Le Cloud Computing

Projet de Synthèse

BERNIER françois

Le Cloud computing annonce la fin d'une ère de l'informatique , celle des systèmes d'informations juxtaposés, de façon parfois chaotique au sein de l'entreprise et le début d'une autre , l'avènement de nouveaux services numériques disponibles en tout lieu, à la demande, et pour toute organisation, quelle que soit leur taille.

Ce déplacement progressif de l'informatique vers les réseaux et les centres de données va rendre notre rapport à l'informatique de plus en plus abstrait, loin des machines et des infrastructures, laissant ainsi toute sa place à l'usage. Car si le Cloud computing est évidemment aussi une révolution de l'informatique hardware, cette révolution fait avant tout la plus large place à de nouveaux usages. Ce n'est pas un hasard si ces usages viennent principalement du grand public (webmail, messagerie instantanée, réseaux sociaux) et que ce sont les acteurs déjà présents sur ces marchés qui figurent aujourd'hui en tête du Cloud computing BtoB(L)…

L'informatique de demain sera donc «bon marché et convivial » ou ne sera pas… Dernière interface avec l'utilisateur, le logiciel est évidemment au cœur de cette révolution « as a service ». Le Software as a service (Saas) est aujourd'hui le principal moteur de croissance du Cloud computing, la dimension Plateform as a service (Paas) étant également le fait d'acteurs majeurs du logiciel. Le logiciel est au cœur de cet environnement en étant aussi présent dans ses couches « basses » où les technologies de virtualisation jouent un rôle crucial.

Qu'on ne s'y trompe pas, il ne s'agit pas d'une simple tendance mais d'une véritable révolution qui touchera dans les années à venir toutes les entreprises, publiques et privées, de toutes tailles, PME comprises, avec des conséquences lourdes sur les organisations, les métiers, les effectifs, pour une raison incontournable : une baisse des coûts d'exploitation dans un rapport de dix.

Le Cloud est tout à la fois synonyme de centralisation au sein d'énormes datacenters (diminution des coûts), de disponibilité via Internet (24/7) et d'agilité (délais de mise en œuvre courts). Il offre surtout au DSI(L) une solution pour réduire, les budgets de la DSI, la contrainte budgétaire de nouveaux projets, les coûts de maintien en condition opérationnelle de l'existant et l'indispensable innovation.

(L) → Voir Lexique en fin de document

Table des Matières

Pourquoi le Cloud ? ..... **Page 3**

- Quelles formes ? A quelle échéance ? Comment s'y préparer ?

Les types de services : IaaS (Infrastructure as a Service), PaaS (Platforme as a Service), SaaS (Software as a Service). ..... **Page 6**

→ **IaaS (Infrastructure as a Service).** p7
→ **PaaS (Platforme as a Service).** p8
→ **SaaS (Software as a Service).** p8

Les modèles de déploiement ..... **Page 12**

- Privé, public, hybride, communautaire.

Les infrastructures technologiques ..... **Page 16**

- Datacenters, infrastructures, technologies utilisées, la technique des containers.
- La virtualisation des serveurs et du poste de travail. L'offre VMWare, HyperV, ... p21

Le contrat ..... **Page 23**

- Les clauses
- Les engagements de service SLA p25
- Les avantages , les freins p29
- Appréhender la Sécurité p31

Le marché et les offres ..... **Page 33**

- Les prévisions chiffrées. Pourquoi une majorité de fournisseurs s'orientent vers le Cloud ?
- Analyse de l'offre des principaux fournisseurs dans chaque catégorie p35

Mise en application ..... **Page 48**

- Installation et configuration d'une solution de Cloud OpenSource : Apache CloudStack 3.02
- Configuration p64
- Prise en main de l'interface p78
- Intégration d'une VM dans la zone Cloud p86
- Problèmes rencontrés lors de l'installation p92

Conclusion ..... **Page 93**

Lexique, Références et Annexes ..... **Page 96**

Pourquoi le Cloud ?

Le Cloud Computing pourrait ainsi être défini de la manière suivante :

Le Cloud Computing est un concept désignant de nouvelles pratiques et services numériques reposant sur l'utilisation d'Internet et de réseaux étendus et sur la mise en commun de ressources numériques et matérielles, qui se caractérisent par : une flexibilité immédiate, une possibilité de paiement à la demande et une virtualisation des systèmes, conférant ainsi une forte abstraction du service du point de vue l'utilisateur.

Quelles que soient les définitions, le Cloud computing se décompose généralement selon trois types de services :

• Le "Software-as-a-Service" (SaaS). Applications informatiques mises à disposition via une infrastructure de Cloud, telle qu'un navigateur Internet, sans gestion par l'utilisateur du réseau, des serveurs, des systèmes d'exploitation, du stockage, voire d'une part majoritaire des paramètres propres aux dites applications.
• Le "Platform-as-a-Service "(PaaS). Possibilité pour l'utilisateur de bénéficier d'un environnement de développement et d'exécution , via l'infrastructure de Cloud, pour les applications qu'il a créé ou acquises, en utilisant des langages de programmation et des outils supportés par le fournisseur, sans avoir à gérer le réseau, les serveurs, les systèmes d'exploitation ni le stockage.
• Le "Infrastructure-as-a-Service" (IaaS). Possibilité pour l'utilisateur de bénéficier, à la demande, d'une infrastructure matérielle lui fournissant une capacité de traitement, sans avoir à gérer le réseau en tant que tel.

Enfin, le Cloud computing se décompose selon quatre usages qui incarnent en fait quatre types d'accessibilité :

• **Cloud privé** : usage interne. L'infrastructure n'est exploitée que par une seule organisation, hébergée à demeure ou à distance.
• **Cloud public** : usage externe. L'infrastructure peut être exploitée par un large public, l'infrastructure restant hébergée par l'entreprise fournissant le service.
• Cloud Communautaire : L'infrastructure est partagée entre plusieurs organisations supportant une communauté précise et ayant des préoccupations communes. Elle peut être gérée par les organisations ou par une tierce partie.
• Cloud hybride : Environnement au sein duquel une organisation fournit et gère certaines ressources à domicile et d'autres de manière externe.

Selon une étude du cabinet Markess, les PME seront de plus en plus nombreuses à utiliser des solutions de cloud.

Selon le cabinet d'analyse spécialisé dans les technologies du numérique, une PME sur 5 aurait déjà recours à des ressources informatiques externes (cloud). Un choix motivé par le fait de permettre à des collaborateurs d'accéder à distance à des applications de l'entreprise (45 %), par le souci de réduire des dépenses d'investissements informatiques (37 %) ou encore par la facilité d'accès (36 %) et la simplification des mises à jour de ces applications (32 %). Des applications distantes dont les plus citées par les 370 dirigeants interrogés sont les agendas, les messageries, les solutions de sauvegarde, de stockage des données et de web conférence.

Pour les DSI, le cloud computing suscite trois questions fondamentales : comment s'y retrouver dans le foisonnement des offres qui évoluent en permanence ? Comment intégrer le cloud computing dans le système d'information existant ? Comment éviter une atomisation du système d'information, les directions métiers étant tentées de souscrire elles-mêmes à des offres cloud sans y associer la DSI ?

La réponse à la première question passe par une prise de position claire du DSI dans le débat sur le cloud computing qui ne manquera pas, si ce n'est pas déjà le cas, de surgir dans l'entreprise. Il s'agit clairement, pour le DSI, d'adopter une posture positive et d'anticipation. D'abord, par la maîtrise des spécificités du cloud computing, qui lui permettra de se préparer aux inévitables évolutions des compétences des équipes de la DSI. Ensuite, le DSI a une mission pédagogique dès lors qu'il faut expliquer, avec la meilleure objectivité, ce qu'apporte le cloud computing et quelles en sont les limites. La principale inquiétude concerne la sécurité, argument largement mis en avant pour s'y opposer. Le rôle du DSI sera alors d'expliquer que les risques peuvent être contrôlés, par exemple par une gouvernance adaptée, des règles contractuelles précises, une bonne connaissance des technologies et une maîtrise des usages. Enfin, le DSI se doit de préempter le sujet du cloud computing, pour éviter de se faire déborder par les fournisseurs qui, eux, ont bien compris qu'ils pouvaient s'adresser, avec autonomie et un certain succès, directement aux directions métiers, y compris en mettant en exergue les ressentis des Directions Métiers souvent synthétisés par une lourdeur de la DSI et un potentiel manque de réactivité pour répondre à leurs besoins.

La réponse à la seconde question amène à rappeler que le DSI est le garant du patrimoine informationnel de l'entreprise, c'est lui qui assure le fonctionnement opérationnel du système d'information pour accompagner les métiers et qui assume les risques numériques. De fait, la DSI est la mieux placée pour susciter de nouveaux usages dans l'entreprise, pour en mesurer les apports concrets et pour trouver et optimiser les ressources.

Eviter l'atomisation du système d'information va consister à adapter les modèles de gestion du système d'information, notamment par la contractualisation, la gestion technique, humaine et financière des ressources, et une adaptation des systèmes de mesure des coûts du SI, en lien avec de nouveaux modèles de facturation spécifiques au cloud computing. Dans la mesure où la logique traditionnelle de gestion du système d'information passe d'un modèle investissement/exploitation à une logique de services basés sur la consommation, le DSI se trouve, qu'il le veuille ou non, dans une zone d'incertitude. Redéfinition des métiers, transformation de l'organisation et des architectures, nouveaux modes de création de valeur, ré-urbanisation du système d'information… : si le cloud computing est synonyme de rupture(s), c'est aussi le terrain naturel et légitime du DSI !

Selon le National Institute for Standards and Technology (NIST) la définition du Cloud Computing est la suivante et se caractérise en 5 fonctions essentielles, 3 niveaux de services, 4 modèles de déploiement

Selon le NIST, le cloud computing doit posséder 5 caractéristiques essentielles :

- Le service doit être en libre-service à la demande
- Il doit être accessible sur l'ensemble d'un réseau
- Il doit y avoir une mutualisation des ressources
- Il doit être rapidement élastique (adaptation rapide à une variation du besoin)
- Le service doit être mesurable (mesure et affichage de paramètres de consommation)

Le NIST distingue 3 niveaux de service :

- **Le logiciel en tant que service (Software as a Service - SaaS)** : par exemple une banque "loue" un logiciel de comptabilité, en ligne, à la demande, chez un prestataire externe;
- **La plateforme en tant que service (PaaS)** : une solution externe qui propose une suite logicielle et les outils d'intégration et de suivi; Par exemple, un serveur web (Linux+Apache+MySQL+Php)
- **L'infrastructure en tant que service (IaaS)** : la totalité de l'infrastructure (ressources matérielles) est externe. Par exemple, capacité de stockage et capacité de calcul à la demande sur un réseau.

Et 4 modèles de déploiement :

- Le **Cloud privé** (au sein d'une même organisation)
- Le **Cloud communautaire** (réservé à une communauté)
- Le **Cloud public** (ouvert au grand public)
- Le **Cloud hybride** (composition de deux ou plusieurs types de nuages)

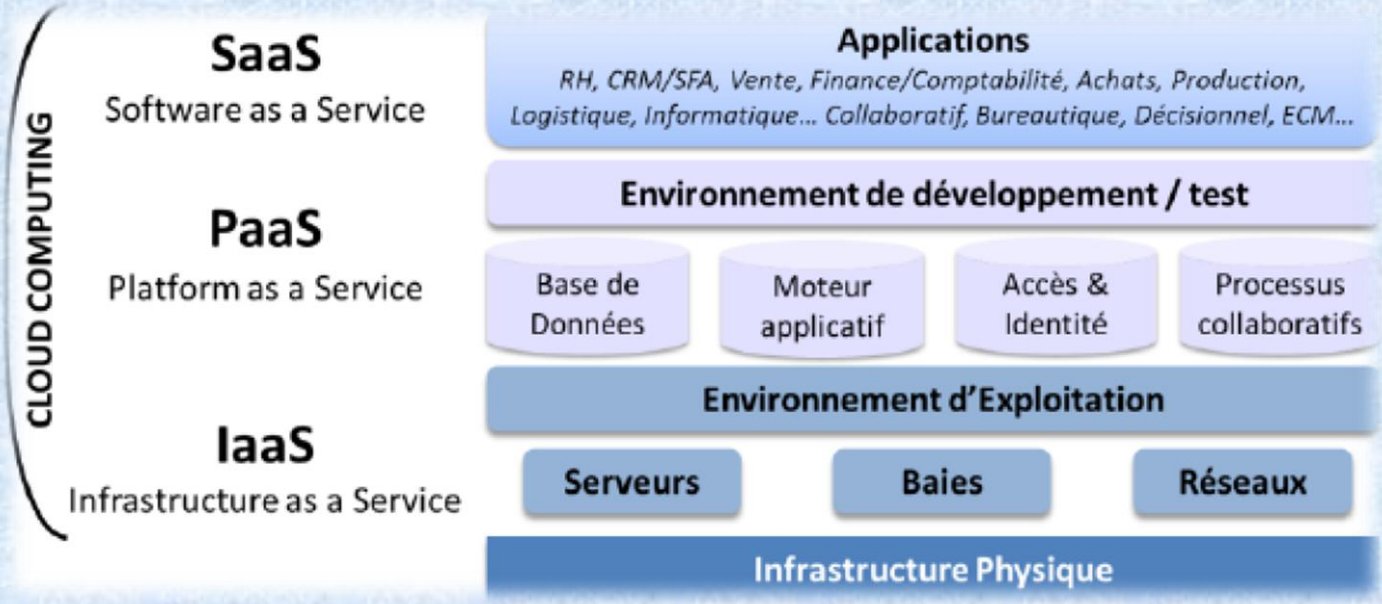
Les types de services.

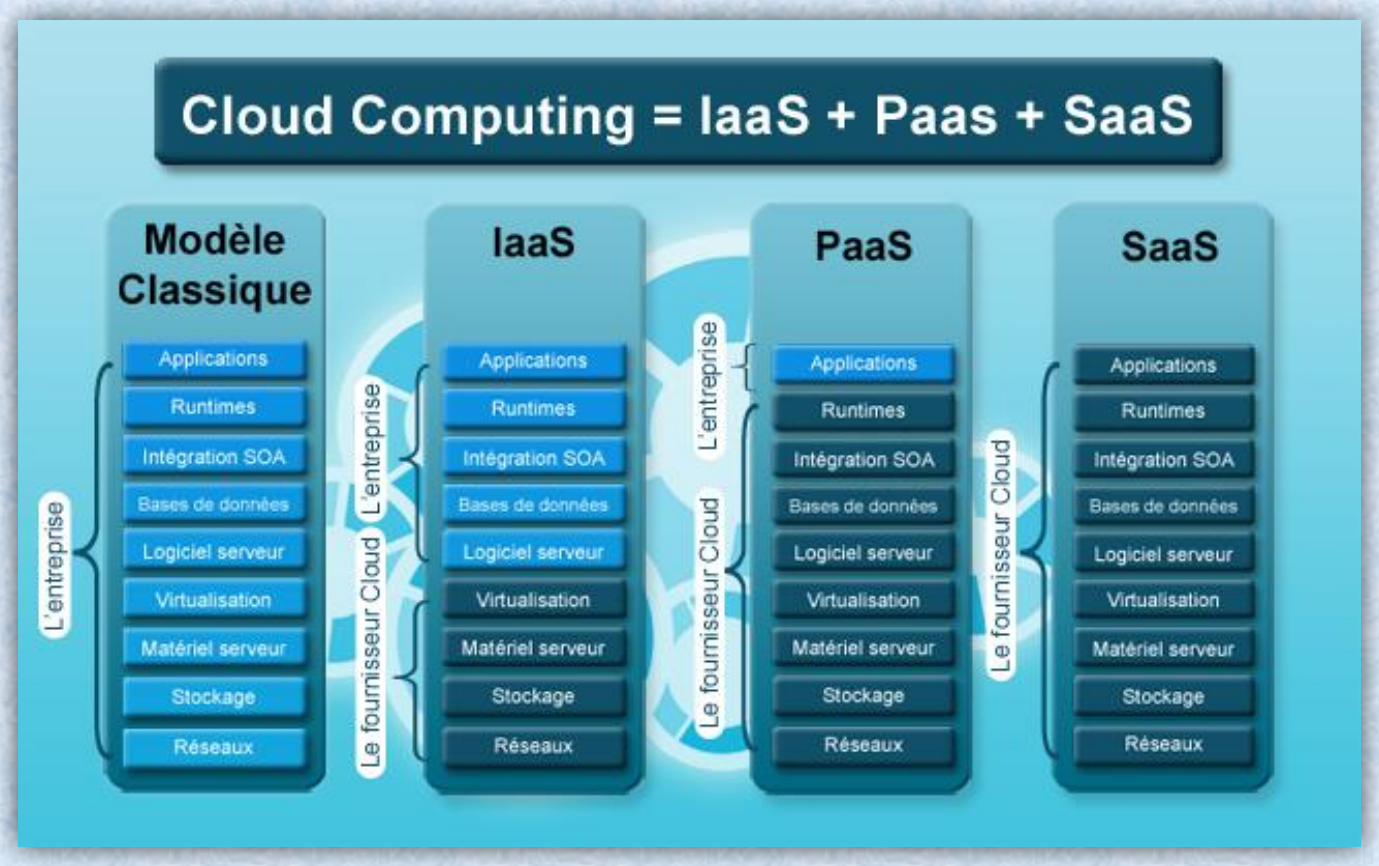
Quand on parle de Cloud Computing, on détermine les offres comme étant « as a *service* » et ce qui détermine le service c'est le contrat. Donc il faut le lire avec beaucoup d'attention. Bien-sûr, il y a les clauses évidentes comme le « service level agreement (ou SLA) » dont nous parlerons plus loin , où il faut à tout prix qu'il y ait des pénalités à la clef, mais il faut aussi regarder les clauses de réversibilité, de localisation des données ; est-ce que les données sont bien en France et si elles ne sont pas en France, où sont-elles ?
Ensuite, il y a des clauses de protection des données, de confidentialité, de propriété intellectuelle, ce sont autant de points qu'il faut absolument regarder pour être sûr de signer un bon contrat qui protège bien le client. Nous détaillerons plus en détail le contrat plus loin dans ce document.

Comme nous avons vu précédemment, le Cloud Computing c'est :

- L'informatique « comme un service », c'est-à-dire à la demande
- Souvent basé sur de la virtualisation (surtout pour l'IaaS et le PaaS)
- Trois couches de service :
  - Infrastructure
  - Plateforme
  - Applicative
- Du « self-service » avec un paiement à la consommation.
- Abstraction, mutualisation et allocation dynamique des ressources physiques.

Quelles sont plus exactement ces trois couches de service, quels sont leurs modes de fonctionnements et leurs périmètres ? Les couches les plus basses le Cloud Computing fournissent un service complet jusqu'à l'utilisateur.





L'INFRASTRUCTURE COMME UN SERVICE (IAAS)

L'infrastructure fournit des capacités de calcul et de stockage ainsi qu'une connectivité réseau. Les serveurs, systèmes de stockage, commutateurs, routeurs et autres équipements, sont mis à disposition pour gérer une charge de travail demandée par les applications.

L'infrastructure comme un service ou IaaS, permet de disposer d'une infrastructure à la demande, pouvant héberger et exécuter des applications, des services ou encore stocker des données.

Concrètement, cela se caractérise par une infrastructure physique souvent mise à disposition par un fournisseur de services. On y trouvera une solution de virtualisation permettant la création de « Datacenters virtuels ».

Grâce aux solutions de virtualisation existantes, il est possible de créer très facilement des machines virtuelles connectées sur des réseaux, eux aussi virtuels, et qui seront exécutés sur les hyperviseurs des machines physiques.

Cette virtualisation nous donne une grande flexibilité parce qu'elle permet d'abstraire la couche matérielle sur laquelle les applications qui vont pouvoir être déployées et redéployées sans être liées à un serveur spécifique. La virtualisation répond de manière dynamique là où les serveurs physiques fournissent un ensemble de ressources allouées selon les besoins, et où la relation entre les applications et les ressources de calcul, de stockage et de réseau, pourront s'adapter de manière automatique pour répondre à la charge de travail et aux exigences demandées.

Amazon AWS propose, par exemple, le service EC2. Il s'agit d'une offre IaaS reposant sur un hyperviseur XenServer, permettant à un client de demander des ressources informatiques pour y héberger ses applications. Sur Amazon EC2, il est possible de demander une ou plusieurs machines virtualisées sur les hyperviseurs d'Amazon. Cela permet de bénéficier d'une infrastructure flexible liée à une facturation en fonction de l'utilisation des ressources exploitées.

EC2 est compatible Windows et Linux pour les systèmes virtualisés. Et de plus en plus d'éditeurs proposent leurs logiciels « EC2 ready » sous forme d'images virtuelles préconfigurées.

Pour créer son propre IaaS, plusieurs solutions existent. VMware propose vSphere et vCloud Director, qui permettent la création d'un « Datacenter virtuel » dans lequel on pourra héberger des « VApp », une (ou plusieurs) application fonctionnant sur un ensemble de machines virtuelles connectées sur leur propre réseau virtuel. Ces « Datacenters » seront virtualisés sur une infrastructure physique partagée, mise à disposition par un fournisseur de services comme Terremark, Verizon ou encore Colt. Microsoft fait de même avec Hyper-V Cloud qui définit les règles d'architectures que les constructeurs utilisent pour proposer des infrastructures clés en main.

LA PLATEFORME COMME UN SERVICE (PAAS)

La plate-forme comme un service est la plate-forme d'exécution, de déploiement et de développement des applications.

Il y a deux types de PaaS :

- Celui qui fournit une plate-forme intégrant le système d'exploitation (OS), la couche middleware et celle applicative qui sont fournies ensuite au client comme un service.
- Un service métier encapsulé et présenté via une API. Le client interagit avec cette plate-forme grâce à une API pour construire un service de plus haut niveau : la plate-forme se gère et s'adapte elle-même pour fournir le niveau de service attendu.

Le PaaS met à disposition des environnements prêts à l'emploi, fonctionnels et performants.

Les offres PaaS commencent à être matures. Parmi les solutions, citons Windows Azure de Microsoft, AppEngine de Google, Force.com de Salesforce. Chaque PaaS propose des modèles de développement différents. Google AppEngine se limite à Java et Python alors que Windows Azure travaille avec les langages .Net, Python, PHP, Ruby, Java.

Pour un développeur .NET, il s'agit de développer son application de manière locale, qui une fois prête, pourra être déployée : une simple commande génère le paquet et le déploiement se fait automatiquement sur le Cloud Windows Azure par exemple. L'application est alors immédiatement disponible et fonctionnelle.

Cependant, les PaaS ne sont pas seulement des environnements prêts à l'emploi pour les déploiements d'applications. Ils peuvent aussi être des services applicatifs accessibles au travers d'API : Citons par exemple les services de stockage de Windows Azure Storage pour le Cloud de Microsoft, ou encore S3 (Simple Storage) chez Amazon.

Grâce aux PaaS, le déploiement d'applications dans différents environnements est très facile (test, pré-production et production sans se soucier de l'infrastructure et de la plate-forme dans lesquelles vont s'exécuter l'application ou le stockage de données).

LE LOGICIEL COMME UN SERVICE (SAAS)

La dernière couche du SaaS est celle applicative mettant à disposition des applications complètes fournies à la demande. On y trouvera différents types d'application allant du CRM, à la gestion des ressources humaines, comptabilité, outils collaboratifs, messagerie, BI et d'autres applications métiers.

Il n'y a donc aucun prérequis sur le poste client si ce n'est d'avoir un accès réseau au Cloud (en général Internet). Le déploiement, la maintenance, la supervision du bon fonctionnement de l'application et la sauvegarde des données, sont alors de la responsabilité du fournisseur de services.

Sur cette couche, des acteurs tels que Salesforce.com, proposent des applications à la demande de type CRM et des outils de collaboration. Cela permet à un client de bénéficier d'une application de manière instantanée et à la demande sans aucun frais en

immobilisation (serveur ou licence), aucun déploiement ou maintenance à assurer. Il suffit de créer un compte et de profiter immédiatement d'un service de collaboration ou d'un CRM prêt à l'emploi.

Prenons l'exemple simple d'une solution de messagerie que l'on souhaite déployer dans une nouvelle entreprise. Le schéma classique intègre l'acquisition ou la location de serveurs et l'installation du système d'exploitation sur lequel la solution sera déployée (comme **Lotus**, **Postfix** ou **Microsoft Exchange**). Suite au déploiement, il y a une phase de configuration puis de test avant de pouvoir passer ce service en production. Il s'agit ensuite de gérer la maintenance de cette messagerie, la supervision de son bon fonctionnement, l'application des mises à jour notamment concernant la sécurité, la réalisation de sauvegarde des données, l'élaboration d'une politique de gouvernance et d'un plan de reprise sur activité en cas d'incident.

Tout cela a un coût, tant sur le plan financier, matériel et humain : en effet, cela nécessite une équipe d'experts qualifiés pour assurer la bonne exploitation de cette solution. Il n'est pas rare d'ailleurs, que les entreprises fassent appel à des sociétés extérieures, notamment sur le secteur de l'infogérance.

Que l'on soit au niveau de l'infrastructure, de la plate-forme ou ici du service ou de l'application, les problématiques restent les mêmes : il faut des moyens financiers, matériels et humains pour maintenir un niveau de service demandé par les utilisateurs.

Avec le Cloud, nous avons des solutions SaaS comme « App » de Google ou encore « Exchange Online » de Microsoft qui mettent à disposition un service de messagerie à la demande : Il suffit qu'un administrateur crée son organisation sur l'un de ces services et il peut l'utiliser instantanément et avec très peu de configuration dans son entreprise.

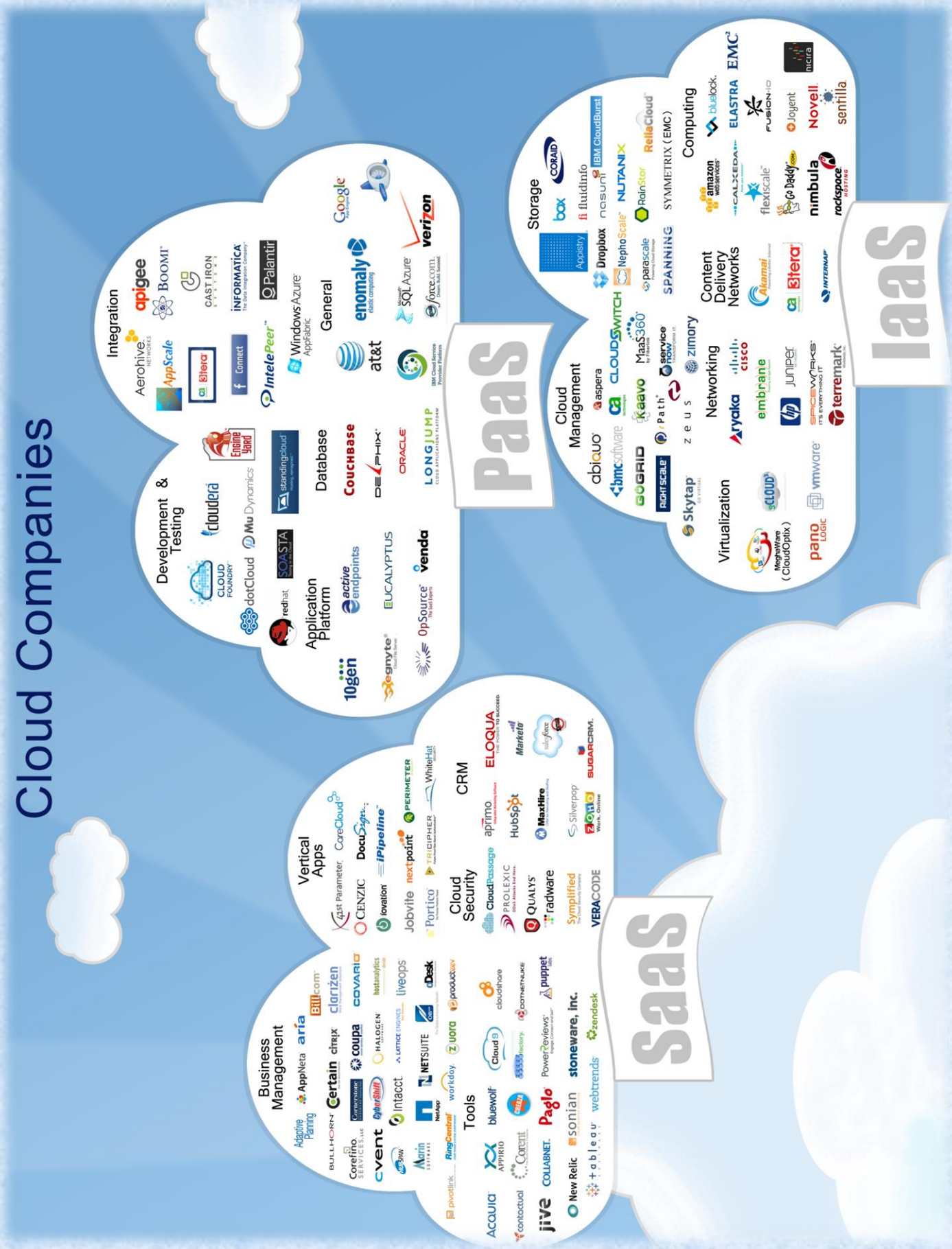
Toute la charge repose sur le fournisseur de service SaaS qui assurera le déploiement de la solution de manière dynamique et instantanée, supervisera le bon fonctionnement, répartira la charge sur ces différentes ressources physiques, assurera la sécurité, les mises à jour et les plans de reprise sur incident. La plupart des services Cloud garantissent la disponibilité du service et des données par différents contrats SLA (nous reviendrons sur cette notion un peu plus tard).

De ce fait, le client est consommateur d'un service lui offrant la possibilité de s'abstraire de toutes contraintes financières, matérielles et humaines, dans le déploiement et l'exploitation de différentes solutions applicatives.

Dans cette notion de « consommation », la facturation est liée à l'utilisation du service. Par exemple sur Exchange Online, le coût est lié au nombre d'utilisateurs dans l'organisation. De plus, Exchange Online fournit un quota de stockage pour l'ensemble des boîtes aux lettres de l'organisation (sur base de 25 Go par utilisateur). Il est ensuite possible d'acheter de la place supplémentaire si besoin (par tranche de Giga à répartir dans l'organisation).

De nombreuses organisations ont fait le choix de solutions SaaS, s'assurant ainsi une disponibilité de services souvent supérieure à ce qu'une équipe peut fournir en interne (surtout pour les PME et institutions) et pour un coût adapté à leurs besoins.

Sur la page suivante vous pouvez visualiser les acteurs principaux des 3 couches de services précédemment décrites.


Cloud Companies
Integration
Aerohive
apigee
AppScale
BOOMI
Bitera
CAST IRON
Connect
INFORMATICA
IntelePeer
Palantir
Development & Testing
cloudera
Engine Yard
dotCloud
Mu Dynamics
standingcloud
Application Platform
redhat
SOASTA
active endpoints
EUCALYPTUS
10gen
egnyte
OpSource
venda
Database
Couchbase
DEPHIX
ORACLE
LONGJUMP
General
Windows Azure AppFabric
enomaly
at&t
Google
SQL Azure
force.com
verizon
PaaS
Storage
box
CORAID
Appistry
Dropbox
fluidinfo
nasuni
IBM CloudBurst
NephoScale
NUTANIX
RainStor
ReliaCloud
parascale
SPANNING
SYMMETRIX (EMC)
Cloud Management
abiquo
aspera
bmcsoftware
CA
CLOUDSWITCH
GOGRID
kaavo
MaaS360
RIGHTSCALE
Path
service now
zeus
zimory
Skytap
Content Delivery Networks
Akamai
Bitera
INTERNAP
Networking
Aryaka
cisco
embrane
juniper
SPICEWORKS
terremark
Virtualization
CLOUD
MegaWare (CloudOptix)
pano LOGIC
vmware
Computing
amazon web services
bluelock
CALXEDA
ELASTRA
EMC²
flexiscale
FUSION-IO
GoDaddy.com
Joyent
nimbula
Novell
nicira
rackspace
senfilia
IaaS
Vertical Apps
4st Parameter
CareCloud
CENZIC
DocuSign
ivation
iPipeline
Jobvite
nextpoint
PERIMETER
Portico
TRICIPHER
WhiteHat
Cloud Security
CloudPassage
PROLEXIC
QUALYS
radware
Symplified
VERACODE
CRM
aprimo
ELOQUA
HubSpot
Marketo
MaxHire
salesforce
Silverpop
zoho
SUGARCRM
Business Management
Adaptive Planning
AppNeta
aria
BILLING.com
BULLHORN
Certain
citrix
clarizen
Corefino
coupa
COVARIO
cvent
DynamicBMR
HALOGEN
hostanalytics
Intacct
LATTICE ENGINES
liveops
Marin
NETSUITE
oDesk
pivotlink
RingCentral
workday
Zuora
productiv
Tools
ACQUIA
bluewolf
cloudshare
contactual
Corent
DATANETWORK
jive
COLLABNET
Paglo
PowerReviews
puppet
New Relic
sonian
stoneware, inc.
tableau
webtrends
zendesk
SaaS

La prolifération des 'aaS'

De nombreux autres acronymes en '**aaS**' émergent, pas toujours à bon escient, mais associés au Cloud Computing qui s'affiche désormais comme un mode de consommation des services IT.

Il devient fastidieux de les décrire tous puisque dans ce contexte de multiplication des services, les offres 'aaS' sont cuisinées à toutes les sauces…. Contentons-nous de citer les principaux :

- **DaaS** (**Data-as-a-Service**, ou… **Desktop-as-a-Service** ?)

  Encore un piège… Un même acronyme pour deux significations (Data ou Desktop). Dans les modèles d'usage du Cloud Computing, l'entreprise peut faire appel à une infrastructure dans le nuage (**IaaS**), ou à une plateforme matérielle et logicielle de base (**PaaS**) sur laquelle elle fera tourner ses logiciels métiers.

  Une autre approche peut consister à confier ses données au cloud (**DaaS, pour Data-as-a-Service**). C'est un concept qui commence à se répandre, car il simplifie le stockage des données et confie au fournisseur le soin de supporter les variations de volume de données stockées, – à la hausse comme à la baisse – que ce stockage soit permanent ou temporaire, et avec une solution contractuellement sécurisée.

  Les modèles de facturation s'appliquent à l'usage. Ils sont souvent accompagnés de clauses de volumétrie afin que le fournisseur, hébergeur, puisse anticiper le dimensionnement de son infrastructure. La facturation prend en compte le volume des données, parfois le type des données (par exemple, une donnée stratégique peut bénéficier d'un traitement particulier), et de l'utilisation de ces données (trafic et bande passante consommée). Il existe également des solutions au forfait.

  Le **Desktop-as-a-Service**, c'est autre chose. De fait, après le serveur, le stockage et aujourd'hui le réseau, le développement de la virtualisation atteint désormais le poste de travail. Pour simplifier, hors de sa partie matérielle, un poste de travail est composé d'un environnement (**OS**) et d'applications destinés aux utilisateurs. Ce poste est souvent identique d'un utilisateur à l'autre. En revanche, sa gestion se complexifie avec la nécessité de suivre chaque poste individuellement, avec sa maintenance et avec ses mises à jour.

  Pour simplifier cela, l'entreprise aura avantage à centraliser les postes de travail sous une forme virtuelle, l'utilisateur pourra ainsi en tout endroit, à tout moment et en mobilité, accéder à son environnement de travail. C'est ce que nous appelons la VDI (Virtual Desktop Infrastructure). Et pour aller jusqu'au bout de la démarche, le bureau de travail virtuel pourra être placé dans le cloud.

- le **MaaS** (Metal-as-a-Service) fait référence à l'automatisation de l'approvisionnement et du déploiement dynamiques dans le cloud des infrastructures physiques de très grande échelle (hyperscale) ;
- le **DRaaS** (DisasterRecovery-as-a-Service) est considéré comme une nouvelle étape du cloud computing, particulièrement aux États-Unis qui ont été sensibilisés à la problématique de la continuité de l'activité des services dans le cloud à la suite des ouragans qui ont dévasté certaines régions et entrainé des interruptions de services ;
- le **BaaS** (Backend-as-a-Service) : dernier entrant des services de cloud, c'est une approche du cloud novatrice imaginée par une start-up californienne.

  Les entreprises spécialisées sur ce secteur proposent des services hébergés dans le Cloud et particulièrement destinés à être accessibles sur les mobiles. Des services de ce type, autant être clair, il y en a de plus en plus… et ce n'est pas prêt de s'arrêter ! 60% des développeurs pourraient être concernés par le **BaaS**.

  Un des éléments expliquant le développement de ce marché est la demande affirmée des utilisateurs de Smartphones pour des services qui leur facilitent la vie et les accompagnent partout – comme par exemple les notifications, l'accès permanent à leurs photos ou l'utilisation d'applications utilisant la localisation géographique.

Les modèles de déploiement.

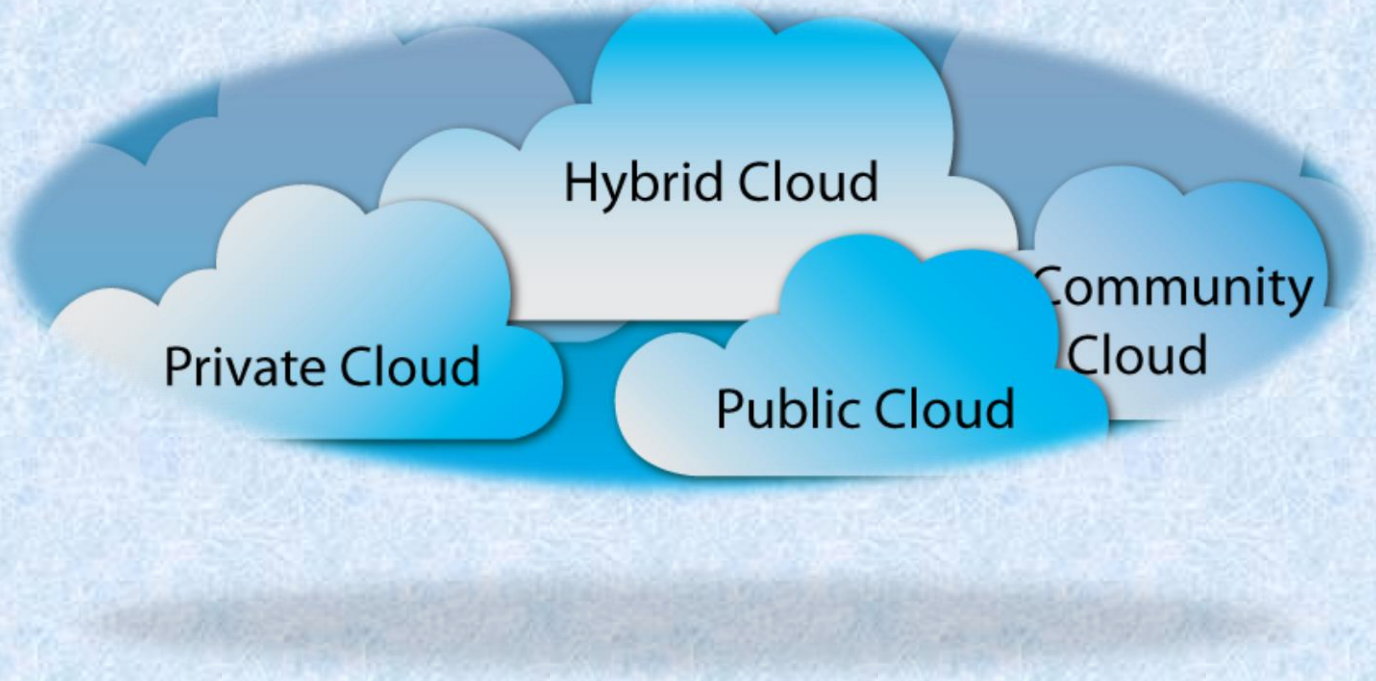
LES ARCHITECTURES CLOUD

Comme nous l'avons vu, le Cloud Computing repose sur des ressources physiques. La question est « où sont ces ressources physiques ? » (Serveurs, commutateurs, routeur, solutions de stockage, etc.).

La réponse « dans le nuage » n'est pas vraiment acceptable. Du point de vue consommateur, l'abstraction[L] est telle qu'on ne peut déterminer sur quelles ressources physiques l'application est hébergée. De par son côté dynamique, les ressources physiques hébergeant une application et des données dans un Cloud ne sont jamais fixes et évoluent dans le temps.

En théorie, le Cloud Computing n'impose aucune dépense en immobilisation, on exploite généralement les ressources physiques d'un fournisseur de Cloud.

Cependant cette technologie de Cloud Computing peut très bien se retrouver sur l'infrastructure physique d'une entreprise : n'étant plus mutualisé, le Cloud reste privé : on parlera alors de Cloud public, de Cloud privé et de Cloud hybride.



Cloud privé – Fonctionnement, avantages, inconvénients et développement

La définition du **Cloud privé** est sujette à des controverses. Les grandes entreprises fournisseurs, considèrent que l'implémentation d'un Cloud privé, consiste à transformer, grâce à des technologies de virtualisation et d'automatisation, l'infrastructure interne d'un système informatique. L'objectif à atteindre ainsi, est de fournir rapidement à des clients, à la demande et d'une manière simple, des services et des ressources. Parfois, vous pouvez entendre parler d'internal Cloud. Ce terme est traduit par Cloud privé interne ou Cloud interne.

Du côté hébergeur, une telle plate-forme est perçue comme la mise à la disposition à un client, d'un ensemble de ressources, telle une Mémoire, un CPU, un Disque, un Réseau et autre, qui lui permet d'installer une infrastructure complète. Dans cette situation, on parlera de cas d'offre IaaS, ou Infrastructure as a Service.

Le Cloud privé est prévu pour offrir aux entreprises, des services qui leur permettront de mieux maîtriser leurs ressources informatiques. L'entreprise peut gérer son infrastructure en solitaire, au rythme de ses besoins, ou passer par la mutualisation. Ce type de stockage peut être ainsi considéré d'une part, comme l'installation d'un réseau informatique propriétaire. D'autre part, on peut le désigner comme un centre de données qui fournit des services hébergés pour un certain nombre d'usagers. Il leur délivre des accès, particulièrement favorables pour leurs applications hébergées.

On distingue les Cloud privés internes, utilisés par une entreprise pour satisfaire ses propres besoins. Ils sont administrés en interne par l'entreprise même. Il y a aussi les Cloud privés externes, destinés à satisfaire les besoins propres d'une entreprise cliente. Leurs gestions sont confiées à un prestataire extérieur. On parle alors de gestion externalisée. Dans ce cas, une partie de ses services externalisés, est prise en charge par un prestataire de confiance.

Avantages du Cloud privé

Le Cloud privé comprend tous les avantages du Cloud Computing. Selon un sondage effectué par le cabinet d'études Pierre Audouin Consultants, aidé par EMS, VMware et Intel, sur 200 décideurs informatiques, 71% choisissent d'investir en Cloud privé, 13% préfèrent un système hybride et 7% seulement optent pour le Cloud public. Le lieu d'hébergement des données est connu de l'entreprise cliente. Il se trouve dans un lieu proche, dans le même pays que l'entreprise, pour éviter les litiges juridiques dus à la différence des législations en vigueur dans chaque pays hébergeur.

Une étude effectuée par la société Syntec cite la possibilité d'ouverture de ce type d'infrastructure. Le Cloud privé permet justement l'ouverture d'une entreprise vers ses partenaires. Il peut par exemple, étendre ses applications à ses fournisseurs, à ses prestataires ou à des bureaux d'études. De plus, sa flexibilité permet l'installation de modules ad hoc à n'importe quel moment, et la consommation se fait à la demande. Les coûts sont donc mieux maîtrisés. Enfin, le respect du caractère de confidentialité est gardé avec ce genre de plate-forme.

Inconvénients du Cloud Privé

L'efficacité d'un Cloud privé dépend beaucoup de la stabilité et des performances de l'infrastructure y afférente. Les problèmes de disponibilité, de sécurité, et surtout la question de réversibilité dans un Cloud, se posent toujours. Ce dernier point est particulièrement pointilleux, lorsque les fournisseurs de services emploient des normes et des outils peu courants, qui risquent de compromettre la qualité de service offerte aux utilisateurs. Mais la tendance actuelle dans ce type de stockage, est de passer d'un modèle personnalisé à un modèle normalisé.

L'adoption d'un Cloud privé, nécessite la bonne évaluation des demandes de performance et des variations cycliques de chaque application. La fluidité de son fonctionnement dépend de la fiabilité et de la rapidité du réseau. Les moindres ralentissements de la vitesse de transfert agissent négativement sur les performances. Ceci implique la surveillance permanente du réseau par un opérateur de site web, en dehors des serveurs. Mais vous pouvez aussi faire appel à l'installation d'un cluster de basculement, qui prendra en charge cette surveillance en continu.

Il faut également une surveillance réseau externe, qui peut s'effectuer avec un logiciel adéquat muni de sondes distantes, remote probes. Ces sondes peuvent assurer par exemple, le contrôle de l'emploi de la mémoire ou du processeur de chaque serveur virtuel dans le Cloud

privé. Les processus les plus sensibles comme les serveurs Web ou SQL, sont suivis en particulier. En pratique, on fixe des seuils à ne pas dépasser. Le dépassement de ces seuils entraîne l'information systématique de l'administrateur.

LE CLOUD PUBLIC

Le **Cloud public** est une plate-forme Cloud Computing, gérée par des entreprises spécialisées. Elles louent ensuite leurs services à plusieurs autres entreprises. Le principe de cette plate-forme est basé sur l'hébergement d'applications, web en général, sur une plate-forme accessible uniquement par internet. Les ressources y sont mutualisées au maximum.

Le Cloud public, permet ainsi, la création de multitudes d'environnements d'exécution, sur une même plate-forme. Pour utiliser ce type de stockage, il vous suffirait de choisir les domaines ou instances de calculs, de composer vos projets par le biais de l'interface gestion, ou à travers vos scripts basés sur le web service correspondant. Chaque domaine ouvert est compté par heure. La facturation de votre Cloud ne contient ni abonnement, ni frais de mise en service, ni frais masqué. Vous règlerez à chaque fin de mois, uniquement votre consommation réelle du mois.

Cependant, le Cloud public ne permet pas l'hébergement de toute une infrastructure informatique. Dans cette forme de stockage, vous pouvez découvrir par exemple, des utilisations en ressources supplémentaires, pour l'absorption de forts trafics ponctuels pendant une période bien définie. L'accès à ces ressources s'arrête dès que le trafic retourne à la normale.

LE CLOUD HYBRIDE

L'idée de combiner le Cloud privé avec le Cloud public, a entraîné la conception d'un autre pseudo-type de Cloud, le **Cloud hybride** ou mixte. En réalité, ce type de plateforme hybride n'est pas un Cloud à part entière. Puisqu'on cherche à mettre ensemble et à faire communiquer les deux modes précités, le Cloud hybride sert donc uniquement de liaison entre eux. La tendance actuelle des services de stockage s'oriente vers l'adoption du Cloud hybride. Dès que vous pensez déployer un Cloud privé, vous devez considérer également celui public en excès, en prévision des surcharges de vos capacités internes. Et l'hybride vient compléter l'ensemble. Mais la mise en place d'une plate-forme de fédération des identités, ou l'utilisation d'un service Cloud, n'est pas un Cloud hybride.

Des problèmes techniques peuvent surgir lors de l'installation du système hybride.

L'hybride est souvent employé, pour englober les pics de charges ponctuelles comme avec le public, tout en restant lié à un privé. Les deux infrastructures communiquent donc ainsi, et forment un Cloud hybride. C'est alors un moyen de combiner, les avantages apportés par les deux plateformes. On peut mentionner la souplesse des infrastructures, la facilité de déploiement d'une application, ainsi que la réalisation d'économies. Il y a en plus, l'amélioration de la performance et la sécurité du système d'information interne.

Les entreprises intéressées, doivent analyser leur niveau d'activité, leur périodicité, leur système d'information et leurs besoins, avant de penser à transférer l'ensemble de leur infrastructure dans un Cloud public. Bien que les Cloud privés soient très sécurisés, leur manque de flexibilité ne doit pas empêcher leur intégration dans des systèmes hybrides. Les hybrides, peuvent associer les ressources physiques et virtuelles, celles virtuelles et propriétaires, ou celles hébergées et internalisées.

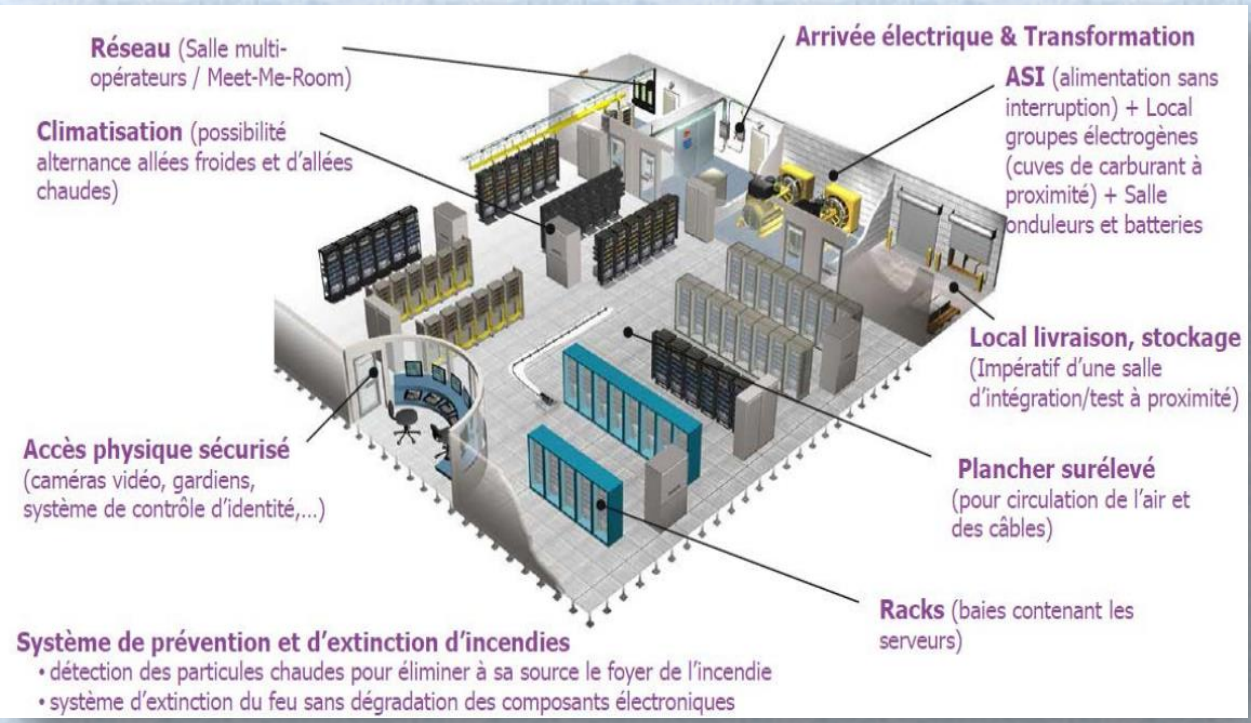
Cloud Communautaire

Le Cloud Communautaire, est un Cloud utilisé par plusieurs entités ou organisations, qui sont animées de besoins communs. Il peut être employé pour des applications génériques, avec des particularités ajustées aux contraintes du groupe. Vous pouvez trouver en exemple le stockage Communautaire monté par la GSA aux Etats Unis, pour les organisations gouvernementales américaines. Ce type de plateforme peut héberger une application métier spécifique, louée en commun par plusieurs entreprises.

Les solutions Cloud Communautaires se sont démarquées par la possibilité à résoudre la complexité grandissante des processus de réservations. On retrouve celles-ci, non seulement pour le trafic aérien, mais aussi pour les hôtels, les locations de voitures… Les vols effectués le même jour, par plusieurs compagnies différentes avec des voyageurs de destinations diverses, sont autant de facteurs difficiles à gérer. Ainsi, une compagnie aérienne logique, ne cherchera plus à créer sa propre application de réservation.

Les infrastructures technologiques

Un datacenter est une infrastructure immobilière et technique permettant d'héberger des équipements informatiques (principalement des serveurs) et disposant de moyens propres à une exploitation performante (électricité, climatisation, accès haut débit) et sécurisée. Il est constitué d'un espace protégé, disposant d'une architecture généralement redondante (alimentation électrique, accès haut débit), ainsi que d'un système de refroidissement.



Les datacenters permettent, entre autres, de mettre à disposition de manière dématérialisée des capacités de calcul ou de stockage (IaaS), des plateformes de développement (PaaS) et des applications (SaaS) à la demande sur la base d'une tarification à l'usage.
Avec 30% de grandes entreprises européennes ayant envisagé un développement de leurs installations en 2011-2012, la France est un pays prisé en Europe pour l'installation de datacenters.

L'infrastructure du datacenter comprend les transformateurs électriques, les alimentations sans interruption (UPS), les générateurs, les armoires de climatisation (CRAC), les systèmes de distribution électrique, etc. Dans certains Datacenter, cette infrastructure consomme deux fois plus d'espace que l'espace destiné à héberger les équipements informatiques.

Pour traiter, stocker et router des informations, le datacenter contient un grand nombre de baies. Ces armoires accueillent différents composants informatiques. Que ce soit le serveur, le stockage ou les éléments réseaux, ils peuvent tous faire l'objet d'amélioration énergétique, l'objectif étant de réduire la consommation et les dépenses énergétiques à la source.

→ Serveurs

Un serveur est, par définition, une machine sur laquelle des logiciels s'exécutent. Les serveurs peuvent être classés suivant leur format et leur capacité de traitement. On distingue trois grandes catégories :

- Les serveurs traditionnels (stand-alone) sont les plus couramment utilisés à l'heure actuelle. Ils hébergent une à deux applications par machine physique, dotée d'un seul système d'exploitation. Leur capacité de traitement est faible, mais largement suffisante pour exécuter une application. Chaque serveur possède sa propre alimentation électrique, son propre système de refroidissement, d'accès au réseau et de périphériques (clavier, souris, écran). Ces serveurs ont généralement un ratio «performances par watt» très faible.

- Les serveurs lame[L] sont conçus pour un très faible encombrement. Plusieurs de leurs composants sont mutualisés dans un châssis capable d'accueillir plusieurs serveurs lames. Le châssis fournit l'alimentation électrique, le refroidissement, l'accès au réseau, la connectique pour écran, clavier et souris. Le contenu ou le rôle du châssis peut varier d'un constructeur à l'autre. Ces serveurs proposent un bon ratio «performances par watt» pour la virtualisation.

- Les serveurs virtualisés sont des copies logicielles de serveurs physiques stand–alone qui s'exécutent sur une seule machine physique. Comme les serveurs stand- alone ne sont exploités que de 10 à 20% de leurs capacités, regrouper plusieurs serveurs virtuels sur une même machine peut s'avérer économiquement et énergiquement rentable si leurs pointes de charge ne coïncident pas dans le temps. La virtualisation des serveurs a donc un impact important sur l'efficience énergétique : on mutualise sur une seule machine plusieurs serveurs, leurs alimentations électriques, et leur dissipation de chaleur. Le refroidissement, le routage et l'accès au réseau sont alors réduits.

→ Stockage

La consommation électrique liée au stockage des données représente environ 30% de celle du datacenter. Lorsque la majorité des serveurs aura été virtualisée, le stockage sera le premier poste de consommation énergétique, représentant la moitié de la facture électrique liée à l'informatique. Cette énergie est utilisée pour écrire et lire l'information mais aussi pour garder l'information inscrite et disponible sur l'emplacement qu'on lui a donné.

On retrouve trois grandes technologies de stockage :

• Dans les salles de petite taille et dans les nouveaux datacenters géants, il n'est pas rare de stocker l'information sur le serveur qui l'utilise, on parle alors de DAS (Direct- Attached Storage). Seul le serveur qui héberge le disque dur peut accéder aux données.

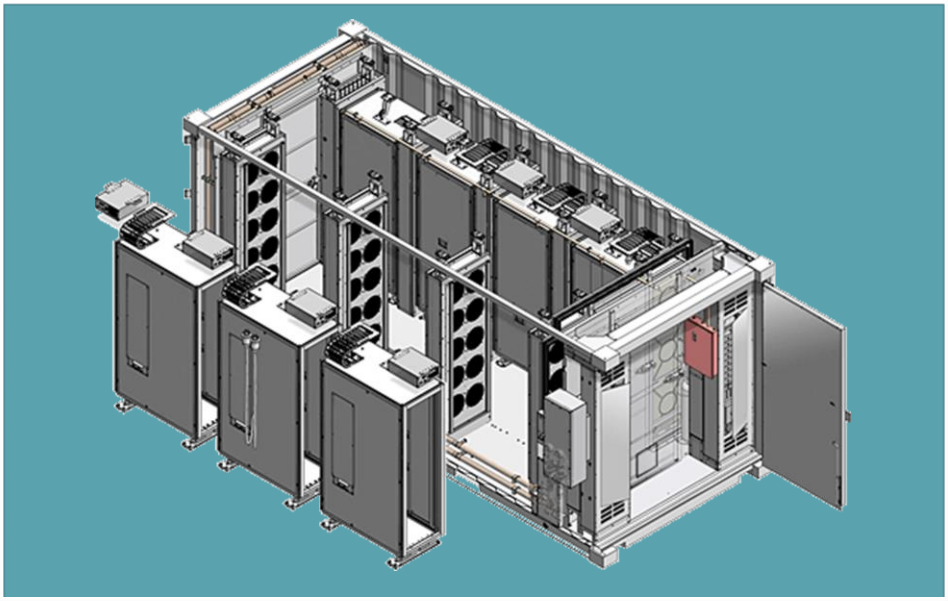
• Dans les salles de taille moyenne ou de grande taille, on dédie à certaines machines une fonction de stockage. Elles constituent alors une «baie de stockage». La plupart des baies sont connectées aux serveurs de traitement soit en SAN (Storage Area Network) ou en NAS (Network Attached Storage).
Le NAS est directement rattaché au réseau local Ethernet et se comporte comme un serveur de fichiers. Le SAN est un réseau local à part entière qui nécessite un accès haut débit.

▪ L'information stockée en local (DAS) doit souvent être répliquée partout où l'information en question sera utile, générant donc plus de consommation d'énergie que si elle n'était stockée qu'une seule fois.

Cependant, l'information ne peut pas être stockée qu'une seule fois pour des raisons de sécurité. On doit alors prendre en compte dans le choix de la technologie utilisée pour stocker l'information sa criticité et son niveau de disponibilité nécessaire.

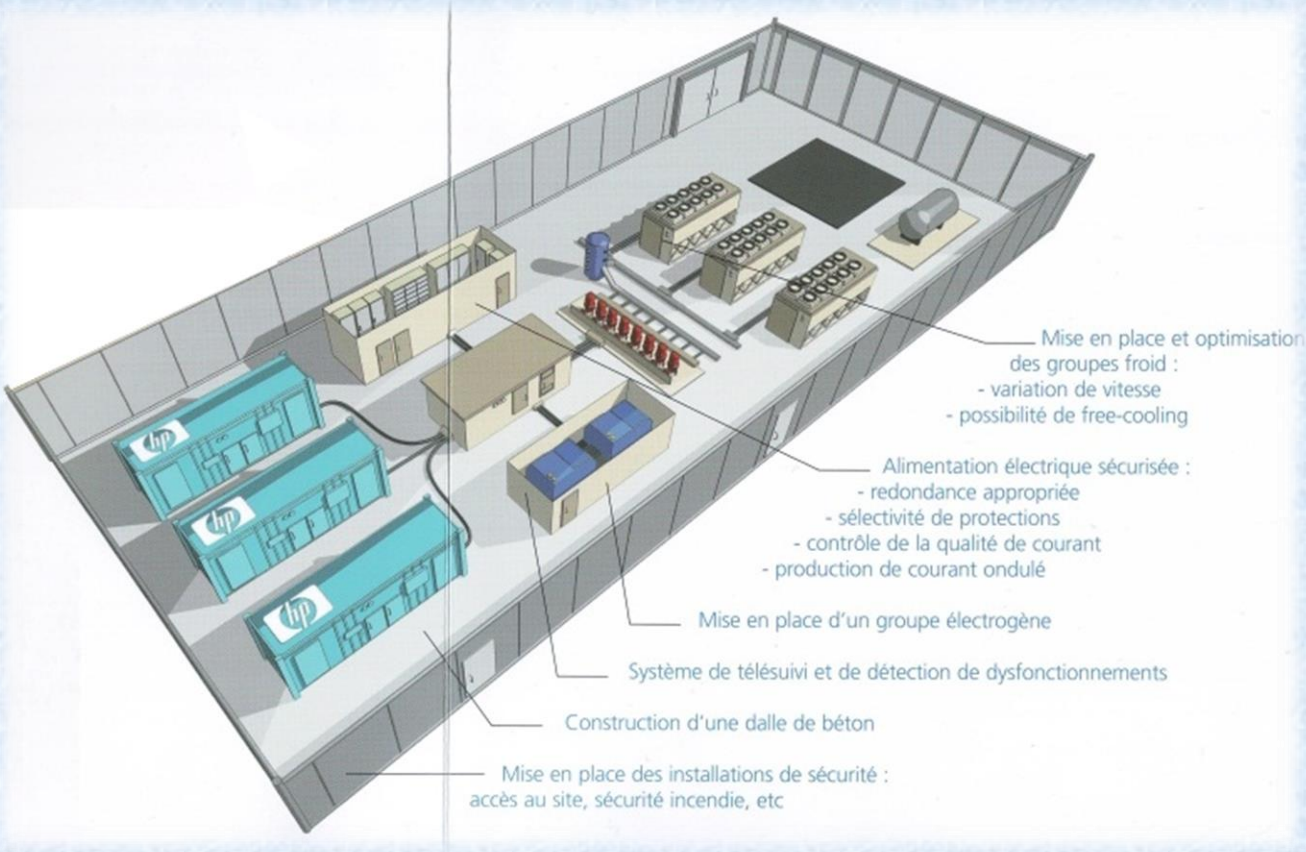
→ Réseau
Les éléments réseau servent à router les informations entre les utilisateurs et les serveurs. Ils sont principalement constitués de commutateurs (switch), routeurs (router), pare- feu (firewalls) et répartiteurs de charge (load balancers). Physiquement, ils sont reliés à différents types de médias : fibre optique pour de longues distances, câble cuivre réseau, liaison radio, etc. Ces éléments supportent des fonctions de qualité de service (QoS) qui leur permettent de gérer plusieurs réseaux distincts en toute sécurité. On peut ainsi mutualiser le routage de plusieurs réseaux sur un même équipement et ainsi consommer moins d'énergie.

→ Un nouveau type de datacenter : **le container**

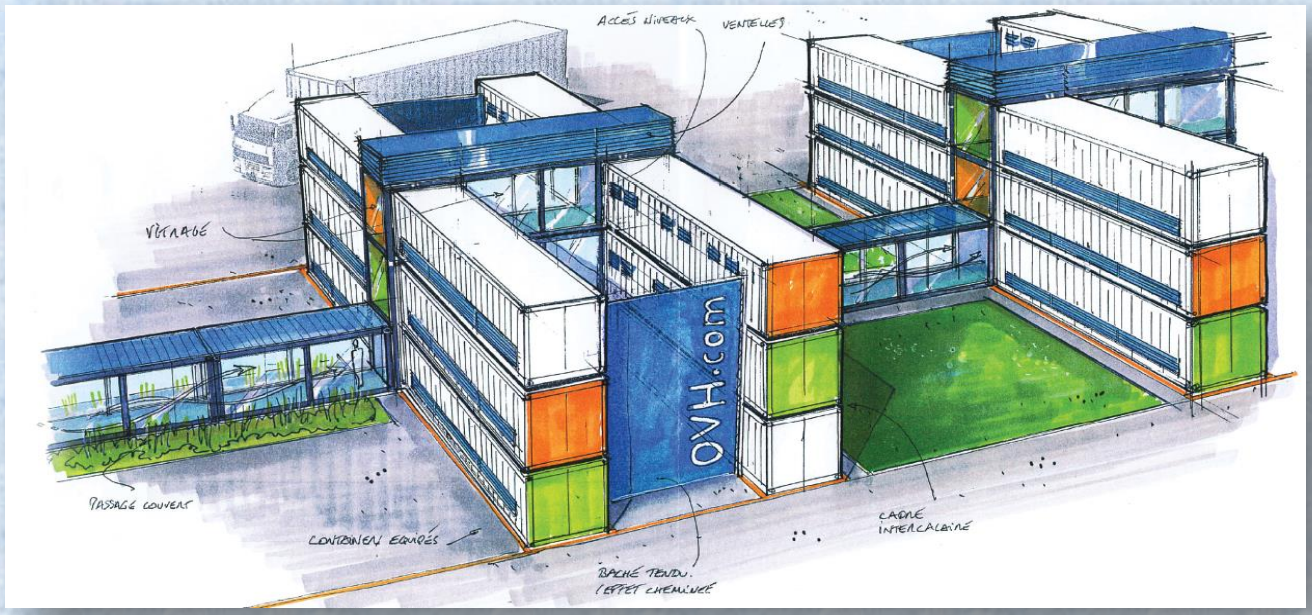


La datacenter en container est la matérialisation concrète des réflexions sur l'urbanisation et la modularité des datacenters. Il propose une alternative viable au datacenter traditionnel. Au point qu'il existe déjà des sites uniquement constitués de containers. Le container demande uniquement d'être raccordé aux différentes sources d'approvisionnement (électricité, télécoms, etc.). À l'intérieur on retrouve tous les éléments d'un datacenter classique : racks accueillant les serveurs, serveurs, baies de stockage, pré-câblage, unités de distribution électrique modulables selon le niveau de disponibilité souhaité et la densité (kW par m²) et la gestion du froid avec les équipements de refroidissement.
La conception interne est basée sur des rangées d'armoires qui hébergent tous les serveurs au format rack positionnées en allées froides et allées chaudes. Cette organisation maximise l'efficacité du refroidissement et permet de gérer la haute densité.

Selon les approches, chaque container est complètement autonome embarquant tous les éléments de la chaîne ou les rôles sont répartis par container, la gestion du froid et de l'énergie se retrouve dans un container, les équipements informatiques dans un autre.



Quelle que soit l'architecture retenue, un container peut supporter des configurations de 30 kW par rack. Il atteint une bonne efficience énergétique grâce à la mutualisation des équipements non informatiques (électricité et refroidissement) et à la circulation de l'air dans le container.



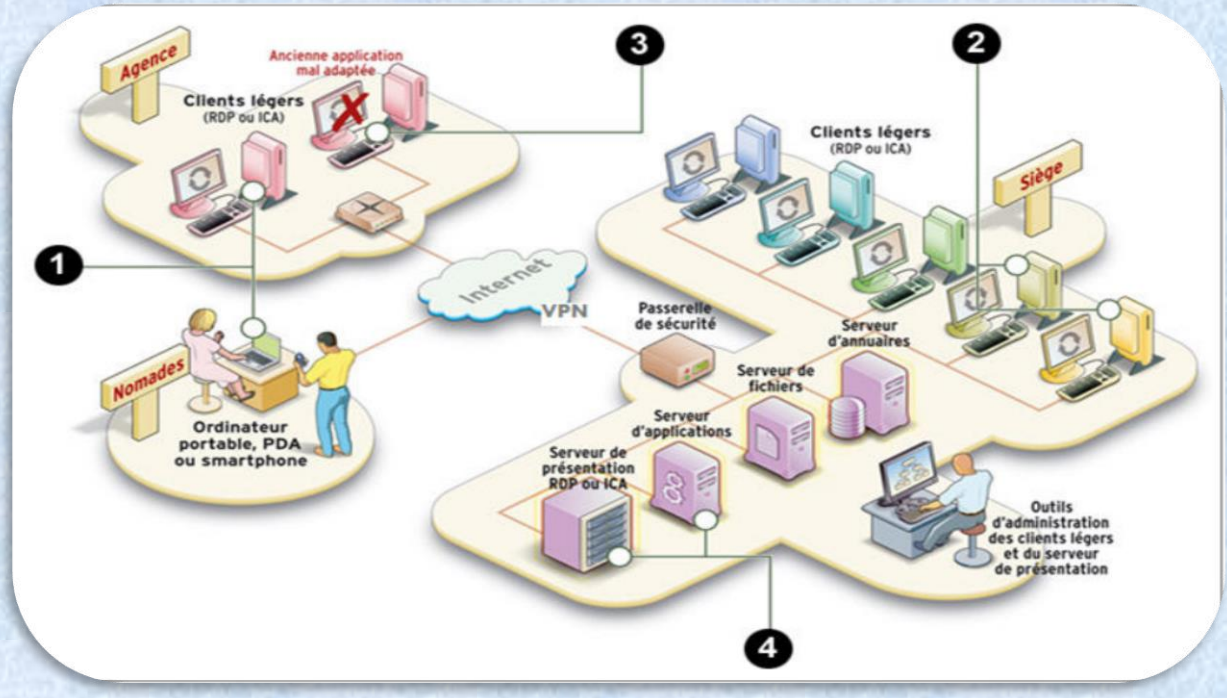
La virtualisation des serveurs et du poste de travail.

La virtualisation est un procédé qui a maintenant fait ses preuves. Techniquement, elle permet d'héberger plusieurs machines virtuelles sur une seule machine physique, en partageant ses ressources. Cela permet un gain de place dans les datacenters, une meilleure gestion de l'énergie nécessaire, une facilité dans l'administration des machines, et un transfert facilité des processus et des données gérés par la machine considérée.

Dans la mise en œuvre d'offres de service au sein de l'entreprise, la virtualisation permet de fournir au demandeur l'exacte quantité de puissance informatique qu'il souhaite, de par la grande liberté de paramétrage que ce procédé offre. Par ailleurs, ces machines pouvant être administrées à distance, le bénéficiaire de l'offre de service peut accéder et gérer facilement ses données. Ainsi, les phénomènes de démultiplication des besoins serveurs sont gérés grâce à la virtualisation.

Au-delà des terminaux mobiles, les usages numériques touchent le poste de travail. Aujourd'hui, afin d'augmenter la flexibilité de son utilisation, la virtualisation sort du cadre des datacenters pour s'attacher aux postes de travail et aux applications auxquelles ils permettent d'accéder.

Le poste de travail évolue avec la mobilité des employés dans l'entreprise. L'utilisateur doit pouvoir accéder à ses données et ses applications en déplacement géographique, mais également d'un poste à un autre au sein d'un même lieu (par exemple une agence commerciale, où les employés sont amenés à changer de fonction au cours de la journée). La virtualisation du poste de travail permet de répondre à ces nouvelles attentes.



Le but de la virtualisation du poste de travail peut être justifié par la grande souplesse et l'agilité que ce procédé apporte.
Le poste virtualisé n'est pas lié à une machine utilisatrice physique, mais est constitué d'une image hébergée sur une infrastructure centralisée (serveur et stockage) dans un datacenter ,soit de l'entreprise soit externalisé.
Le poste virtualisé offre notamment la possibilité d'ouvrir des services à l'international sans avoir à installer des infrastructures locales particulières, le seul besoin étant une connexion à Internet suffisamment rapide et sécurisée pour accéder au datacenter hébergeant l'image.

De même, dans le cas où un prestataire, doit avoir accès au SI de l'entreprise, il est intéressant de l'équiper d'un poste de travail virtualisé, et hébergé dans les *datacenters* de l'entreprise cliente en France. Il est alors aisé d'organiser un changement de prestataire, sans s'inquiéter de la sécurité des données.
Enfin, le déploiement de postes de travail virtuels et la diffusion de nouvelles applications peuvent être réalisés à très grande vitesse. En effet, contrairement à une installation classique nécessitant une action manuelle sur chaque poste de travail, la constitution d'une image des applications et la sauvegarde des sessions utilisateurs sur les infrastructures centralisées sont suffisantes, leur diffusion étant automatisée.

La virtualisation est mise en place grâce à des hyperviseurs.
L'hyperviseur prend en charge la virtualisation de niveau matériel sur les périphériques sans OS tels que le processeur, la mémoire, le disque et les interfaces réseau. Le logiciel d'hyperviseur est intercalé directement entre le matériel physique et l'OS, et cette couche de virtualisation est appelée VMM ou hyperviseur.

Quatre offres principales d'hyperviseurs de serveurs virtualisés sont présentes actuellement au sein des datacenters :
- VMWARE : C'est l'hyperviseur le plus utilisé par environ 69% des utilisateurs
- Citrix XenServer à 8,5 %
- KVM à 8 %
- et Microsoft Hyper-V qui lui est présent à 7 %

Le Contrat

Au-delà des particularités propres à chaque contrat de "cloud computing" (Saas, Staas ou autre), les clients des prestataires doivent conserver à l'esprit plusieurs règles essentielles ainsi que l'idée selon laquelle le choix du prestataire et des conditions dans lesquelles les données seront, en pratique, stockées et transmises sont aussi importants que la nature des prestations ou les stipulations contractuelles.

Quel que soit le prestataire, il convient, avant de signer le contrat, de vérifier l'efficacité des clauses assurant la sécurité, l'intégrité et la disponibilité des données.

1. Les clauses permettant de garantir la sécurité et l'intégrité des données

Il est primordial de savoir où sont physiquement stockées les données. Une clause de localisation des données incluant une liste des pays hébergeant les serveurs du prestataire est donc indispensable. Il convient, à tout le moins, de s'assurer que le transfert des données n'est possible qu'au sein des pays membres de l'Union européenne.

Il est à noter que la Commission européenne considère que les Etats-Unis n'offrent pas – les accords de « Safe harbor [(L)] » étant considérés comme caducs - un niveau de protection adéquat, le Patriot Act [(L)] permettant d'accéder aux données hébergées par les prestataires américains, quel que soit le pays de stockage.

Même la conservation des données sur le sol européen ne serait pas un gage suffisant de sécurité dès lors que le « data center » appartient à une société américaine.

[(L)] → Voir Lexique en fin de document

De même, le contrat de cloud computing doit prévoir la conservation des données dans le respect des lois en vigueur. L'attention doit être portée notamment sur les clauses relatives à :

- la durée de conservation des données, qui doit être limitée et raisonnable au regard des finalités pour lesquelles les données ont été collectées,

- la coopération du prestataire avec les autorités de protection de données (Google, à cet égard, n'est pas un exemple…),

- respect du droit d'accès et de modification des données.

Le respect de l'intégrité et de la confidentialité des données suppose que le contrat stipule des conditions propres à garantir qu'elles ne seront ni altérées (mesures physiques de protection, authentification et connexion sécurisée des utilisateurs, cryptographie des données, etc.), ni susceptibles d'être utilisées par le prestataire de façon illicite.

Une clause prévoyant le contrôle des mesures de protection par le biais d'audits externes réguliers serait précieuse.

2. Les clauses de responsabilité

Le client demeure responsable du traitement des données qu'il a collectées. Aussi, la question de la responsabilité en cas d'incident doit-elle figurer au contrat.

Une clause doit donc envisager clairement les responsabilités de chacun, par exemple en cas de vol ou de perte des données ou d'utilisation illicite des informations confiées, sans que la responsabilité du prestataire ne soit exclue ou trop limitée.

3. Les clauses permettant de garantir la disponibilité des données

Le contrat doit enfin envisager les moyens de garantir une disponibilité des données pour le client, que ce soit en cas de perte ou d'indisponibilité temporaire de celles-ci du fait du prestataire, ou à l'échéance du contrat.

Aussi la clause de réplication est-elle incontournable. Elle doit prévoir que les données seront dupliquées sur d'autres sites distants et/ou feront l'objet d'une restauration dans des délais et des modalités prédéfinis.

Enfin, une clause de réversibilité des données permettant d'organiser le retour des données chez le client ou leur transfert chez un autre prestataire sera nécessaire. Elle doit fixer les conséquences pratiques de la fin du contrat (remise d'une copie des données, modalités de transfert des données, délais, etc.).

C'est uniquement en s'assurant de la présence de telles clauses que le client est juridiquement garanti contre les risques liés aux solutions de cloud computing. Il convient toujours de garder à l'esprit qu'en l'absence de « précautions utiles […] pour préserver la sécurité des données », le responsable du traitement risque rien moins que 5 ans d'emprisonnement et 300.000 € d'amende.

Les Engagements de service SLA

Avoir à sa disposition à la demande et sans limite: des capacités de calcul, des données et des applications; c'est la promesse du cloud computing. Du coup on a parfois l'impression que le cloud est une solution miracle et qu'une fois qu'on a mis son application ou ses données dans le cloud, on peut "dormir tranquille".

Mais quels engagements prend le fournisseur de cloud que vous avez choisi ? Combien de temps mettra-t-il pour redémarrer votre solution en cas de problème ? Peut-il perdre vos données ? Voilà des questions classiques que l'on se pose régulièrement lorsqu'on parle de cloud computing et auxquelles je vais essayer de répondre ici en explorant les contrats de différents fournisseurs.

Engagements ?
Lorsqu'un informaticien propose une solution informatique à un utilisateur, la première chose qu'il définit ce sont les engagements qu'il prend. Ces engagements lui permettent de répondre à des interrogations simples (et légitimes !) de l'utilisateur, notamment:
- Quel sera la disponibilité de la solution: 24h/24h, 7j/7j, les heures ouvrées, ...
- En cas de problème sur la solution, en combien de temps la solution sera-t-elle à nouveau disponible ?
- Quelle garantie y a-t-il sur les données: risque de perte, périodicité des sauvegardes, ...

Ces "engagements" que prennent les Directions Informatiques auprès de leurs utilisateurs métiers s'appellent habituellement "SLA" (Service Level Agreement) ou en français "Contrat de service". Evidemment, plus la SLA est contraignante, plus le prix de la solution proposée par l'informatique est élevé.

Définition d'un accord de niveau de service

La définition d'un SLA est selon de nombreux guides des bonnes pratiques une étape importante qui ne doit en aucun cas être négligée et demande une attention particulière, du fait de ses enjeux.
Cette phase consiste à définir les grandes lignes de l'accord pour préparer les négociations. En effet, à partir de cette définition plusieurs accords peuvent être établis suite à un processus de négociation détaillé dans la sous-section suivante.
Pour pouvoir proposer une base de négociation, un fournisseur de service doit connaître ses capacités en termes de niveau de service. Ainsi l'étape de définition implique généralement une évaluation du service, la définition des indicateurs de performance suivie de la prise de mesures.
Afin d'établir les lignes directrices d'un SLA, il est aussi souvent fait usage de modèles, plus communément appelés templates pour constituer la base du document.

Comme des hébergeurs traditionnels, les fournisseurs de solutions Cloud s'engagent sur des SLA. Pour bien comprendre sur quoi ils s'engagent (et sur quoi ils ne s'engagent pas).

- Disponibilité,
- Pérennité des Données,
- Périmètre de responsabilité,
- Dédommagement.

Disponibilité: "99,95%" [A]

La disponibilité des solutions de Cloud est assez uniforme entre les différents acteurs: le chiffre à retenir est : 99,95% de disponibilité. C'est un niveau de service très élevé; à titre indicatif si on le rapporte aux nombres de minutes dans 1 année cela signifie à peine 4 heures d'indisponibilité par an. Mais, ce n'est pas aussi simple que cela car le mode de calcul est assez différent d'un fournisseur à l'autre.

Pérennité des données: "on fait notre possible"

Au-delà de la disponibilité, on attend d'une solution de cloud qu'elle garantisse la pérennité des données afin d'être sûr de ne rien perdre. Si évidemment toutes les plateformes mettent en avant la pérennité comme point fort, cela ne se traduit pas clairement par des engagements dans la SLA.

Quel périmètre de responsabilité ?

Si un fournisseur de solutions Cloud ne tient pas ses engagements, est-il nécessairement responsable ? Là-dessus, même si le libellé diffère légèrement, on retrouve une réponse commune (et habituelle dans des contrats de services) : on ne peut pas demander l'impossible à un fournisseur.

Dédommagement :

Les clauses d'un accord de niveau de service comportent à l'instar de tout contrat diverses politiques.
Ces politiques, en plus de définir par exemple le prix du service permettent de prévoir les futurs litiges potentiels et de leur apporter des solutions. Ces politiques font généralement mention des crédits de service, compensations financières, pénalités ou autres conséquences de la fourniture défectueuse des services. Des politiques peuvent faire référence à un **SLO** (Service Level Objectives), ou de manière globale à plusieurs SLOs.
C'est le cas des politiques de recours. Ainsi quand un ou plusieurs **SLOs** ne sont pas respectés, ces politiques définissent si l'accord doit être résilié, si une compensation est prévue pour la partie lésée, ou bien si une pénalité doit être appliquée à la partie fautive.

Les parties peuvent bénéficier de diverses formes de compensation dont :

- la compensation d'un consommateur en cas de défaillance de la part du prestataire peut-être financière (remboursement, réduction sur le prix du service, ou dédommagement : une somme prévue par l'accord est versée à la partie lésée) ou se faire sur le service (le consommateur peut bénéficier d'un plus gros volume de service ou d'une meilleure qualité par exemple).
- la facturation du service (le prix pouvant être forfaitaire, dépendre de l'utilisation du service, ...) est en quelque sorte une compensation perçue par le fournisseur en échange de sa prestation.

Les pénalités pouvant être appliquées à la partie fautive sont diverses. Une pénalité peut, comme une compensation être strictement financière (amende ou baisse de la tarification dans le cas du prestataire, et surfacturation dans le cas du client), ou bien de nature différente (un fournisseur peut-être mis sur la liste noire d'un client, recevoir une évaluation négative, etc).

Il est aussi courant qu'une politique soit dédiée à la définition des conditions de résiliation. Elle définit alors entre autres les conditions sous lesquelles l'accord peut être résilié, et ce qu'entraîne la rupture de l'accord. Par exemple, si la résiliation est initiée par un client alors que ce dernier n'est pas encore arrivé au terme de sa période d'engagement, il peut être amené à dédommager le prestataire auprès duquel il s'était engagé.

"je vous fait un Avoir"

Supposons que le fournisseur de cloud n'ait pas tenu ses engagements et que sa responsabilité soit clairement engagée, quel dédommagement pouvez-vous attendre ? Sur ce point, les fournisseurs de cloud proposent tous la même chose: un Avoir sur l'utilisation de leur service, plafonné au montant de ce que vous avez déjà acheté. Autrement dit, quel que soit la valeur réelle de vos données, le fournisseur n'est engagé que sur la somme que vous lui avez versé. Et si vous n'êtes pas content de son service, il vous propose... de continuer.

En synthèse on se rend donc compte que les fournisseurs de cloud:

- S'engagent sur une disponibilité de l'ordre de 99,9%
- Réalisent des sauvegardes de vos données mais ne prennent pas d'engagement sur leur pérennité,
- Que leur responsabilité n'est engagée que sur des erreurs directement dans leur périmètre et au maximum pour le montant de la facture.

[A] Voir calculs des mesures de disponibilité en annexe

Faut-il être inquiet de ce constat ? Non. D'une part parce que les engagements sont déjà très forts et d'autres part parce qu'au-delà des engagements contractuels, dans un marché hautement concurrentiel aucun fournisseur de cloud ne peut aujourd'hui laisser supposer qu'il n'est pas fiable. Il n'y a qu'à voir comment la presse se fait l'écho de la moindre défaillance, qu'elle soit chez Amazon, Google ou Microsoft pour comprendre que chaque fournisseur fera un effort considérable pour corriger le moindre problème.

Pourtant, il faut être réaliste, la défaillance d'un fournisseur de cloud est possible et elle a toute les chances d'arriver pour un client donné à un moment donné. L'erreur serait simplement de ne pas l'avoir anticipée et d'avoir fait confiance aveuglément en son fournisseur de cloud sous prétexte qu'il a une infrastructure redondante/sécurisée/haute performance.

Les avantages du Cloud Computing

Derrière ce terme qui peut faire peur avec sa tonalité « anglophone », le **cloud computing** est une révolution qui touche largement le monde de l'entreprise, du grand groupe à la PME.
Le cloud computing gomme un frein majeur du développement informatique des entreprises : le prix. Avec le cloud, pas d'investissement lourd dans le matériel, et la maintenance est externalisée, tout comme la gestion des sauvegardes.
Le cloud computing, permet ainsi un accès aux nouvelles technologies informatiques à des acteurs qui, pour des raisons essentiellement économiques, ne pouvaient pour le moment pas en profiter. Mais le cloud apporte aussi aux entreprises qui ont déjà aujourd'hui de gros services informatiques, une aide précieuse.
Le cloud computing permet ainsi une meilleure tenue en charge lors des pointes d'activité, mais aussi une utilisation optimale des ressources et de l'énergie. De la start-up à la PME, le cloud computing apporte une plus grande souplesse.

6 avantages du cloud computing :

- Réduction des couts
- La disponibilité des informations partout et tout le temps
- Le développement d'une Informatique décisionnelle
- Une plateforme plus simple pour le travail collaboratif
- Une meilleure hiérarchisation de l'information
- Un gain de productivité et de temps

Le cloud computing, révolution pour l'informatique en entreprises, sans aucun point noir ?

Pas exactement, le Cloud Computing pose la question essentielle du contrôle des données. En n'ayant plus « physiquement chez soi » sa comptabilité, ses e-mail, sa liste de contacts ou encore ses projets de R&D… on se sent moins en sécurité. En effet, les données sont stockées dans le cloud, dans le « nuage », bref dans la nature.
De manière plus technique, l'entreprise (le service informatique) perd la main sur ses applications, et devient dépendant du fournisseur du cloud. Une fois la liste des avantages et des inconvénients dressée, une comparaison entre le modèle traditionnel et le modèle de cloud computing s'impose.

Le système du cloud computing, gomme l'aspect humain du modèle traditionnel, avec un parc « classique », il existe une véritable relation de confiance avec les fournisseurs tant du matériel que du réseau, ainsi que les éditeurs des solutions qui y sont installées. Avec le cloud, on est à l'heure actuelle dans une confiance plus « aveugle » pour la plupart des solutions envisagées. Les acteurs sont encore jeunes, et assez hétéroclites dans leur forme, avec par exemple de super structures, du type Google.

Les freins au Cloud Computing et les problèmes éventuels de sécurité

Si les PME œuvrant dans le secteur des nouvelles technologies adeptes des appareils mobiles et du télétravail sont déjà acquises au cloud, d'autres entreprises, considérées comme plus traditionnelles, rechignent à sauter le pas. Parmi les freins mis en avant par ces dernières, on peut noter les problèmes de confidentialité des données (42 %), les risques de dépendance à un fournisseur (40 %), la question de la restauration des données en cas de rupture contractuelle (30 %), ou encore les difficultés d'intégration de ces solutions externalisées au système d'information existant dans l'entreprise.

Les bénéfices du cloud computing d'un point de vue opérationnel et économique sont nombreux : évolutivité et flexibilité, rapidité de mise en œuvre, faibles coûts d'investissement, service à la demande, paiement à l'usage… Mais quand vient la question de la sécurité, un certain nombre d'interrogations sont soulevées. Les risques encourus par l'entreprise sont-ils bien maîtrisés et en rapport avec les bénéfices attendus ? Exposition des données sur Internet, fuite d'information sur des infrastructures partagées, intrusion avec effets collatéraux… ces risques dépendent du type de cloud computing choisi mais une chose est sûre : le manque de préparation affaiblit la sécurité du cloud, qu'il soit privé ou public.

Des questions à se poser et plusieurs choix possibles

Outre la viabilité du fournisseur et la maturité des offres, la sécurité est le principal frein du passage au cloud computing. Toutefois, même si les failles de sécurité liées au cloud sont bien réelles, elles ne sont pas une fatalité ! Mais avant de se lancer, il est essentiel de se poser les bonnes questions : quelle politique et quelles règles de sécurité sont applicables à « mon » cloud ? Quels sont les moyens dont je dispose pour assurer la disponibilité des ressources ? Qui garde le contrôle ? Quelles sont les garanties de protection de la plate-forme exposée ? La sécurité de mes données est-elle optionnelle ou incluse dans le prix ?…

Le cloud computing n'est pas monolithique : on distingue traditionnellement le SaaS , le PaaS et l'IaaS . Dans chacun des cas, le niveau de contrôle conservé par le client est différent, laissant ainsi un choix parmi les modèles de service. De plus, qu'il s'agisse d'un cloud privé (dédié à une seule entreprise), public (mis à disposition de plusieurs clients) ou encore communautaire (infrastructure partagée entre entités dont l'objectif est le même), là encore, un choix se présente. Restent encore le choix des informations et services éligibles ou non au cloud computing, le choix des mesures de sécurité additionnelles à mettre en œuvre, le choix du fournisseur entre spécialiste du cloud computing et éditeur ayant transformé son offre…

Appréhender la sécurité dans un projet de cloud computing : une nécessité !

Quatre étapes sont à considérer pour assurer la prise en compte de la sécurité dans un tel projet :

1. Une vision et une stratégie basée sur les risques

Dès les premières réflexions de cadrage, il est capital de mener une analyse de risques qui permettra d'orienter les décisions relatives au périmètre et au type de service de cloud computing. Il s'agit d'identifier les enjeux en partant du métier de l'entreprise, de classifier les informations concernées, d'analyser le cycle de vie de ces informations, d'identifier les mesures de sécurité et d'en déduire le risque résiduel en termes de probabilité et d'impact. Sur cette base, il sera possible d'intégrer les coûts de la sécurité dans le business case global, d'objectiver les choix en lien avec l'appétit de l'entreprise pour la prise de risque et finalement de retenir le périmètre pour lequel l'équilibre entre les coûts et la valeur est optimisé.

2. Une architecture et une intégration de la sécurité

Ensuite, les solutions techniques adaptées à l'environnement de cloud computing doivent être étudiées pour réduire les risques identifiés et intégrer ces solutions au reste du système d'information. Les mécanismes de sécurité doivent être cohérents entre l'environnement dédié à l'entreprise et celui du cloud. Idéalement, ils devraient être gérés globalement. A ce jour, l'interopérabilité des offres du cloud reste à établir. Une chose est sûre, l'architecture de sécurité doit aborder au moins les sujets suivants :

- La gestion des identités, des habilitations et des accès,
- Le cloisonnement des services et le nettoyage des supports (destruction des données),
- Le contrôle d'intégrité des configurations,
- La confidentialité et l'intégrité des données avec la gestion des clés de chiffrement éventuelles,
- L'archivage,
- La haute disponibilité et le secours informatique,
- L'imputabilité des actions et l'administration des preuves.

3. Une gestion du changement sous contrôle

Une fois les risques jugés à un niveau acceptable, le changement doit être accompagné pour s'assurer que la sécurité est bien prise en compte notamment dans le contrat avec le fournisseur. Dans un projet de cloud computing, il est crucial de bien définir les rôles et responsabilités de chacun tant au niveau du fournisseur que du client, de s'entendre sur des niveaux de service sans oublier les aspects de sécurité et de s'assurer que les moyens d'assistance seront bien disponibles en cas de crise. Les contrats doivent permettre la mise en place d'une gouvernance efficace et identifier clairement les moyens de recours pour notamment assurer la réversibilité et ce, même en cas de défaillance du fournisseur.

4. Une gouvernance et une assurance sécurité

Enfin, l'assurance de la sécurité doit être adressée de manière permanente tout au long de la vie du service. Même si une entreprise confie certaines activités à un fournisseur de services cloud, elle reste responsable de la sécurité de ces activités vis-à-vis des organismes de régulation, de ses lignes métier, de ses actionnaires, de ses clients et de ses partenaires. La surveillance opérationnelle de la sécurité, la gestion des événements et incidents de sécurité, le reporting périodique sur la base de métriques définies doivent permettre de développer la confiance nécessaire entre le fournisseur et son client. L'efficacité des mesures de sécurité doit être contrôlée et des garanties doivent être obtenues sur la manière dont l'environnement est nettoyé avant réutilisation et dont les données sont détruites. La certification du système de gestion de la sécurité de l'information – ISO 27001 – du fournisseur n'est pas la réponse à tous les besoins d'assurance mais elle offre la garantie d'une certaine dynamique autour de la sécurité.

Améliorer la sécurité de mes données grâce au cloud computing… C'est pour demain ?
Et si le cloud computing permettait aussi d'améliorer la sécurité ? Et si les attraits du cloud computing devenaient un plus pour la sécurité ?

Qui n'a jamais rêvé de projets de sécurité menés à terme tels qu'une authentification forte généralisée qui protège le poste de travail, permette les accès distants, n'expire pas, dispose d'une solution de secours, évite des appels au helpdesk… ?

Et si la solution était « Security as a Service » ? On peut s'attendre à voir fleurir des offres en matière de sécurité hébergées dans le cloud, par exemple :

- « Identity as a service » : provisioning automatique des identités puis authentification unique en ligne pour accéder à différents services.
- « Log as a service » : collecte et analyse de logs en ligne par des outils et équipes spécialisées.
- « Signature as a service » : signature de documents en ligne avec horodatage et éventuellement notarisation ; contrôle de signature.
- « Secure storage as a service » : stockage en ligne avec garantie de redondance et moteur de chiffrement en ligne.

Certes, le stockage sur Internet de secrets d'état n'est probablement pas pour demain mais la flexibilité apportée par le cloud computing ne tardera pas à séduire les directions informatiques, les lignes métier à la recherche de réactivité ou même les directions générales avides de réduire leurs capitaux immobilisés.

Le marché et les offres

Fort d'une croissance de 46% en 2012, contre 0,7% pour l'ensemble de l'informatique, le marché du cloud computing en France représente désormais 2 milliards d'euros selon le cabinet d'études IDC .

Le segment du Cloud Computing a dépassé la barre symbolique des 2 milliards d'euros en 2012, en progression de 46% sur un an (contre +0,7% pour l'ensemble du secteur informatique professionnel). Les chiffres donnés par IDC qui vient de publier trois études sur le sujet. Pour 2013, le cabinet anticipe par ailleurs une progression de 35% du marché du cloud dans l'Hexagone, à 2,645 milliards d'euros. Un segment qui dépassera alors en poids, des marchés de référence tels que celui de l'externalisation applicative, le marché du conseil en informatique ou le marché des postes de travail pour les entreprises", commente IDC.

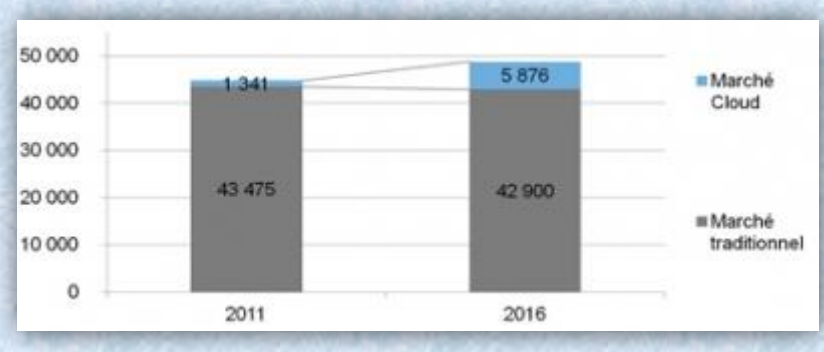
Marché du cloud en France

	En milliards d'euros
2013 (prévisionnel)	2,645
2012	1,959
2011	1,341

Source : IDC

44% des entreprises françaises ont déployé au moins une solution de cloud

Et la courbe de progression du cloud en France ne devrait pas s'infléchir. Selon IDC, les dépenses informatiques d'entreprises françaises dédiées à ce domaine émergeant devraient passer de 3% en 2011 à 12% en 2016. Qu'en est-il en matière de projets ? De 22% en novembre 2011, les entreprises françaises sont désormais 44% à avoir déployé au moins une solution de cloud. Et "parmi les entreprises non équipées, 24% ont un projet à l'étude".
Face à cette montée en puissance, IDC confirme le virage en cours du modèle économique des éditeurs. Avec à la clé un curseur de croissance qui devrait basculer sur les offres cloud (+34% anticipés entre 2011 et 2016), au détriment du modèle traditionnel (-0,3%).



Même si la part du cloud demeure minoritaire sur le marché IT en France, ce nouveau modèle devrait néanmoins pousser la croissance,

Les dépenses en solutions et services professionnels en matière de cloud public sont aussi en plein essor. Ainsi, toujours selon le cabinet IDC, elles devraient atteindre cette année en France près d'1,78 milliard d'euros. Soit une croissance attendue de plus de 38% par rapport à 2012 - année lors de laquelle les dépenses ont été évaluées à près d'1,3 milliard d'euros. Cette progression devrait d'ailleurs se confirmer dans les années à venir. Le cabinet IDC estime en effet que les dépenses en cloud public sur le marché français devraient se hisser à 2,39 milliards d'euros en 2014, et dépasser les 3,14 milliards en 2015.
La part du cloud public dans le marché global du cloud en France a en outre significativement progressé en 2012. Alors qu'elle s'élevait à 63,08% en 2011 elle a atteint 65,5% en 2012. Pour 2013, elle devrait de nouveau progresser pour se hisser à 67,22%.
De son côté, le cabinet Markess International estime le marché français du cloud (comprenant solutions et services de cloud computing à 3,4 milliards d'euros cette année contre 2,8 milliards en 2012. Soit une croissance annuelle de plus de 21%. A horizon 2015, Markess table sur un marché du cloud de 5 milliards d'euros.

Marché du cloud public en France

	En milliards d'euros
2013 (prévisionnel)	1,778
2012	1,284
2011	0,846
2010	0,526

Source : IDC

Dans le monde, le marché du cloud public n'est pas en reste, tiré notamment par la forte demande en matière de solutions et services IaaS (Infrastructure as a Service). Alors que sur 2012 les dépenses mondiales dans le cloud computing public se sont élevées à 111 milliards de dollars, elles devraient atteindre 131 milliards cette année. Concernant les dépenses en IaaS, elles sont attendues autour des 9 milliards de dollars cette année versus 6,1 milliards de dollars en 2012, soit une croissance annuelle attendue de 47,5% contre 18% pour celle du marché cloud dans son ensemble.

Analyse des offres des principaux fournisseurs

CloudScreener : le comparateur de clouds

Conçu pour aider néophytes et experts en cloud computing à faire un choix, CloudScreener compare les offres du marché selon des critères présélectionnés par l'utilisateur (Mise en fonction Avril 2013).

Quand les offres foisonnent, le choix est difficile, surtout sur un marché où les solutions et les tarifs varient énormément d'un fournisseur à l'autre. Conçu selon le modèle éprouvé dans les domaines de la billetterie d'avion ou encore de l'assurance, CloudScreener est un comparateur d'offres de cloud computing qui part du besoin exprimé pour proposer la solution la plus adaptée.

Prise en compte de 120 critères

Créé par une start-up française, CloudScreener propose un formulaire à partir duquel l'utilisateur effectue une première sélection parmi les trois options proposées : héberger un site Web, héberger une application et ses données, stocker et partager des données. Conviviale, l'interface propose ensuite un ensemble d'options que l'utilisateur doit sélectionner ou paramétrer à l'aide de curseurs pour affiner sa demande. Au total, 120 critères sont proposés, parmi lesquels le prix, les performances, les ressources, la sécurité, la flexibilité, la localisation du datacenter, etc. En fin de parcours, il suffit de cliquer sur le bouton "comparer les offres" pour obtenir une liste des fournisseurs répondant aux critères sélectionnés.

Une solution adaptée à tous les profils

Simple d'utilisation, Cloudscreener n'en repose pas moins sur des technologies pointues, dont notamment un algorithme maison, un mode expert pour les utilisateurs exigeants ou avancés sans oublier des outils qui permettent à la start-up d'éprouver réellement les performances de 20 critères sur les 120 proposés. Ce dernier point explique très probablement la limitation des comparaisons à 10 offres du marché (Amazon Web Services, CloudSigma, Skydrive, Sugar Sync et Google Drive, etc.).
Toutefois, CloudScreener ambitionne à terme de couvrir tous les clouds existants

Notre comparatif se basera sur l'externalisation d'un serveur d'une PME avec les éléments suivants :

COMPARAISON CLOUD COMPUTE EN MODE EXPERT

Localisation du datacenter	Utilisation	Durée d'engagement	OS
Europe	24h/jour	Sans	Linux / Windows

CPU	RAM	Stockage
8 CS Processing Unit - 2Ghz	32 Go	4 To

Trafic entrant	Trafic sortant	Stockage objet
Go/mois	Go/mois	Go

La grille tarifaire proposée par Cloudscreener est la suivante :

Fournisseur	Coût mensuel estimé	Performances	Sécurité	Flexibilité	€ $
Meilleure proposition	amazon webservices	aruba CLOUD	rackspace	amazon webservices	
amazon webservices	783 €	★★★½	★★★★	★★★★½	Voir l'offre / Plus d'infos
rackspace	997 €	★★★★	★★★★	★★★★	Voir l'offre / Plus d'infos
aruba CLOUD	1 086 €	★★★★½	★★★	★★★½	Voir l'offre / Plus d'infos
Windows Azure	1 135 €	★★★★	★★★½	★★★★	Voir l'offre / Plus d'infos
CloudSigma	1 297 €	★★★★	★★★½	★★★	Voir l'offre / Plus d'infos

Etudions de plus près les offres disponibles.
Les offres qui louent de la puissance informatique à la demande se sont multipliées et de nouveaux entrants ont fait leur entrée dont Google, HP et IBM.

Le géant américain Amazon, qui compte tirer plus de 2 milliards de dollars du cloud en 2013, a réalisé en mars dernier une baisse de prix importante sur ses offres Elastic Compute Cloud (EC2). Elle a concerné les "instances réservées standard" et les "instances réservées à CPU élevé" dont les prix ont pu baisser jusqu'à 28%.
"Amazon EC2 a la plus grande notoriété, la couverture fonctionnelle la plus complète et de nombreux partenariats avec des éditeurs (IBM, Oracle, Microsoft, Red Hat...) facilitant le licensing du mode Cloud. Le pendant de cette multitude d'options réside dans la complexité de la tarification qui demande une étude complexe pour anticiper les coûts induits. Il est à noter qu'Amazon étant une société américaine, elle est soumise au Patriot Act, ce qui peut être un frein.
La tarification pour des petites instances standard AWS EC2 à la demande (région UE en Irlande) débute à 0,091 dollar de l'heure en environnement d'exploitation Windows, et grimpe à 0,728 dollar de l'heure pour les plus puissantes. Parmi les clients utilisant Amazon EC2, on trouve notamment Ericsson, The Giardian, Hootsuite, QlikTech ou encore Unicredit.

Fonctionnalités et caractéristiques techniques	
Source : JDN Tech	
Provisionning/deprovisionning de ressources (puissance CPU, mémoire, stockage...) à chaud avec prise d'effet immédiat	Oui pour le stockage (un reboot machine est nécessaire pour CPU et mémoire)
Self-service de gestion	Oui
Autoscalling pour s'adapter aux montées en charge	Oui
OS préconfigurés	Windows Server 2012, 2008, 2008 R2 et 2005, RHEL 5.5, 5.6, 5.7, 5.8, 5.9, 6.0, 6.1, 6.2, 6.3 et 6.4, Oracle Linux 5.5, SuSE Linux Enterprise 10.11, Ubuntu, Gentoo, Fedora, Debian...
Répartition de charge	Oui
API ouvertes pour gestion à distance	Oui
MultiVLAN et multi VPN	Oui (via Amazon VPC)
Sécurité (antivirus, chiffrement...) avec prise en main possible par l'entreprise	Oui
Couplage à un CDN	Oui

Souscription, facturation et niveaux de SLA	
Source : JDN Tech	
Self service de souscription par carte bancaire et disponibilité immédiate après souscription	Oui
Facturation à l'heure en fonction	Oui

Souscription, facturation et niveaux de SLA	
Source : JDN Tech	
des ressources utilisées	
Facturation de Frais mensuels même en cas de non utilisation	Non
Seuils de délimitation de ressources Cloud	Système de monitoring à J+1 et alerte en cas de dépassement de seuils
Prévisionnel et estimation des factures à venir en fonction de la consommation passée des ressources	Oui (via CloudWatch)
Niveaux de SLA	99,95% (Amazon EC2), 99,9% (Amazon S3) et 99,9% (Amazon CloudFront) et 100% (Amazon Route 53)
Durée minimale d'engagement	Non
Nombre de jours pour le paramétrage	0
Support	Support en anglais. Temps de réponse de 15 minutes avec l'AWS Enterprise Support, 1 heure avec AWS Business Support et 12 heures avec AWS Enterprise Developper Support. La Tarification de l'AWS Business Support varie entre 3 et 10% du coût de l'utilisation mensuelle d'AWS avec un minimum de 100 dollars

Google Compute Engine, en version Limited Preview depuis l'annonce de son lancement en juin 2012, est sortie de la version d'essai gratuite le 1er mars dernier. En France, le site d'e-commerce Cdiscount fait partie des utilisateurs de cette solution. Le tarif à l'heure d'une instance standard (4 cœurs virtuels, 15GB de RAM et 1,77TB de stockage) hébergée en Europe est de 0,58 dollar.
Pour autant, on peut s'interroger sur le niveau de performance de ce service par rapport à celui d'Amazon. Utilisées pour répondre à un besoin d'encodage vidéo, les instances EC2 se sont ainsi révélées plus rapides que celles de Google Cloud Compte Engine, selon Zencoder. En février dernier, une autre étude réalisée par Nasuni a par ailleurs fait ressortir un avantage certain pour Microsoft Azure en matière de stockage cloud, devant Amazon et HP, loin devant Rackspace et Google.

Fonctionnalités et caractéristiques techniques	
Source : JDN Tech	
Provisionning/deprovisionning de ressources (puissance CPU, mémoire, stockage...) à chaud avec prise d'effet immédiat	Oui
Self-service de gestion	Oui
Autoscalling pour s'adapter aux montées en charge	Oui
OS préconfigurés	Ubuntu, CentOs et GCEL
Répartition de charge	Oui

API ouvertes pour gestion à distance	Oui
MultiVLAN et multi VPN	NC
Sécurité (antivirus, chiffrement...) avec prise en main possible par l'entreprise	Oui
Couplage à un CDN	Oui avec prestataire externe

Souscription, facturation et niveaux de SLA	
Source : JDN Tech	
Self service de souscription par carte bancaire et disponibilité immédiate après souscription	Oui
Facturation à l'heure en fonction des ressources utilisées	Oui
Facturation de Frais mensuels même en cas de non utilisation	Persistent Disk (provisioned space) : 0,10 dollar par GB/mois. Snapshot storage (0,125 dollar par GB/mois) et I/O Operations (0,10 dollar par million)
Seuils de délimitation de ressources Cloud	NC
Prévisionnel et estimation des factures à venir en fonction de la consommation passée des ressources	Non
Niveaux de SLA	Taux de disponibilité garanti de 99,95%
Durée minimale d'engagement	Aucune
Nombre de jours pour le paramétrage	Aucun
Support	Support Bronze gratuit (documentation en ligne et forums), support Silver (150 dollars par mois) et 400 dollars par mois ou 9% de la facture mensuelle pour le support Gold (tel 24h/24)

HP propose deux offres de cloud : HP Cloud Services et HP Enterprise Cloud Services. La première cible les PME, et la seconde les grands comptes - sachant que HP Enterprise Services permet également de construire un cloud privé.
Reposant notamment sur l'environnement Open Source OpenStack, HP Cloud Services propose plusieurs niveaux de facturation en fonction des types d'instances demandées. A titre d'exemple, la tarification par heure débute à 0,035 dollar (avec les instances XS config, comprenant 1 vCPU, 1GB de RAM et 30GB d'espace disque),et va jusqu'à 1,12 dollars (avec les instances XXL config, comprenant 8vCPU, 32GO de RAM et 960GB d'espace disque). Le stockage objet est facturé 0,10 dollar par mois et par GB.

Fonctionnalités et caractéristiques techniques pour HP Cloud Services	
Source : JDN Tech	
Provisionning/deprovisionning de ressources (puissance CPU, mémoire, stockage...) à chaud avec prise d'effet	Oui

Fonctionnalités et caractéristiques techniques pour HP Cloud Services	
Source : JDN Tech	
immédiat	
Self-service de gestion	Oui
Autoscalling pour s'adapter aux montées en charge	Non
OS préconfigurés	Windows Server 2008 SP2, Windows Server Enterprise Edition 2008 R2, CentOS (2 releases), Ubuntu (5 releases), Debian, Fedora et packages LAMP
Répartition de charge	Oui
API ouvertes pour gestion à distance	Oui
MultiVLAN et multi VPN	Oui
Sécurité (antivirus, chiffrement…) avec prise en main possible par l'entreprise	Non (pas fourni dans l'image, c'est à l'entreprise d'installer ses logiciels de sécurité dans les VM)
Couplage à un CDN	Oui (Akamai)

Souscription, facturation et niveaux de SLA pour HP Cloud Services	
Source : JDN Tech	
Self service de souscription par carte bancaire et disponibilité immédiate après souscription	Oui
Facturation à l'heure en fonction des ressources utilisées	Oui
Facturation de Frais mensuels même en cas de non utilisation	Non
Seuils de délimitation de ressources Cloud	Non
Prévisionnel et estimation des factures à venir en fonction de la consommation passée des ressources	Non
Niveaux de SLA	Aucun
Durée minimale d'engagement	Aucun
Nombre de jours pour le paramétrage	0
Support	Support Téléphonique gratuit en anglais 24x365. Support gratuit par mail, chat en anglais; accès à une base de connaissances

IBM est entré en 2012 sur le marché du IaaS et du cloud public. Un marché sur lequel Big Blue était jusqu'à présent encore peu présent, préférant principalement concentrer ses efforts dans le cloud privé.
IBM SmartCloud permet de gérer par serveur jusqu'à 16 CPU virtuels, 32Go de RAM et 3OTO de stockage par disque. A noter qu'IBM propose également une offre de machines virtuelles managées à la demande pour l'hébergement de systèmes de production critiques, mais également des déclinaisons centrées sur SAP (SmartCloud for SAP) et l'archivage (SmartCloud Archive). La tarification par Go débute à 0,12 dollar.
La solution IaaS d'IBM est utilisée par 178 entreprises dans le monde dont en France Altares, Cap Sciences, EffiScience, Synox, Zodiac Marine & Pool, Trace, E-Doceo et Galigeo. A l'étranger, la solution a été choisie par Saatchi & Saatchi, Danske Bank Group ou Japan Architecture Inspection Center. Pour son offre cloud, IBM mobilise six datacenters dans le monde dont un localisé en Europe (en Allemagne).

Fonctionnalités et caractéristiques techniques	
Source : JDN Tech	
Provisionning/deprovisionning de ressources (puissance CPU, mémoire, stockage...) à chaud avec prise d'effet immédiat	Oui
Self-service de gestion	Oui
Autoscalling pour s'adapter aux montées en charge	Oui
OS préconfigurés	Windows 2003 R2, 2008 R1 & R2, Red Hat 5.7, 5.8, 6.2, Suse 11 SP1
Répartition de charge	Oui (via Load Balancer Virtuel)
API ouvertes pour gestion à distance	Oui
MultiVLAN et multi VPN	5 VLAN et 5 VPN par compte par datacenter
Sécurité (antivirus, chiffrement...) avec prise en main possible par l'entreprise	Sécurité du portail via HTTPS, sécurité des API via inscription, sécurisation de l'accès réseau via VPN site à site
Couplage à un CDN	A la charge du client

Souscription, facturation et niveaux de SLA	
Source : JDN Tech	
Self service de souscription par carte bancaire et disponibilité immédiate après souscription	Non
Facturation à l'heure en fonction des ressources utilisées	Oui
Facturation de Frais mensuels même en cas de non utilisation	Non
Seuils de délimitation de ressources Cloud	Oui
Prévisionnel et estimation des factures à venir en fonction de la consommation passée des	Oui

Souscription, facturation et niveaux de SLA	
Source : JDN Tech	
ressources	
Niveaux de SLA	99,9%
Durée minimale d'engagement	Aucune
Nombre de jours pour le paramétrage	Aucun
Support	Support par mail gratuit. Support téléphonique 24/7 facturé 10% de la consommation des ressources Cloud consommées sauf celles liées au middleware

Présent sur le terrain du PaaS (Platform as a Service), Microsoft a complété son offre avec une couche IaaS (Infrastructure as a Service) en juin 2012. Windows Azure Infrastructure Services est par ailleurs sorti de la beta le mois dernier.
L'offre IaaS de Microsoft compte plusieurs clients en France dont MisterGoodDeal, LeGuide.com, Talentsoft ou encore Compario. Windows Azure est un service fourni dans le monde grâce à huit datacenters : quatre aux Etats-Unis, deux en Asie et deux en Europe (Amsterdam et Dublin).
Chaque serveur Azure dispose de huit coeurs, 14GB de RAM et 2To d'espace disque. Deux autres ressources machines dites High Memory sont proposées avec 28GB et 56GB de RAM.

Fonctionnalités et caractéristiques techniques	
Source : JDN Tech	
Provisionning/deprovisionning de ressources (puissance CPU, mémoire, stockage...) à chaud avec prise d'effet immédiat	Oui
Self-service de gestion	Oui
Autoscalling pour s'adapter aux montées en charge	Oui
OS préconfigurés	Windows Server 2008 R2 SP1, Windows Server 2012, Windows Server 2008 R2 avec SQL server 2012 evaluation, Windows Server 2008 R2 avec Biztalk Server, OpenLogic CentOS 6.2, SUSE Linux Enterprise Server, Ubuntu Server 12.04 LTS et openSUSE 12.1
Répartition de charge	Oui (NLB Round Robin et Azure Traffic Manager avec diverses règles paramétrables)
API ouvertes pour gestion à distance	Oui
MultiVLAN et multi VPN	Non
Sécurité (antivirus, chiffrement...) avec prise en main possible par l'entreprise	En option
Couplage à un CDN	Oui (Azure CDN ou CDN tiers)

Souscription, facturation et niveaux de SLA	
Source : JDN Tech	
Self service de souscription par carte bancaire et disponibilité immédiate après souscription	Oui
Facturation à l'heure en fonction des ressources utilisées	Oui
Facturation de Frais mensuels même en cas de non utilisation	Non
Seuils de délimitation de ressources Cloud	Oui (portail dédié dans le cadre d'un accord entreprise)
Prévisionnel et estimation des factures à venir en fonction de la consommation passée des ressources	Non
Niveaux de SLA	Machine virtuelle (99,95%), stockage (99,9%), SQL database (99,9%), CDN et ESB as a service (99,9%)
Durée minimale d'engagement	Aucune
Nombre de jours pour le paramétrage	Aucun
Support	Standard à 223,41 euros par mois (temps de réponse 2 heures et 3 rappels téléphoniques par mois), développeur à 21,6 euros par mois (temps de réponse en moins de 8 heures), gratuit (tél. et forum). Un support Premier est aussi disponible avec temps de réponse inférieur à 15 minutes et une gestion de compte dédié

Orange Business Services (OBS) a réalisé un chiffre d'affaires de 113 millions d'euros en 2012 grâce à ses offres cloud. Soit une croissance de 33% par rapport à l'année précédente. Pour 2015, OBS espère réaliser un chiffre d'affaires de 500 millions d'euros dans le cloud.
Les offres cloud d'OBS se répartissent autour de 4 gammes de solutions :
Flexible Computing Premium (catalogue de services informatiques à la carte et plusieurs niveaux de management pour répondre aux problématiques des plus grandes entreprises),
Flexible Computing Private (offre d'infrastructure dédiée pour les systèmes nécessitant une sécurisation maximale des données),
Flexible Computing Santé (offre IaaS dédiée aux acteurs du monde de la santé conforme à l'agrément "Hébergeur de données de santé à caractère personnel"),
Flexible Recovery, Flexible Backup et Storage as a Service (plan de reprise d'activité).
Parmi les utilisateurs français d'OBS Flexible Computing Express, on trouve la Direction Générale des Douanes et Droits Indirects, Orditech, GFI Progiciels ou encore CBS.

Fonctionnalités et caractéristiques techniques	
Source : JDN Tech	
Provisionning/deprovisionning de ressources (puissance CPU, mémoire, stockage…) à chaud avec prise d'effet immédiat	Oui
Self-service de gestion	Oui
Autoscalling pour s'adapter aux montées en charge	Oui (via dépassement BURST au niveau d'une machine)
OS préconfigurés	Windows Server 2003 et 2008, Debian, Ubuntu et CentOS
Répartition de charge	Oui
API ouvertes pour gestion à distance	Non (disponibilité en 2013)
MultiVLAN et multi VPN	Oui
Sécurité (antivirus, chiffrement…) avec prise en main possible par l'entreprise	Oui
Couplage à un CDN	En option

Souscription, facturation et niveaux de SLA	
Source : JDN Tech	
Self service de souscription par carte bancaire et disponibilité immédiate après souscription	Non
Facturation à l'heure en fonction des ressources utilisées	Non (facturation à la journée)
Facturation de Frais mensuels même en cas de non utilisation	Oui (un minimum de 200 euros par mois qui comprend notamment le firewall virtuel dédié avec 3 VLAN dédié minimum, et le load-balancer)
Seuils de délimitation de ressources Cloud	Oui
Prévisionnel et estimation des factures à venir en fonction de la consommation passée des ressources	Oui
Niveaux de SLA	99,95% (infrastructure) et 99,8% (portail self-service). Taux mensuel avec des pénalités de 100% en cas de non délivrance
Durée minimale d'engagement	Oui (3 mois, 1 an ou 3 ans)
Nombre de jours pour le paramétrage	6 jours maximum
Support	Niveau 1 gratuit 24h/24 et 7j/7, niveau 2 et 3 en option en 24h/24 et 7j/7, sinon aux heures ouvrées

SFR Business Team propose une offre de Cloud Computing de type IaaS depuis 2010. Le groupe s'est appuyé sur plusieurs datacenters basés en France, et des partenariats notamment HP (il a recours à ses serveurs en lames Bladesystem Matrix), Cisco (pour ses équipements réseau) et VMware. SFR fournit par ailleurs une grande partie des infrastructures de Numergy, opérateur de cloud soutenu par l'Etat via la Caisse des dépôts et dont Bull et SFR sont actionnaires.
"SFR Suite infrastructure Cloud propose des déclinaisons Cloud publique et privée de son offre. SFR s'appuie sur ses infrastructures réseau pour proposer une offre de bout en bout, incluant les moyens d'accès aux infrastructures", explique Julien Contal (Solucom). A noter par ailleurs que Numergy, fournisseur de cloud soutenu par l'Etat, fait reposer une grande partie de ses infrastructures sur celles de SFR, l'un de ses actionnaires aux côtés de Bull et de la Caisse des dépôts.

Fonctionnalités et caractéristiques techniques	
Source : JDN Tech	
Provisionning/deprovisionning de ressources (puissance CPU, mémoire, stockage...) à chaud avec prise d'effet immédiat	Oui
Self-service de gestion	Oui
Autoscalling pour s'adapter aux montées en charge	Via API uniquement
OS préconfigurés	Windows Standard et Windows Entreprise 2008 et 2008R2, CentOS 6.4, Debian Lenny 5.0.9 et Squeeze 6.0.5, RedHat 5.7 et 6.4 et Ubuntu 12.04.2. Packages LAMP disponibles tous OS Linux et packages IIS+MSSQL disponibles tous OS Windows
Répartition de charge	Oui
API ouvertes pour gestion à distance	Oui
MultiVLAN et multi VPN	Oui
Sécurité (antivirus, chiffrement...) avec prise en mains possible par l'entreprise	Oui
Couplage à un CDN	Oui

Souscription, facturation et niveaux de SLA	
Source : JDN Tech	
Self service de souscription par carte bancaire et disponibilité immédiate après souscription	Juin 2013
Facturation à l'heure en fonction des ressources utilisées	Non
Facturation de Frais mensuels même en cas de non utilisation	Non
Seuils de délimitation de ressources Cloud	Non

Souscription, facturation et niveaux de SLA	
Source : JDN Tech	
Prévisionnel et estimation des factures à venir en fonction de la consommation passée des ressources	Oui
Niveaux de SLA	99,7% (formule Start), 99,9% (formule Internet) et 99,99% (formule Critique). Garantie sur les débits, disponibilité des IHM, garantie de latence, du taux de perte de paquet et du temps de création des VM
Durée minimale d'engagement	1 an
Nombre de jours pour le paramétrage	7 jours maximum
Support	Support mail et tél 24h/24 et 7j/7 en français : temps de réponse de 30 minutes.

Parmi les autres offres IaaS présentes en France, on trouve notamment celles proposées par Alter Way, BT Global Services, Claranet, eNovance, Ikoula ou encore OVH. Ces offres proposent toutes la possibilité de provisionner et de déprovisionner des ressources cloud. Peu en revanche permettent un couplage natif avec un opérateur de réseau de diffusion de contenu de type CDN (Content Delivery Network). Seuls eNovance et OVH annoncent en être dotés.
Côté facturation, BT Global Services, eNovance et OVH ne facturent pas de coûts additionnels par mois. A noter qu'Alter Way, BT Global Services et Ikoula proposent un outil pour prévoir et estimer sa facturation en fonction de l'historique de consommation des ressources.

Fonctionnalités et caractéristiques techniques des autres solutions de IaaS présentes en France				
	Provisionning ou deprovisionning immédiat de ressources à chaud	Self-service de gestion et Autoscalling	OS préconfigurés	Répartition de charge, API ouvertes et couplage CDN
Source : JDN Solutions				
Alter Way H2O	Oui	Oui	Linux	Oui (couplage CDN en option)
BT Cloud Compute	Oui	Self-service de gestion	Linux et Windows	Oui (couplage CDN en option)
Claranet Virtual Data Centre	Oui	Oui	Windows Server 2003 R2 SP2, Windows Server 2008 SP2, RedHat 5.5 et 6	Oui (couplage CDN en option)
eNovance eNocloud	Oui	Oui	Windows Server, Red Hat, Ubuntu...	Oui
CloudStack by Ikoula	Oui	Oui	Windows 2012 RTM, CentOS 6.4, Debian 6.0.7, Fedora 18, Ubuntu 12.04, Ubuntu 12.04.2 LTS, Windows 2008 R2, Open Suse	Répartition de charge et API ouvertes

Fonctionnalités et caractéristiques techniques des autres solutions de IaaS présentes en France				
	Provisionning ou deprovisionning immédiat de ressources à chaud	Self-service de gestion et Autoscalling	OS préconfigurés	Répartition de charge, API ouvertes et couplage CDN
			12.2	
OVH Cloud Instances	Oui	Oui	Windows 2008 SP2 Standard, CentOS 5, Ubuntu 10.04, Debian 6, Fedora 16 et Debian Wheezy (tous ces OS en 64-bit)	Oui

Souscription, facturation et niveaux de SLA des autres solutions IaaS présentes en France				
	Self service de souscription par CB avec prise d'effet immédiat et facturation à l'heure	Facturation de Frais mensuels même en cas de non utilisation	Niveaux de SLA et durée d'engagement	Prévisionnel et estimation des factures à venir
Source : JDN Solutions				
Alter Way H2O	Non	Oui (à partir de 29€)	99,99% et 1 mois d'engagement	Oui
BT Cloud Compute	Facturation à l'heure	Non	99,95% en standard et aucun engagement	Oui
Claranet Virtual Data Centre	Facturation à l'heure	Oui (ressources réservées) mais pas en burst	99,95% (infrastructure) et 99,9% (portail). 6 mois d'engagement	Non
eNovance eNocloud	Facturation à l'heure	Non	99,90% et aucun engagement	Non
CloudStack by Ikoula	Oui	Instance non facturée hors réservation	99,95 %, aucun engagement	Oui
OVH Cloud Instances	Oui	Non	99,90% et aucun engagement	Non

Mise en Service d'une solution de Cloud Computing

Installation et configuration d'une solution de Cloud OpenSource : Apache CloudStack

Cloudstack est une solution de gestion de service d'infrastructure (IaaS) Opensource pour le cloud. Il prend en charge l'orchestration de l'ensemble des briques techniques de l'infrastructure (réseau, serveurs, stockage…) ainsi que la gestion des utilisateurs.
Les API lui permettent un interfaçage avec l'ensemble des composants compatibles et une ouverture vers Amazon EC2 et S3 pour les besoins de cloud hybride.

CloudStack supporte les principaux hyperviseurs du marché : VMware, KVM, XenServer et Xen Cloud Platform (XCP).

A quoi ca sert ?

Vous avez:
- une ferme d'hyperviseurs potentiellement hétérogène: Xen, KVM, VMware …
- du Stockage
- du Réseau

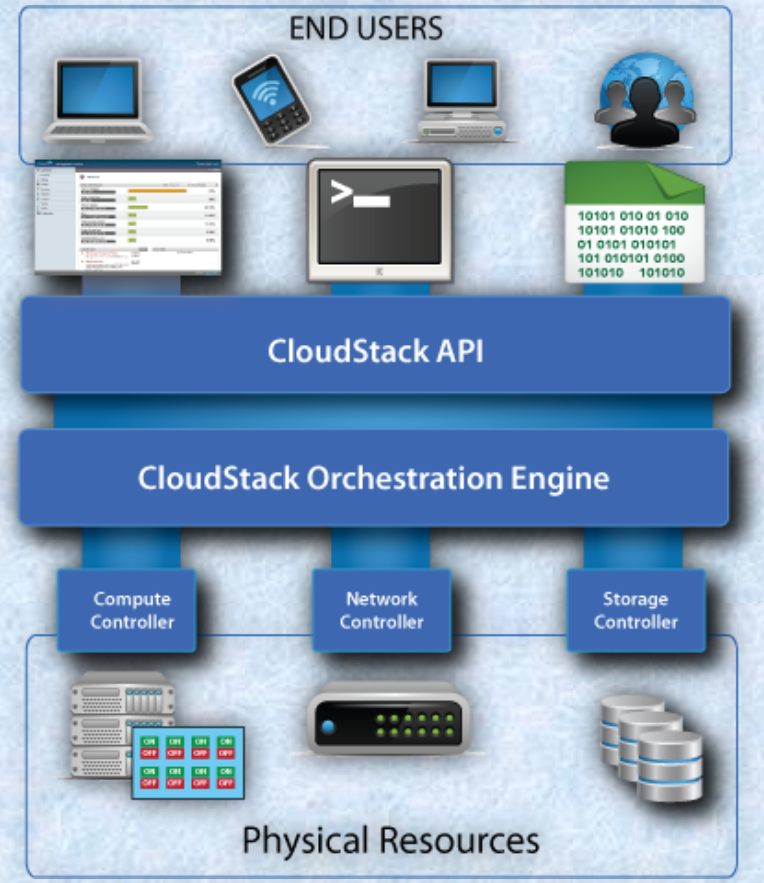
CloudStack pilote ces 3 groupes d'éléments pour réaliser votre IaaS (Infrastructure as a Service).

Rappel historique
En incubation chez Apache avec presque 150 entreprises et 350 contributeurs. Le succès du projet semble bien assuré.
Les années 2007/2008 ont vu une floraison de projets liés au Cloud en général. Chez Apache apparaissent beaucoup de logiciels de type Hadoop, Cassandra, CouchDb …

Du coté des hyperviseurs, KVM préinstallé dans les noyaux Linux prend l'avantage sur Xen.

Le marché IaaS comprend: Eucalyptus ; OpenNebula (projet espagnol et donc boudé par les US) ; OpenStack (projet US porté par la NASA) ; oVirst (RH) ; Ganeti (Google plus simple, moins ambitieux).
CloudStack joue la carte Apache pour attirer un maximum de contributeurs et de partenaires. Typiquement, les projets développant des solutions réseaux contribuent les plugins nécessaires à leur intégration dans CloudStack. Mais on trouve aussi des entreprises de toutes taille avec des hébergeurs comme iKoola ou GoDaddy mais jusqu'à des solutions qui fournissent des services de plus haut niveau comme UShareSoft à Grenoble !!

Cloudstack sera la version communautaire pour Citrix et son CloudPlateform .
Comme de nombreux produits 'cloud' les releases sont de type code source. Les packages sont distribués par des membres de la communauté, mais ne font pas partie du projet.



Technique

CloudStack communique avec tous ces équipements grâce à un système de plugins et offre une API riche comportant plus de 200 classes (configuration de firewall, des hôtes, gestion de routeurs, des utilisateurs, des images ...)

CloudStack fournit aussi:

- une interface Web
- une interface en ligne de commande
- CloudBridge EC2 : pour faciliter la migration des scripts EC2 sur CloudStack.
- DevCloud : une machine virtuelle Virtualbox pouvant lancer des machines virtuelles Xen à l'intérieur de la première vm pour tester.

Tous ces projets utilisent l'API de CloudStack. Certains clients (INRIA) ont même re-développé une interface Web spécifique à leur besoin.

Un cloud d'infrastructure en tant que service (IaaS) peut être difficile à mettre en place, et a, par définition, une multitude d'options possibles, qui peuvent troubler même les administrateurs expérimentés qui n'auraient pas forcément d'expérience préalable de mise en place de plateformes de cloud computing.

Que va-t-on construire exactement ?

Nous allons déployer CloudStack rapidement en utilisant KVM(Hyperviseur), CentOS 6.3 et NFS pour le stockage des images.
KVM supporte la virtualisation native sur la base de processeurs pourvus d'extensions matérielles de virtualisation.

Pourquoi KVM ?

En termes de performance, KVM se rapproche de VMware. Ils s'éloignent de la pure émulation de hardware existant pour préférer l'utilisation de pseudo hardwares spécifiques dédiés à la virtualisation.

Les hyperviseurs alternatifs, ont rattrapé leur retard technique, de manière fulgurante pour certains, et proposent des approches innovantes pour un coût bien inférieur au regard d'une infrastructure VMware.
En quelques années, avec une approche nouvelle de la virtualisation, le projet KVM offre déjà toutes les fonctionnalités de l'hyperviseur VMware.

L'approche est pourtant simple et très fidèle à la philosophie de l'Open Source : réutiliser l'existant. KVM est un module kernel agrémenté d'un outil userland qemu. Les machines virtuelles bénéficient alors de toute la puissance et de la robustesse du noyau Linux : les couches réseau, la gestion mémoire, etc. Cette approche ouverte permet à la communauté utilisant le produit de se concentrer sur l'hyperviseur, et donne à l'architecte de nombreuses possibilités et alternatives pour le design de son architecture..

Le stockage est devenu le nerf de la guerre des centres d'hébergement virtuels ! Le besoin en IOs par seconde est très souvent sous-estimé, la taille des disques explose et beaucoup de centres d'hébergement ou d'entreprises possèdent déjà un système de stockage centralisé qu'il faut réutiliser. KVM réussit à associer performances, flexibilité et interopérabilité dans ce domaine.

L'hyperviseur, qui s'appuie sur le noyau Linux pour la gestion du stockage, est capable de s'interfacer avec quasiment tous les systèmes de stockage existants. De plus tous les formats sont supportés : RAW, iSCSI, un fichier image sur un NAS… Côté réseau, KVM propose des interfaces simples et performantes permettant de s'interfacer et de bénéficier de toutes les capacités de l'OS Linux. Au-delà du support des fonctionnalités de base, KVM intègre également un client du protocole « Virtual Ethernet Port Aggregator » (VEPA). Ce protocole permet de déporter la configuration du réseau directement sur le switch, plutôt que sur l'hyperviseur.

Du point de vue de la performance, KVM se rapproche de VMware. Tous deux s'éloignent de la pure émulation de hardware existant pour préférer l'utilisation de pseudo hardwares spécifiques dédiés à la virtualisation (le VMware tools, côté vmware, et virtio, côté KVM). **Qemu** se base sur le format d'interface libre VirtIO pour la gestion du stockage, du réseau ou de la RAM. Les performances sont équivalentes, voire meilleures dans certains cas d'utilisation, à celles observées sur VMware.

L'hyperviseur KVM est donc particulièrement complet. C'est l'interface d'administration qui va faire la différence avec VMware. Là où ce dernier propose une interface de management centralisée complète, graphique et accessible, **qemu** n'offre que la ligne de commande.L'interface graphique de Cloudstack permet donc de profiter pleinement de sa puissance.

La philosophie de l'Open source créé une émulsion, et de nombreux outils d'administration existent déjà. Quasiment tous ont fait le choix de se baser sur un autre composant de la galaxie KVM : **libvirt**. Produit également soutenu par les équipes de « Redhat emerging technologies », **libvirt** offre une API aux fonctionnalités KVM et permet également de piloter Xen, VMware, openvZ ou d'autres.

Soutenu par **une communauté hyperactive** et bénéficiant d'une architecture simplifiée, plébiscitée par les entreprises et les acteurs du cloud, KVM gagne en renommée et se positionne comme un acteur technique incontournable de la virtualisation. La solution Qemu/KVM est développée dans la philosophie de **l'Open Source** avec comme mot d'ordre l'interopérabilité.

Le réseau sera un simple Layer-2 à plat[(L)], avec de l'isolation au Layer-3 [(L)] qui utilise les "security groups[(L)] ". Tout s'installe sur une seule machine physique.
Les groupes de sécurité fonctionnent comme des pare-feu distribués qui contrôlent l'accès à des groupes de machines virtuelles.

Avant d'entreprendre l'installation de CloudStack à proprement parler, on commencera par l'installation du système d'exploitation, pour ensuite configurer un serveur NFS avec plusieurs types de stockage. Ensuite, le serveur de management sera installé, les machines virtuelles seront téléchargées et enfin le logiciel agent sera installé.

Durant la dernière étape, on s'étendra sur la configuration complète du cloud à partir de l'interface web de CloudStack.

Besoins matériels :

Nous effectuerons nos tests sur 1 machine virtuelle (VM) sous VMWARE Workstation, installée sur un ordinateur supportant la virtualisation matérielle (dans notre cas un AMD Phenom II X6 cadencé à 3.2 Ghz).
Pour exécuter KVM, vous avez besoin d'un processeur qui prenne en charge la virtualisation. Pour les processeurs Intel, cette extension porte le nom INTEL-VT, pour les processeurs AMD, il porte le nom AMD-.V .Effectuer la commande suivante après l'installation du système d'exploitation :

```
# egrep --color=auto '(vmx|svm)' /proc/cpuinfo
```

Si rien n'est imprimé, cela signifie que votre CPU ne prend pas en charge la virtualisation matérielle. Sinon, il est compatible. Mais vous devez vous assurer que la virtualisation est préalablement activée dans le BIOS. Si l'indicateur svm est retourné, votre processeur prend en charge AMD-V ou si l'indicateur vmx est retourné, votre processeur prend en charge Intel VT. Dans le résultat de la commande précédente , nous comptons le nombre de lignes contenant “vmx” ou “svm” si le résultat est supérieure ou égale à 1, la virtualisation est supportée.

Un réseau /24 avec une gateway à xxx.xxx.xxx.254, pas de serveur DHCP sur le réseau et aucun des serveurs contenant CloudStack n'auront d'adresse dynamique, pour simplifier l'installation.

La VM sera équipée de 6 processeurs à 3.2 Ghz , 6 Go de mémoire et de 200 Go de disque dur.
Elle accueillera Centos 6.3 64 bits comme système d'exploitation et comme support pour l'installation de CloudStack.

Nous utiliserons l'ISO installation minimal CentOS 6.3 x86_64 sur notre machine virtuelle. Les valeurs par défaut devraient normalement être acceptables pour cette installation.

[(L)] → Voir Lexique en fin de document

Lors de l'installation il faudra configurer une adresse Ip statique, pour notre cas voici les paramètres configurés pour l'interface eth0.

```
-bash-4.1# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:0C:29:FA:82:E8
          inet addr:10.0.2.50  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fefa:82e8/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:51748 errors:0 dropped:0 overruns:0 frame:0
          TX packets:33443 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:62981170 (60.0 MiB)  TX bytes:3583639 (3.4 MiB)
```

Et le nom d'Hôte sera « **cloudstack.cloud.fr** ».

Une fois l'installation terminée, il est utile de pouvoir se connecter en SSH en tant que root à la machine fraichement installée. Nous utiliserons le logiciel «SSH Secure Shell Client » Il est à noter que l'authentification en tant que root ne devrait pas être autorisée en environnement de production; s'assurer de désactiver l'authentification à distance une fois l'installation et la configuration terminées.

Après redémarrage, nous pourrons vérifier le nom d'hôte avec la commande « uname –a »

```
-bash-4.1# uname -a
Linux cloudstack.cloud.fr 2.6.32-358.6.2.el6.x86_64 #1 SMP Thu May 16 20:59:36 U
TC 2013 x86_64 x86_64 x86_64 GNU/Linux
```

Configurer le Hostname dans le fichier **/etc/sysconfig/network**

Configuration du réseau

Par défaut, le réseau ne sera pas disponible sur votre matériel, et il faudra le configurer pour qu'il fonctionne dans l'environnement. Puisqu'il a été spécifié qu'il n'y aura pas de serveur DHCP dans cet environnement, on configurera manuellement l'interface réseau.

« eth0 » est la seule interface réseau qui sera connectée et utilisée. Il faut donc en premier l'activer :

```
# ifup eth0
```

Pour se connecter à la console, s'authentifier en tant que root. Vérifier que le fichier **/etc/sysconfig/network-scripts/ifcfg-eth0** ressemble par défaut à ceci :

```
DEVICE="eth0"
HWADDR="52:54:00:B9:A6:C0"
NM_CONTROLLED="yes"
ONBOOT="no"
```

Malheureusement, cette configuration ne permet pas de se connecter au réseau, ni ne convient aux besoins de Cloudstack. On souhaite configurer ce fichier pour qu'il spécifie l'adresse IP, le masque réseau, etc., comme dans l'exemple suivant:

```
DEVICE=eth0
HWADDR=52:54:00:B9:A6:C0
NM_CONTROLLED=no
ONBOOT=yes
BOOTPROTO=none
IPADDR=10.0.2.50
NETMASK=255.255.255.0
GATEWAY=10.0.2.254
DNS1=8.8.8.8
DNS2=8.8.4.4
```

Une fois les fichiers de configuration correctement paramétrés, il faut lancer quelques commandes pour démarrer le réseau automatiquement au démarrage :

```
# chkconfig network on
# service network restart
```

Configuration du nom d'hôte

Cloudstack exige que le nom d'hôte soit paramétré correctement. Celui-ci doit pointer sur la bonne adresse Ip.

Pour rectifier cette situation, on paramétrera le nom d'hôte en éditant le fichier **/etc/hosts** pour que son format ressemble à l'exemple suivant :

```
127.0.0.1       localhost localhost.localdomain localhost4
localhost4.localdomain4
10.0.2.50       cloudstack.cloud.fr
```

Une fois ce fichier modifié, continuer et redémarrer le réseau en utilisant :

```
# service network restart
```

Puis vérifier avec la commande hostname --fqdn et s'assurer qu'elle renvoie une réponse FQDN

Configuration de SELINUX

À ce point, SELinux doit être paramétré comme permissif pour que CloudStack fonctionne correctement. On souhaite à la fois configurer ceci pour des démarrages futurs et le modifier dans le système en cours de fonctionnement.
Pour configurer SELinux en mode permissif dans le système en cours de fonctionnement, lancer la commande suivante :

```
# setenforce 0
```

Afin de s'assurer que SELinux reste dans cet état, on doit configurer le fichier **/etc/selinux/config** pour refléter l'état permissif, comme dans l'exemple suivant :

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
# enforcing - SELinux security policy is enforced.
# permissive - SELinux prints warnings instead of enforcing.
# disabled - No SELinux policy is loaded.
SELINUX=permissive
# SELINUXTYPE= can take one of these two values:
# targeted - Targeted processes are protected,
# mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Configuration de NTP

La configuration de NTP est nécessaire pour que les horloges de tous les serveurs du cloud restent synchronisées.
Cependant, NTP n'est pas installé par défaut, donc on l'installera et on le configurera à ce stade. L'installation de NTP se fait comme suit :

```
# yum -y install ntp
```

L'actuelle configuration par défaut est convenable pour nos besoins, donc il est surtout nécessaire de l'activer et de faire en sorte qu'elle se charge au démarrage. Ce qui se fait de la façon suivante :

```
# chkconfig ntpd on
# service ntpd restart
```

Installation du serveur de management

Installer wget

```
# yum install wget
```

Effectuer un Update de l'OS

```
# yum update
```

Télécharger le fichier d'installation de Cloudstack

```
# wget
http://sourceforge.net/projects/cloudstack/files/CloudStack%20Acton/3.0.
2/CloudStack-oss-3.0.2-1-rhel6.2.tar.gz/download
```

Décompressez le fichier

```
# tar xvf CloudStack-oss-3.0.2-1-rhel6.2.tar.gz
```

Démarrer l'installation

```
# cd CloudStack-oss-3.0.2-1-rhel6.2

# ./install.sh
```

Sélectionner "M" pour l'installation du Management Server

Il faut à présent configurer le service « nfs » pour qu'il se lance au démarrage, et le lancer sur l'hôte en exécutant les commandes suivantes :

```
# service rpcbind restart
# service nfs restart
# chkconfig rpcbind on
# chkconfig nfs on
```

Installation et Configuration de la base de données

Commencer par installer MySQL et configurer quelques options pour s'assurer du bon fonctionnement de CloudStack.
Pour installer MySQL, relancer le programme d'installation:

```
# ./install.sh
```

Et selectionner l'option « D » Install the database Server
Une fois MySQL installé, il faut procéder à quelques changements de configuration dans **/etc/my.cnf**. Plus particulièrement, on doit ajouter les options suivantes à la section [mysqld]:

```
innodb_rollback_on_timeout=1
innodb_lock_wait_timeout=600
max_connections=350
log-bin=mysql-bin
binlog-format = 'ROW'
```

Maintenant que MySQL est configuré correctement, on peut le démarrer et le configurer de la façon suivante pour qu'il se lance au démarrage:

```
# service mysqld restart
```

```
# chkconfig mysqld on
```

Création du mot de passe de l'administrateur Mysql

```
# mysql -u root

mysql> SET PASSWORD =  PASSWORD ('password');
```

Configuration de la base de donnée

Toujours sous mysql , taper la ligne suivante en remplaçant « password-root » par le mot de passe que vous venez de définir

```
mysql> \! cloud-setup-databases cloud:password@localhost --deploy-
as=root:"password-root"
mysql> exit
```

- cloud correspond à l'utilisateur de la base de données suivi de son mot de passe

Après la fin de ce processus, un message du style "CloudStack has successfully initialized the database." devrait s'afficher.
On pourra vérifier la configuration de la base dans le fichier **/etc/cloud/management/db.properties**

Si l'hyperviseur KVM est installé sur la même machine que le Management Server il faut modifier la ligne suivante du fichier **/etc/sudoers**

```
Defaults:cloud !requiretty
```

Maintenant que la base de données a été créée, on peut procéder à l'étape finale en configurant le management server, par les commandes suivantes:

```
# cloud-setup-management
```

Donner les droits en écriture au fichier /usr/share/cloud/management/logs/catalina.out

```
# chown cloud:cloud  /usr/share/cloud/management/logs/catalina.out

# chkconfig cloud-ipallocator on
# chkconfig cloud-management on
```

Configuration de Nfs

Notre configuration va utiliser NFS pour le partage. Le paquet NFS Utilities contient le serveur utilisateur et le client nécessaires pour utiliser les possibilités NFS du noyau.

NFS est un protocole qui permet le partage rapide et transparent de systèmes de fichiers sur un réseau. Ainsi, on va configurer deux périphériques NFS.

Le système de fichiers réseau (NFS pour Network File System) fut développé pour permettre aux machines de monter la partition d'une machine distante comme si c'était un disque local.

L'avantage de NFS aujourd'hui est qu'il est mature, universel, bien compris et solidement supporté sur de nombreuses plateformes.

Le stockage primaire servira à stocker les VM , le stockage secondaire servant à stocker les isos et les snapshots.

```
# yum install nfs-utils
```

Il faut à présent configurer NFS pour fonctionner avec deux périphériques différents. Ceci est réalisé assez facilement dans le fichier **/etc/exports** . On doit s'assurer qu'il contient les données suivantes:

```
/primary *(rw,async,no_root_squash)
/secondary *(rw,async,no_root_squash)
```

On va continuer en créant les répertoires, et en configurant leurs permissions de façon appropriée à l'aide des commandes suivantes :

```
# mkdir -p /primary
# mkdir -p /secondary
```

Après toute modification au fichier exports, il convient d'exécuter la commande **/usr/sbin/exportfs** afin de réaliser l'exportation à proprement parler Appelée avec l'option -a, cette commande réalise l'export de tous les répertoires listés dans **/etc/exports.**

```
# exportfs -a
```

Vérifier que les 2 répertoires sont bien activés :

```
# exportfs
```

Les versions CentOS 6.x utilisent NFSv4 par défaut. NFSv4 exige que les configurations de domaines concordent sur tous les clients. Dans le cas présent, le domaine est « cloudstack.cloud.fr », donc il faut s'assurer que la configuration du domaine dans **/etc/idmapd.conf** est décommentée et fixée comme suit:

```
Domain = cloud.fr
```

À présent, décommenter les valeurs de configuration dans le fichier **/etc/sysconfig/nfs**

```
LOCKD_TCPPORT=32803
LOCKD_UDPPORT=32769
MOUNTD_PORT=892
RQUOTAD_PORT=875
STATD_PORT=662
STATD_OUTGOING_PORT=2020
```

Puis relancer NFS

```
# service nfs restart
# chkconfig nfs on
```

Il faut ensuite configurer le pare-feu pour autoriser les connexions NFS entrantes.

Le plus célèbre pare-feu utilisé sous Linux est **iptables**. Il permet d'établir un certain nombre de règles pour dire par quels ports on peut se connecter à votre ordinateur, mais aussi à quels ports vous avez le droit de vous connecter
Nous allons donc donner les droits à notre réseau **10.0.2.0/24** à pouvoir accéder aux ports utilisés par le serveur NFS.

Éditer le fichier **/etc/sysconfig/iptables** en y ajoutant les lignes suivantes:

```
-A INPUT -s 10.0.2.0/24 -m state --state NEW -p udp --dport 111 -j ACCEPT
-A INPUT -s 10.0.2.0/24 -m state --state NEW -p tcp --dport 111 -j ACCEPT
-A INPUT -s 10.0.2.0/24 -m state --state NEW -p tcp --dport 2049 -j ACCEPT
-A INPUT -s 10.0.2.0/24 -m state --state NEW -p tcp --dport 32803 -j ACCEPT
-A INPUT -s 10.0.2.0/24 -m state --state NEW -p udp --dport 32769 -j ACCEPT
-A INPUT -s 10.0.2.0/24 -m state --state NEW -p tcp --dport 892 -j ACCEPT
-A INPUT -s 10.0.2.0/24 -m state --state NEW -p udp --dport 892 -j ACCEPT
-A INPUT -s 10.0.2.0/24 -m state --state NEW -p tcp --dport 875 -j ACCEPT
-A INPUT -s 10.0.2.0/24 -m state --state NEW -p udp --dport 875 -j ACCEPT
-A INPUT -s 10.0.2.0/24 -m state --state NEW -p tcp --dport 662 -j ACCEPT
-A INPUT -s 10.0.2.0/24 -m state --state NEW -p udp --dport 662 -j ACCEPT
```

De manière générale, l'ajout d'une règle se passe suivant ce schéma :

iptables -A (chain) -p (protocole) --dport (port) -j (décision)

Remplacez chain par la section qui vous intéresse (INPUT ou OUTPUT), protocole par le nom du protocole à filtrer (TCP, UDP, ICMP…) et enfin décision par la décision à prendre : ACCEPT pour accepter le paquet, REJECT pour le rejeter ou bien DROP pour l'ignorer complètement.

La Chain INPUT : correspond aux règles manipulant le trafic entrant

On peut maintenant redémarrer le service **iptables** par la commande suivante:

```
# service iptables restart
```

```
# chkconfig iptables on
```

Test d'ouverture des ports avec Nmap

Nmap est un scanneur de port réseau disponible sur Linux, Mac, FreeBSD, Windows… Le but de ce logiciel est de détecter les ports réseau ouvert sur des machines. Il permet donc de détecter si une machine est sur un réseau, d'identifier les services qui tournent dessus et même d'en déduire dans certain cas le type d'operating system.

Vérifions les ports ouverts avec la commande nmap à partir d'un autre poste connecté au réseau

```
# nmap 10.0.2.50
```

```
Scanning 10.0.2.50 [1000 ports]
Discovered open port 8080/tcp on 10.0.2.50
Discovered open port 3306/tcp on 10.0.2.50
Discovered open port 111/tcp on 10.0.2.50
Discovered open port 22/tcp on 10.0.2.50
Discovered open port 9090/tcp on 10.0.2.50
Discovered open port 2049/tcp on 10.0.2.50
Discovered open port 10002/tcp on 10.0.2.50
Completed SYN Stealth Scan at 00:13, 0.08s elapsed
(1000 total ports)
Initiating Service scan at 00:13
Scanning 7 services on 10.0.2.50
Completed Service scan at 00:15, 131.01s elapsed (7
services on 1 host)
Initiating OS detection (try #1) against 10.0.2.50
NSE: Script scanning 10.0.2.50.
Initiating NSE at 00:15
Completed NSE at 00:16, 30.15s elapsed
Nmap scan report for 10.0.2.50
Host is up (0.000062s latency).
Not shown: 993 closed ports
```

```
PORT      STATE SERVICE     VERSION
22/tcp    open  ssh         OpenSSH 5.3 (protocol 2.0)
| ssh-hostkey: 1024
ab:a2:a8:5b:c5:19:1d:3e:ec:82:f6:9d:55:69:b5:59 (DSA)
|_2048
8f:f9:c5:ef:cf:4b:c4:2d:61:0a:1b:8f:45:d0:89:7a (RSA)
111/tcp   open  rpcbind     2-4 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4        111/tcp  rpcbind
|   100000  2,3,4        111/udp  rpcbind
|   100003  2,3,4       2049/tcp  nfs
|   100003  2,3,4       2049/udp  nfs
|   100005  1,2,3        892/tcp  mountd
|   100005  1,2,3        892/udp  mountd
|   100021  1,3,4      32769/udp  nlockmgr
|   100021  1,3,4      32803/tcp  nlockmgr
|   100024  1          43252/udp  status
|   100024  1          44012/tcp  status
|   100227  2,3         2049/tcp  nfs_acl
|_  100227  2,3         2049/udp  nfs_acl
2049/tcp  open  nfs         2-4 (RPC #100003)
3306/tcp  open  mysql       MySQL 5.1.69-log
| mysql-info: Protocol: 10
| Version: 5.1.69-log
```

Nous constatons que les ports configurés précédemment (**111,2049,892,32769 et 32803**) sont ouverts.

Les ports **892** et **662** n'apparaissent pas car ils ne sont pas encore utilisés par le serveur NFS.

Le port **22** nous permet de se connecter au serveur en SSH.

```
| Thread ID: 19
| Some Capabilities: Long Passwords, Connect with DB,
Compress, ODBC, Transactions, Secure Connection
| Status: Autocommit
|_Salt: "S\W{*\o:pFN6``Co$a?
8080/tcp  open  http        Apache Tomcat/Coyote JSP
engine 1.1
|_http-methods: No Allow or Public header in OPTIONS
response (status code 400)
|_http-title: Site doesn't have a title.
9090/tcp  open  tcpwrapped
10002/tcp open  documentum?
MAC Address: 00:0C:29:FA:82:E8 (VMware)
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/
o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.6
Uptime guess: 0.023 days (since Tue Jun 04 23:42:29
2013)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE
HOP RTT     ADDRESS
1   0.06 ms 10.0.2.50
```

Nous constatons également ici que le port **8080** est ouvert, celui-ci est Utilisé par Apache Tomcat qui permet de se connecter à Cloudstack via l'interface Web.

Configuration de la Template système

CloudStack utilise un certain nombre de machines virtuelles système pour permettre l'accès aux consoles des machines virtuelles, fournir divers services réseau, et gérer divers aspects de stockage.
Cette étape permet d'acquérir les images système correspondant à ces machines virtuelles système, images prêtes au déploiement lors du bootstrap (amorçage) du cloud à créer.
Il faut à présent télécharger le template de la machine virtuelle système et déployer ce template sur le périphérique monté juste avant.
Le serveur de management comprend un script pour manipuler correctement les images des machines virtuelles système.

```
# /usr/lib64/cloud/agent/scripts/storage/secondary/cloud-install-sys-tmplt -m /secondary -u http://download.cloud.com/templates/acton/acton-systemvm-02062012.qcow2.bz2 -h kvm -F
```

Ceci conclut la configuration du serveur de management. Il est encore nécessaire de configurer CloudStack, mais cela sera fait après la configuration de l'hyperviseur.

Installation et configuration de KVM

Configuration de KVM

KVM est l'hyperviseur qui sera utilisé, ici sera rétablie la configuration initiale sur l'hôte de l'hyperviseur, et l'installation du logiciel agent sera détaillée. La même démarche pourra être suivie pour ajouter des nœuds KVM supplémentaires sur l'environnement CloudStack.

L'installation de KVM est très simple et se fait avec une seule commande mais il y a quelques configurations à faire.

Pour pouvoir installer l'agent pour KVM , il faut d'abord ajouter le repository d'EPEL .

```
# rpm -Uvh http://fr2.rpmfind.net/linux/epel/6/i386/epel-release-6-8.noarch.rpm
```

Vérifier qu'il soit bien actif dans la liste des repository disponibles

```
# yum repolist all
# yum repolist all | grep enabled
```

Relancer le programme d'installation

```
# ./install.sh
```

Sélectionner l'option « A » → Install the Agent

Puis

```
# service cgconfig restart
# service cgred restart
# chkconfig cgconfig on
# chkconfig cgred on
```

Vérifier que les service sont bien actifs

```
# service cgconfig status
# service cgred status
```

Configuration de QEMU

La configuration de KVM est relativement simple et se fait en une seule étape. Il faut modifier la configuration de QEMU VNC.
Cela se fait en modifiant **/etc/libvirt/qemu.conf** , en s'assurant que la ligne suivante est présente et décommentée:

```
vnc_listen=0.0.0.0
```

Configuration de Libvirt

CloudStack utilise **libvirt** pour gérer les machines virtuelles. Il est donc impératif que libvirt soit bien configuré. Le paquet cloud-agent dépend de libvirt et devrait donc déjà être installé.

Pour pouvoir utiliser la migration à chaud, libvirt doit accepter des connections TCP non sécurisées. Nous devons aussi désactiver les requêtes multicastDNS de libvirt. Ces deux configurations sont dans le fichier **: /etc/libvirt/libvirtd.conf**

Configurez les paramètres suivant:

```
listen_tls = 0
listen_tcp = 1
tcp_port = "16059"
auth_tcp = "none"
mdns_adv = 0
```

Activer "listen_tcp" in libvirtd.conf n'est pas suffisant, vous devez aussi modifier les paramètres suivant:

Modifier **/etc/sysconfig/libvirtd**

Décommenter la ligne suivante:

```
# LIBVIRTD_ARGS="--listen"
```

Redémarrer **libvirt**

```
# service libvirtd restart
# chkconfig libvirtd on
# service cloud-agent restart
# chkconfig cloud-agent on

# service libvirtd status
```

Ceci conclut l'installation et la configuration de KVM, ce qui permet maintenant de se concentrer sur l'utilisation de l'interface utilisateur CloudStack avec la configuration actuelle de notre cloud.

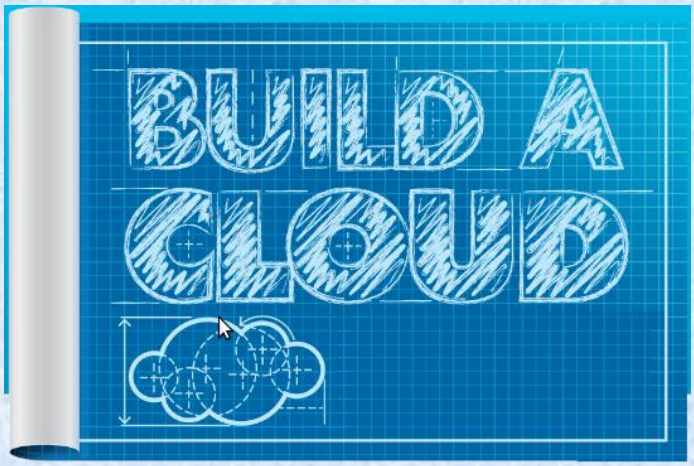
Avant redémarrage du serveur quelques modifications restent à apporter.

Rajouter les informations suivantes à la fin du fichier **/etc/cgconfig.conf**

```
group virt {
    cpu {
        cpu.shares = 9216;
        }
}
```

Redémarrer le service

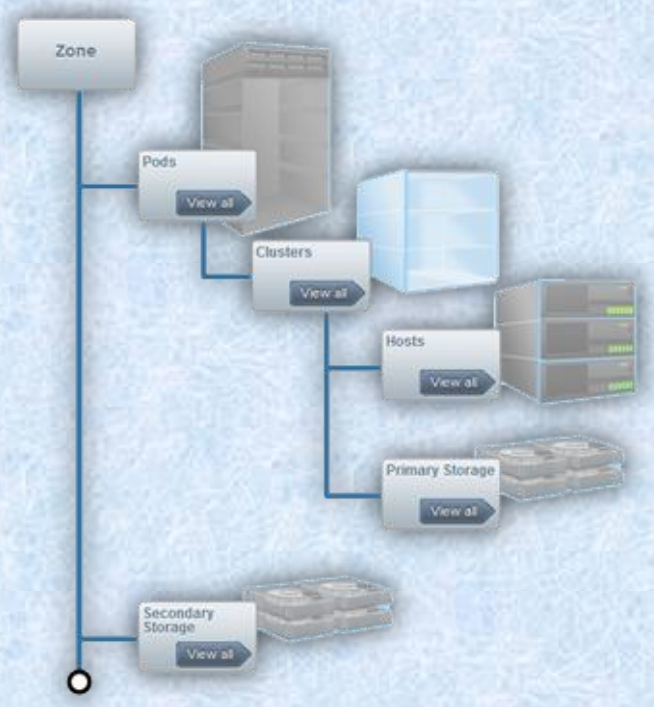
```
# service cgconfig restart
```

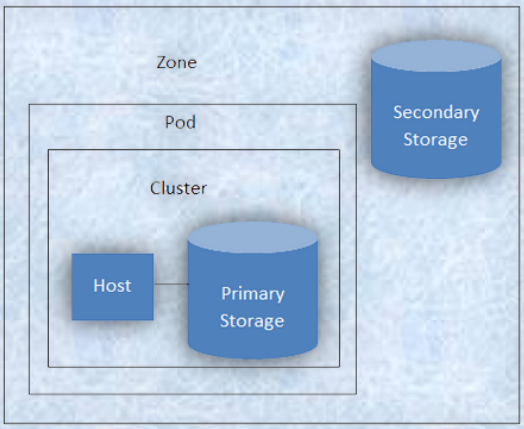


Configuration et Utilisation de Cloudstack

Déploiement d'une Zone

Voici l'infrastructure d'une zone que nous allons déployer à l'intérieur de CloudStack.

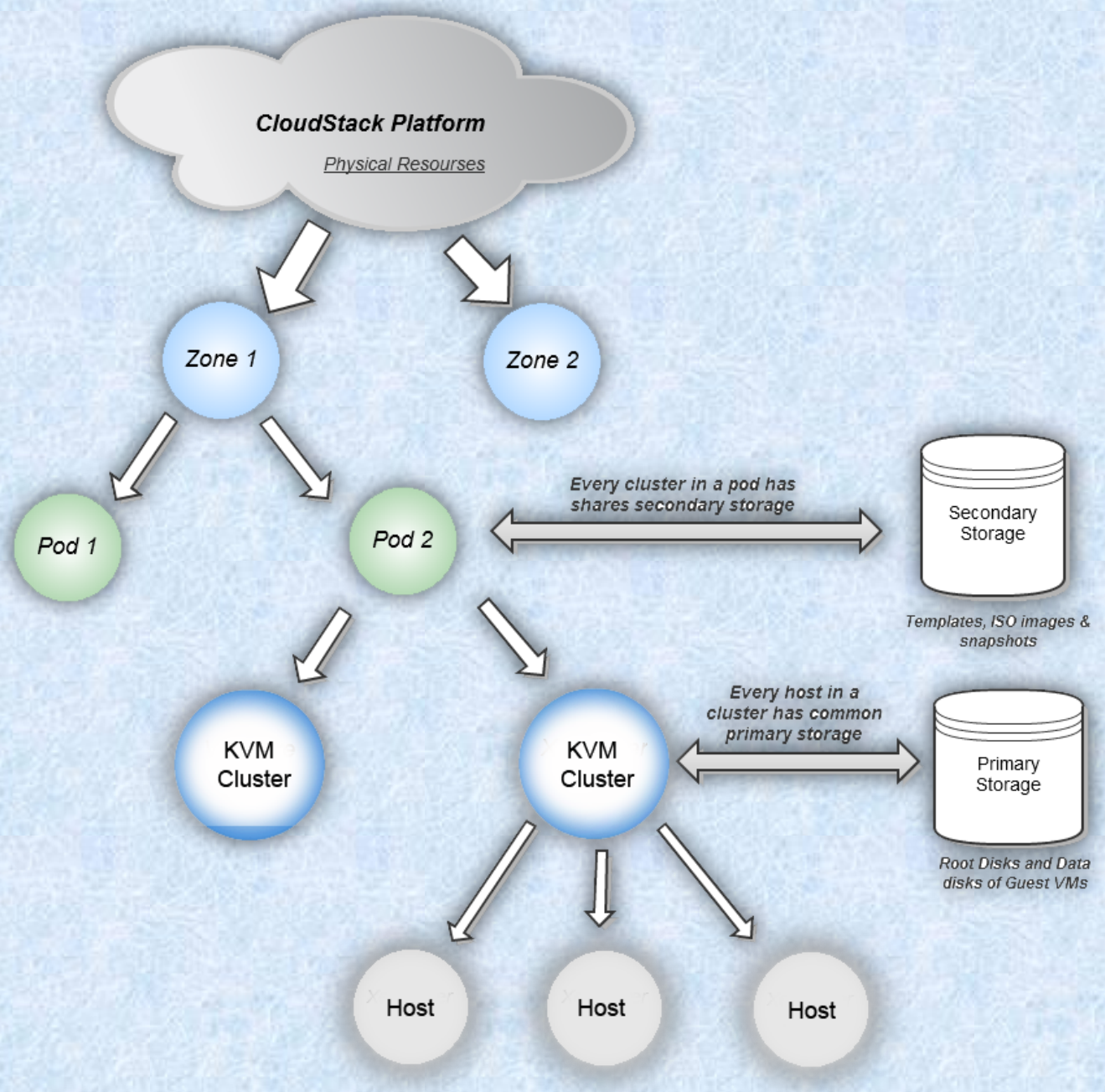




Le **Management Server** gère une ou plusieurs zones (en général des **datacenters**) contenant des ordinateurs hôtes où les machines virtuelles invitées seront exécutés.

L'infrastructure du cloud est organisée comme suit:

- **Zone**: Typiquement, une zone est équivalent à un Datacenter Une zone est constituée d'une ou plusieurs cosses et le stockage secondaire.
- **Un Pod:** Un Pod représente un rack qui comporte un commutateur de couche 2 et un ou plusieurs Clusters.
- **Cluster**: Un cluster est constitué d'un ou plusieurs hôtes et du stockage primaire.
- **Host**: Un seul nœud de calcul au sein d'un cluster. Les hôtes sont où les services de cloud computing sont exécutés sous la forme de machines virtuelles invitées.
- **Stockage primaire** est associé à un cluster, et il stocke les volumes de disque pour toutes les machines virtuelles fonctionnant sur les hôtes de ce cluster.
- **Stockage secondaire** est associé à une zone, et il stocke des modèles, des images ISO, et les snapshots de volume.



CloudStack offre deux types de scénarios de mise en réseau:

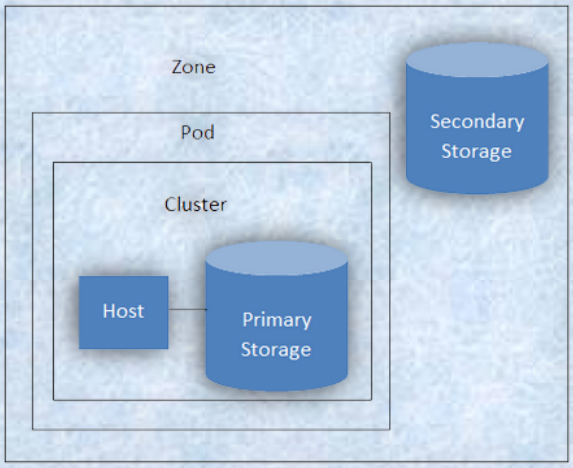
- **Basic**.. Fournit un réseau unique où l'isolement d'hôtes peut être fournie par des moyens de couche 3 tels que les groupes de sécurité (filtrage source d'adresse IP).
- **Avancé**. Pour les réseau de topologies plus sophistiquées. Ce modèle de réseau permet plus de souplesse dans la définition des réseaux invités.

Nous utiliserons dans notre cas un déploiement de réseau Basic.

Description d'une Zone :

Une **zone** est la deuxième plus grande unité organisationnelle au sein d'un déploiement de CloudStack. Une zone correspond typiquement à un centre de données unique, mais il est permis d'avoir plusieurs zones dans un datacenter. L'avantage d'organiser l'infrastructure en zones est de fournir une isolation physique et la redondance.
Par exemple, chaque zone peut avoir sa propre alimentation électrique et réseau de liaison montante, et les zones peuvent être très éloignés géographiquement (même si ce n'est pas nécessaire).
Une zone se compose de:

- Un ou plusieurs **Pods**. Chaque **Pods** contient un ou plusieurs groupes **d'hôtes** et un ou plusieurs **serveurs de stockage primaire**.
- Stockage secondaire, qui est partagé par tous les Pods dans la zone.



Les **zones** sont visibles pour l'utilisateur final. Lorsqu'un utilisateur démarre une machine virtuelle invitée, l'utilisateur doit sélectionner une zone pour leur invité. Les utilisateurs peuvent également être tenus de copier leurs modèles privés de zones supplémentaires pour permettre la création de machines virtuelles invitées en utilisant leurs modèles dans ces zones.
Les zones peuvent être **publiques** ou **privés**.

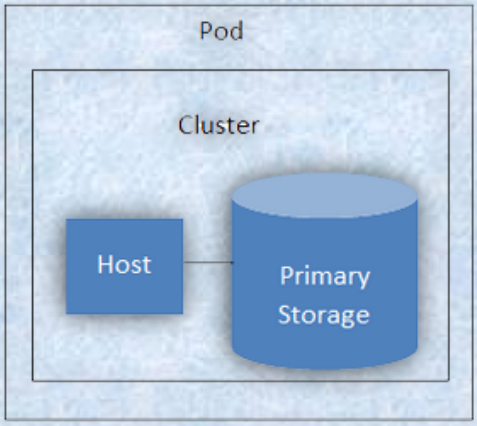
- Les **zones publiques** sont visibles à tous les utilisateurs. Cela signifie que n'importe quel utilisateur peut créer un invité dans cette zone.
- **Zones privées** sont réservées à un domaine spécifique. Seuls les utilisateurs de ce domaine ou de ses sous-domaines peuvent créer des invités dans cette zone.

Les hôtes dans la même zone sont directement accessibles à l'autre sans avoir à passer par un pare-feu. Les **hôtes** dans des zones différentes peuvent accéder à l'autre par des tunnels VPN configurés de manière statique.

Pour chaque **zone**, l'administrateur doit décider ce qui suit.

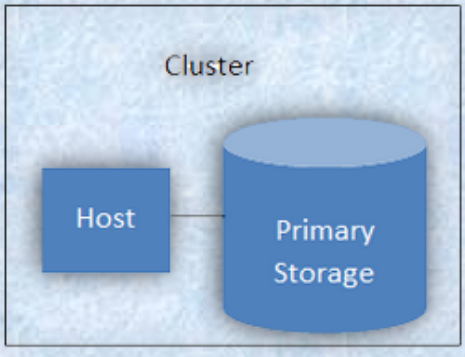
- Combien de **Pods** à placer dans une zone.
- Combien de **Cluster** à placer dans chaque **Pod**.
- Combien **d'hôtes** à placer dans chaque **cluster**.
- Combien de serveurs de **stockage primaire** à placer dans chaque **Cluster** et la capacité totale pour les serveurs de stockage.
- Combien de **stockage secondaire** à se déployer dans une **zone**.
- Lorsque vous ajoutez une nouvelle **zone**, vous serez invité à configurer le réseau physique de la zone et ajouter le premier **Pod**, un **Cluster** les **hôtes**, le **stockage primaire** et le **stockage secondaire**.

Description d'un Pod



Un **pod** représente souvent un seul rack. Les **hôtes** dans la même **Pod** sont dans le même sous-réseau. Un pod est la seconde plus grande unité dans un déploiement de CloudStack.
Les **Pods** sont contenus à l'intérieur des zones. Chaque zone peut contenir un ou plusieurs Pods. Un Pod est composé d'une ou plusieurs **Clusters** d'ordinateurs et un ou plusieurs serveurs de stockage primaire. Les Pods ne sont pas visibles à l'utilisateur final.

Description d'un Cluster



Un **cluster** est un moyen pour grouper les hôtes . Pour être précis, un cluster est un groupe de serveurs XenServer, un ensemble de serveurs KVM ou un cluster VMware préconfiguré dans vCenter.
Les hôtes d'un cluster ont tous un matériel identique, exécutent le même hyperviseur, sont tous sur le même sous-réseau et accèdent au même stockage partagé.

Les **i nstances de machines virtuelles (VM)** peuvent être directement migrées d'un hôte à un autre au sein du même Cluster, sans interrompre le service à l'utilisateur.
Un **cluster** est la troisième unité organisationnelle troisième dans le déploiement de CloudStack. Les Clusters sont contenus dans les Pods et les Pods sont à l'intérieur des zones.

Un cluster est constitué d'un ou plusieurs hôtes et d'un ou plusieurs serveurs de stockage primaire.

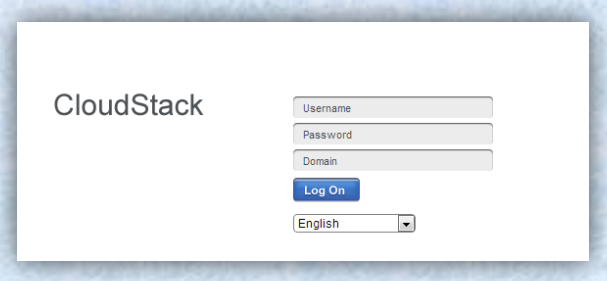
Accès à l'interface utilisateur

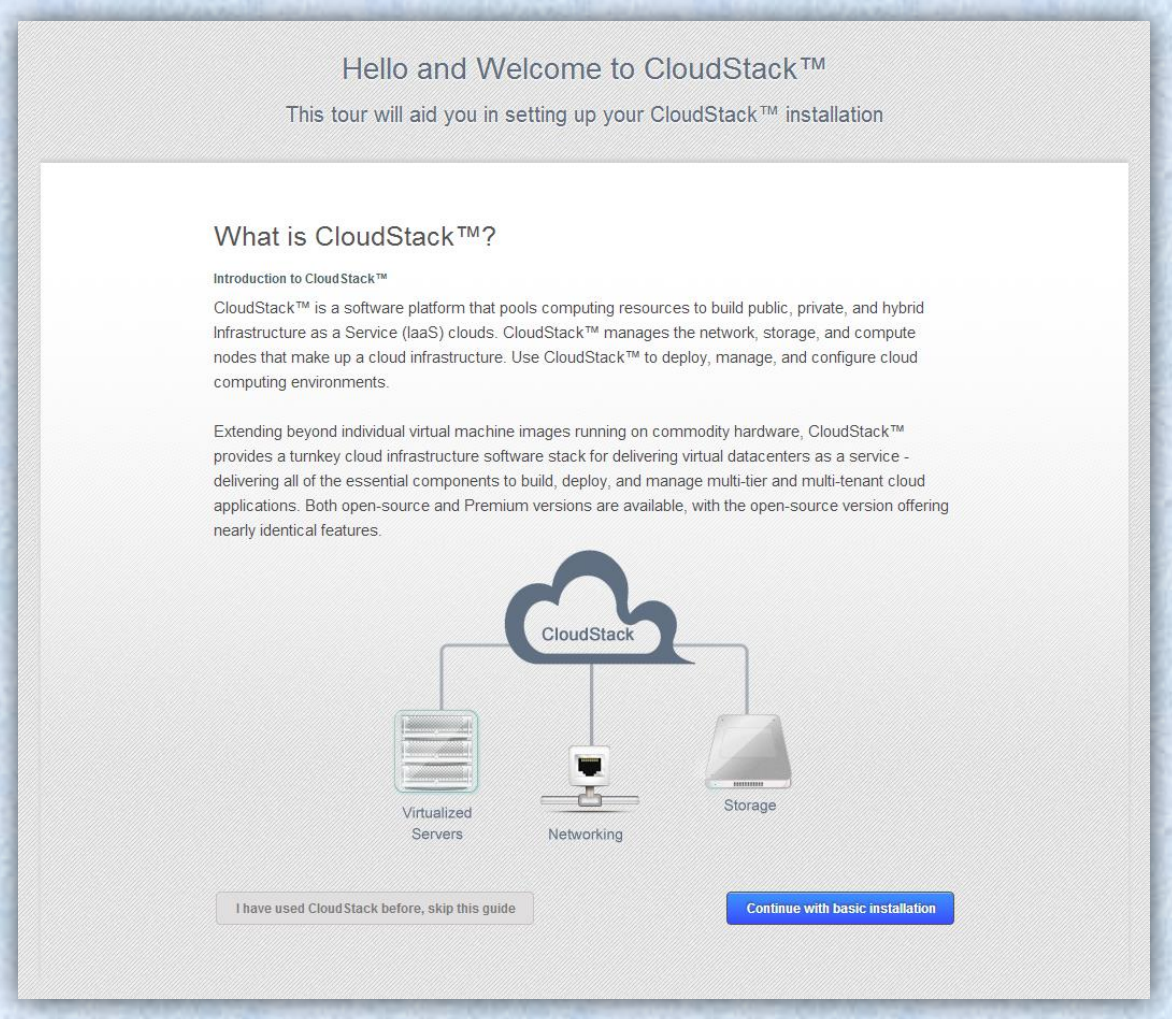
Pour accéder à l'interface web de CloudStack, il suffit de visiter **http://10.0.2.50:8080/client** à l'aide d'un navigateur.
L'utilisateur par défaut est 'admin' et le mot de passe par défaut est 'password'.

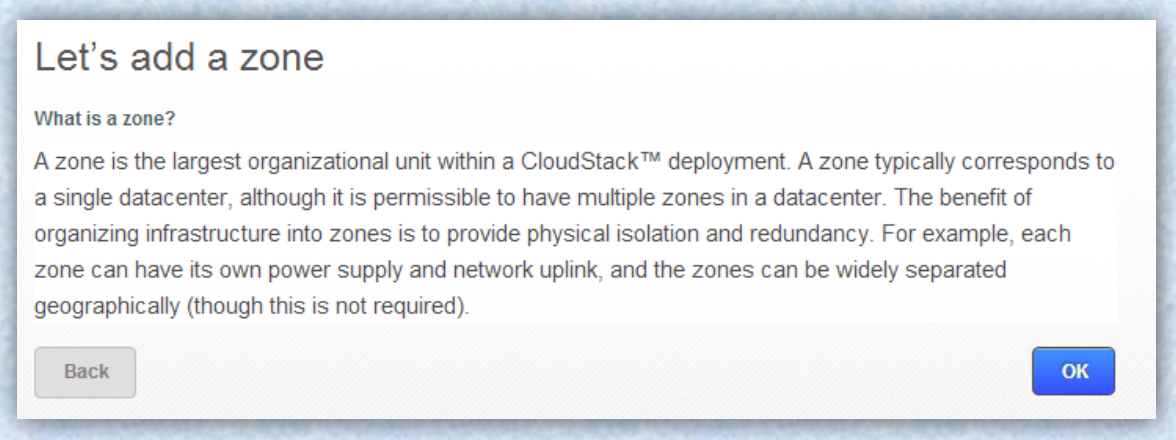
Un écran d'accueil permet alors de choisir entre différentes options pour configurer CloudStack.

Choisir l'option "Continue with Basic Setup".

Un formulaire demande alors de changer le mot de passe pour l'administrateur. Il est recommandé de changer ce mot de passe immédiatement.



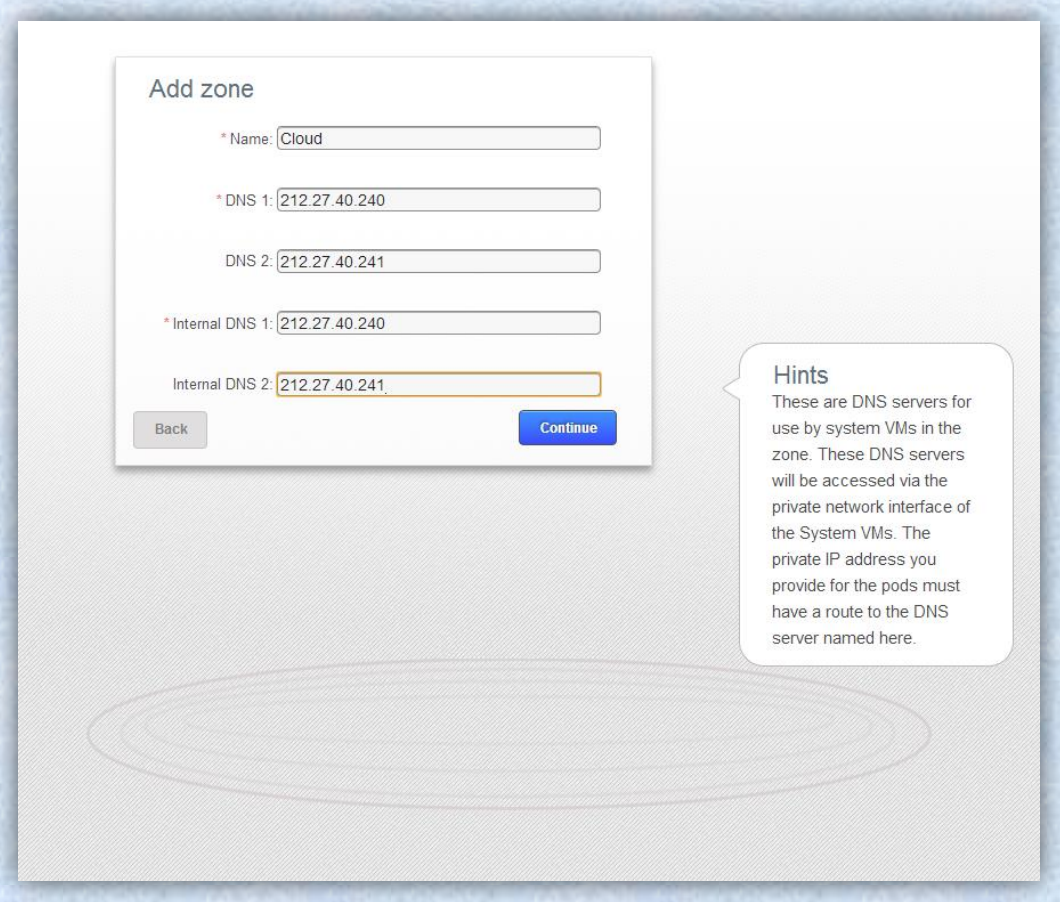




Configurer une zone

Une zone est l'entité la plus large de CloudStack, cet écran en décrit les détails. Il contient cinq informations essentielles :

1. **Name** - le nom sera défini à 'Cloud'
2. **Public DNS 1** - '212.27.40.240'
3. **Public DNS 2** - '212.27.40.241'
4. **Internal DNS 1** - '212.27.40.240'
5. **Internal DNS2** - '212.27.40.241'



CloudStack fait la distinction entre les DNS public et interne. Le DNS interne est capable de résoudre seulement les noms de domaine internes, comme le nom DNS du serveur NFS.Le DNS public est fourni aux machines virtuelles invitées pour leur permettre de résoudre les adresses IP publiques. Il est possible d'utiliser les mêmes serveurs DNS pour les deux types, mais il faut alors être sûr que les adresses IP interne et publique puissent router vers le serveur DNS. Pour la suite, dans le cas présent, aucun nom ne sera donné aux ressources en interne, et elles seront définies afin de pointer vers la même ressource externe pour ne pas ajouter la configuration d'un serveur de noms dans la liste des besoins matériels.
Maintenant que la zone est ajoutée, la prochaine fenêtre qui apparaît concerne la création d'un pod. Elle demande 4 éléments.

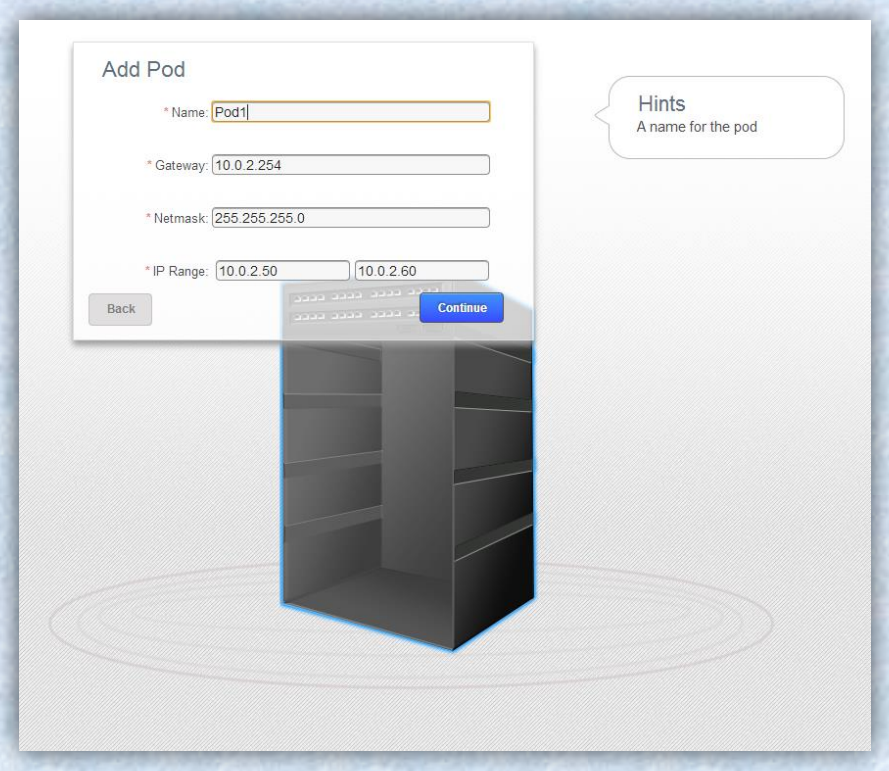
Un point of delivery, ou **POD** , est "un module de réseau, de calcul, de stockage et des composants d'application qui travaillent ensemble pour offrir des services de réseau. Le **POD** est un modèle de conception, et ses composants augmentent la modularité, l'évolutivité et la gérabilité des datacenters . . Les clients peuvent acquérir, à la demande, une autre plage de VLAN distincte sur le commutateur, pour construire leur propre topologie du réseau.

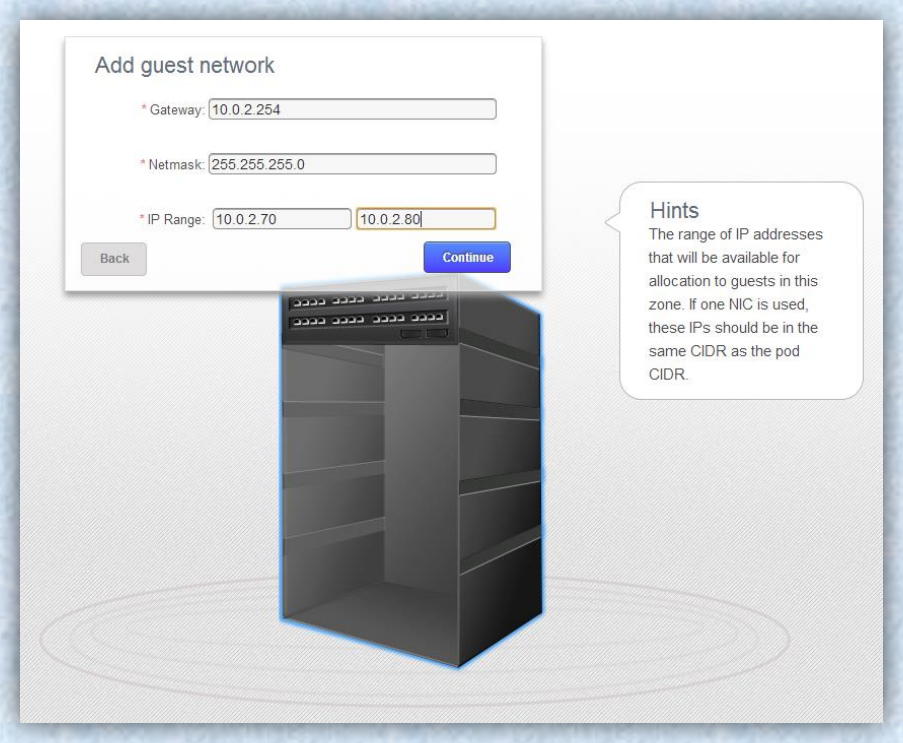
1. **Name** - Le nom sera Pod1 pour ce cloud.
2. **Gateway** – 10.0.2.254 sera utilisé comme passerelle
3. **Netmask** - 255.255.255.0
4. **Start/end reserved system IPs** – nous utiliserons 10.0.2.50-10.0.2.60 comme plage d'adresses IP système réservées.

Configuration Guest Network

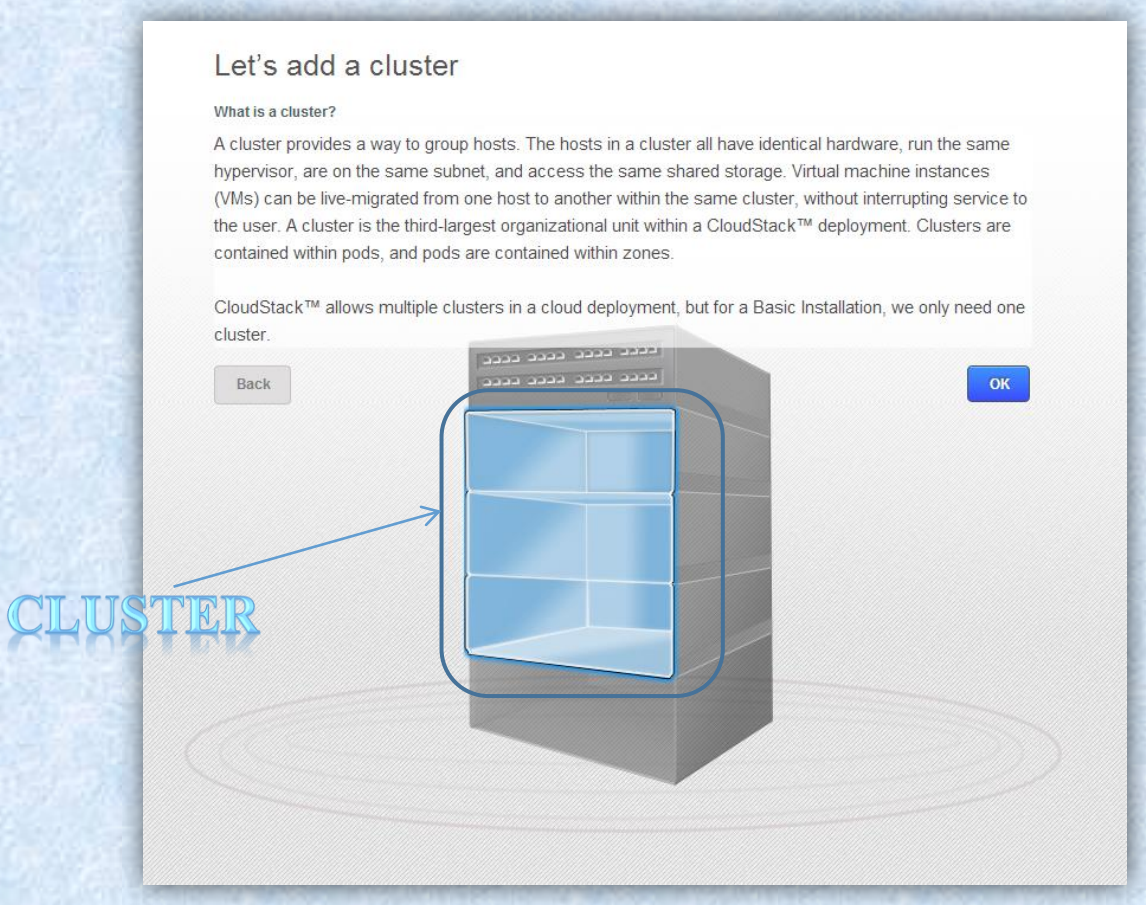
Correspond à la plage d'adresse IP qui seront données aux VM crées à l'intérieur du Cloud.

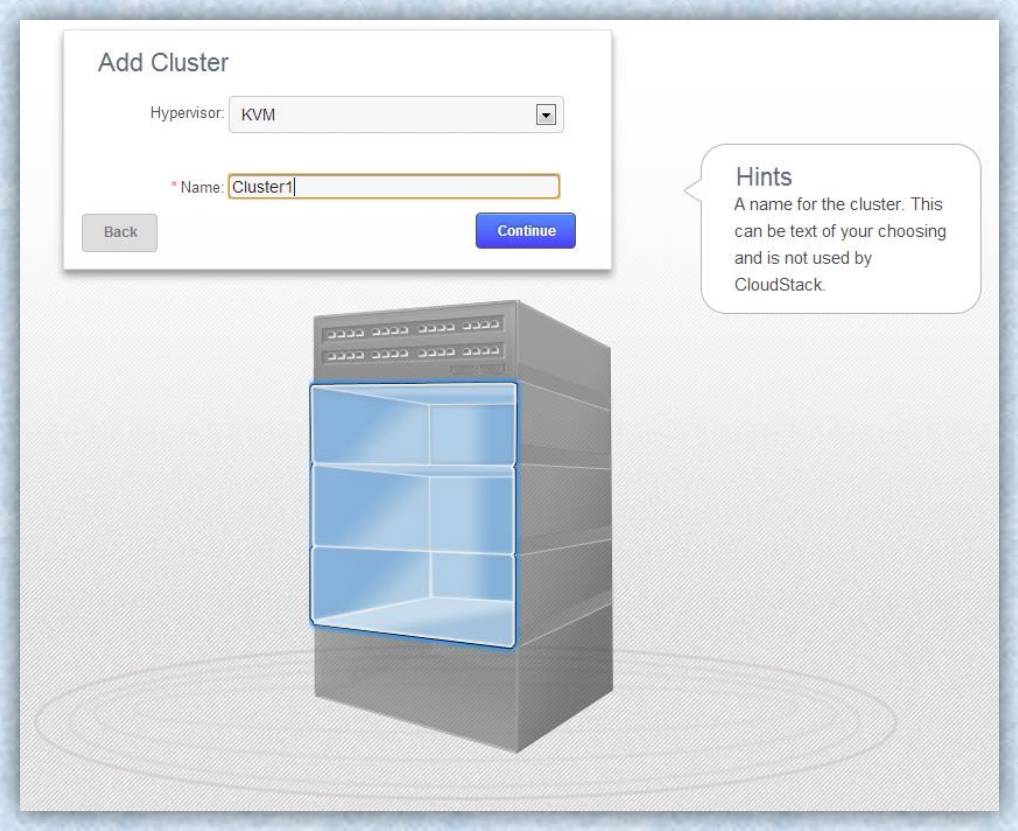
1 – **Gateway** : 10.0.2.254
2 – **Netmask** : 255.255.255.0
3 – **Ip Range** : 10.0.2.70 – 10.0.2.80





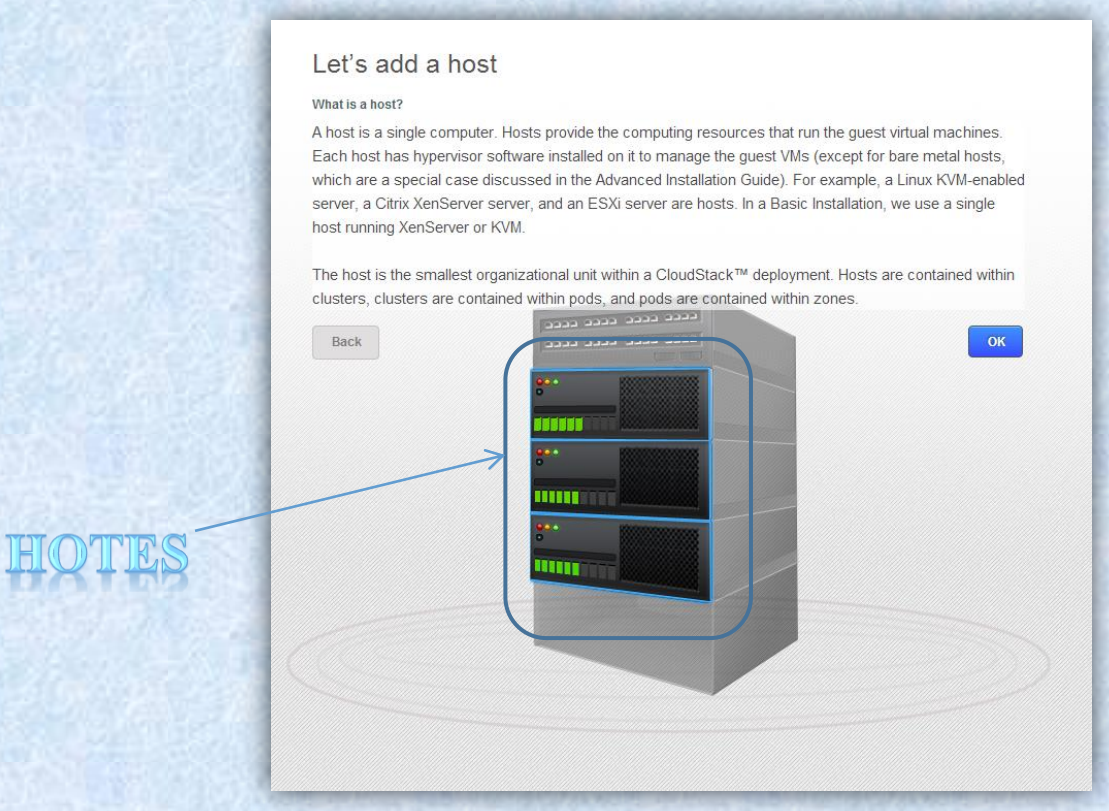
Maintenant que la zone est ajoutée, seules quelques informations supplémentaires sont nécessaires pour configurer le cluster.

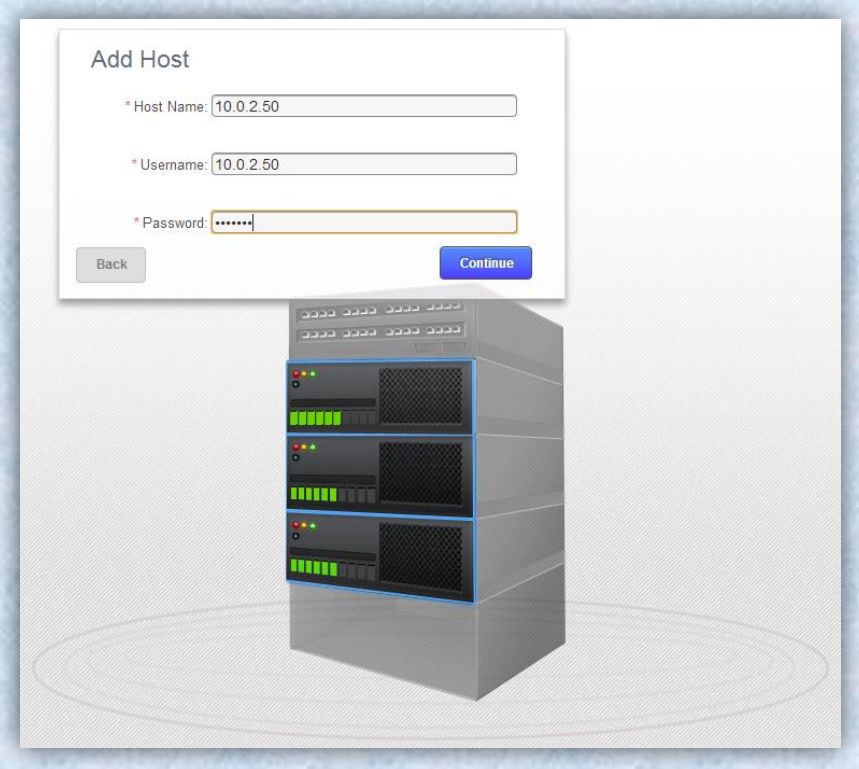




Le premier hôte du cluster peut alors être ajouté. Seuls quelques détails sont nécessaires.

1. **Hostname** - l'adresse IP 10.0.2.50 sera utilisée puisque le serveur DNS n'est pas configuré.
2. **Username** - root
3. **Password** - entrer le mot de passe du système d'exploitation correspondant à l'utilisateur root



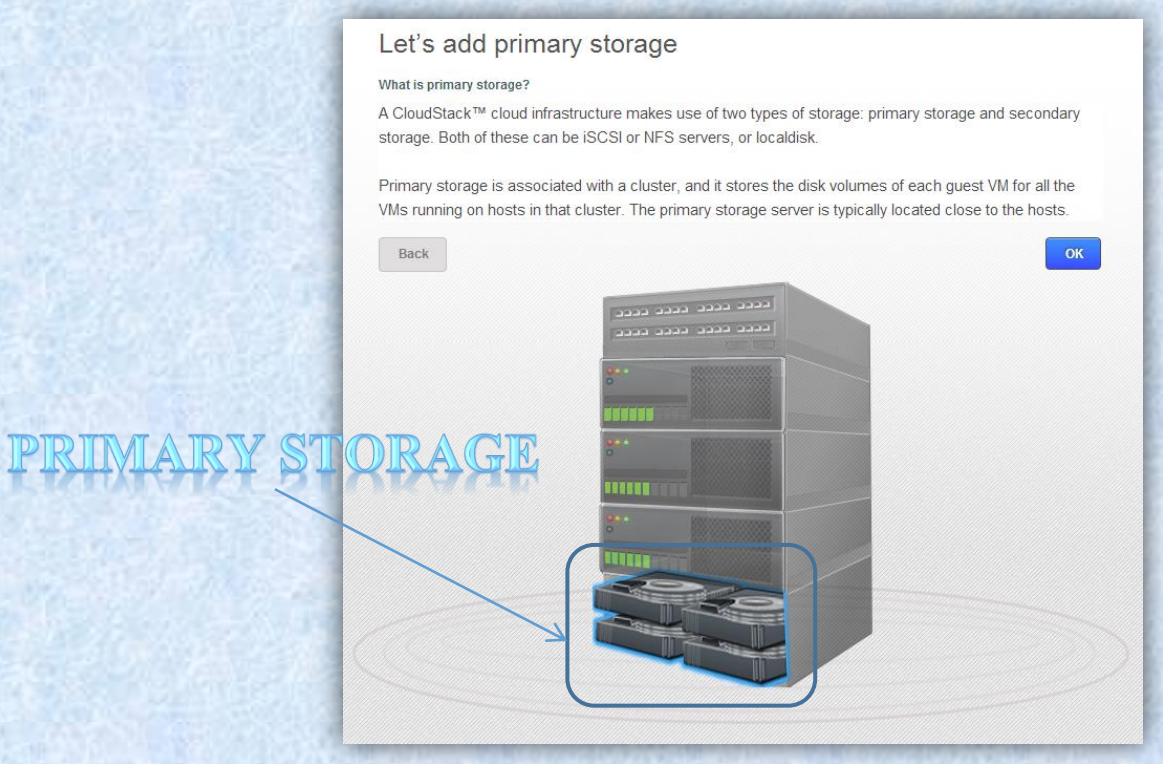


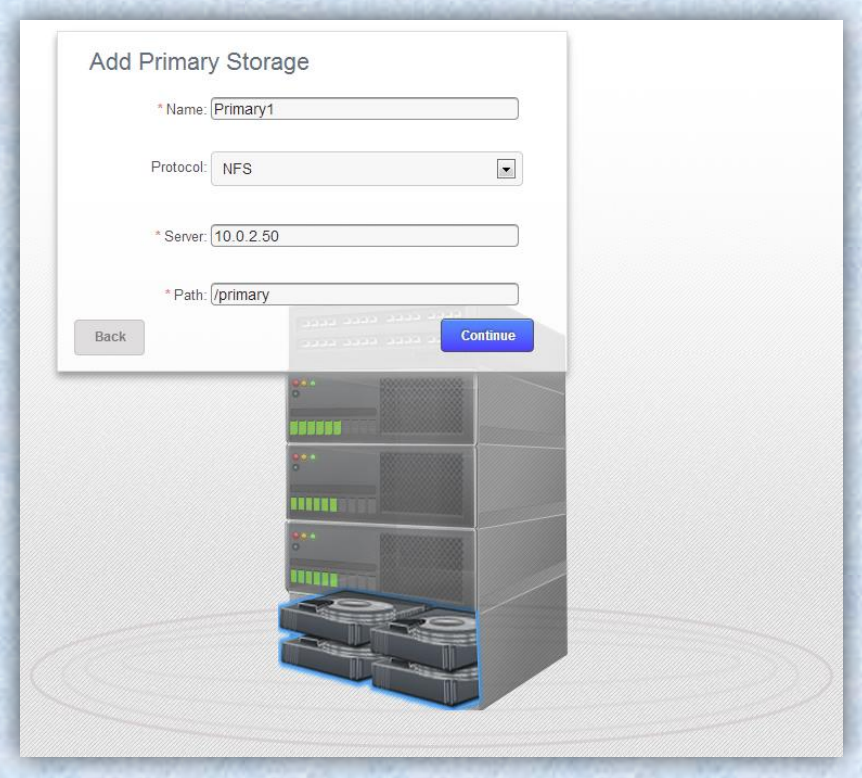
Stockage Primaire

Maintenant que votre cluster et votre hôte sont configurés, vous devez rentrer les informations pour le système de stockage primaire. Choisissez NFS comme type de stockage et entrez les valeurs suivantes:

1. **Name** - utiliser 'Primary1'
2. **Server** - utiliser l'adresse IP 10.0.2.50

3. **Path** - définir « **/primary** » comme chemin utilisé

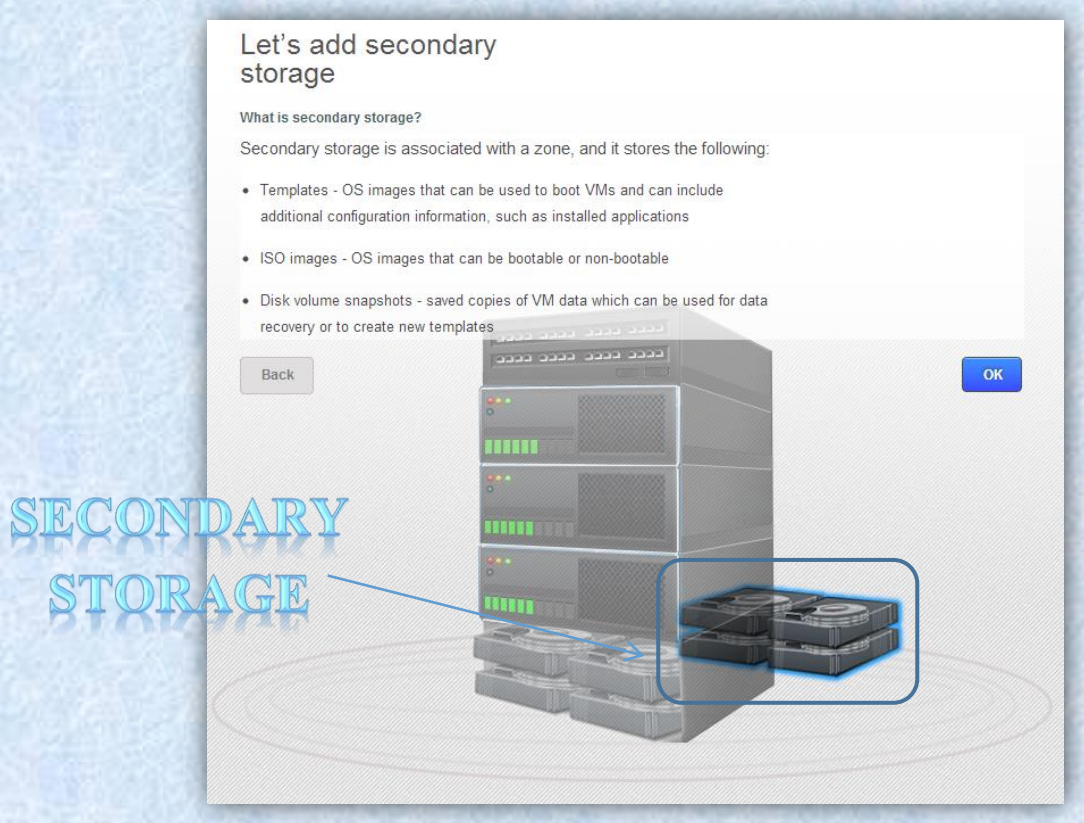


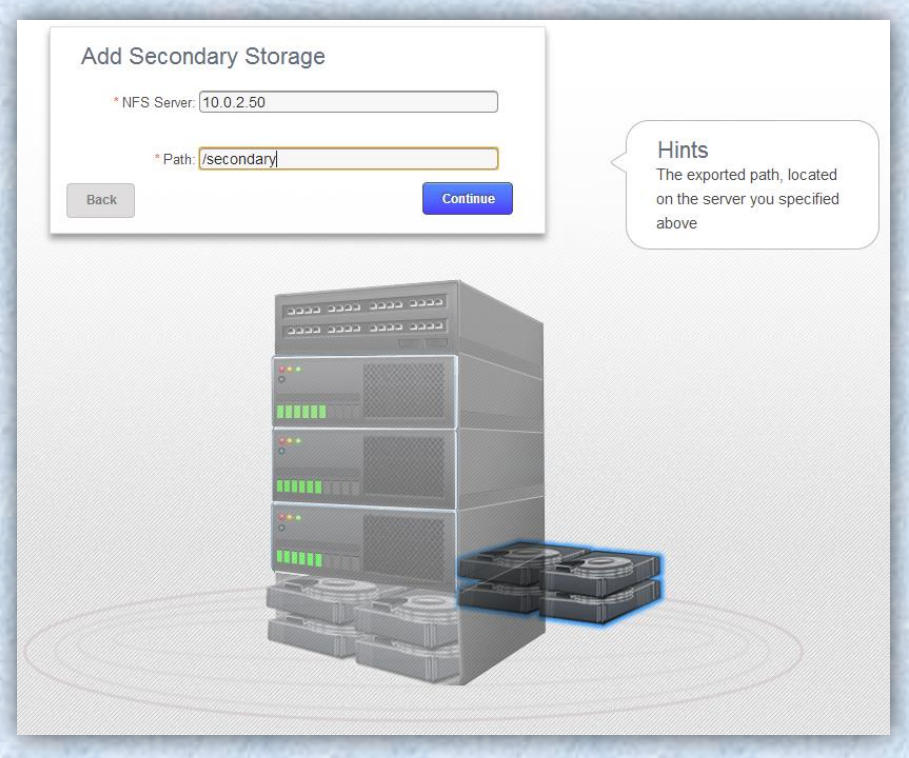


Stockage secondaire

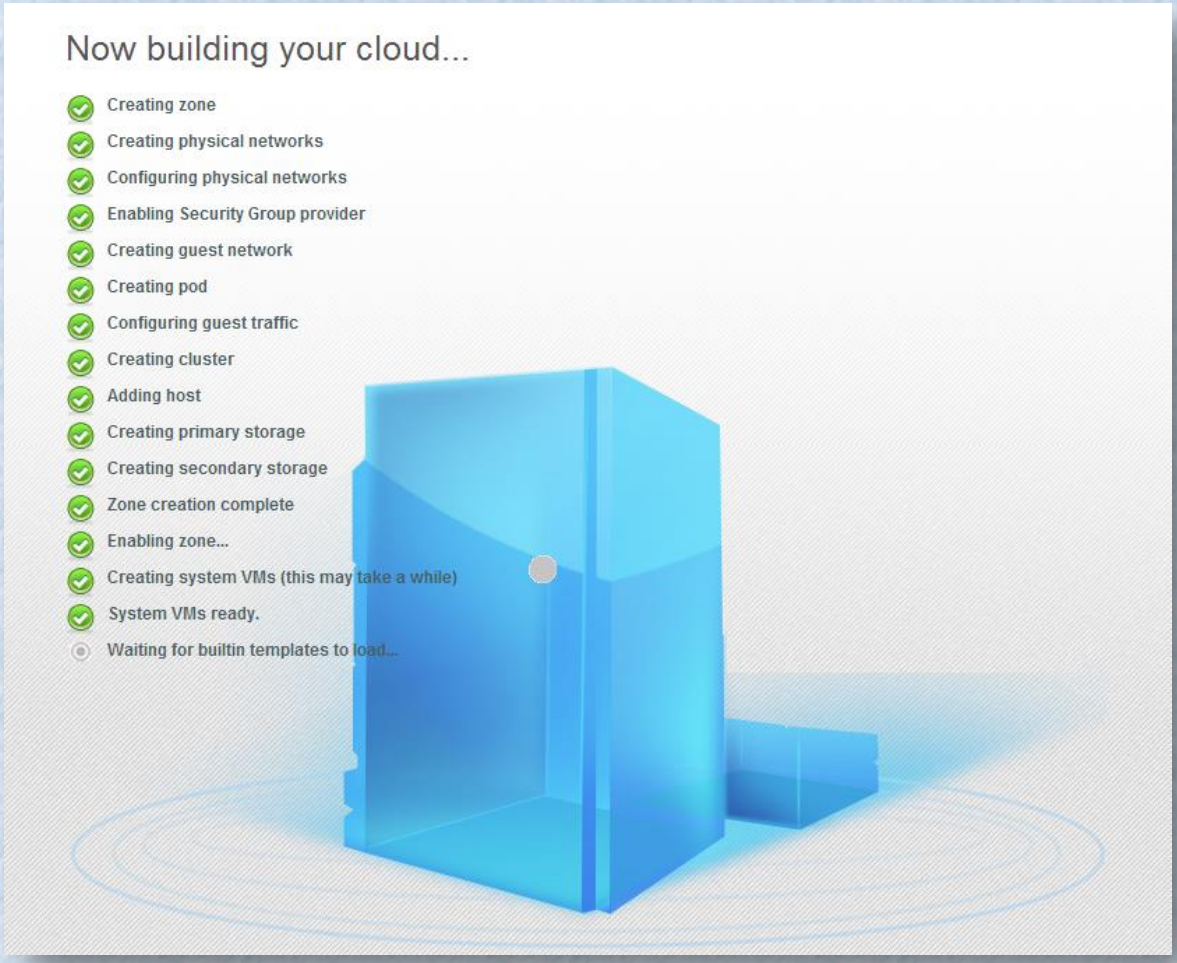
Si c'est une nouvelle zone, il sera demandé des informations complémentaires pour l'espace de stockage secondaire les renseigner comme suit :

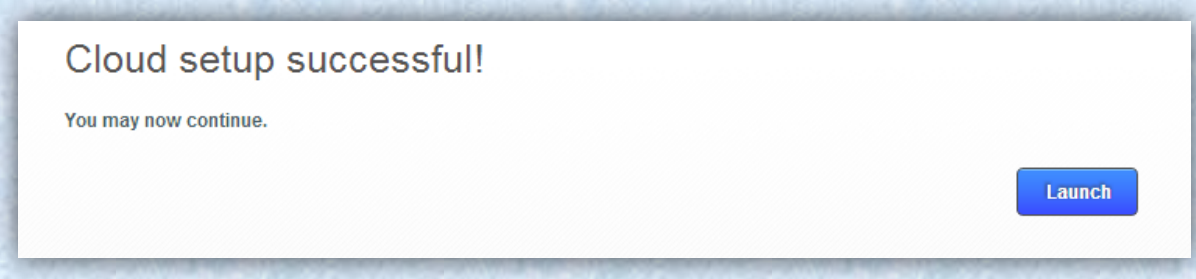
1. **NFS server** - utiliser l'adresse IP 10.0.2.50
2. **Path** - utiliser le répertoire « **/secondary** »





Maintenant, cliquer sur Launch , le cloud devrait commencer à se configurer - cela peut prendre plusieurs minutes selon la vitesse de la connexion internet lors de la finalisation de la configuration.



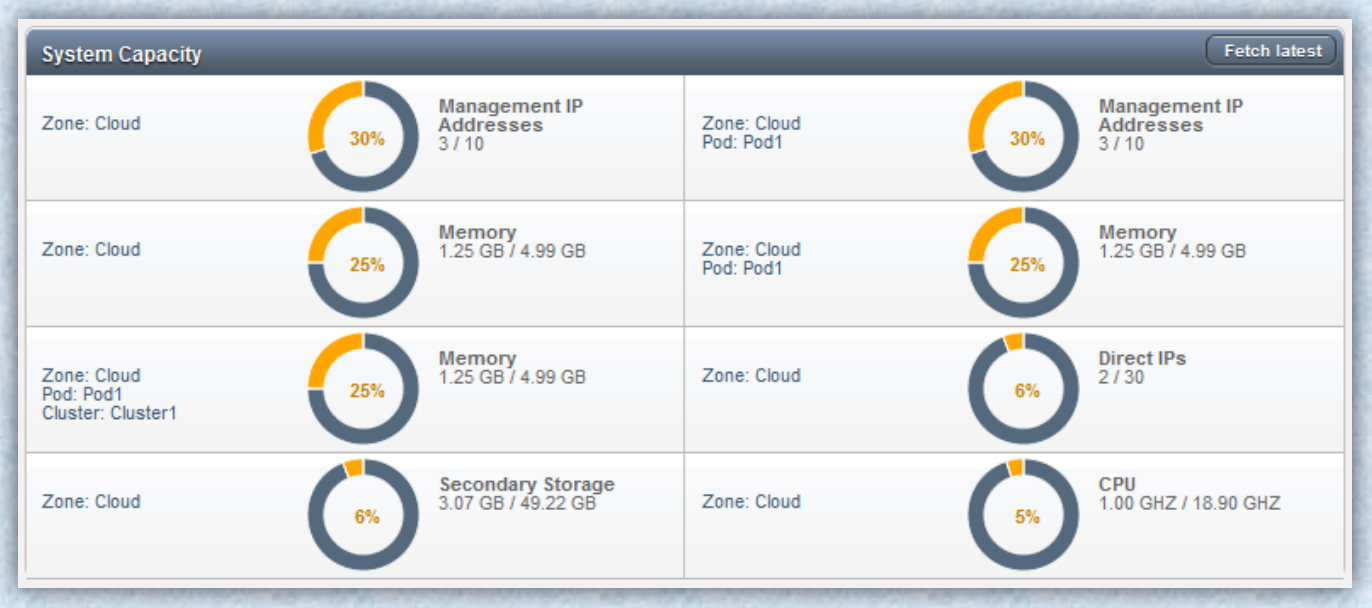


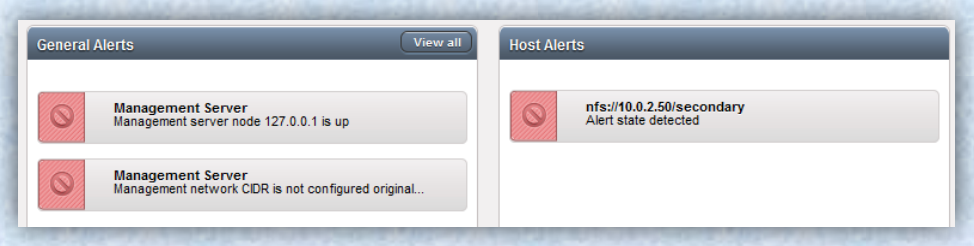
Après la fin de la construction du Cloud , vous pouvez vérifier que tous les services sont bien actifs.

```
# service cloud-agent status
# ps -ef | grep agent
# service cgconfig status
# service cgred status
# service libvirtd status
```

Prise en main de l'interface WEB de Cloudstack

Le Dashboard de Cloudstack permet de visualiser les informations principales du fonctionnement du Cloud

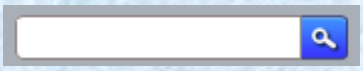




En premier quelques réglages de configuration sont à effectuer.
Après configuration il faudra relancer le service

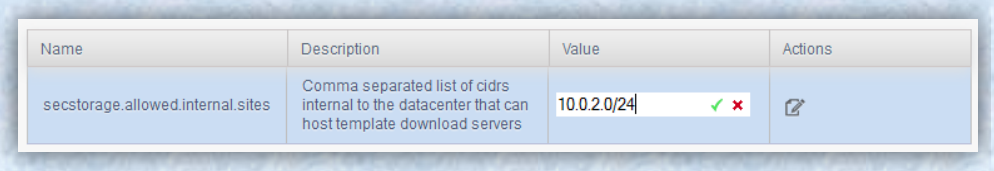
```
# service cloud-management restart
```

Comme le même serveur héberge le CS Management , les hôtes ,les disques primaires et secondaires....) nous devons autoriser le réseau à utiliser le disque secondaire :
Dans le menu principal , selectionner « Global Settings » et dans l'onglet de recherche

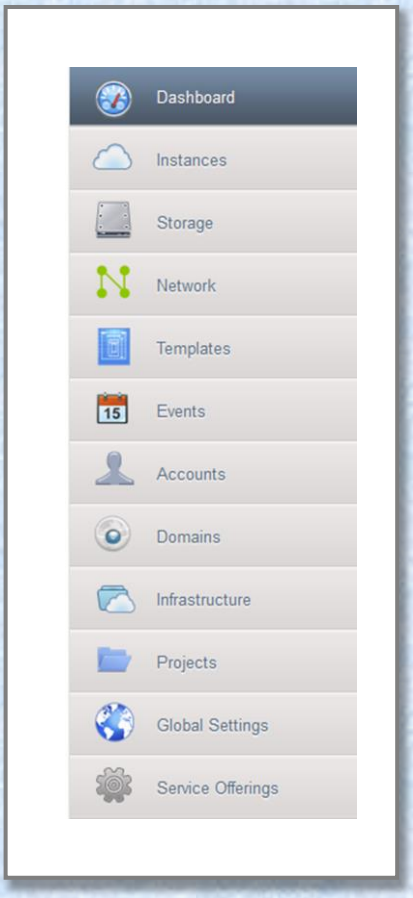


entrer l'option « **secstorage.allowed.internal.sites** »

Et configurer l'adresse du réseau utilisé :



Name	Description	Value	Actions
secstorage.allowed.internal.sites	Comma separated list of cidrs internal to the datacenter that can host template download servers	10.0.2.0/24	



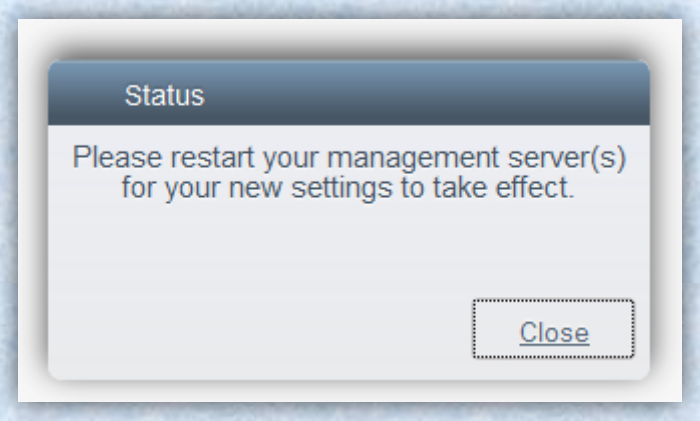
Configurer également les options suivantes :

On autoriser les VM à utiliser l'espace disque local

Name	Description	Value	Actions
system.vm.use.local.storage	Indicates whether to use local storage pools or shared storage pools for system VMs.	true	

On règle le délai de purge des VM supprimées comme ceci

Name	Description	Value	Actions
expunge.delay	Determines how long (in seconds) to wait before actually expunging destroyed vm. The default value = the default value of expunge.interval	1000	
expunge.interval	The interval (in seconds) to wait before running the expunge thread.	1000	
expunge.workers	Number of workers performing expunge	1	



Pour une meilleure visualisation du fonctionnement de la base de donnée de Cloudstack , installer « phpMyAdmin »

```
# yum install php-mysql

# yum install phpmyadmin
```

Il faut ensuite effectuer une autre modification : l'autorisation des machines du réseau à accéder à **phpMyAdmi**n. Pour cela il nous faut éditer le fichier **/etc/httpd/conf.d/phpMyAdmin.conf**

```
# vi /etc/httpd/conf.d/phpMyAdmin.conf
```

On pourra également limiter l'accès à **phpMyAdmin** uniquement à l'adresse Ip de l'Administrateur Système

```
<Directory /usr/share/phpMyAdmin/>
   <IfModule mod_authz_core.c>
     # Apache 2.4
     <RequireAny>
       Require ip 127.0.0.1
       Require ip ::1
     </RequireAny>
   </IfModule>
   <IfModule !mod_authz_core.c>
     # Apache 2.2
     Order Deny,Allow
     Allow from 10.0.2.0/24
     Allow from 127.0.0.1
     Allow from ::1
   </IfModule>
</Directory>
```

```
<Directory /usr/share/phpMyAdmin/setup/>
   <IfModule mod_authz_core.c>
     # Apache 2.4
     <RequireAny>
       Require ip 127.0.0.1
       Require ip ::1
     </RequireAny>
   </IfModule>
   <IfModule !mod_authz_core.c>
     # Apache 2.2
     Order Deny,Allow
     Allow from 10.0.2.0/24
     Allow from 127.0.0.1
     Allow from ::1
   </IfModule>
</Directory>
```

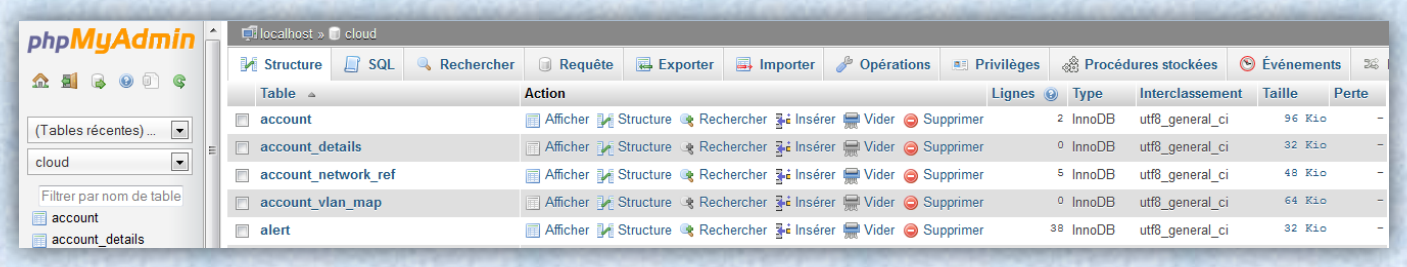
On lance le service httpd

```
# service httpd start
```

On programme son lancement au démarrage

```
#chkconfig httpd on
```

On peut dorénavant accéder aux informations de la base de données de Cloudstack

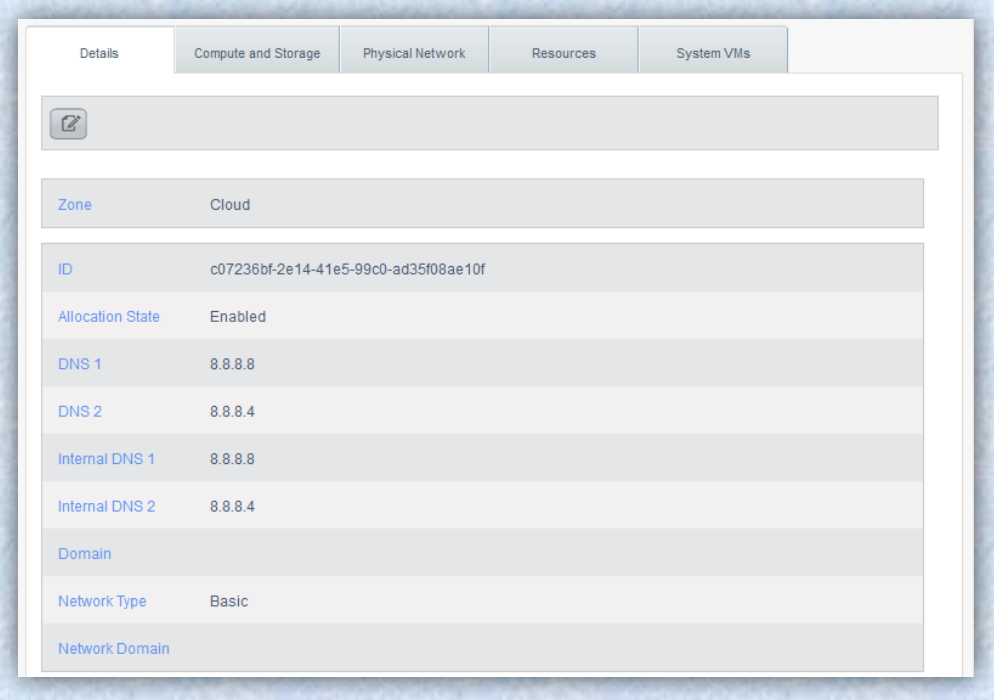


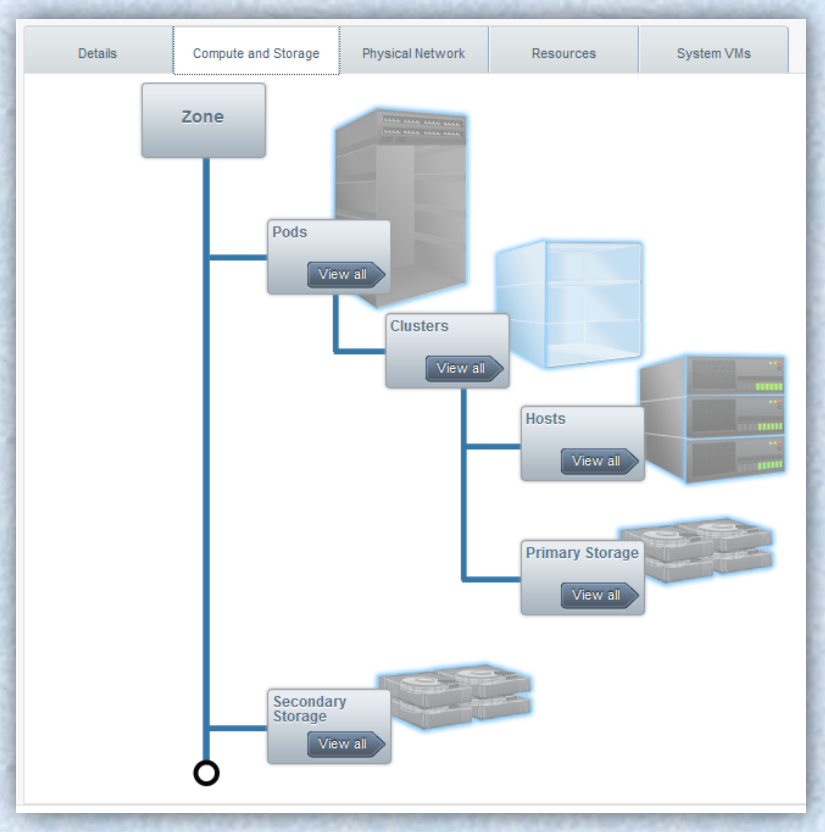
On pourra plus facilement accéder à différents réglages comme :

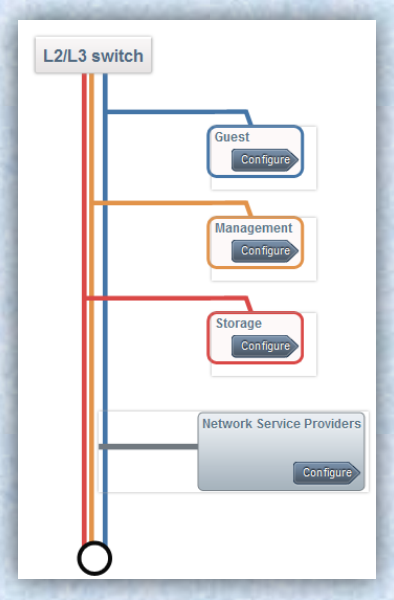
- La suppression des messages d'erreur affichés sur le dashboard
- La configuration des ressources
- La purge des VM , des adresses IP……

Vérification de la bonne configuration du Cloud

Dans le menu Infrastructure, sélectionner la zone créée, nous pouvons vérifier dans les différents onglets les différentes fonctions.







Ici est détaillée la partie réseau avec les configurations des adresses IP , les routeurs virtuels qui géreront les VM installées et les groupes de sécurités (Firewalls)

Name	State
NetScaler	Disabled
Virtual Router	Enabled
Security Groups	Enabled

La page de ressources :

Details | Compute and Storage | Physical Network | Resources | System VMs

System-wide capacity

Memory	Allocated: 1.25 GB / 4.99 GB	25%
CPU	Allocated: 1.00 GHZ / 18.90 GHZ	5%
Storage	Allocated: 3.09 GB / 49.22 GB	6%
Primary Storage Allocated	Allocated: 408.00 KB / 98.43 GB	0%
Public IP Addresses	Allocated: 0 / 0	0%
Management IP Addresses	Allocated: 3 / 10	30%
Secondary Storage	Allocated: 3.09 GB / 49.22 GB	6%
VLAN	Allocated: 0 / 0	0%
Direct IPs	Allocated: 2 / 30	6%
Local Storage	Allocated: 0 / 0	0%

Le dernier onglet correspond aux 2 VM qui gèrent la zone

Name	Type	Zone	Status
s-1-VM	Secondary Storage VM	Cloud	Running
v-2-VM	Console Proxy VM	Cloud	Running

La première, « Secondary Storage » gère le stockage des futures VM , la seconde « Console proxy « permet d'accéder aux VM grâce à une console propriétaire à Cloudstack.

Sélectionner par exemple la 1ere VM

Details

Name	s-1-VM
ID	f01d1b62-d11a-4f42-b373-ef16e8634447
State	Running
Type	Secondary Storage VM
Zone	Cloud
Public IP Address	10.0.2.70
Private IP Address	10.0.2.57
Link Local IP Adddress	169.254.2.141
Host	cloudstack.cloud.fr
Gateway	10.0.2.254
Created	21 Jun 2013 04:43:35

Puis cliquer sur l'icône d'accès en mode console

```
Ctrl-Alt-Del   Ctrl-Esc   Keyboard
Starting ACPI services....
Starting the system activity data collector: sadc.
Starting OpenBSD Secure Shell server: sshd.
cloud.com sevice is already running, PID = 2524
Starting OpenBSD Secure Shell server: sshd.
Starting NFS common utilities: statd.
Starting portmap daemon...Already running..
Password server is not running

Debian GNU/Linux 6.0 s-1-VM tty1

s-1-VM login:
Debian GNU/Linux 6.0 s-1-VM tty1

s-1-VM login: root
Password:
Linux s-1-VM 2.6.32-5-686-bigmem #1 SMP Mon Jan 16 16:42:05 UTC 2012 i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@s-1-VM:~# _
```

L'accès à la console des VM système se fait en « root » avec le mot de passe suivant : « 6mIIIIOn »

On peut également accéder aux VM système en mode « ssh » avec SSHSecureShell à l'aide de la commande suivante.
L'adresse Ip de la VM à accéder sera celle détaillée dans « Link Local Ip Address »

```
# ssh -i /root/.ssh/id_rsa.cloud -p 3922 root@169.254.2.141
```

L'authentification se fait par échange de clé.

Nous pouvons maintenant vérifier la bonne configuration de la VM Secondary Storage avec la commande suivante

```
# /usr/local/cloud/systemvm/ssvm-check.sh
```

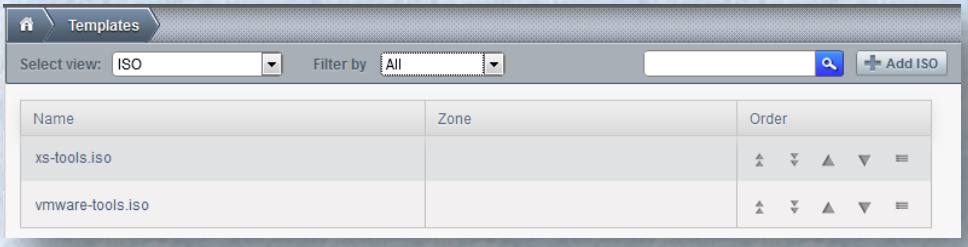
Ce programme verifie :

- la connectivité au Management Server
- La connectivité au serveur NFS
- La résolution de noms
- La connectivité au serveur DNS

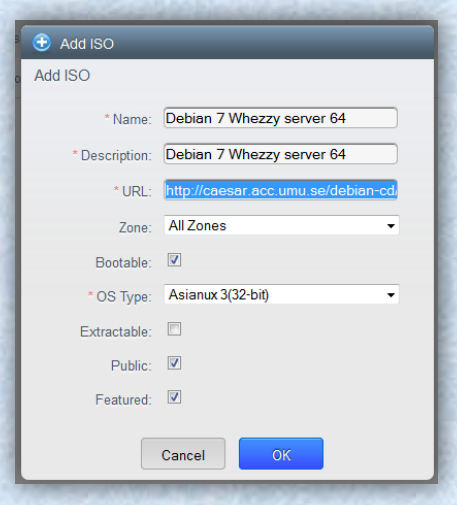
```
root@s-1-VM:~#  /usr/local/cloud/systemvm/ssvm-check.sh
================================================
First DNS server is  8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=44 time=53.066 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=44 time=51.637 ms
--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max/stddev = 51.637/52.352/53.066/0.715 ms
Good: Can ping DNS server
================================================
Good: DNS resolves download.cloud.com
================================================
NFS is currently mounted
Mount point is /mnt/SecStorage/b989f800-bf43-3790-a070-265a24c23d0c
Good: Can write to mount point
================================================
Management server is 10.0.2.50. Checking connectivity.
Good: Can connect to management server port 8250
================================================
Good: Java process is running
================================================
Tests Complete. Look for ERROR or WARNING above.
root@s-1-VM:~#
```

Intégration d'une VM dans la zone

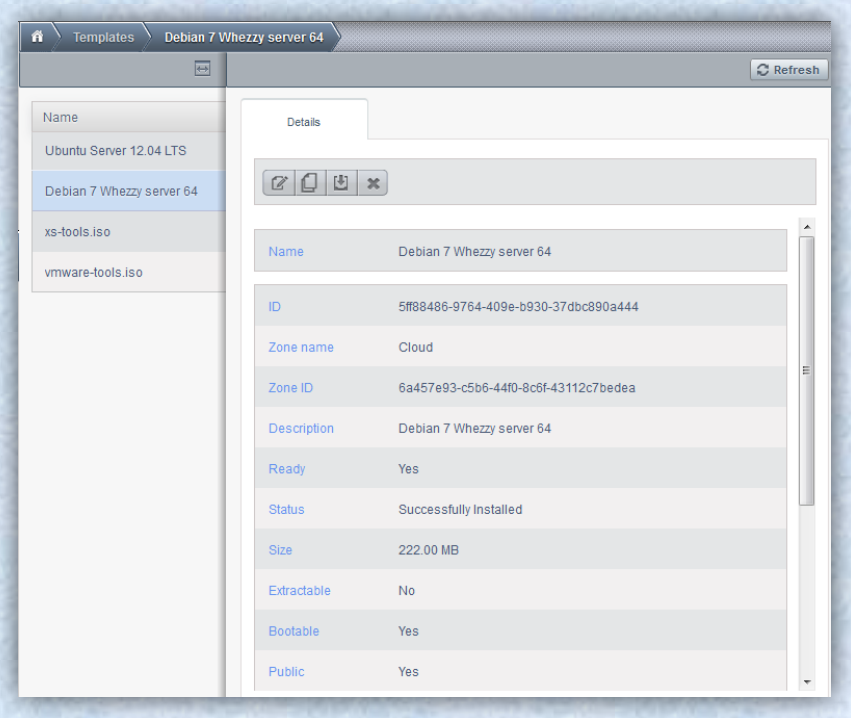
Nous allons maintenant créer une VM à l'intérieur de notre Cloud.
Pour cela nous devons intégrer un ISO d'installation au Cloud, dans le menu TEMPLATE, sélectionner ADD ISO



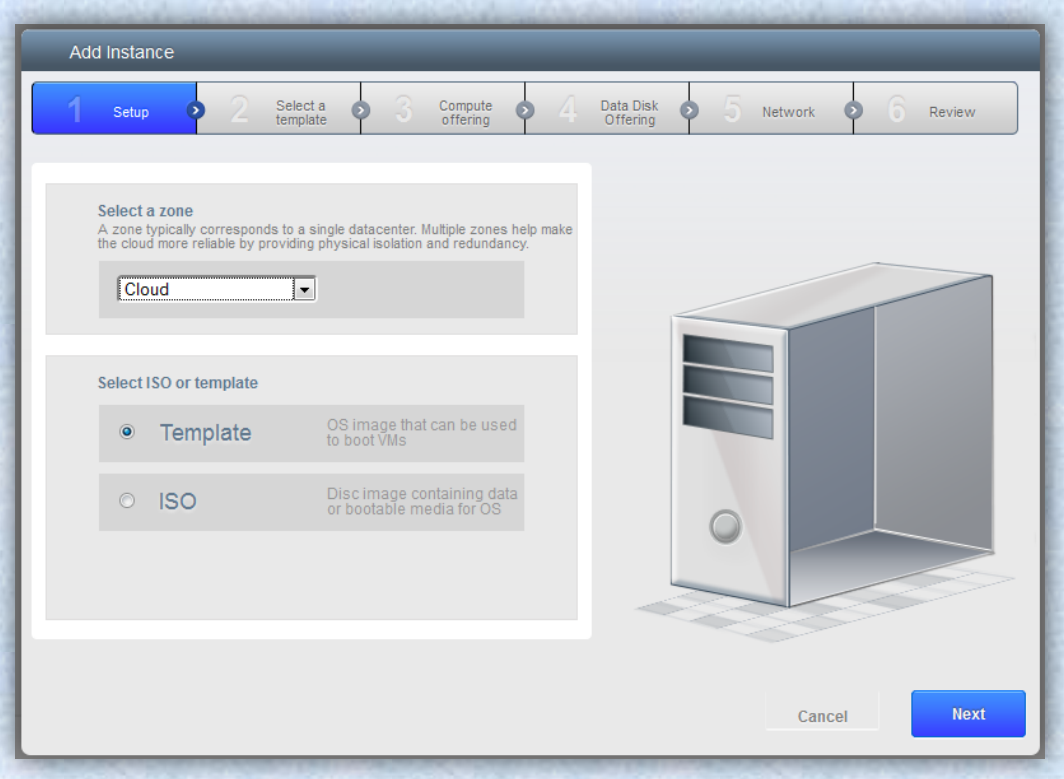
L'intégration des ISOs se fait uniquement à partir de téléchargement http



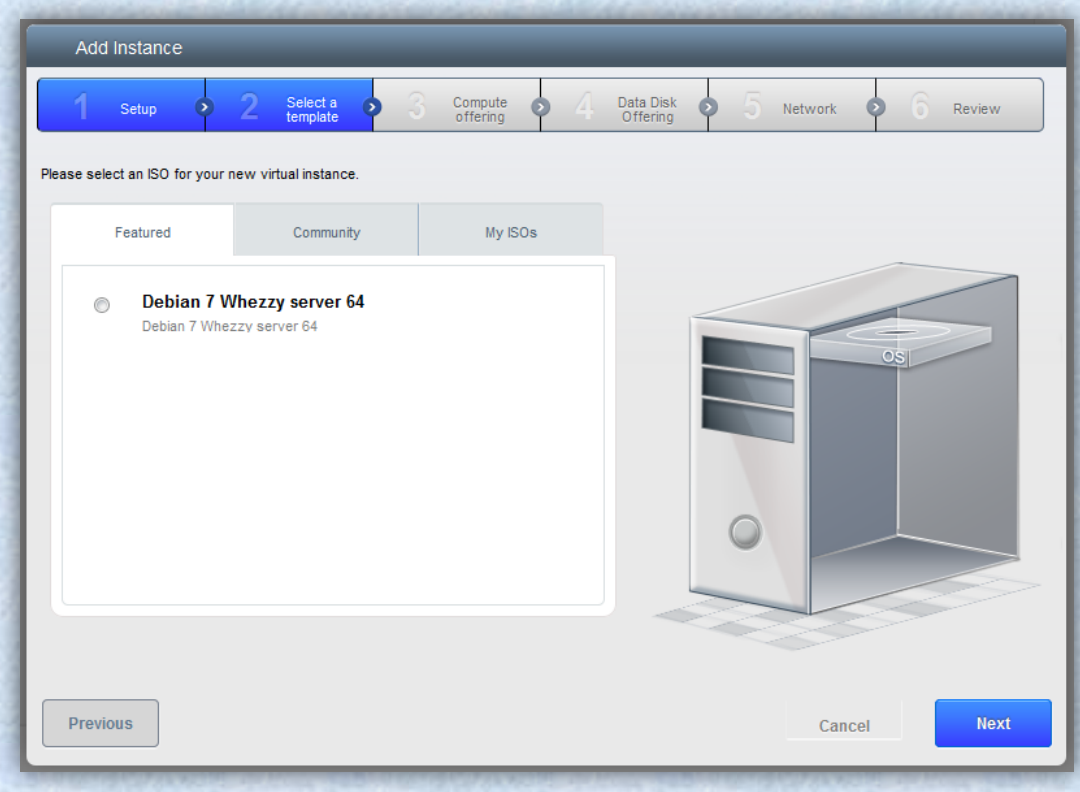
Une fois l'ISO téléchargé, l'onglet du template devra indiquer « Successfully Installed »



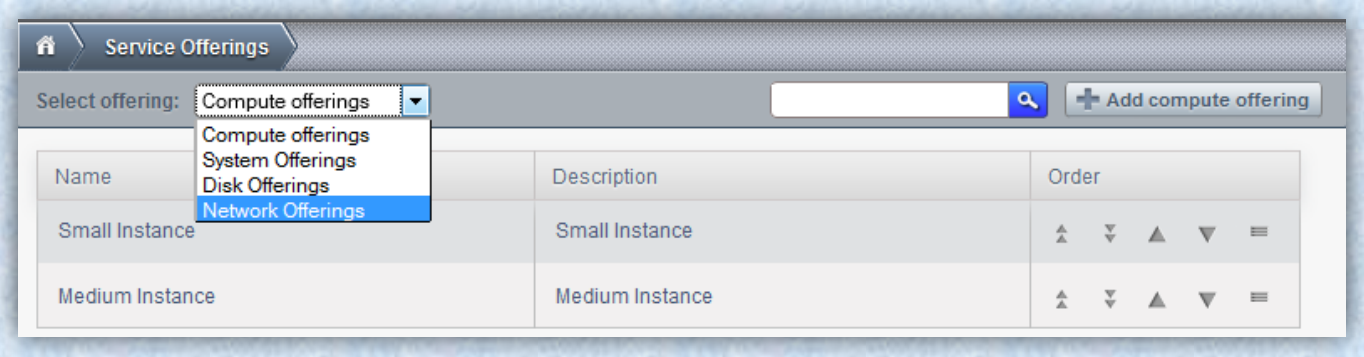
Nous allons maintenant créer une Instance à partir de ce Template.
Dans le menu Instance, sélectionner l'option « Add Instance » , un menu de configuration apparait.
Sectionner la zone dans laquelle créer l'instance puis sélectionner l'option ISO.



Sélectionner ensuite l'ISO à utiliser



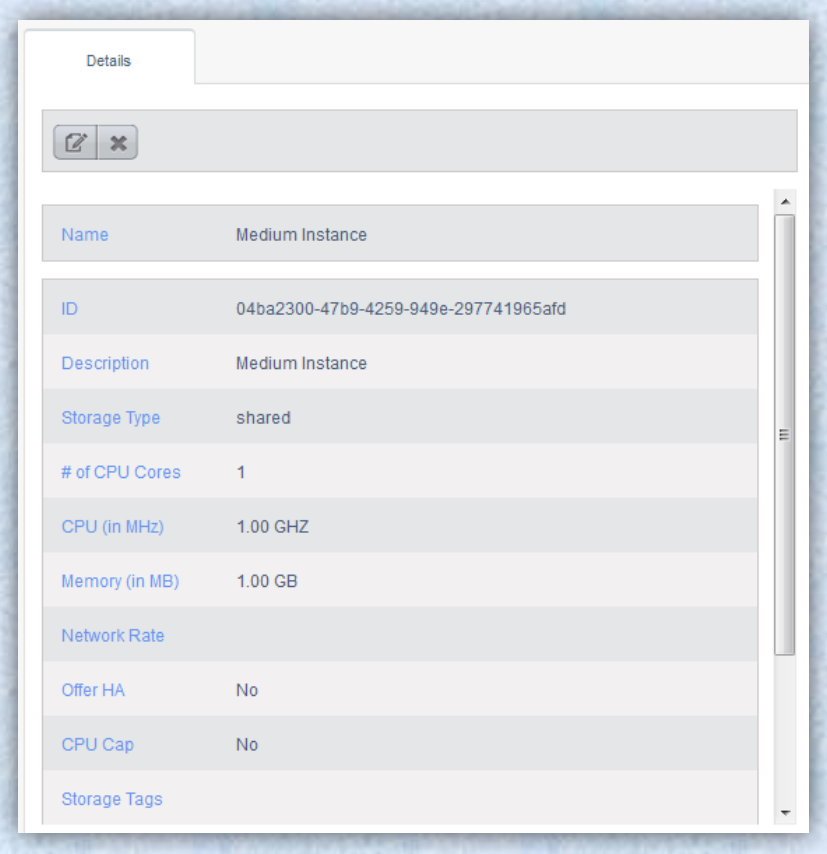
Sélectionner ensuite le type d'instance à créer. Les modèles d'instances sont configurés dans le menu principal → Service Offering



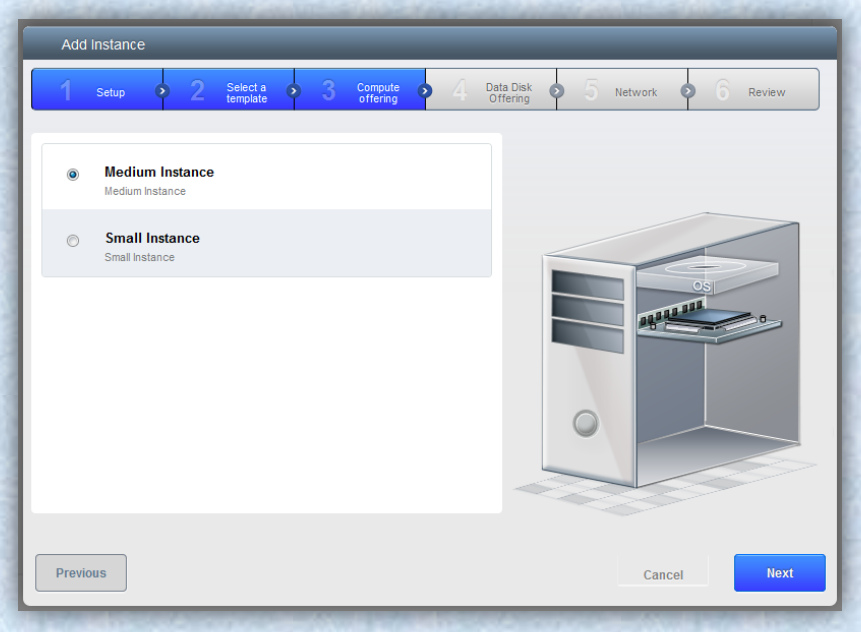
Dans cette section sont préconfigurées les offres :

- Compute offering : nombre de processeurs, fréquence allouée, mémoire allouée, vitesse du réseau…
- System offering : permet de préconfigurer les instances pour les éléments du système (Routeurs, disques de stockage….)
- Disk offering : permet de déterminer l'espace disque alloué
- Network offering : permet de préprogrammer le type de réseau dans lequel la VM sera installée

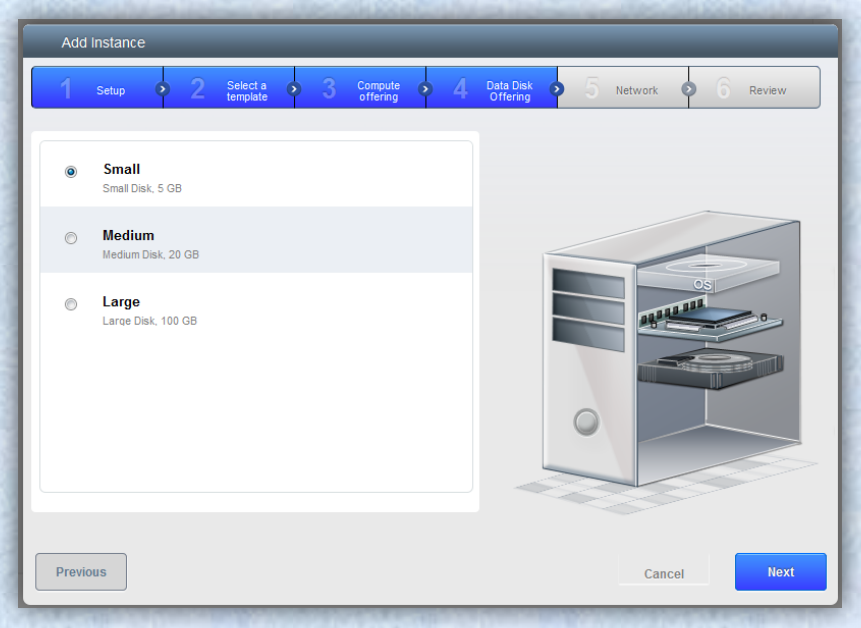
Dans notre cas Medium Instance correspond aux données suivantes



Sélectionner Medium Instance

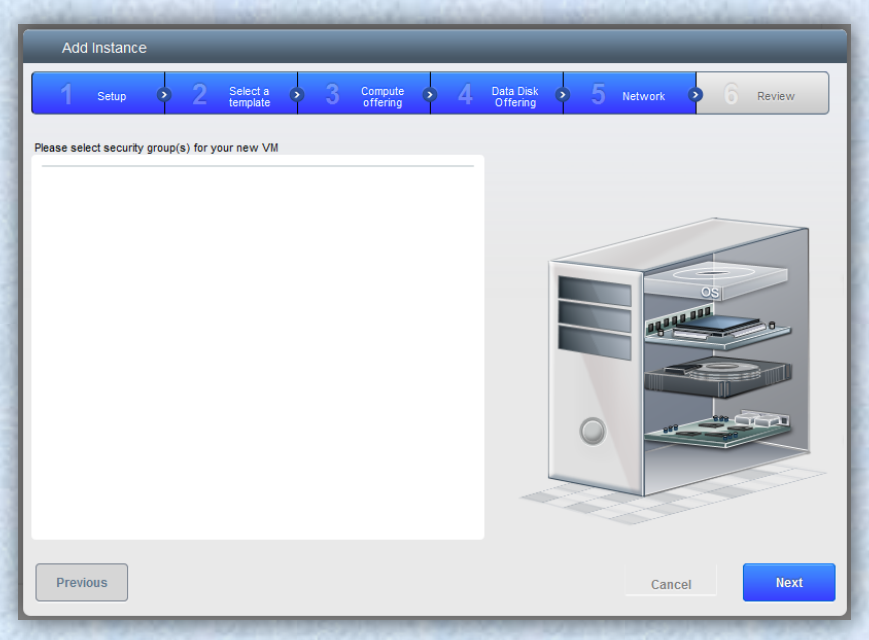


Sélectionner ensuite l'espace disque alloué à cette instance, 5GB suffiront

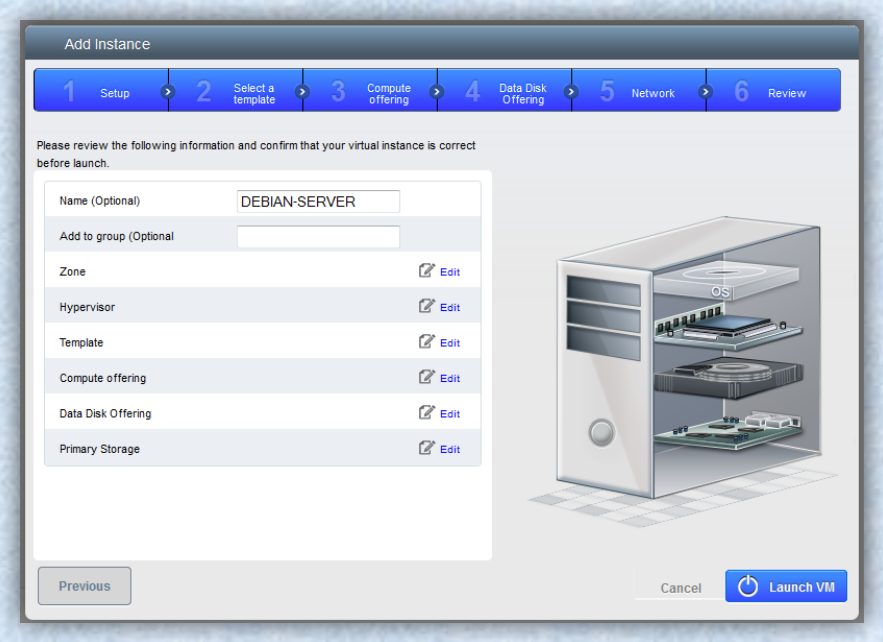


Name	Description	Custom Disk Size	Disk Size (in GB)	Order
Small	Small Disk, 5 GB	No	5	
Medium	Medium Disk, 20 GB	No	20	
Large	Large Disk, 100 GB	No	100	

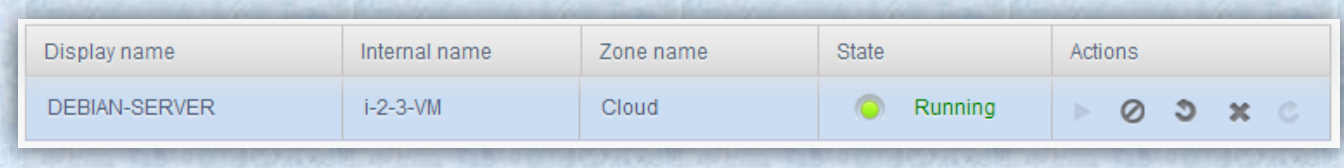
Il faut ensuite sélectionner le groupe de sécurité (Configuration Firewall) auquel sera reliée la VM, sans configuration le groupe de sécurité par défaut sera appliqué à l'instance.



Dans le dernier onglet, il faut juste donner un nom à l'instance qui sera créée.

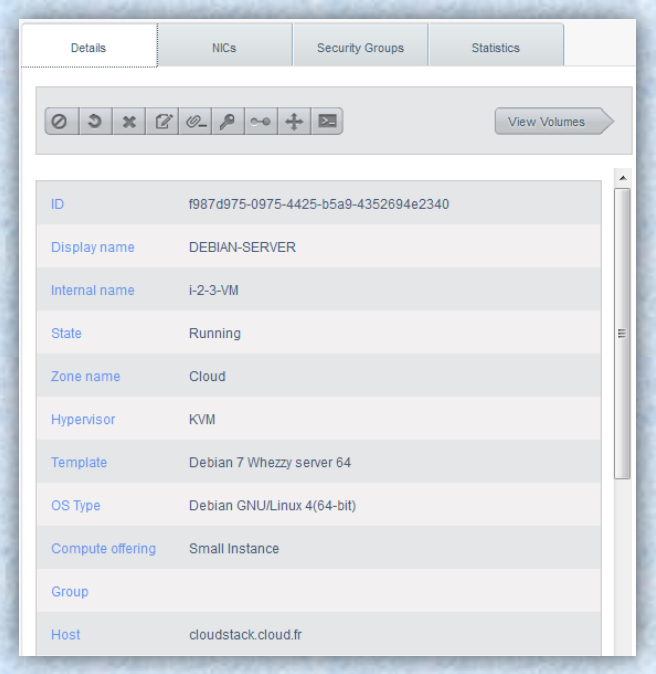


Cliquer ensuite sur LAUCH VM, la création de la VM prendra quelques minutes et si tout se passe bien la nouvelle instance devra se trouver présente dans la liste avec l'état « Running »



Display name	Internal name	Zone name	State	Actions
DEBIAN-SERVER	i-2-3-VM	Cloud	Running	

Nous allons maintenant devoir prendre la main sur cette nouvelle VM pour effectuer l'installation du système d'exploitation.
En cliquant sur le nom de l'instance nous accédons aux données de configuration de celle-ci.



Cette Icone permet de détacher l'ISO de la VM après installation

Permet de modifier le mot de passe d'accès à la VM

Permet de changer le type de service alloué

L'icône console permet de prendre en main la VM

Problèmes rencontrés lors de l'installation

Comme vous avez pu le remarquer, la mise en place de Cloudstack est assez longue et fastidieuse.
Quelques problèmes ont naturellement été présents lors de cette installation.

L'installation correcte de la version de Cloudstack 3.02 ne fonctionne correctement qu'à partir de la version 6.3 mini de Centos.
Impossible de l'installer à partir de la version 6.4 mini ou DVD.
Mais tout fonctionne correctement en démarrant de la version 6.3 mini et en effectuant ensuite l'update vers la version 6.4.
Le problème provient de paquets utilisés dans la version 6.3 mais n'étant plus présents dans la version 6.4.
L'installation est possible sous Ubuntu mais uniquement la version 10.04.

La configuration du nom de domaine est obligatoire dans les fichiers **/etc/sysconfig/network** et **/etc/hosts** sous peine de ne pouvoir créer l'hôte correspondant à ce domaine dans la zone.

Le premier Bug rencontré concerne la mise à jour d'Apache Tomcat6 (conteneur web libre de servlets et JSP Java EE qui permet d'accéder à l'interface de Cloudstack).
La mise à jour actuelle au 02 juin 2013 présente un Bug de configuration des droits d'accès au fichier de Log **/var/log/cloud/management/catalina.out**. Les droits en écriture n'étant plus présents dans les propriétés du fichier, le Management Server , ne voulait pas démarrer puisque celui-ci écrit ses logs dans ce fichier ainsi que dans **/var/log/cloud/management/management-server.log.**

Le second bug concerne la configuration du service **cgconfig.**
Après finalisation de l'installation le fonctionnement des VMs se fait correctement, or après redémarrage impossible de redémarrer les VMs système.
Dans les fichiers de Log de **Libvirtd** , **/var/log/libvirt/libvirtd.log** , on constate que le service **cgconfig** se lance correctement mais que le service **cgred** bloque. Ce qui empêche le démarrage de **Libvirtd** et bloque le démarrage du **Cloud-agent de KVM.**

Les données suivantes concernant la gestion du Cpu étant manquantes dans le fichier **/etc/cgconfig.conf**

```
group virt {
   cpu {
      cpu.shares = 9216;
      }
}
```

http://support.citrix.com/article/CTX135208

Et en dernier, lors de la création de La VM principale avec VMWARE Workstation, l'oubli de configuration du processeur avec les modes Intel VT et AMD-V activés.
Problème de configuration qui empêche la création de l'hôte au moment de la génération de la zone principale dans le mode d'installation basique.

Conclusion Cloudstack

Le projet de Iaas Open Source CloudStack est devenu un projet de premier niveau au sein de la Fondation Apache, donnant ainsi un signal au marché : le projet dispose d'une vraie communauté indépendante, hors du giron de Citrix, et gérée par les principes de gouvernance d'une institution Open Source. La communauté n'a pas d'yeux que pour OpenStack.
OpenStack n'a officiellement pas rallié toute la communauté de l'Open Cloud à sa cause. Il faut aussi compter avec Cloudstack. Le projet d'infrastructure Iaas Open Source, transmis par Citrix à la l'institution Open Source en avril 2012 vient d'être promu au rang de projet de premier niveau (Top-Level Project – TLP) Apache. Un rang qui illustre le fait que le projet Cloudstack a acquis ses lettres de noblesse au sein de la communauté Open Source Apache. Il s'est surtout construit, lui-même, une communauté indépendante et ouverte, dont les soumissions de code ne sont plus le simple fait de Citrix.

Citrix a fait un choix stratégique quant à sa pile Iaas en avril 2012. A cette époque, le spécialiste de la virtualisation a décidé de basculer tous ses développements sur CloudStack, qu'il avait hérité avec le rachat de cloud.com. Abandonnant ainsi OpenStack, une pile concurrente au projet. Le groupe reprochait notamment à OpenStack de bâtir une n-ième alternative aux API cloud d'Amazon et d'être moins « mature » que CloudStack. En confiant le projet à la fondation Apache en 2012, Citrix, qui entend également bâtir une distribution commerciale de CloudStack à partir de code Apache, avait donné un signal clair : proposer une alternative à OpenStack, devenu aujourd'hui le standard de fait de l'infrastructure de cloud privé ouverte ,ainsi qu'à VMWare .
Une communauté très diversifiée

En sortant CloudStack de son incubateur et en le positionnant au rang de projet de premier niveau, la fondation Apache illustre également que le projet Open Source a lui aussi pu trouver une communauté large et diversifiée, conforme aux principes de gouvernance de la fondation. Une forme de sceau Apache, certifiant ainsi l'ouverture et l'indépendance du projet.

Le nombre de contributeurs à CloudStack a progressé de 185% sur les douze derniers mois, avec 134 contributeurs à ce jour, issu de différentes sociétés, hors Citrix. Quelque 5 500 commits ont été réalisés sur la même période. Au total, quelque 16 795 commits ont été réalisés par 164 contributeurs, ce qui représente 1 161 748 lignes de code.

CloudStack a également pu profiter de sa base d'utilisateurs bien en place pour consolider sa communauté. CloudStack avait l'avantage de disposer de nombreux déploiements à grande échelle, sur le long terme, démontrant ainsi la stabilité et la scalabilité du projet. Citons en effet Zynga, BT, Korea Telecom et SunGard.

En France, l'hébergeur Ikoula a également fait le choix de CloudStack pour bâtir son offre de cloud privé. Son patron, Jules-Henri Gavetti, a indiqué avoir été rassuré par le fait que CloudStack soit un projet hébergé par la fondation Apache.

Conclusion Générale :

Face au phénomène médiatique que représente le Cloud Computing actuellement, nous avons ici effectué une définition de cette technologie à partir de la littérature d'experts en système d'information et en Cloud. Cette technologie en plein essor permet aux entreprises de disposer d'infrastructures et de progiciels directement en ligne sur Internet. On a distingué les différents types de Cloud possibles avec **l'IAAS** pour les infrastructures techniques, le **PAAS** pour les infrastructures habillées avec des outils de middleware comme les bases de données par exemple et le **SAAS** pour les services logiciels. Ces trois types peuvent se déployer sous quatre formes de topologies différentes : le **Cloud public** pour du déporté en ligne, le **Cloud privé** pour l'utilisation des concepts du Cloud en interne à l'organisation, le **Cloud hybride** pour l'utilisation commune du public et du privé et enfin le **Cloud communautaire** pour des entreprises géographiquement proches ou à intérêts communs.

Les possibilités de ce concept complètement novateur dans ses approches technologiques et fonctionnelles sont importantes pour les entreprises et on comprend l'intérêt des DSI face au concept. On pense tout d'abord à la réduction des coûts que doit permettre le Cloud, les services sont effectivement facturés en fonction de leurs utilisations et les ressources utilisées évoluent en fonction des besoins parfois automatiquement. Cela peut éviter d'investir lourdement dans des infrastructures, il n'y a plus de serveurs sous utilisés. Le Cloud peut se révéler pratique pour lancer un nouveau service sans l'investissement habituel, de même pour les utilisateurs métiers des organisations, un terminal et un accès réseau suffisent pour profiter de l'accès aux progiciels du nuage. Autre avantage, si les data center des fournisseurs du Cloud public sont des consommateurs importants en énergie, cette mutualisation des ressources du Cloud permet en fait d'adopter un comportement écologique.

Si la flexibilité et l'économie de ressources affichées constituent des points positifs, le Cloud Computing génère quelques craintes au sein des DSI et des instances dirigeantes car le concept dans le monde professionnel, notamment en mode public, des questions se posent concernant les aspects juridiques et sécuritaires. La confidentialité des données est un frein, déporter ses données stratégiques vers le nuage semble risqué. La disponibilité n'est non plus garantie complètement car le Cloud n'est pas à l'abri de tout péril. C'est pour cela que les entreprises adopteront plutôt un mode de Cloud hybride en déportant les données non stratégiques et l'utilisation de services pour l'informatique de commodité sur le Cloud public, le Cloud privé étant davantage réservé pour les applicatifs spécifiques et cœur de métier où l'on conservera également les données clés.

Autre point critique, côté humain, les impacts ne sont pas neutres. Nous constatons que le Cloud par ses aspects doit modifier automatiquement l'organisation en place dans les équipes informatiques. Cela se limite toutefois au Cloud public. Le Cloud privé, restant interne à l'entreprise, s'il profite des progrès apportés par le Cloud, ne perturbe que très peu le fonctionnement des équipes en place.

Si on revient au Cloud public, l'impact ne modifie pas le rôle majeur des DSI dans le pilotage et la gestion du système d'information. Bien au contraire, avec cette technologie et cette externalisation des données et des services, les compétences managériales et les visions transversales des équipes sont primordiales, de nouveaux besoins de compétences voient même le jour pour faire face aux particularités des projets de type Cloud et les métiers proches des utilisateurs et du cœur de métier de leur entreprise se renforcent naturellement. Il apparaît toutefois que si certaines compétences demeurent vitales et confirment leurs positionnements et que d'autres se créent ; c'est l'inverse pour certains métiers qui voient leurs compétences disponibles en ligne', plus particulièrement pour les équipes systèmes et réseaux et les développeurs.

Les différentes interviews des professionnels font ressortir ces points de vigilance auxquels doivent prêter attention les directeurs des systèmes d'information. Le Cloud public redessine un nouveau département en système d'information, les collaborateurs dont les compétences spécifiques sont moins pertinentes doivent être accompagnés par les DSI qui doivent mener une vraie conduite de changement, en formant éventuellement sur les nouvelles compétences à acquérir. Cette nouvelle donne du Cloud permet une ouverture facilitée au cœur de métier de l'entreprise, des reconversions sont donc possibles, la présence des ressources au sein des organisations leur a permis d'appréhender le métier central de leur entreprise et si leur métier évolue c'est pour un rapprochement des utilisateurs.

La technologie du Cloud modifie l'organisation des équipes informatique car elle fait évoluer les métiers de ses membres. Toutefois, l'histoire du Cloud s'écrit encore et les effets pressentis sur les métiers ne sont pas à mon sens déjà effectifs pour les collaborateurs déjà en poste. Par contre, les recrutements des DSI seront forcément en phase avec leurs nouveaux besoins, certains métiers risquent dès maintenant de voir leurs perspectives d'emplois chuter pour les organisations pour qui l'informatique n'est pas le métier premier.

Les solutions de cloud computing d'entreprise continuent leur développement en proposant toujours plus de services, de SDKs et d'APIs. Même s'il existe des différences dans la facturation de ces solutions, nous retrouvons toujours dans les ressources facturables, la bande-passante sortante, le temps processeur réservé et la volumétrie des données occupée par le système hébergé. Le choix d'une solution par rapport à une autre devra se faire en fonction des caractéristiques de l'application à migrer vers le cloud computing.

Dans le cadre de la formation TSGERI , la mise en place d'un Cloud Privé m'a permis d'avoir une vision globale de l'infrastructure future du SI d'une entreprise employant les dernières technologies disponibles sur le marché en matière de Cloud.
Grâce au cloud computing,, nous **allouons les machines et leurs ressources** uniquement lorsque cela est nécessaire, permettant ainsi une meilleure gestion de l'infrastructure matérielle.

Le Cloud computing permet de concrétiser la collaboration de tous, en tout lieu, pour améliorer les processus et, au final, accélérer l'innovation au sein d'une entreprise.

LEXIQUE :

Abstarction : En informatique, le concept d'abstraction identifie et regroupe des caractéristiques et traitements communs applicables à des entités ou concepts variés ; une représentation abstraite commune de tels objets permet d'en simplifier la manipulation.

Api : En informatique une interface de programmation (abr. API pour Application Programming Interface) est un ensemble normalisé de classes, des méthodes ou des fonctions qui sert de façade par laquelle un logiciel offre des services à d'autres logiciels. Elle est offerte par une bibliothèque logicielle ou un service web, le plus souvent accompagnée d'une description qui spécifie comment des programmes consommateurs peuvent se servir des fonctionnalités du programme fournisseur.

BtoB : L'expression « business to business » (« B2B », ou « commerce B to B ») désigne:

- l'ensemble des activités d'une entreprise visant une clientèle d'entreprises (voir pour plus de détail l'article Marketing industriel) ;
- l'ensemble d'architectures techniques et logicielles informatiques permettant de mettre en relation des entreprises (voir Business to business (internet))

CRM : Customer Relationship Management, en anglais, soit en français « gestion de la relation client »

Commit : Un commit (terme anglais, de "commettre" [un changement, une transaction]) est une validation de transaction qui fait référence à la commande synonyme Commit présente dans la plupart des systèmes de gestion de base de données et des logiciels de gestion de versions.

DSI : Directeur des systèmes d'information ou Direction des systèmes d'information selon qu'il désigne une personne ou une entité d'une organisation.

Isolation au Layer-3 : Comprend les Firewell/Router/VPN/Load Balancer

Patriot Act : Le USA PATRIOT Act (acronyme traduisible en français par : « Loi pour unir et renforcer l'Amérique en fournissant les outils appropriés pour déceler et contrer le terrorisme »1) est une loi antiterroriste qui a été votée par le Congrès des États-Unis et signée par George W. Bush le 26 octobre 2001.
L'un des axes centraux de ce long texte (132 pages2) est d'effacer la distinction juridique entre les enquêtes effectuées par les services de renseignement extérieur et les agences fédérales responsables des enquêtes criminelles (FBI) dès lors qu'elles impliquent des terroristes étrangers. Elle crée aussi les statuts de combattant ennemi et combattant illégal, qui permettent au gouvernement des États-Unis de détenir sans limite et sans inculpation toute personne soupçonnée de projet terroriste.

Simple Layer-2 à plat : La topologie à plat (non hiérarchique) est adéquate pour un réseau de petite taille
Avec la topologie à plat il n'y a pas de hiérarchie dans le réseau
- Tous les dispositifs du réseau sont équivalents
- Facile à implémenter et à maintenir si la taille du réseau reste petite
Quand la taille du réseau augmente, la topologie à plat est indésirable
Comprend les VLANs/Security Groups

SDK : Les kits de développement logiciels sont souvent désignés par le sigle anglais SDK (Software Development Kit). Un kit de développement ou trousse de développement logiciel est un ensemble d'outils permettant aux développeurs de créer des applications de type défini (par exemple pour iOS, Android, Symbian, Bada, Windows Phone 7, Windows Phone 8 ou Windows 8)

Security Groups : Les groupes de sécurité fournissent un moyen d'isoler le trafic des machines virtuelles. Un groupe de sécurité est un groupe de machines virtuelles qui filtrent le trafic entrant et sortant en fonction d'un ensemble de règles, appelées infiltration et de règles de sortie. Ces règles trafic sur le réseau de filtrage selon l'adresse IP qui tente de communiquer avec la machine virtuelle. Les groupes de sécurité sont particulièrement utiles dans les zones qui utilisent des réseaux de base, car il existe un réseau d'hôtes unique pour toutes les machines virtuelles invitées. Dans CloudStack 3. les groupes de sécurité sont pris en charge que dans les zones qui utilisent des réseaux de base.

Serveur Lame : Un Serveur Lame (appelé encore Serveur Blade ou carte serveur) est un serveur conçu pour un très faible encombrement. Alors qu'un serveur en rack n'est qu'un serveur traditionnel de taille un peu réduite, le serveur lame est beaucoup plus compact, car plusieurs composants sont enlevés, étant mutualisés dans un châssis capable d'accueillir plusieurs serveurs lames.

Safe harbor : Les principes de la Sphère de sécurité (Safe Harbor) permettent à une entreprise américaine de certifier qu'elle respecte la législation de l'Espace économique européen (EEE) afin d'obtenir l'autorisation de transférer des données personnelles de l'EEE vers les Etats-Unis.

Le Cloud Computing :
Reference ,Livres et Liens Utiles

- Livre blanc « Cloud Computing et confidentialité » Microsoft, Novembre 2009
- Livre blanc « La protection de la vie privée à l'ère du Cloud Computing - Le point de vue de Microsoft », Microsoft, Novembre 2009
- Livre blanc « Windows Azure™ Security Overview » par Charlie Kaufman et Ramanathan Venkatapathy
- Livre blanc « Le Cloud en toute confiance » Septembre 2010
- Regards sur le numérique, hors-série, « Le Cloud Computing, qu'est que ça va changer »
- Syntec Informatique, « Le livre blanc du Cloud Computing »
- Livre blanc de François Tonic « Cloud Computing » Septembre 2009
- Cloud Computing & SaaS de Guillaume Plouin, éditions Dunod, mars 2009.

http://computinginthecloud.wordpress.com/2008/09/25/utility-cloud-computingflashback-to-1961-prof-john-mccarthy/

http://www.zdnet.fr/blogs/cloud-news/amazon-voit-le-cloud-prive-comme-une-arnaque-39755491.htm

http://www.zdnet.fr/actualites/le-cloud-computing-place-en-tete-des-investissements-a-realiser-en-2010-selon-gartner-39709836.htm

http://www.lemonde.fr/technologies/article/2009/08/24/le-cloud-computing-bouscule-l-informatique_1231357_651865.html

http://www.microsoft.com/windowsazure/whitepapers/default.aspx

http://www.sfrdeveloppement.fr/index.php?post/2009/11/02/Place-du-Cloud-Computing-en-France

http://www.microsoft.com/france/securite/guides-conseils/cloud.aspx

http://www.guardian.co.uk/technology/2008/sep/29/cloud.computing.richard.stallman

http://www.reseaux-telecoms.net/actualites/lire-coup-de-projecteur-sur-le-cloud-computing-par-le-gartner-19798.html

http://www.journaldunet.com/solutions/systemes-reseaux/marche-francais-du-cloud-computing-2009-2011.shtml

http://www.mascre-hequy.com/htm/fr/conseils/conseil_cloud_computing_aspects_juridiques.html

http://www.antoinebenkemoun.fr/2010/03/dangers-du-cloud-computing-linteroperabilite/

http://www.silicon.fr/le-cloud-computing-mode-ou-tendance-lourde-40238.html

http://www.silicon.fr/cloud-computing-un-marche-a-149-milliards-de-dollars-en-2014-40946.html

http://fr.wikipedia.org/wiki/Hyperviseur

http://www.lemagit.fr/technologie/datacenter-technologie/virtualisation-serveurs/hyperviseurs-serveurs/2012/01/06/virtualisation-2012-vers-affrontement-relanc-eacute-entre-vmware-microsoft/

http://www.itpro.fr/a/virtualisation-complete/

http://technet.microsoft.com/fr-fr/magazine/hh300651.aspx

http://www.lemagit.fr/rubrique/technologie/datacenter-technologie/virtualisation-serveurs/hyperviseurs-serveurs/page/2/

http://www.cnil.fr/fileadmin/images/la_cnil/actualite/Recommandations_pour_les_entreprises_qui_envisagent_de_souscrire_a_des_services_de_Cloud.pdf

http://www.commentcamarche.net/news/5850141-la-virtualisation-et-le-cloud-bouleversent-le-monde-de-l-hebergement

http://www.ethantang.fr/2009/10/1378-le-cloud-computing-sera-la-tendance-technologique-en-2010/

http://www.ethantang.fr/2009/10/1378-le-cloud-computing-sera-la-tendance-technologique-en-2010/

http://www.journaldunet.com/solutions/dsi/standardisation-du-cloud-computing.shtml

http://www.responcia.fr/blog/2010/03/04/retour-sur-les-prix-du-cloud-computing/

http://www.sysprobs.com/disable-enable-virtualization-technology-bios

http://fr.slideshare.net/cloudstack/cloudstack-architecture

Annexes

Sécurisation authentification interdite en root

1) Exécuter ces commandes :

```
useradd -g root -u "0" -o -s "/bin/bash" -d "/home/toto" -m "toto"
passwd toto
```

2) Éditer le fichier **"/etc/ssh/sshd_config"** et ajouter cette ligne en bas de page :

```
AllowUsers toto
```

Et enfin exécuter cette commande et tester l'accès !

```
/etc/init.d/ssh reload
```

Bien entendu il faudra changer **"toto"** par un nom d'utilisateur valide, il aura identiquement les mêmes permissions que root,
On peut également changer le home de toto avec l'argument **-d** de useradd.

Purger la base de données et réinitialiser Cloudstack

Attention tous les Isos et tous les templates seront perdus !!!
Cette réinitialisation remet Cloudstack à son état d'origine

```
service cloud-management stop
service cloud-agent stop
service nfs stop

rm -rf /primary
rm -rf /secondary

mkdir -p /primary
mkdir -p /secondary


mysql -ppassword -e 'drop database cloud'
mysql -ppassword -e 'drop database cloud_usage'
```

```
cloud-setup-databases cloud:password@localhost --deploy-as=root:password


rm -rf /var/log/cloud/management/*
cloud-setup-management

Redonner les droits en écriture au fichier

/var/log/cloud/management/catalina.out

Retélécharger le template de KVM

# /usr/lib64/cloud/agent/scripts/storage/secondary/cloud-install-sys-tmplt -m /secondary -u http://download.cloud.com/templates/acton/acton-systemvm-02062012.qcow2.bz2 -h kvm -F


service cloud-management restart

cloud-setup-agent
```

Mesure de la disponibilité d'un service

La discontinuité (également appelée interruption) de service dure généralement plusieurs heures et affecte la disponibilité de l'application, disponibilité qui peut se mesurer en pourcentage par an. Par exemple, une application disponible à 99% (un chiffre qui peut paraître élevé) souffre déjà d'environ 4 jours d'indisponibilité par an ! C'est un résultat souvent critique pour la bonne marche de l'entreprise (imaginez l'impact sur une société d'e-business privé de son site marchand pendant 4 jours…).

Il n'y a pas de seuil normé à partir duquel on peut considérer une application comme étant hautement disponible. En électronique militaire par exemple, les logiciels embarqués sont souvent développés et testés pour atteindre les « 5 neuf » : 99,999% de disponibilité, soit moins de 5 minutes d'indisponibilité par an ! A contrario, dans les systèmes d'information (moins critiques que le logiciel embarqué ou temps réel), les chiffres sont plus modestes, avec 2 chiffres maximum après la virgule.

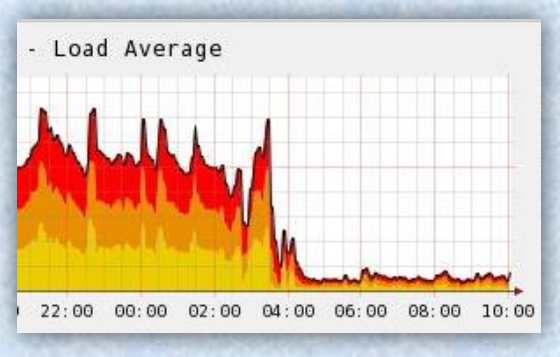
On estime la disponibilité attendue du service (ESA) suivant la formule suivante :

ESA = MTBF / (MTBF + MTTR)

Le MTBF (mean time between failure) est la mesure du temps estimé (ou moyen) entre deux défaillances d'un système donné. Ceci reflète la fréquence de défaillance du système considéré.

Le MTTR (mean time to repair) est la mesure du temps estimé (ou moyen) pour réparer le système suite à une défaillance.

Le temps attendu de récupération du service est alors :



	Indisponibilité/*downtime*			
Disponibilité	secondes/an	minutes/an	heures/an	jours/an
90 %	3 155 760	52596	877	37
98 %	631 152	10519	175	7
99 %	315 576	5 260	88	4
99,8 %	63115	1 052	18	
99,9 %	31558	526	9	
99,99 %	3 156	53		
99,999 %	316	5		
99,9999 %	32			
99,99999 %	3			

ESRT = (deadtime/2) + EFT + ESST

Le deadtime, comme mentionné précédemment, est le délai spécifié avant de considérer qu'une application ne répond plus. S'il est réglé trop court, des faux positifs seront détectés (l'application sera déclarée défaillante alors qu'elle ne l'est pas). S'il est réglé trop long, un temps trop important sera nécessaire avant de détecter la défaillance d'une application.

L'EFT (expected fencing time) est le temps estimé pour détruire (proprement ou non) l'application crashée.

L'ESST (expected service start time) est le temps estimé pour redémarrer l'application.