Définir les besoins du site web

L'hébergeur a ses contraintes techniques ou légales, il faut les connaître et les comprendre pour vous permettre de définir et exprimer clairement votre besoin. C'est ce que nous allons faire ensemble au cours de cette leçon en abordant chaque question que vous allez devoir vous poser.

I. Affluence des visiteurs

Fig. 1 Salle de centre de données Internet avec serveur
©Yanawut Suntornkij - stock.adobe.com

A. Quelle est l'affluence de visiteurs attendue ?

En matière d'affluence, l'unité de mesure est le nombre de visiteurs uniques (on dit couramment « nombre de vues »).

B. Quelle est la différence entre un visiteur et un utilisateur ?

Un visiteur ne fait que consulter le site. Un utilisateur participe à la vie du site web : il y dépose des commentaires, des données ou y télécharge des fichiers (photos, fichiers audio ou binaires). Généralement, il possède un compte utilisateur.

C. Comment mesure-t-on le nombre de visiteurs uniques ?

Sur un site web en production, le nombre de visiteurs uniques est donné par des outils logiciels de statistiques que l'hébergeur ou l'hébergé installe et/ou configure.

Ils fournissent des indications très détaillées comme :
- le nombre de visites par heure, jour, mois ;
- le temps de visite ;
- la localisation géographique des visiteurs ;
- le volume de données échangé entre le site et le navigateur du visiteur
- le nombre de pages vues dans le site (ce qu'on appel le taux de rebond).

Le terme « visiteurs uniques » lui-même peut prêter à confusion. Il serait plus clair de parler de « visites ». Une visite est considérée comme unique tant que le visiteur sollicite le site web dans un rythme ne dépassant pas un intervalle de temps déterminé (généralement 30 minutes). Ainsi, un même visiteur peut générer plusieurs visites uniques ; par exemple, s'il consulte un site web d'une manière un peu soutenue, s'absente 30 minutes pour aller manger, puis revient consulter le site, cette dernière consultation sera comptabilisée comme nouveau visiteur unique.

Google Analytics et les autres

Le plus connu des logiciels de statistiques web, **Google Analytics**, est accessible sous forme de service en ligne gratuit. Il vous permettra un suivi de l'activité de votre site en temps réel à l'aide de tableau synthétique.

C'est un très bon candidat pour commencer. Son installation et sa configuration relativement simples nécessitent, cependant, des compétences techniques que vous pourrez trouver aisément chez votre développeur.

Il existe d'autres très bons logiciels gratuits ou payants. Parmi les logiciels gratuits et très répandus, nous pouvons vous conseiller **AWSTATS, ou Open-Web-Analytics.** Deux logiciels open source d'analyse web qui se télécharge sur le site de partage Git-Hub.

Ces logiciels analysent les journaux et nécessitent des compétences « système » pour leur installation, mais certains hébergeurs les incorporent dans leurs solutions, parfois gratuitement. Renseignez-vous en consultant leur site ou en les contactant.

D. Comment évaluer le nombre de visiteurs futurs ?

Comment évaluer un nombre de visiteurs avant que le site ne soit lancé ?

Dans vos rêves, ce nombre est explosif, mirifique ! Cependant, pour être sérieux, on se base sur un **business plan**.

Écrire un business plan n'est pas l'objet de ce module ; disons, pour schématiser, que l'on prend une feuille Excel que l'on remplit de prévisions de vues, mois par mois sur 1 à 3 ans, en essayant de les justifier par du concret, c'est-à-dire tout ce qui peut avoir un impact réel sur vos courbes ou les justifier :

- référencement ;
- viralité ;
- campagne publicitaire ;
- comparaison avec des sites similaires ;
- contenu ;
- partenariats.

Vous pouvez faire un tableau pour une hypothèse basse et un autre pour une hypothèse haute, vous disposerez ainsi des chiffres qui permettront d'évaluer dans le temps toutes les capacités matérielles nécessaires.

II. Trafic et bande passante

En matière d'hébergement, on parle de « bande passante » nécessaire pour désigner la capacité réseau dont vous avez besoin pour que vos visiteurs puissent accéder à votre site dans de bonnes conditions.

Cela peut être vu comme un tuyau, ou comme un canal.

Bande passante
Ce terme désigne le débit binaire d'un canal de communication (typiquement en relation avec les accès à Internet à haut débit), du fait que ce débit découle directement de la fréquence maximale à laquelle le canal peut être employé pour transmettre du signal électrique de façon fiable.

Imaginons que votre site soit un port maritime où vos visiteurs ont parqué leurs bateaux et qu'un canal de 10 mètres de largeur relie votre port à la pleine mer. Si 50 visiteurs décident en même temps de sortir ou de rentrer leurs bateaux, il va y avoir embouteillage, voire accident… Et s'ils doivent attendre des heures, ils vont dire que cela « rame » trop, ils finiront par aller parquer leurs bateaux ailleurs. Il vous faut donc construire un canal de la bonne largeur, mais cela coûte cher, vous devez donc calculer ce qui est nécessaire et prévoir l'augmentation du trafic.

Dans le monde de l'hébergement, le canal, c'est la bande passante ; les bateaux, ce sont les fichiers images/textes/sons, les pages web. Ceux-ci ont un poids, que vous avez évalué au chapitre précédent. Il vous faut maintenant évaluer la largeur du canal nécessaire pour assurer un temps de réponse acceptable, donc évaluer le trafic.

A. Comment évaluer le trafic et la bande passante nécessaire ?

L'unité de mesure est le nombre d'octets par seconde.

Là aussi, pas facile de calculer ce qui n'existe pas encore. Faites fonctionner votre bon sens.

Voici la méthode théorique :

1. Déterminez la bande passante nécessaire pour une requête en utilisant les chiffres du chapitre précédent.

2. Fixez un délai maximum (en secondes) pour « honorer » la requête.

3. Fixez un nombre maximal de requêtes simultanées en vous basant sur :

- le nombre de visites en période de pic (par exemple 100 visites en 1 heure entre 12 heures et 14 heures) ;
- un nombre de requêtes par visite.

4. Multipliez le tout (voir exemple).

5. Pondérez le taux en appliquant une marge d'erreur de 50 %.

Voici un exemple :
Calcul de la bande passante nécessaire pour 1 requête

Tableau n°1 Bande passante pour une requête

Taille maximum d'une requête	200 Ko
Délai maximum pour honorer la requête	2 secondes
Bande passante nécessaire pour une requête	200 / 2 = 100 Ko/sec

Calcul du nombre de requêtes simultanées

Tableau n°2 Nombre de requêtes simultanées

Nombre de visites maximum en 1 minute	20
Nombre de requêtes par visite et par minute	6
Nombre de requêtes simultanées dans 1 seconde	(20 × 6) / 60 =2

Calcul de la bande passante globale nécessaire :

2 requêtes × 100 Ko = 200 Ko/sec

On ajoute une marge d'erreur de 50 % par exemple, 50% de 200 = 100

Soit 200 + 100 = 300 Ko/sec

Mettez le tout dans un tableur et faites varier vos chiffres mois par mois comme pour les tableaux précédents.

Requête
C'est un accès serveur. Lorsqu'un internaute accède à une page de votre site, il y a :
- 1 requête pour le document HTML ;
- 1 requête par fichier JavaScript ou CSS inclus dans la page web ;
- 1 requête par image, vidéo ou fichier flash inclus dans la page web.

1. Qu'est-ce qu'un pic d'affluence ?

Un pic d'affluence est un afflux soudain de visites sur votre site web. C'est souvent dû à un événement extérieur (exemple : on cite votre site dans une émission de télé). Votre serveur doit pouvoir tenir le coup, ne pas s'effondrer en cas de pic d'affluence.

Il peut aussi y avoir des pics d'affluence réguliers, par exemple tous les jours de 12 heures à 14 heures… pendant la pause déjeuner. Ce sont des moments importants, il faut que le serveur soit au rendez-vous.

B. Bande passante mutualisée ou dédiée

Les hébergeurs proposent souvent deux « types » de bandes passantes : mutualisée ou dédiée.

Sur une bande passante mutualisée, la bande passante est partagée entre tous les utilisateurs. Si l'un d'eux se met à télécharger comme un fou, votre service peut être affecté.

Conseil : si vous commencez, optez pour la bande passante mutualisée, il vous sera loisible d'opter pour un autre choix si vous vous apercevez que les temps de réponses chutent ou sont trop inconstants.

Sur une bande passante dédiée, vous êtes sûr de disposer de toute la bande passante à laquelle vous aurez souscrit à votre seul usage. Mais c'est plus cher, il faut compter environ 100 € le mégaoctet. Certains prestataires proposent de vous facturer au volume de données, d'autres en bande passante. Concernant la bande passante mutualisée, de nombreux prestataires affichent des dispositifs gratuits pour vous prémunir de la monopolisation par un seul utilisateur d'une bande passante mutualisée.

1. Accords de transit

Le réseau Internet est constitué d'une dorsale (*backbone*) reliant tous les prestataires entre eux par des contrats dits de **transit**. En effet, les fournisseurs de dorsale facturent (assez cher) leurs services selon le débit de raccordement.

Si votre prestataire a des accords de transit sous-tail-lés, les sites qu'il héberge en seront affectés.

2. Cas particulier : diffusion de vidéos ou du son en « streaming »

Le streaming est la technologie logicielle utilisée pour diffuser de la vidéo en continu, c'est-à-dire sans avoir à attendre d'avoir téléchargé tout le fichier correspondant.

Si votre site comporte un tel service, vous devez mettre en place les logiciels nécessaires ou les faire héberger chez un prestataire spécialisé, gratuit ou pas.

Beaucoup d'hébergeurs limitent les capacités de diffusion pour maîtriser leurs coûts en bande passante. Cette limitation joue généralement sur le nombre de lectures de vidéos simultanées. Vous devez donc évaluer vos besoins et vous assurer qu'ils sont couverts.

Si cinq internautes regardent une vidéo sur votre site et si vous ne pouvez diffuser que 4 vidéos simultanées, cela pose un problème au cinquième internaute… à vous de peser les conséquences.

Conseil : si vous projetez de diffuser plus d'une dizaine de vidéos en simultané, envisagez d'utiliser le service d'un prestataire spécialisé. Cela vous reviendra beaucoup moins cher : vous ferez des économies de serveurs, de gestion et vous bénéficierez de prix attractifs et d'une grande scalabilité.

Benchmark

Si l'enjeu est important (exemple : site web pour un événement), des logiciels dits de « benchmark » permettent de simuler du trafic et donc de tester la résistance du serveur. En voici quelques-uns, tous gratuits : Siege, Tsung, JMeter, Selenium.

III. Environnements et caractéristiques nécessaires

A. Environnements logiciels

Pour créer votre site, votre développeur a utilisé :
- un langage comme PHP, RUBY, C+, C#, etc. ;
- un environnement logiciel (Ruby on Rails, Zend, Symphony, Cake, etc.) ;
- un OS système comme Linux, Windows, ou Mac OS pour citer les plus courants ;
- un système de base de données (MySQL, PostgreSQL, Oracle, SQL Server, Mongodb, etc.).

Ces éléments doivent être fournis ou installables sur le serveur que mettra à disposition votre hébergeur. Certains sont plus spécialisés dans un type d'environnement et/ou ne pratiquent pas les mêmes tarifs selon le cas.

Il faut donc avoir ces informations à portée de main, c'est-à-dire dans votre descriptif.

Demandez ces informations à un ou votre développeur et veillez à ce qu'il précise pour chaque environnement/langage/logiciels/système de base de données les versions requises.

B. Puissance CPU (processeur) et mémoire

La mémoire se calcule en Go ; la puissance s'évalue en considérant le type de traitement effectué sur les données. Par exemple, un traitement d'images ou une reconnaissance de caractères nécessitent un traitement lourd en puissance et en mémoire. C'est à évaluer. Si c'est un traitement « standard », dites-le simplement, si c'est un traitement lourd, décrivez-le.

IV. Qualité de service et disponibilité

Il s'agit ici de la qualité de service minimum que l'on considère nécessaire et acceptable par les « clients » du site. On la mesure selon la disponibilité et la **garantie de temps de rétablissement** ou **garantie de temps d'intervention**, mais aussi selon l'accessibilité des locaux abritant le ou les serveurs du site.

A. Disponibilité

On mesure le temps de disponibilité en pourcentage calculé généralement sur un mois. Les hébergeurs sérieux s'engagent à des taux de disponibilité de 99,99 %, ce qui correspond à un arrêt de service toléré d'un peu plus de 4 heures par mois.

Certains hébergeurs s'engagent à des pénalités en cas de dépassement.

B. Garantie de temps d'intervention (GTI)

Il s'agit du délai, calculé en heures ou en jours, d'intervention des équipes en cas de panne.

Selon les prestataires (et le coût que l'on est prêt à payer), cela s'élever à 1 heure, 4 heures voire un jour, et cela peut fluctuer s'il s'agit d'un jour férié ou pas.

En effet, pour garantir des temps d'intervention réduits, les hébergeurs mettent en place des équipes de surveillance et d'intervention disponibles parfois 24 heures sur 24, cela a donc un coût.

C. Garantie de temps de rétablissement (GTR)

C'est l'engagement de l'hébergeur à remettre le site web disponible dans un certain délai en cas d'indisponibilité. Certains hébergeurs ne s'engagent que sur une GTI, pas une GTR.

D. Accessibilité des locaux

Parfois, en cas de panne ou de mise à jour du système abritant le site, il est nécessaire que votre ingénieur système, ou vous-même ayez accès au serveur. Dans un tel cas, il faut vous assurer que vous aurez cet accès, dans quelle tranche horaire, ainsi que l'adresse des locaux.

V. Sécurité

En matière d'hébergement, on considère trois types de sécurité : la sécurité réseau, la sécurité système et la sécurité physique des serveurs et des locaux les abritant.

A. La sécurité réseau

Sécuriser un accès réseau, c'est avant tout mettre en place les moyens de filtrages nécessaires à l'aide matérielle dits « *firewall* » ou « pare-feu » et leur configuration afin de garantir que les internautes n'aient accès qu'aux services nécessaires.

Pour un site web, il s'agit principalement des accès http, https ; attention concernant le http, ce protocole d'échange d'information entre le serveur web et les visiteurs se fait sans aucun cryptage. Si votre site gère des informations sensibles comme des informations confidentielles de paiement, il est impératif que le site possède un protocole de cryptage. Renseigner vous auprès de votre développeur.

On parle aussi de sécurité sortante. Imaginez qu'un pirate se procure l'accès aux données de votre serveur. Grâce à une configuration appropriée des *firewalls*, le transfert des données de votre serveur vers l'ordinateur du pirate peut être bloqué.

Attention toutefois, aucune sécurité n'est à 100 % fiable, aucun hébergeur ne peut s'engager sur des garanties absolues ; l'imagination des pirates est infinie. La période du confinement dû Covid-19 a été particulièrement propice aux piratages en tout genre.

1. Comment marche un *firewall* ?

Un *firewall* (pare-feu en français) filtre les requêtes allant d'Internet vers le serveur (et vice versa).

Il faut savoir que chaque application web ou autre est accessible par ce qu'on appelle un port TCP. Par exemple, l'adresse réseau d'un site web est composée de son adresse IP et du numéro de port TCP 80 (http) ou 443 (https).

Il suffit donc au *firewall* d'interdire toute autre requête pour mettre en sécurité le serveur, c'est-à-dire qu'il interdit d'adresser d'autres applications ou services sur le serveur.

B. La sécurité système

Elle n'est proposée comme service que par les hébergeurs assurant la gestion complète de votre ou vos serveurs (*full management*).

Il s'agit alors de s'assurer :

- que les logiciels abrités sur le serveur soient régulièrement mis à jour en appliquant « les corrections de sécurité » émises par leurs éditeurs ;
- de mettre en place des logiciels de sécurité sur le ou les serveurs permettant de détecter les intrusions, voire de les interdire.

C. La sécurité physique

Il s'agit de l'accès aux serveurs, aux supports et aux locaux.

Imaginez encore que tous les clients de votre hébergeur aient accès aux locaux abritant les serveurs. Vous ne voudriez pas que ces gens puissent regarder ce qu'il y a sur votre serveur, l'éteindre ou le débrancher du réseau par inadvertance. Et vous devez vous en prévenir d'autant plus si votre site web abrite des données « sensibles », chères à vos utilisateurs.

Vous devez donc vous renseigner sur les conditions physiques d'accès sont hébergés vos serveurs. Les dispositifs de sécurité les plus courants sont :
– emplacement dans une baie dédiée fermée à clé ;
– box dédié (si vous avez beaucoup de serveurs) ;
– personnel supervisant tous les accès ;
– dispositif de badge, voire de reconnaissance rétinale ou faciale ;
– liste de personnes habilitées.

D. Supports de stockage des sauvegardes

Si les supports de stockage des sauvegardes de votre site web sont à côté des serveurs, il y a un risque en cas d'incendie des locaux ou de dégâts des eaux que vos serveurs soient détruits ainsi que vos sauvegardes. Vous n'avez alors plus rien.

Certains hébergeurs proposent d'externaliser les sauvegardes sur d'autres sites d'hébergement. Dans tous les cas, ils doivent pouvoir vous fournir des garanties de sécurité incendie. Le plus courant est un dispositif d'émission de gaz qui supprime tout l'oxygène des salles d'hébergement afin d'éteindre un feu sans endommager les serveurs.

E. Sécurité électrique et sécurité des accès réseaux

Que se passe-t-il en cas de panne EDF, ou en cas de coupure des câbles réseaux alimentant les locaux d'hébergement suite à des travaux extérieurs ? Ce sont des cas relativement fréquents.

Les hébergeurs « sérieux » ont leurs standards :
– double accès au réseau électrique ;
– groupes électrogènes ;
– onduleurs pour prémunir les serveurs des microcoupures ;
– double accès au réseau Internet.

Ces dispositifs sont généralement décrits sur les sites web des hébergeurs, ils vous assurent que votre prestataire emploie les moyens physiques et humains nécessaires pour tenir ses engagements en matière de qualité de service et de sécurité.

VI. Architecture

On parle d'architecture logicielle ou matérielle.

A. Architecture logicielle

L'architecture logicielle décrit les composantes logicielles que l'on peut séparer, généralement de la façon suivante :

– un serveur http qui reçoit les requêtes des utilisateurs via le réseau et transmet les requêtes à l'application ;

– l'application et son environnement d'exécution qui reçoivent les requêtes du serveur http et les traitent en interrogeant un système de base de données ;

– le système de base de données qui gère les demandes d'accès en lecture-écriture aux bases de données ;

– le système de gestion de fichiers (images, documents, vidéos…) que l'application utilise.

Pour des raisons de scalabilité ou de sécurité, on peut mettre en œuvre plusieurs instances d'une même composante que l'on peut répartir sur un ou plusieurs serveurs. Dans un tel cas, on utilise des répartiteurs de requêtes logiciels ou matériels pour distribuer les requêtes entre les instances.

B. Architecture matérielle

Elle est définie par les serveurs, le support de stockage (disques) et leur liaison réseau que l'on utilise pour répartir les composantes logicielles.

Parmi les architectures simples courantes, on peut avoir tout sur le même serveur :

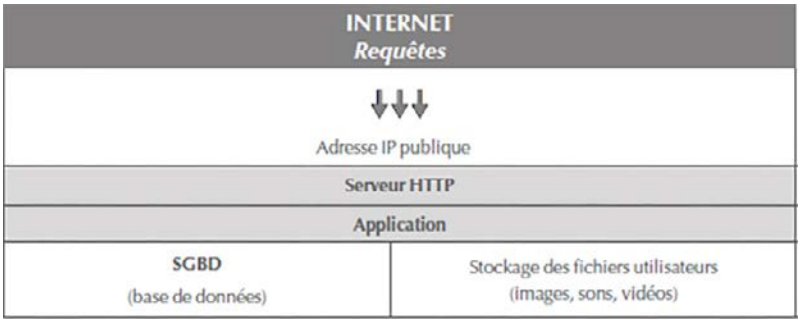

Fig. 2 Architecture sur serveur unique © Skill and You

Sur deux serveurs (on parle alors d'architecture 2/3) :

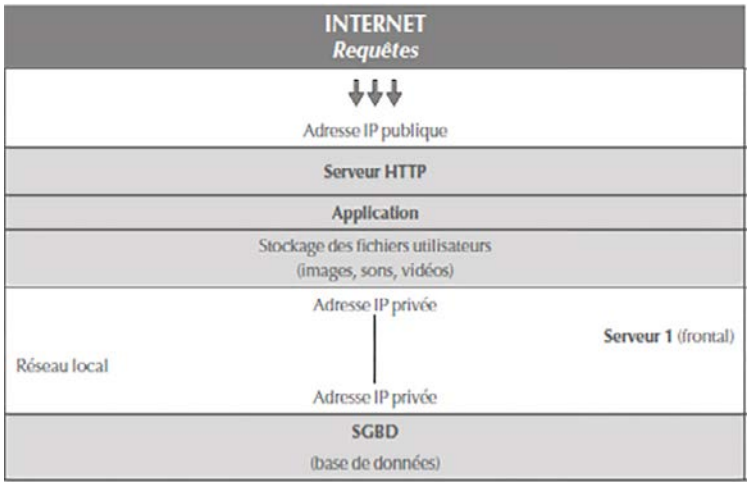

Fig. 3 Architecture 2/3 © Skill and You

Sur 3 serveurs :

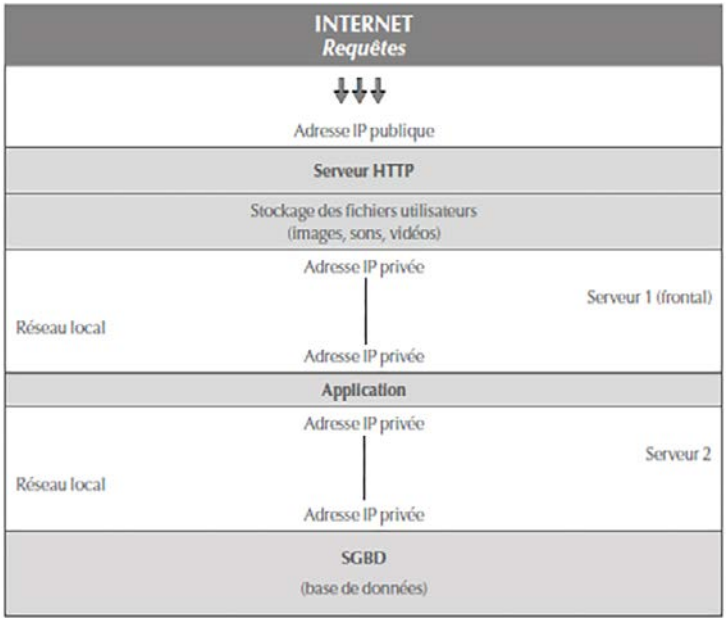

Fig. 4 Architecture sur 3 serveurs © Skill and You

Ou plus :

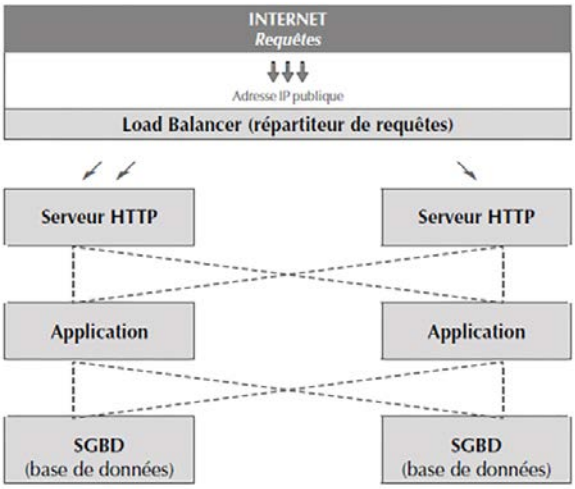

Fig. 5 Architecture sur plus de 3 serveurs © Skill and You

C. Serveurs virtuels et matériels

Pour compliquer un peu la chose, mais aussi pour donner plus de souplesse, on peut utiliser des serveurs matériels… ou virtuels.

En effet, aujourd'hui la puissance des serveurs matériels est suffisante pour faire tourner plusieurs systèmes d'exploitation sur la même machine.

C'est un peu comme si on avait plusieurs ordinateurs dans le même ordinateur.

Chaque serveur virtuel est isolé des autres et possède sa propre configuration. Il utilise une partie des capacités mémoire, processeurs et disques du serveur matériel, le tout étant géré par un logiciel système dit « hyperviseur ».

Avantages :

– meilleure optimisation des ressources du serveur physique et donc des coûts ;

– souplesse d'architecture : on peut décider, si nécessaire, de dupliquer les serveurs virtuels pour une bonne tolérance de panne ou pour de meilleures performances.

On peut migrer aisément les serveurs virtuels sur d'autres serveurs physiques, voire allouer tout un serveur physique à une seule instance.

Inconvénients :

Même si les serveurs virtuels sont isolés logiquement, leur performance peut être impactée par l'activité de leurs « colocataires ». Cependant, les meilleurs hyperviseurs sont capables d'allouer les ressources de façon prédictive afin d'éviter qu'une instance monopolise une partie des ressources.

Le Cloud

L'utilisation ultime de cette virtualisation donne le « Cloud ». On ne se soucie plus du matériel, on ne « joue » qu'avec des instances de serveurs virtuels que l'on crée, détruit, reconfigure en quelques clics. Concrètement, les instances virtuelles sont réparties sur des « *grids* » (grilles) de serveurs physiques qui ne sont vues par l'hyperviseur que comme une seule machine.

Si l'on ne connaît pas d'avance le nombre d'utilisateurs ou la réaction du système et que l'on suppute des afflux importants et rapides, mieux vaut être scalable (voir section suivante), c'est-à-dire rapidement adaptable au flux d'utilisateurs et à la charge occasionnée.

On peut :

– utiliser des logiciels de simulation de trafic pour tester la résistance du système ;

– utiliser la technologie du Cloud pour tous les composants ou en partie ;

– s'appuyer sur les relevés de temps de réponses, de consommation CPU, mémoire et disque pour intervenir à temps.

Quelques règles usuelles cependant :

– les serveurs http consomment beaucoup moins en CPU/mémoire/disques qu'un serveur d'application ou qu'un SGBD (Système de Gestion de Base de Données) ;

– les fichiers images, sons, vidéos peuvent être délivrés directement par le ou les serveurs https sans passer par les serveurs d'application ;

– il faut optimiser les caches (requêtes au SGBD et pages web) pour limiter autant que faire se peut les traitements ;

– isoler l'application du SGBD améliore grandement les temps de traitements (si les serveurs sont correctement « taillés » bien sûr) ;

– d'un point de vue sécurité, seul le ou les serveurs http (ou le ou les *load balancers*) devraient être accessibles à partir d'Internet.

VII. Capacité d'adaptation à la charge : la scalabilité

La **scalabilité** est un anglicisme utilisé pour désigner la possibilité d'une architecture serveur et réseau à s'adapter à des charges fluctuantes.

Une architecture **scalable** est une architecture que l'on peut faire évoluer à la demande, sans mettre en cause l'existant : on rajoute ou on retranche du débit ou des serveurs pour faire face à la demande.

A contrario, une architecture **non scalable** est une architecture qu'il faut repenser pour pouvoir supporter une augmentation ou une diminution de charge importante. On recommence à zéro, on réinstalle, on commande de nouveau débit réseau.

Il existe deux types de scalabilité : horizontale et verticale.

Horizontale
La scalabilité horizontale consiste généralement à rajouter ou retrancher des serveurs à la demande. La technique la plus utilisée pour ce faire est le *load balancing* ou répartition de charge.

Verticale
La scalabilité verticale est la possibilité d'augmenter les ressources d'un serveur.

Sur un serveur matériel, on peut rajouter des disques, des processeurs, de la mémoire, si le serveur le permet. Cela suppose une intervention physique, donc un arrêt du serveur, sauf s'il dispose d'une architecture permettant des changements « à chaud » de tel ou tel composant matériel.

Sur un serveur virtuel, c'est la même chose, sauf que tout se fait par configuration logicielle, parfois en quelques clics. On maîtrise ainsi les coûts, la performance et la scalabilité.

VIII. Le choix du nom de domaine et adresses IP DNS

Pas de site digne de ce nom sans nom de domaine. Le nom de domaine est la partie droite du nom de site. Par exemple dans **www.exemple.com**, le nom de domaine est exemple.com, l'ensemble forme le *hostname*, « www » est le host dans le domaine. À un *hostname* correspond une adresse IP. Vous achetez un nom de domaine pour 1 an ou 3 ans renouvelables.

Libre à vous ensuite d'utiliser le préfixe qu'il vous plaira pour adresser le ou les sites que vous mettez en ligne (exemples : www.exemple.com, blog.exemple.com, forum.exemple.com).

Les noms de domaines peuvent être :
– fournis par votre hébergeur, parfois gratuitement (compris dans le pack hébergement) ;
– achetés auprès de votre hébergeur ;
– achetés auprès de prestataires spécialisés (les « registrars »), vous en trouverez une liste en annexe.

A. Comment associe-t-on un *hostname* à une adresse ?

Un nom de domaine ne suffit pas pour que vos utilisateurs puissent accéder à votre site. En effet, le navigateur de l'utilisateur utilise l'adresse IP de votre site pour y accéder. Pour cela il prend l'URL que l'internaute a requis (exemple : https://www.exemple.com/products), isole le *hostname* (www.exemple.com) et recherche dans le répertoire de noms (DNS : *Data Name Service*) de votre fournisseur d'accès l'adresse IP correspondante.

L'ensemble des répertoires de noms sont reliés afin que la traduction *hostname*/adresse IP soit accessible pour n'importe quel navigateur.

B. Par qui sont fournies les adresses IP ?

Les hébergeurs disposent de quotas d'adresses IP qu'ils allouent à leur client. La première adresse est généralement gratuite, les autres sont payantes (quelques euros).

De combien d'adresses IP avez-vous besoin ?

Cela dépend de votre architecture. Si vous n'avez qu'un seul système hébergé, une seule suffit généralement. Si vous avez plusieurs serveurs, virtuels ou non, vous aurez besoin d'une adresse IP par serveur accessible à partir d'un navigateur (les serveurs frontaux).

Pour les autres serveurs, vous pourrez utiliser à votre guise des adresses IP dites « privées », c'est-à-dire inaccessibles d'Internet (avantage sécurité) mais utilisables pour la communication interserveurs sur le réseau local de votre hébergeur.

Adresses privées
Plages d'adresses privées, inaccessibles à partir d'Internet : 192 168.0.0 à 192.168.255.255, 10.0.0.0 à 10.255.255.255, 172.16.0.0 à 172.16.255.255).

C. Comment configurer les répertoires DNS ?

Les prestataires fournissent généralement une interface web pour que vous puissiez configurer votre « traduction ». Si ce n'est pas le cas, il se chargera lui-même de cette tâche.

Si vous êtes un expert et que vous disposez des serveurs nécessaires, vous pouvez installer vous-même des serveurs DNS et les relier à ceux de votre prestataire selon ses indications.

D. Prendre le nom de domaine et le DNS chez l'hébergeur ou un prestataire spécialisé

Changer de prestataire DNS ou registrar n'est pas chose aisée. Il faut envoyer un courrier ou un e-mail officiel de résiliation en indiquant le nouveau prestataire choisi. La procédure peut prendre jusqu'à 3 semaines, et lors du changement effectif, il se peut que votre site soit par endroits inaccessible, le temps que les caches des répertoires DNS dans Internet soient mis à jour.

Conseil
En général, mieux vaut acheter vos noms de domaines chez un prestataire spécialisé. Leurs tarifs sont imbattables (5 à 10 € par an) et ils fournissent souvent des DNS fiables et des interfaces performantes. En cas de changement d'hébergeur, vous ne serez pas tributaire de celui-ci.

IX. Sécurité des données

A. Certificats SSL

Les certificats électroniques permettent de crypter les communications entre les navigateurs et un site web selon le protocole HTTPS que vous avez peut-être remarqué dans la barre d'adresse de votre navigateur. Si vous hébergez des données sensibles pour vos utilisateurs, mieux vaut donc en disposer.
Il est difficile de s'y retrouver dans les offres. En effet, il existe des certificats SSL pour tous types de fonctions (e-mail, accès aux serveurs, identification de personnes, etc.) et pas seulement pour le Web. D'autre part, beaucoup d'offres sont en fait un bundle (ensemble) de plusieurs.

Le certificat web standard :

- a une clé de cryptage ;
- permet de sécuriser un seul nom de site (exemple : www.exemple.com) ou un domaine (www.exemple.com, forum.exemple.com, exemple.com, blog.exemple.com) mais c'est plus cher ;
- ce service est souvent inclus dans les sites personnels ;
- s'achète pour 2 ou 3 ans (voire 4) ;
- vaut entre 50 et 120 € l'an ;
- l'option EV (*Extended Validation*) permet d'afficher dans le navigateur une information supplémentaire pour rassurer encore plus l'internaute sur l'identité du site (et de son propriétaire, validée par le prestataire).

Cette option vaut cher (+ 100 à 200 € l'an) et elle est réservée aux entreprises.
Vous trouverez une liste de prestataires dans le module suivant. Parfois, votre hébergeur vous propose ce service. La configuration de votre serveur http doit être effectuée par vos soins.

Conseil
Si vous êtes un peu perdu dans les offres, choisissez un prestataire spécialisé dans le Web uniquement (comme les registrars ou votre hébergeur). Vous pouvez aussi utiliser les certificats à l'essai que proposent certains, pour savoir si ceux-ci vous conviennent.

B. Paiement électronique

En matière de paiement électronique, il existe deux types de prestataires : les banques et les collecteurs. Le service est généralement gratuit, le prestataire prélevant une commission sur chaque vente que vous effectuez.

Les banques ont une bonne couverture nationale et un taux de prélèvement plus bas que les collecteurs.

Les collecteurs collectent le revenu de vos ventes et les transmettent à votre banque. Ils ont l'avantage d'avoir une couverture multinationale, voire mondiale et d'offrir des moyens de paiements que votre banque ne peut offrir.

Certains collecteurs sont spécialisés dans le micro-paiement et les modes alternatifs (via la facture de votre opérateur téléphonique par exemple, ou via SMS surtaxé). Leur couverture est souvent nationale.

B. Adresses e-mail

Avoir des adresses e-mail dans le même domaine que votre site web rassure vos utilisateurs, cela fait plus sérieux. Un service d'adresses e-mail est souvent fourni par votre prestataire, là aussi soumis à quota et souvent tarifé selon le nombre de boîtes aux lettres et l'espace de stockage des e-mails pour chacune d'entre elles. Il faut donc se renseigner. Des prestataires spécialisés existent également et non des plus chers et des moins performants.

Conseil

Toujours penser à l'avenir. Si vous changez de prestataire d'hébergement et que vos boîtes e-mail sont chez lui, cela devient compliqué à gérer. Comme pour les DNS ou les noms de domaines, choisissez un prestataire spécialisé indépendant. Par exemple, Google APP offre jusqu'à 10 boîtes e-mail gratuites et plusieurs Go de stockage par boîte e-mail ainsi qu'une interface puissante de configuration, un service difficile à concurrencer.

X. Adresses e-mail et envoi d'e-mails

A. Relai SMTP : Envoyer des mails via le site

La plupart des sites web envoient des e-mails à leurs utilisateurs, le vôtre aussi sans doute. Pour pouvoir envoyer des e-mails sans être considéré comme spam, le site web est configuré pour utiliser ce qu'on appelle un relai SMTP (*Simple Mail Transfer Protocol* = protocole simple de transfert de courrier), celui de son prestataire d'hébergement ou d'un prestataire spécialisé.

Ce service est généralement soumis à quota : gratuit jusqu'à un certain nombre d'envois par jour ou par mois, payant en cas de dépassement.

Il vous faut donc choisir une solution ou du moins vérifier que votre prestataire fournit ce service et à quel prix.

Relai SMTP

Simple Mail Transfer Protocol (SMTP, littéralement « protocole simple de transfert de courrier ») est un protocole de communication utilisé pour transférer le courrier électronique (courriel) vers les serveurs de messagerie électronique.

XI. Serveurs et budget

A. Serveur Linux, Windows, macOS ou autre ?

Cela dépend de l'application développée. Une application développée avec un langage et un environnement Windows ne fonctionnera généralement que sur un serveur Windows.

Pour tout le reste, Linux est roi, moins cher, plus souple, bien moins consommateur en ressources et disposant d'une immense bibliothèque d'outils systèmes open source gratuits.

B. Serveurs loués ou achetés ?

Le moindre serveur sérieux vaut de 1 500 à 5 000 €. Vous pouvez décider de les acheter ou de les louer.

1. Serveurs loués

Voici une liste des avantages :
- coût lissé par mois et souvent bon marché ;
- matériel fiable (déjà testé) ;
- management bien maîtrisé par les équipes de l'hébergeur ;

– tout-en-un ;
– gestion des pannes et des pièces de rechange assurée par l'hébergeur à ses frais ;
– une seule facture, un seul interlocuteur.

2. Serveurs achetés

Acheter permet de mettre cet actif dans le bilan et fait grimper la valeur de votre société.

Si vous achetez, les pannes devront être gérées par votre vendeur, selon une GTI et des garanties à souscrire.

Parmi les vendeurs les plus connus, on peut citer : **Dell et IBM**. Il existe aussi des « *brokers* » (vendeur d'occasion) qui proposent du matériel d'occasion performant et souvent encore sous garantie.

Quand acheter ?

Acheter les serveurs n'a de sens que si vous avez déjà un business stable et une équipe de techniciens. Pour commencer à faire héberger, mieux vaut « se faire » la main sur de la location. Quand le business devient florissant, alors on peut reconsidérer la chose.

3. Budget

En matière d'hébergement, tout est possible, mais le coût peut varier de 100 à 1 000 €, voire plus. Il faut être raisonnable quant aux services souhaités et se focaliser sur le strictement nécessaire pour atteindre vos objectifs en matière de business. Commencez « juste avec ce qui est suffisant » et puis souscrivez à d'autres services lorsque vous le jugerez nécessaire. Prévoyez les carences possibles au niveau de l'organisation personnelle.

Tout ce qui ne sera pas assuré par l'hébergeur devant être assuré par vous-même ou votre équipe, un coût est à prévoir ; il faut donc disposer des compétences nécessaires en cas de besoin.

Il vous faut arbitrer en considérant avant tout la qualité du service souhaité et ne pas prendre de risques inconsidérés.

Posez-vous les bonnes questions, faites une liste : que se passe-t-il si… ?

Clause de désengagement

Certains hébergeurs vous demandent de vous engager sur 6 mois ou 1 an. D'autres sont plus souples : 1 mois à 3 mois. Peut-être ne savez-vous pas si votre « business » va tenir ses promesses et vous ne voulez pas vous engager sur une longue période ? Lisez bien les clauses de désengagement.

XII. Descriptif synthétique

Voici le plan d'un descriptif type pour exprimer les besoins du site :
– nom du site ;
– type de site ;
– nom de domaine ;
– description (succincte) ;
– criticité ;
– type de données stockées ;
– traitement effectué ;
– nombre de vues prévisionnel (tableau nécessaire) ;
– espace disque consommé (tableau prévisionnel) ;
– bande passante nécessaire (tableau prévisionnel) ;
– environnements logiciels et système nécessaires ;
– services complémentaires souhaités : boîtes e-mail, nom de domaine, relai SMTP, DNS, adresses IP, supervision ;
– budget ;
– clause de désengagement.

Maintenant, vous possédez tous les éléments de langage et de compréhension nécessaires pour exprimer votre besoin, dialoguer avec un expert, et éviter les déconvenues.

XIII. Superviser le bon fonctionnement du site

Superviser, c'est :

– surveiller que sur le site web, toutes les parties fonctionnent correctement ; que les temps de réponse sont corrects et pas trop fluctuants ;

– surveiller l'utilisation des ressources du serveur (espace disque, CPU, mémoire, bande passante utilisée, etc.) pour planifier les évolutions avant que les problèmes n'apparaissent ;

– veiller également à ce que la sécurité de votre système ne soit pas compromise ;

– être prévenu rapidement lorsqu'un problème arrive et avoir dans un tel cas des moyens d'action.

Les prestataires fournissent généralement des prestations de supervision a minima : vérification que le serveur HTTP répond, qu'il affiche une page d'erreur ou une page blanche. Quelques prestataires dit B2B offrent des services (tarifés) plus poussés : test de contenu de certaines pages, déroulement de scénario.

De base, on est averti des incidents ou des retours à la normale par e-mail, quelquefois par SMS.

Si vous voulez une surveillance plus poussée, vous devrez soit vous tourner vers un prestataire spécialisé, soit faire les choses par vous-même. Cependant, monter un serveur (virtuel ou non) avec un logiciel de monitoring adéquat (le plus connu des logiciels de monitoring open source est Nagios) et configurer les alertes est un travail relativement complexe qui doit être effectué par un technicien ou un ingénieur système.

A. Surveiller l'utilisation des ressources

Cette surveillance peut parfois être faite grâce aux outils fournis par votre hébergement. Dans le cas contraire, votre technicien ou ingénieur système doit mettre en place les outils nécessaires sur les serveurs à surveiller.

B. Veiller à la sécurité

Là plus qu'ailleurs, seul un technicien averti ou un ingénieur système peut mettre en place les composants nécessaires pour ce type de surveillance.

C. Accès au support, pouvoir agir

Qu'importe d'être averti des problèmes si on ne peut pas agir (voire si on n'a personne pour agir). Dans le cas d'une indisponibilité ou d'une performance dégradée, il faut parfois pouvoir accéder à l'équipe de support de l'hébergeur pour savoir s'il s'agit d'un problème général ou d'un problème spécifique à notre site web.

Les hébergeurs bon marché offrent un accès limité au support : e-mail et avis d'incident sur une page web. Il faut monter en gamme pour avoir le droit au téléphone.

Nous l'avons vu, il est difficile de se passer d'un technicien pour superviser votre site web et vos serveurs. Votre développeur n'a généralement pas les compétences pour le faire. Une seule solution, étoffer son organisation si nécessaire.