être passé en revue.

Prudence est mère de sûreté

En cas de pic d'activité, la prudence est à privilégier. L'e-commerçant doit évaluer la capacité actuelle de son site : combien de visiteurs simultanés le site peut-il supporter ? Le site est-il capable de gérer tous les utilisateurs sans que les accès soient perturbés ? Une des premières indications est d'analyser l'audience habituelle du site et de regarder la marge de manoeuvre. Il faut prévoir en moyenne une audience multipliée par 3 - mais ce chiffre peut être encore plus conséquent si l'e-commerçant lance une grande campagne de promotions et de communication.

A l'approche des soldes - les boutiques « physiques » renforcent leurs équipes et leurs stocks. Les e-commerçants doivent suivre la même stratégie en analysant les éléments les plus critiques afin de les renforcer.

Les sites de vente en ligne, conformément au standard PCI/DSS, doivent procéder à des audits réguliers. Mais, dresser le bilan de ses forces et faiblesses avant le pic peut permettre de révéler quelques points d'amélioration essentiels. La base de données est - par exemple - l'un des éléments clés. Si elle n'est pas optimale, toute l'activité du site sera ralentie. De la même manière, des caches peuvent aussi être mis en place pour alléger l'affichage des images ou des feuilles de styles, particulièrement importantes pour attirer le client. Tout doit être pensé pour éviter les ralentissements qui pourraient décourager les clients.

Dans la même optique, il faut également réaliser un test de charge, si possible en production, c'est-à-dire en conditions réelles, même si cela peut s'avérer complexe. Ce test permettra d'identifier les goulots d'étranglement afin de pouvoir y pallier, soit en amont, soit en mettant en place des processus de gestion automatisée de la montée en charge. Autre point crucial : l'état des sauvegardes et du plan de reprise d'activité doivent être vérifiés. Si le site venait à être victime d'un « bug », il faudrait être en mesure de rapidement remettre le site sur pied pour minimiser l'impact sur les ventes.

Enfin, pour éviter d'en arriver au « bug », il est important de mettre en place un monitoring qui pourra alerter les équipes techniques en cas de problème. Ces dernières pourront ainsi intervenir et régler les dysfonctionnements au plus vite, avant que les « bugs » n'impactent réellement le site Internet et ses performances. Ajouter des sondes de performances est également un plus pour le monitoring, on peut par exemple mettre en place une surveillance sur la rapidité de réponse d'un service web, le taux d'utilisation des disques ou de la mémoire vive.

Au-delà de la surveillance de l'état de santé de la base de données et des serveurs applicatifs, il faut également surveiller l'expérience client qui n'est pas forcément corrélée à ces éléments techniques. Des indicateurs de performance sur les pages doivent être installés pour accompagner le pic d'activité. Il faudra également compléter les actions classiques par la mise en place de plusieurs scénarii de visite automatisés avec les moyens de les gérer, via un système alertes et de seuils par exemple.

Une attention particulière à la sécurisation

Les e-commerçants reçoivent des données critiques tout au long de l'année, comme les coordonnées bancaires, et ils n'attendent bien évidemment pas les périodes de forte activité pour sécuriser leurs sites. Cependant, les soldes entraînent souvent des ajouts de nouvelles pages, de nouveaux formulaires, ou encore d'autres animations flash ou html5.

C'est sur ces ajouts qu'il faut être particulièrement vigilant, un audit poussé avant la mise en production de ces nouveaux éléments doit ainsi être réalisé. L'ennemi, dans les périodes de forte activité, c'est surtout la précipitation. Enfin, des mesures complémentaires doivent être mises en place, comme le renforcement ou l'augmentation de la capacité des pare-feux et des équilibreurs de charge.

Un choix d'infrastructure à ne pas négliger

On dit souvent que le Cloud est idéal pour obtenir plus de flexibilité et absorber aisément des pics de trafic. Bien évidemment, les machines virtuelles et les technologies de conteneurs sont idéales, puisque rapidement déployables pour encaisser l'accroissement soudain de l'activité. Pourtant, il n'est pas pertinent d'agir dans la précipitation. Certaines applications s'adaptent mal voire pas du tout à cette élasticité pour diverses raisons - comme les technologies utilisées, ou le caractère fortement transactionnel de l'application. Dans ces conditions, un Cloud hybride sera préconisé. Ce dernier est constitué de machines physiques puissantes, sur lesquelles certaines applications critiques peuvent être hébergées et de machines virtuelles, simples à ajouter et à supprimer, en cas de besoin.

En cas de pic de trafic très important, on complètera ce dispositif par l'ajout d'un service de CDN - Content Delivery Network - par exemple. Il s'agit d'un ensemble de localisations à travers le monde qui redistribuent localement le contenu des serveurs et conservent en cache les fichiers qui n'ont pas besoin de mises à jour permanentes. Ce principe permet de décharger partiellement l'infrastructure, et donc de pouvoir supporter une hausse inattendue du trafic. En conclusion, le plus important est de profiter du calme avant la tempête pour analyser et préparer l'ensemble de son infrastructure à la hausse soudaine du trafic et des demandes. En amont, via la mise en place de machines virtuelles supplémentaires, la refonte des sauvegardes, et aussi pendant tout le pic via un monitoring rapproché et des systèmes d'alertes.