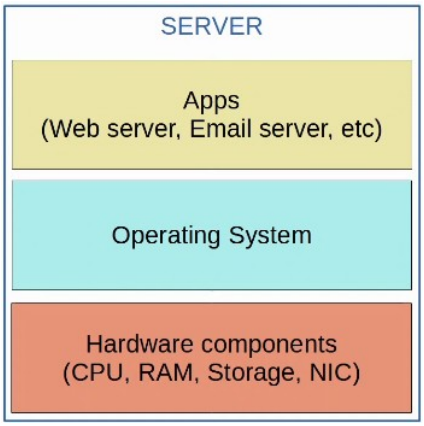
Cours 54 : Virtualisation & Cloud

Dans ce cours nous verrons deux sujet qui sont la virtualisation et le Cloud.
Nous ferons d'abord une introduction du fonctionnement de la virtualisation avec les serveurs virtuels et les réseaux virtuels. Puis nous ferons une introduction sur le Cloud Computing en donnant ses caractéristiques essentiels, ses modèles de services et les modèles de déploiements.
Nous verrons comment faire pour se connecter à des Cloud publique.

Cisco est l'un des vendeurs les plus connu pour ses appareils de réseaux comme les routeurs, les Switchs, les murs de feu, ils offrent aussi du matériel de serveurs comme UCS (Unified Computing System). Voici un exemple de à quoi ressemble UCS :

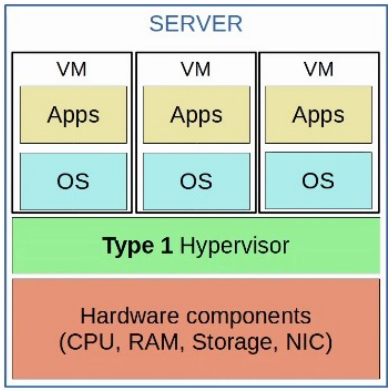
D'autres grand vendeurs sont aussi présent sur le marché qui sont Dell EMC, HPE et IBM.

Voyant tout d'abord comment un serveur fonctionne sans virtualisation :



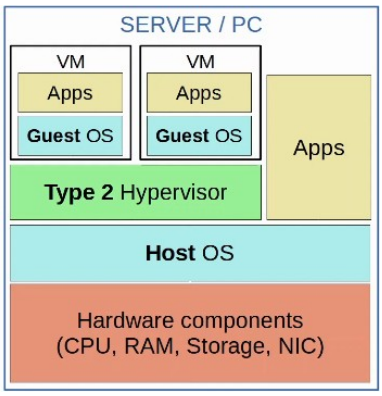
Avant la virtualisation il y avait une relation direct entre le serveur physique et le système d'exploitation (OS pour Operating System). Dans ce système d'exploitation des applications qui fournissent différents services comme le serveur Web, le serveur de Mail, etc...
Un serveur physique serait utilisé pour le serveur Web, le serveur Mail, la base de données, etc...
Cela n'est pas efficace pour plusieurs raisons :
Chaque serveur physique coûte chère et prend de la place, de l'énergie etc...
Les ressources pour chacun des serveurs (CPU, Stockage, RAM, NIC) sont parfois sous utilisés.

Avec la virtualisation cela est différent :



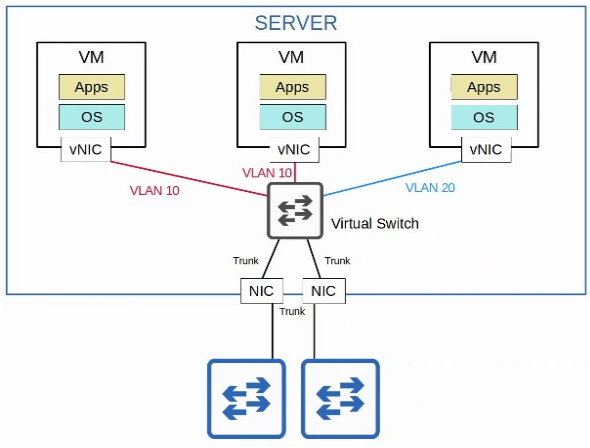
La virtualisation permet de changer la traditionnel relation entre le matériel de l'OS ce qui permet de lancer plusieurs systèmes d'exploitation dans un seul serveur physique.
Chaque instance est appelé une VM (Virtual Machine ou Machine Virtuel en Français).
Sur le diagramme précédent, 3 système d'exploitation sont lancés sur un seul serveur.
Un hyperviseur est utilisé pour gérer et allouer les ressources matériel (CPU, RAM, etc.) pour chacune des VM.
Un autre nom pour les hyperviseur est VMM (Virtual Machine Monitor)
Le type d'hyperviseur qui se lance directement en haut du matériel est appelé hyperviseur de type 1.
Des exemples incluent Vmware ESXi, Microsoft Hyper-V, etc...
Les hyperviseurs de type 1 sont aussi appelés « bare-metal hypervisors » car ils se lancent directement sur le matériel (qui est du métal). Un autre terme est « native hypervisor ».
C'est le type d'hyperviseur qui est utilisé dans un environnement de centre de données.

Les hyperviseurs de Type 2 se lancent comme un programme sur un système d'exploitation comme des programmes normaux. Par exemple cela inclus VMware Workstation, Oracle VirtualBox, etc.



L'OS qui se lance directement sur le matériel est appelé Host OS, et l'OS qui se lance dans la CM est appelé Guest OS. Un autre nom pour les hyperviseurs de Type 2 est « hosted hypervisor »
Les hyperviseurs de type 2 sont rarement utilisés dans des environnements de data center, ils sont commun dans l'utilisation personnel des appareil (par exemple si un utilisateur MAC/Linux a besoin de lancer une application qui est seulement supporté par Windows et l'inverse).
Sur le site de Vmware est donné plusieurs informations sur la virtualisation. La virtualisation permet le partitionnement, en lançant plusieurs systèmes d'exploitations sur une seule machine physique, et permet de diviser les ressources systèmes entre des machines virtuel.
La virtualisation permet aussi l'isolation en fournissant isolation de faute et de sécurité à un niveau matériel mais aussi en préservant les performance avec un contrôle avancé des ressources.
La virtualisation permet l'encapsulation qui sauvegarde l'état entier d'un machine virtuel dans un fichier, et change et copie la machine virtuel aussi facilement que déplacer et copier des fichiers.
La virtualisation permet l'indépendance du matériel en provisionnant ou migrant n'importe quelle machine virtuel vers n'importe quelle serveur physique.

La virtualisation permet une réduction des coût conséquent car il y a moins de serveurs physique et donc de coût dans l'utilisation de l'énergie du serveur. Les VM requière aussi moins de temps à configurer. Les VM sont bien plus rapide et productive comparé au traditionnel serveur uniquement physique.
Voici une explication de comment les VM peuvent se connecter entre elles vers un réseau externe de l'hôte physique.



Les VM sont connectés entre elles avec le réseau externe par le Switch virtuel qui se lance sur l'hyperviseur. Tout comme un Switch normal l'interface vSwitch peut fonctionner comme port trunk ou access et utiliser des VLANs pour séparer les VM en couche 2.
Les interfaces sur le vSwitch se connectent ensuite au NIC physique du serveur pour communiquer avec le réseau externe.
Il est possible d'utiliser un VPC (Virtual Port Channel) pour former un port channel entre deux Switch pour une redondance.

Voyons à présent le fonctionnement du Cloud.
Le déploiement d'infrastructure IT traditionnel se fait en général comme suit :
- On Premises : Tous les serveurs, appareils réseau et autres infrastructure sont localisé par la propriété de l'entreprise. Tous les équipements sont achetés et acquis par l'entreprise pour être utilisé. L'entreprise est responsable de l'espace nécessaire, la puissance et la ventilation.
- Colocation : Les Data center qui vendent des espaces pour leurs clients afin qu'ils placent leurs infrastructures (Serveurs, appareils réseau). Le Data center fournit l'espace, l'électricité et la ventilation pour tous les appareils. Les serveurs, appareils réseau, etc.. sont toujours sous la responsabilité du client final, bien que le matériel ne soit pas localisé dans les locaux de l'entreprise cliente.
Les services Cloud fournissent une alternative très populaire et qui continue à augmenter en popularité. La plupart des gens associent « cloud » avec un fournisseur cloud publique comme AWS car c'est l'utilisation la plus commune du Cloud mais ça n'est pas la seule option existante.

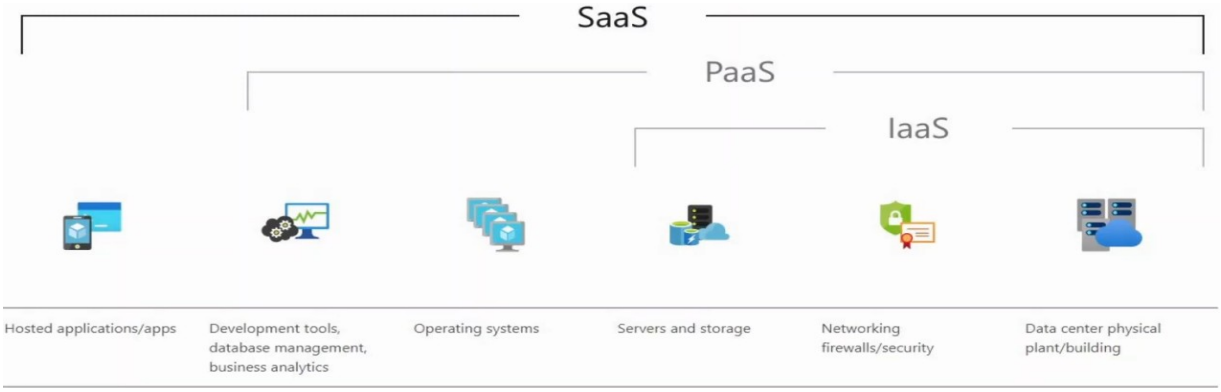
Le American NIST (National Institute of Standards and Technology) définit le Cloud Computing dans le SP (Special Publication) 800-145. Il est possible de le lire sur ce lien :
https://csrc.nist.gov/publications/detail/sp/800-145/final
Voici la définition en Anglais donnée par NIST :
Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

Voici les 5 caractéristiques essentiels du cloud computing :
- On demand self-service : le service sur demande consiste en un client qui utilise des capacités informatique comme le temps d'un serveur, le stockage dans un réseau et qui change automatiquement selon le besoin sans que cela ne requière d'interaction humaine avec chaque fournisseur de service. Le client a donc la possibilité d'utiliser le service (ou le stopper) gratuitement (par le portail web) sans avoir à communiquer à un fournisseur de service.
- Broad network access : Les capacités sont disponible sur le réseau et accessible par un mécanisme standard qui encourage l'utilisation fine ou épaisse de plateforme client (Par exemple des téléphones mobile, tablettes, ordinateurs portable, et station de travail). Le service est disponible par une connexion réseau standard (comme une connexion internet privée ou WAN) et peut être accessible par plusieurs type d'appareils.
- Ressource pooling : Les ressource Informatique du fournisseur sont regroupé pour servir plusieurs clients en utilisant un model multi locataire, avec différentes ressources physique et virtuel qui sont assignés dynamiquement et réassignés en accord avec la demande client. Il y a un sens de localisation indépendant dans cela le client généralement n'a pas de contrôle ou connaissances de la localisation exacte des ressources fournis mais est capable de spécifier la localisation à un haut niveau d'abstraction (par exemple le pays, ou le datacenter). Des exemples de ressources incluent le stockage, le processeur, la mémoir, et la bande passante réseau. Pour résumer, un groupement de ressource est fournit par le fournisseur de service et lorsque l'utilisateur fait la requête d'un service (par exemple créer une nouvelle VM), les ressources pour répondre à cette requête sont alloué depuis le groupement de ressource partagés.
- Rapid elasticity : Ces capacités peuvent être de manière élastique fournit et publiés, dans certains cas automatiquement, pour échelonner rapidement vers l'intérieur ou l'extérieur proportionnelement à la demande. Pour le client ces capacités sont disponible pour fournir souvent et apparaissent comme étant illimité et peuvent être acquise dans n'importe quelle quantité à n'importe quelle moment. Le client peut dont rapidement étendre les services qu'ils utilisent dans le Cloud (par exemple ajouter des Vms, étendre le stockage, etc...) depuis un groupe de ressource qui apparaissent comme illimités. Dans un autre sens ils peuvent rapidement réduire leurs service lorsque non nécessaire.
- Measured service : Le système Cloud contrôle automatiquement et optimise la ressource utilisé en mesurant la capacité à un certain niveau d'abstraction appropriés au type de service (par exemple le stockage, le processeur, la bande passante, et les comptes utilisateurs). L'utilisation de ressource peut être géré, contrôlé, et reporté, ce qui fournit une transparence pour le fournisseur et le client des service utilisés. Le fournisseur de service Cloud mesure l'usage client en ressource Cloud, et le client peut mesurer sa propre utilisation. Les clients sont chargés basé sur l'utilisation (Par exemple, X Dollar par Gigabyte de stockage par jour)

Voyons les 3 modèles de service du Cloud. Dans le cloud computing tout est fournit par un modèle de service. Par exemple au lieur que le client achète un serveur physique, le monte sur un rack, installe un hyperviseur, crée les Vms, etc. le fournisseur de service offre tout cela comme un service. Il y a une variété de services qui prend la forme « …. as a Service » or « ...aaS »
Les trois modèles de service du cloud computing sont :
- Software as a Service (SaaS) : La capacité fournit au client est d'utiliser le fournisseur d'applications lancé sur l'infrastructure Cloud. Les applications sont accessible depuis des appareils client variés comme une interface client « fine » comme un navigateur web, ou une interface d'un programme. Le client ne gère ou ne contrôle pas les sous niveaux de l'infrastructure Cloud en incluant le réseau, les serveurs, l'OS, le stockage, ou même les capacité individuel de chaque applications, mais une possible exception sur la limite d'un utilisateur spécifique des paramètres de configuration. Microsoft 365 est un exemple populaire de SaaS.

- Platform as a Service (PaaS) : La capacité fournit au client est de déployer dans l'infrastructure Cloud les créations du clients ou applications acquises crées en utilisant un langage de programme, des librairies, des services, et des outils supportés par le fournisseur. Le client ne gère ou ne contrôle pas les sous couches de l'infrastructure Cloud en incluant le réseau, les serveur, l'OS, ou le stockage, mais a le contrôle à travers les applications déployés et possiblement les paramètres de configuration pour environnement de l'application hôte. Des exemples d'offres sont AWS Labda et Google App Engine.
- Infrastructure as a Service (IaaS) : La capacité fournit au client est de provisionner le stockage, le réseau et d'autres ressources fondamentales Informatique ou le client est capable de déployer et lancer des logiciel arbitraire, qui incluent des OS et applications. Le client ne gère pas ou ne contrôle pas les sous couches de l'infrastructure cloud mais a le contrôle sur le système d'exploitation, le stockage, les applications déployés, et possibilité de limiter le contrôle de composants réseau sélectionné (par exemple un mur de feu). Des exemple d'offres sont Amazon EC2 et Google Compute Engine.

Voici une image provenant de chez Microsoft qui permet de résumer les modèle de Cloud :



Voyons les 4 formes de déploiement de Cloud.
Pour la plupart des gens le Cloud signifie des fournisseur Cloud comme AWS, Azure et GCP.
Le Cloud publique est le modèle de déploiement le plus commun mais il ne s'agit du seule moyen de déploiement Cloud. Il en existe 4 :

- Private Cloud : L'infrastructure cloud est fournit pour l'utilisation exclusive par une seule organisation comprenant plusieurs clients (Par exemple des unités de Business). Cela peut être acquis, géré, et modifié par l'organisation, un tiers partie, ou certaines combinaisons de cela, et peut exister en « on » ou « off » premise. Les Cloud privée sont généralement uniquement utilisé par de grandes entreprises. Bien que le cloud soit privée, il peut appartenir à des tiers partie comme par exemple des service fournisseurs AWS privée cloud pour le American DoD. Les cloud privée peuvent être « on » ou « off » premise. De nombreuses personne assument que le Cloud et On premise sont deux choses différentes, mais ça n'est pas toujours le cas. Le même type de services offerts sont les même que sur le cloud publique (SaaS, PaaS, IaaS), mais l'infrastructure est réservé pour une seule organisation.

- Community Cloud : Cette infrastructure cloud fournit une utilisation exclusive par une communauté spécifique de clients depuis des organisations qui concernent des partages (par exemple des mission, des prérequis de sécurité, prérequis de conformité). Cela peut appartenir, être géré et fonctionner par un ou plus des organisation dans la communauté, un tiers partie, ou une combinaison des deux, et peut exister en « on » et « off » premise. C'est le type de déploiement Cloud le moins fréquent. C'est similaire au Cloud privée mais l'infrastructure est réservé pour être utilisé uniquement par un groupe spécifique ou des organisations.

- Public Cloud : Cette Infrastructure cloud est fourni pour une utilisation ouverte par un publique général. Cela peut appartenir, être géré, et fonctionner par un Business, une académie, ou une organisation du gouvernement, ou une combinaison de cela. Il peut exister en on premise du fournisseur Cloud. C'est le modèle de Cloud le plus fréquent. Des service cloud populaire inclus : AWS (Amazon Web Service), Microsoft Azure, GCP (Google Cloud Platform), OC (Oracle Cloud Infrastructure), IBM Cloud, Alibaba Group.

- Hybrid Cloud : Cette infrastructure Cloud est composé de deux ou plus d'infrastructures Cloud (Privée, communauté, ou publique) qui reste une entité unique mais qui sont lié ensemble par une technologie propriétaire ou standardisé qui permet la portabilité des données et des application (Par exemple Cloud bursting pour load balance entre plusieurs Cloud). Cette une combinaison des trois différents type de déploiement précédemment vu. Par exemple un cloud privée qui peut décharger ses ressources vers un cloud publique lorsque nécessaire.

Les bénéfices du cloud computing sont les suivant :
- Coût : CapEx (Capital Expenses) les coûts de l'achat du matériel et logiciel, mise en place des data centers, etc. sont réduis ou éliminés.
- Scalabilité Global : Les services Cloud peuvent être évolutif globalement avec une mis en place rapide. Les services peuvent être mis en place et offets aux clients depuis une localisation géographique proche de chez eux.
- Rapidité/Agilité : Les services sont fournis sur demande, et un vaste montant de ressources peut être provisionné dans les minutes.
- La productivité : Les services Cloud supprime le besoin pour plusieurs tâches de consommation de temps comme de se procurer un serveur physique, le rackage, le câblage, l'installation, la mise à jour des systèmes, etc...
- Fiabilité : Les Backups sur le Cloud sont vraiment facile à fonctionner. Les données peuvent être mis en miroir (copiés) sur plusieurs sites sur des localisations géographique différentes pour supporter la récupération des désastres (feu, inondation etc..)

Il faut garder en tête que le Cloud n'est pas toujours la meilleur option. La plupart des compagnies de nos jours utilisent une combinaison d'équipements On premises, Colocation et Publique Cloud. Une compagnie ne devrait pas utiliser le Cloud seulement puisque c'est populaire de nos jours.

Voyons comment une entreprise fait pour se connecter leur réseau aux ressources d'un cloud publique.
Il existe plusieurs moyens qui peuvent être :
- Un WAN privée par un fournisseur de services
- Un service Internet
- Un tunnel VPN IPsec

Le schéma suivant résume cela :