Conception et réalisation d'une plateforme de cloud privé au profit de la formation des administrateurs systèmes de l'École des Transmissions (ETRS)

Antoine Le Morvan

le cnam

CONSERVATOIRE NATIONAL DES ARTS ET METIERS

CENTRE REGIONAL ASSOCIE DE BRETAGNE

MEMOIRE

présenté en vue d'obtenir

le DIPLOME D'INGENIEUR CNAM

SPECIALITE : Informatique

OPTION : Réseaux, systèmes et multimédia

par

Antoine LE MORVAN

Conception et réalisation d'une plateforme de cloud privé au profit de la formation des administrateurs systèmes de l'École des Transmissions (ETRS)

Soutenu le 6 janvier 2017

JURY

PRESIDENT :	**Pr. Yann POLLET**	**Professeur des Universités - CNAM**
MEMBRES :	**Pr. Charles PREAUX**	**Professeur des Universités - CNAM**
	IDEF Patrick JAOUEN	**Responsable informatique -ETRS**
	LTN Valentin MIGEON	**Formateur cyberdéfense - ETRS**

Remerciements

Je remercie :

Le Pr. Yann POLLET de m'avoir fait l'honneur de présider ce jury.

Le Pr. Charles PREAUX, directeur de l'EICNAM Bretagne, d'avoir accepté d'être mon tuteur CNAM.

Je tiens à exprimer toute ma gratitude à mes tuteurs en entreprise :

- M. Patrick JAOUEN, Ingénieur Divisionnaire d'Etudes et Fabrications, responsable de l'informatique dédiée à la formation à l'École des Transmissions (ETRS) pour sa confiance, ses conseils avisés, son temps et ses relectures ;
- le Lieutenant Valentin MIGEON, Ingénieur des mines, formateur CyberSécurité à l'ETRS, pour ses relectures et ses conseils techniques ;

ainsi qu'à toutes les personnes qui ont rendu ce projet possible :

- le capitaine Benoît WOLFF, formateur au cours systèmes de l'ETRS, qui m'a proposé l'idée du projet et m'a mis en relation avec M. JAOUEN ;
- M. Fabrice POLLET, Ingénieur d'Etudes et Fabrications, administrateur système du réseau du campus et de l'Espace Numérique de Travail de l'ETRS, pour sa disponibilité et ses avis techniques qui m'ont fait progresser et sans qui la configuration de la plateforme n'aurait pas pu se faire.

J'ai une pensée pour tous les enseignants du CNAM rencontrés durant ces 6 dernières années, qui m'ont permis d'être ici aujourd'hui : M. Pierre SWEID, M. Hassan EL GOHARI, M. Romain HENNION, Mme Elisabeth MARTOUREY, M. Xavier BOTTEX, M. Christophe LE CLAINCHE.

Enfin, je remercie tout particulièrement mon épouse, Laurence, de m'avoir encouragé à reprendre mes études et de m'avoir consacré tant de temps.

Liste des abréviations

AMDEC	Analyse des Modes de Défaillances, de leurs Effets et de leur Criticité.
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information.
API	Application Programming Interface - Interface de programmation.
AFP	Apple Filing Protocol. Protocole de partage de fichiers sous Apple Mac OS.
ASF	Apache Software Foundation.
AWS	Amazon Web Service.
BTAC	Brigade de Transmissions et d'Appui au Commandement.
CAL	Computeur Aided Learning. Enseignement Assisté par Ordinateur.
CAN	Campus Area Network - Réseau du campus.
CAS	Central Authentication Service - Service central d'authentification.
CFIM	Centre de Formation Initiale des Militaires du Rang.
CFT	Commandement des Forces Terrestres.
CIFS	Common Internet File System. Protocole de partage de fichiers sous Microsoft Windows.
COMSIC	COMmandement des Systèmes d'Information et de Communication.
CORTECS	Centre Opérationnel des Réseaux SIC Terre et de Cybersécurité.
DAAS	Data As A Service - Données en libre service.
DAS	Direct Attached Storage - Technologie : attachement direct des disques.
DEP	Direction des Etudes et de la Prospective.
DFS	Distributed File System - Système de fichiers distribué.
DHCP	Dynamic Host Configuration Protocol - Protocole de configuration dynamique des hôtes.
DIRISI	Direction interarmées des réseaux d'infrastructure et des systèmes d'information de la défense.
DNS	Domain Name System. Système de nom de domaine.
DRHAT	Direction des Ressources Humaines de l'Armée de Terre.
EAD	Enseignement à distance.
EAO	Enseignement Assisté par Ordinateur.
ENT	Environnement Numérique de Travail.
ESI	Emploi des Systèmes d'Information.
ESXi	Hyperviseur de niveau 1 édité par la société VMware [1].
ETRS	École des Transmissions de Cesson-Sévigné.
FAFP	Face à Face Pédagogique.
FAI	Fournisseur d'Accès à Internet.
FCoE	Fibre Channel over Ethernet - Protocole d'encapsulation de trames Fibre Channel, provenant d'un réseau de stockage SAN, sur un

1 VMware est une marque déposée de VMware, Inc aux Etats Unis.

	réseau Ethernet.
FEROS	Fiche d'Expression Rationnelle des Objectifs de Sécurité.
FOAD	Formation Ouverte et/ou A Distance.
GFS2	RedHat Global File System.
GPL	GNU General Public License.
GTRS	Groupement de Transmissions.
HA	High Availability – Haute disponibilité.
IAAS	Infrastructure As A Service. Infrastructure à la demande.
IDEF	Ingénieur Divisionnaire d'Études et de Fabrications.
IDP	Identity Provider – Fournisseur d'identité.
IEF	Ingénieur d'Études et de Fabrications.
IOOPS	Input/Output Operations Per Second - opérations d'Entrées/Sorties par seconde. Unité de mesure pour les supports de stockage.
IP	Internet Protocol - Protocole Internet.
iSCSI	Internet Small Computer System Interface. Protocole de stockage en réseau basé sur le protocole IP.
ISO	Image d'un CD-ROM/DVD-ROM d'installation directement utilisable par les outils virtuels.
ISP	Internet Service Provider - Fournisseur d'accès à l'Internet.
IT	Information Technology - Technologies informatiques.
KVM	Le Kernel-based Virtual Machine est un hyperviseur libre de niveau 1 disponible sous Linux.
LACP	Link Aggregation Control Protocol. Protocole 802.3ad.
LDAP	Lightweight Directory Access Protocol. Protocole d'accès à un annuaire.
LUN	Logical Unit Number - Numéro d'Unité Logique. Il s'agit du numéro d'identification d'une unité de stockage SAN ou l'unité de stockage elle-même.
NAS	Network Attached Storage. Stockage réseau.
NAT	Network Address Translation. Un routeur fait correspondre les adresses IP internes non uniques et souvent non routables d'un intranet à un ensemble d'adresses externes uniques et routables.
NEF	Numérisation de l'Espace de Formation.
NFS	Network File System. Protocole de partage de fichiers standard sous Unix/Linux.
NIST	National Institute of Standards and Technology - L'institut national des normes et de la technologie est une agence du département du Commerce des États-Unis.
NODE	Noeud. Elément de l'infrastructure.
OCFS	Oracle Cluster File System.
OS	Operating System - Système d'exploitation.
PAAS	Plateform As A Service - Plateforme à la demande.
PES	Procédures d'Exploitation de la Sécurité.
PFI	PlateForme d'Instruction.
PMC	Project Management Commitee - Comité de management de projet.

POC	Proof Of Concept - Démonstration de faisabilité.
PRSI	PRogrammation des Systèmes d'Information.
PSSI	Politiques de Sécurité des Systèmes d'Information.
RAM	Random Access Memory - Mémoire à accès direct.
RDP	Remote Desktop Protocol. Protocole permettant à un utilisateur de se connecter graphiquement sur un système distant.
RTD	Réseau de Transmission de Données.
SAAS	Software As A Service - Logiciel à la demande.
SAML	Security Assertion Markup Language – Protocole d'échange d'informations liées à la sécurité basé sur le langage XML.
SAN	Storage Area Network - Réseau spécialisé dans la mutualisation des ressources de stockage.
SCSI	Small Computer System Interface - Standard de bus informatique.
SCVMM	System Center Virtual Machine Manager.
SGA	Secrétariat Général pour l'Administration.
SGBD	Système de Gestion de Base de Données.
SIC	Systèmes d'Information et de Communication.
SMB	Server Message Block.
SSH	Secure SHell. Shell d'administration à distance et sécurisé.
SSI	Sécurité des Systèmes d'Information.
SSO	Single Sign On. Authentification unique.
STCIA	Socle Technique Commun InterArmées.
STU	Soutien Technique aux Utilisateurs.
TICE	Technologies de l'Information et de la Communication pour l'Education.
TLP	Top Level Project - Projet haut niveau.
TSEF	Technicien Supérieur d'Études et de Fabrications.
VPS	Virtual Private Server - Serveur privé virtuel.
VPN	Virtual Private Network - Réseau virtuel sécurisé.
VLAN	Virtual Local Area Network - Réseau Local Virtuel.
VLE	Virtual Learning Environnement - Environnement Virtuel d'Apprentissage.
VM	Virtual Machine. Serveur ou station virtualisé. Le terme "boxes" sera rencontré dans la littérature anglophone.
VMFS	VWware File System.
vCPU	Virtual CPU - CPU Virtuel.
WWN	Wold Wide Name. Identifiant unique dans un réseau SAN.

Glossaire

Active Directory	Active Directory (AD) est le service d'annuaire LDAP pour les systèmes Microsoft Windows.
Cloud Computing	Informatique en nuage. Les capacités de calcul et de stockage sont louées à la demande.
Cluster	Ensemble de serveurs, formant une "ferme de calcul".
Commutateur virtuel	Un commutateur virtuel (Virtual Switch) est un système logiciel de l'hyperviseur permettant d'offrir une connectivité réseau à ses machines virtuelles invitées.
Exchange	Serveur de Messagerie de Microsoft.
Fibre Channel	Protocole de connexion haut débit entre un ordinateur et son système de stockage.
IIS	Internet Information Services. Serveur Web de Microsoft.
Lync	Lync est la plate-forme de communications unifiée destinée aux entreprises de Microsoft.
Provisionning	Terme informatique désignant l'allocation automatique de ressources.
Snapshot	Un snapshot est une capture en lecture seule d'un volume de données ou d'une machine virtuelle à un instant donné.
Soutien PFI-ENT	Le personnel de la section soutien PFI-ENT administre les plateformes d'instruction et l'espace numérique de travail de l'École des Transmissions.
vCenter	Outil de gestion des serveurs et de la virtualisation chez VMware.

Table des matières

Introduction

Ce mémoire traite de la mise en œuvre d'un cloud privé au sein de l'Espace Numérique de Formation de l'École des Transmissions (ETRS) de Cesson-Sévigné, au profit des formateurs et stagiaires du Groupement des Systèmes d'Information de la Direction Générale de la Formation de l'école.

Cette plateforme offre les ressources matérielles, logicielles et documentaires, nécessaires à la formation des futurs administrateurs systèmes du Ministère de la défense. Désormais, ils peuvent déployer, en fonction de leurs besoins et de façon autonome, les serveurs et les infrastructures réseaux nécessaires à leurs travaux pratiques.

Ce projet prend en compte les aspects techniques du projet, ainsi que ceux liés à la Sécurité des Systèmes d'Information, l'évolutivité et l'élasticité (montée en puissance) de la plateforme, l'orientation des nouveaux usages pédagogiques, l'adaptation de la solution à la spécificité de la formation, l'automatisation du provisionnement, sans oublier l'accompagnement du changement.

I Présentation du projet

Durant son cursus à l'École des Transmissions, un stagiaire en formation « administrateur système » est amené à faire fonctionner simultanément jusqu'à 5 machines virtuelles sur son poste de travail. Cela nécessite un espace de stockage important, une puissance de calcul élevée et une capacité de mémoire RAM conséquente.

La section soutien PFI-ENT, qui administre le parc informatique dédié à la formation, recherche une solution de cloud privé, afin d'offrir certains avantages par rapport à une gestion de parc traditionnelle :

- sécurité et maintenance du poste de travail améliorées ;
- durée de vie des postes allongée ;
- besoin de performance réduit ;
- ouverture du cloud vers la zone d'hébergement des stagiaires (travail hors heures ouvrables) voire vers l'extérieur pour l'enseignement à distance (EAD) dans le cadre de la préparation du cursus, de la remise à niveau, l'auto-formation ;
- archivage numérique des données d'évaluation pour une durée légale d'un an (résultats des examens, l'école délivrant des diplômes homologués et étant normé ISO 9001 version 2000).

L'architecture technique dans laquelle la plateforme doit s'intégrer est complexe : il faut s'appuyer sur le serveur d'authentification CAS et sur l'annuaire LDAP pour récupérer les comptes et les droits. De plus, la mise en œuvre de cette plateforme ne doit pas perturber les autres services en production, notamment les salles de travaux pratiques et les séances d'examens.

Les besoins sont de plus totalement différents selon les matières enseignées (développement, système Linux, système Windows) et selon les niveaux de formation des stagiaires (utilisation ou administration de services). Ils doivent donc être précisement définis.

I.1 Environnement du projet

L'École des Transmissions de Rennes forme une partie des spécialistes et des experts des Systèmes d'Information et de Communication (SIC) et de la Guerre Électronique des armées (Terre, Air et Marine).

De niveau National, l'école réalise des missions à caractère interarme et interarmées. Les stages organisés durent d'un jour à une année. L'école est certifiée ISO 9001.

Figure 1 L'École des Transmissions : site de Cesson-Sévigné

Depuis le 1er juillet 2016, l'ETRS est devenue la division formation du Commandement des systèmes d'information et de communication (COMSIC), également implanté sur le site de Cesson Sévigné.

Subordonné au Commandement des Forces Terrestres (CFT), le COMSIC est :

- autorité organique des unités subordonnées ;
- tête de chaîne des Systèmes d'Information et de Communication (SIC) pour l'ensemble de l'Armée de Terre.

Une présentation plus détaillée du COMSIC est disponible en Annexe 1.

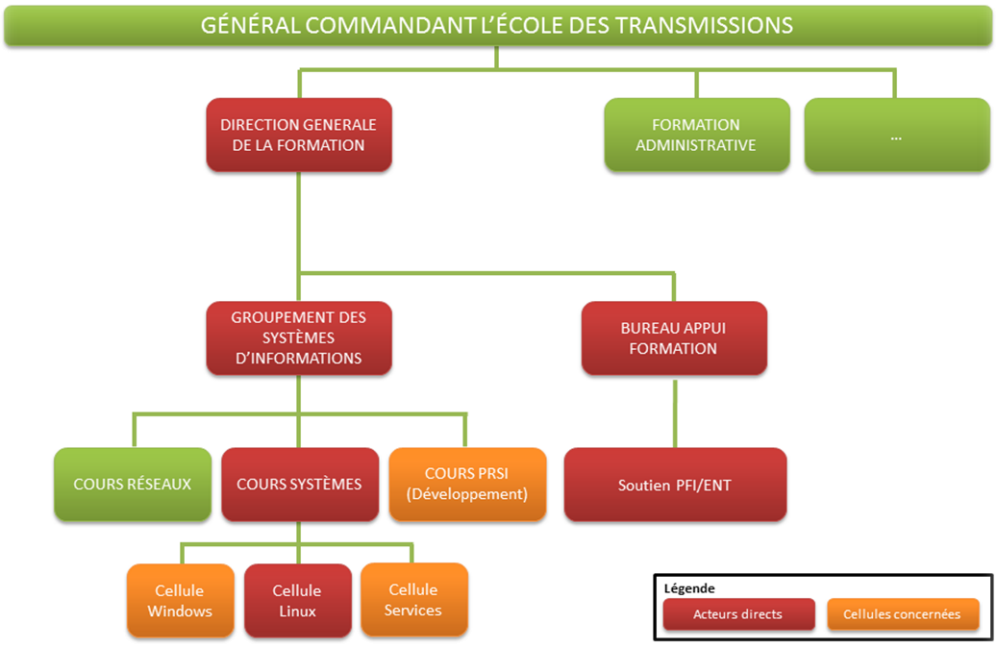


Figure 2 Les acteurs du projet Cloud Formation

Au sein de l'ETRS, la section "Soutien PFI-ENT", placée sous la responsabilité du Bureau Appui à la Formation (BAF), administre le parc informatique dédié à la formation (2200 postes, 80 serveurs) et les services de l'Environnement Numérique de Travail (ENT). Elle assure le maintien en condition opérationnelle du réseau du Campus (CAN - Campus Area Network) et sa sécurité informatique.

Au sein de la Division Générale de la Formation (DGF), le Groupement des Systèmes d'Information (GSI), directement chargé de la formation des administrateurs système, regroupe 3 cours :

- *le cours RTD* "Réseau de Transmissions de Données" ;
- *le cours PRSI* "PRogrammation des Systèmes d'Information" ;
- *le cours systèmes*.

Le cours systèmes est principalement impacté par le projet. Il accueille les cellules :

- *Windows* (6 formateurs) ;
- *Linux* (5 formateurs) ;
- *Services* (3 formateurs).

Au profit de ces acteurs ou clients du projet, mon rôle est de faciliter le dialogue entre ces entités pour décrire le plus précisement possible le besoin des utilisateurs, qu'ils soient formateurs ou stagiaires et ainsi définir les solutions techniques les plus adaptées.

I.2 Problématiques

Former des techniciens à l'administration de systèmes informatiques et télécom, complexes et à la pointe de la technologie est rendu encore plus ardu par le flux important des 3000 stagiaires annuels venus suivre une formation diplômante et par les enjeux technologiques en constante évolution. Il faut concilier ces aspects pour trouver une solution permettant de moderniser les infrastructures existantes, d'améliorer la pédagogie de l'enseignement dispensé, de réduire les coûts, et d'atteindre une satisfaction maximale de la part des stagiaires et de leurs organismes de rattachement.

Entre les possibilités logicielles existantes, les choix organisationnels, la priorisation de l'utilisation des ressources disponibles et les attentes opérationnelles fortes des formateurs, une méthode de sélection doit être trouvée pour répondre aux critères suivants :

- Optimiser le fonctionnement de l'ETRS : gestion des salles de formation, simplifier l'administration, réduire les accès en heures non ouvrables aux salles de classe ;
- Ouvrir de nouvelles perspectives dans le domaine de la formation : classes virtuelles, formation à distance ;
- Moderniser ses actions de formation : catalogues de modèles, gestion des VM de devoirs ;
- S'intégrer dans le CAN-ENT, environnement complexe et déjà riche en fonctionnalités.

D’autre part, le contexte budgetaire, comme dans de nombreuses administrations, se restreint d’années en années, alors que dans le même temps les charges de travail augmentent. Ce paradoxe impose de trouver des compromis dans les domaines stratégiques et financiers :

- S’inscrire dans la carte stratégique du commandement du COMSIC et de l’ETRS, où la Numérisation de l’Espace de Formation (NEF) et la qualité de la pédagogie tiennent une place importante ;
- Disposer d’une quantité confortable de ressources disponibles (puissance processeur, mémoire et stockage) ;
- Tout en réalisant des économies : réduction des performances utiles des postes de formation, centralisation des ressources.

C’est dans ce contexte que l’École des Transmissions de Rennes me confie la gestion du projet Cloud Formation : analyser le besoin, étudier l’existant, concevoir et réaliser la plateforme, en adoptant une méthode de projet adaptée.

Ce nouveau service doit s’intégrer dans une architecture complexe et répondre aux besoins des formateurs, avec lesquels je suis en étroite relation et pour qui il faut mettre en place des outils de communication adaptés.

Lorsque la situation l’exige, je suis aidé par l’administrateur du CAN/ENT, M. Fabrice POLLET, notamment pour l’intégration de la plateforme avec les structures existantes. Une stratégie de travail en équipe et de répartition des tâches rend notre travail efficace.

Enfin, je suis supervisé par M. Patrick Jaouen, mon tuteur en entreprise.

II Gestion du projet

Un rappel de l'historique du projet est tout d'abord nécessaire, afin d'exposer les résultats d'une précédente expérimentation de Cloud de Formation.

Puis sera développée la démarche que j'ai menée dans le but de choisir une méthode de gestion de projet, ainsi que pour planifier les différentes tâches du projet.

II.1 Historique du projet

Le projet d'installation d'une plateforme de cloud privé est né en 2014. Il a déjà fait l'objet d'une première expérimentation [Jaouen-2014].

Durant cette étude, menée conjointement par la société APX et un stagiaire de l'Université de Rennes 1[2], une plateforme de cloud privé a été testée. Ce POC (Proof Of Concept) a démontré la faisabilité du projet avec la solution technique CloudStack.

En effet, dès 2004, la cellule Soutien PFI-ENT identifie un point d'amélioration dans le domaine de la virtualisation des moyens de formation. Le logiciel VMware Workstation installé, permit :

- de standardiser et d'homogénéiser le parc informatique de formation (2200 stations de travail réparties notamment entre 20 salles de 24 stations et les bureaux des formateurs) ;
- d'apporter une grande souplesse dans la programmation des cours et l'attribution des salles banalisées ;
- de simplifier l'administration des postes de formation ;
- de globalement réduire la quantité de stations informatiques nécessaires à l'accomplissement de la mission.

10 ans plus tard, l'expérimentation vise à centraliser les ressources dédiées à la virtualisation. Les formateurs du cours systèmes, présentant les exigences fonctionnelles les plus critiques, en sont les principaux bénéficiaires.

Les volumes de ce cours ont été évalués à 400 machines virtuelles actives simultanément (cours Windows et Linux confondus). Cette estimation étant un indicateur critique, elle sera nécessairement actualisée.

[2] Le stagiaire a été accueilli à l'ETRS pour un stage d'avril à juin 2014.

Les capacités retenues, à cette époque, comme nécessaires à l'établissement d'un cursus complet du cours systèmes, sont résumées dans le tableau ci-dessous :

Tableau 1 Machines virtuelles nécessaires à l'établissement d'un cursus standard du cours systèmes.

Système d'exploitation	Espace de stockage	vCPU	Mémoire
Windows 7	12 Go	1	1 Go
Windows Server 2008	30 Go	2	1 Go
Microsoft Exchange Server 2010	30 Go	2	4 Go
Linux CentOS 6 administration	10 Go	1	1 Go
Linux CentOS 6 serveur	10 Go	1	2 Go

Les machines virtuelles des devoirs Windows, Exchange, Linux, Apache (qui ne sont pas comptabilisées dans le tableau ci-dessus) font l'objet d'une attention particulière (archivage électronique sur 1 an).

L'expérimentation a mis en évidence que :

- les architectures Cloud actuelles ne sont pas nativement conçues pour une utilisation en contexte pédagogique. L'ETRS a besoin d'un outil organisé autour de la notion de stage ou d'action de formation ;
- un stagiaire bénéficie d'une puissance de calcul et d'un espace de stockage contingenté mais suffisant durant l'ensemble de ses travaux pratiques ;
- le formateur gère les machines de devoirs mais également les ressources de ses stagiaires.

L'organisation des comptes utilisateurs et des projets dans l'outil retenu doit être réfléchie en conséquence :

- l'utilisation des outils en ligne de commande permet de répondre à ces spécificités, mais la mise en œuvre s'est montrée laborieuse ;
- l'organisation devra faire l'objet d'un développement spécifique, en s'appuyant sur les API de la solution retenue ;
- cet outil devra permettre de créer automatiquement les objets nécessaires à un stage depuis l'annuaire LDAP de l'école.

3 profils sont identifiés :

- le profil administrateur : administration des ressources physiques ;
- le profil formateur : gestion des stagiaires, des quotas, des modèles, création de machines virtuelles ;
- le profil stagiaire : création de machines virtuelles depuis un modèle ou installation depuis un média d'installation et dans la limite de ses quotas, exploitation des machines.

Le bilan de cette expérimentation a été très concluant. Elle démontre qu'un cloud pour la formation :

- apporte une réelle plus-value aux formateurs et aux stagiaires. Ses atouts sont indéniables, notamment pour la gestion des devoirs et la préparation des salles de classes ;
- facilite l'administration des plateformes de formation ;
- réduit les besoins de puissance rendus nécessaires sur chacun des postes de formations qui s'avèrent du coup très coûteux ;
- 2 serveurs de stockage NAS et 8 hyperviseurs ont été commandés. L'expérimentation a été mise en pause jusqu'à ce jour, en attendant la livraison de ce matériel.

Si les cas d'usage restent à affiner, la solution est proche des attendus de l'ETRS. Elle s'appuie sur des solutions techniques (Linux, NFS, KVM) déjà bien maîtrisées par les administrateurs.

II.2 Choix de la méthode

La gestion du projet a été adaptée d'une démarche de développement de projet suivant un cycle en V, afin de répondre au besoin de progression par étapes, ainsi qu'au besoin de tracabilité (expression des besoins, dossier d'études et cahier des charges, dossier de sécurité, documents descriptifs et schémas techniques).

Le projet a ainsi été mené en suivant 6 étapes :

- étude préalable ;
- recueil des besoins ;
- étude et conception du projet ;
- phase de réalisation ;
- mise en œuvre ;
- évaluation.

Le matériel définitif n'ayant pas encore été livré, la phase d'evaluation sera restreinte aux capacités des serveurs en place.

II.3 Planification du projet

La planification du projet a consisté en une phase d'étude (étude préalable et conception) de 2 mois, suivie d'une phase de réalisation d'un mois. Puis le déploiement de la plateforme se fait au mois de juillet, durant la période la plus calme de l'école.

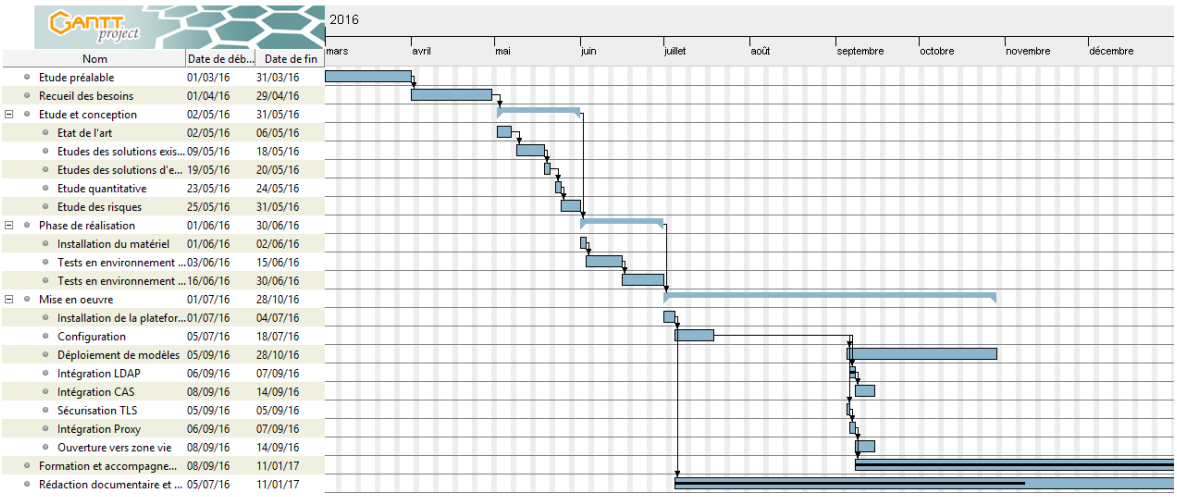


Figure 3 Planification du projet - Diagramme de Gantt

Ainsi les formateurs ont pu commencer à évaluer et utiliser la plateforme dès la rentrée de septembre 2016.

Enfin, les parties accompagnement et documentation ont pu se réaliser de façon progressive durant les phases de mise en œuvre et d'évaluation. Cette démarche a fait de gagner du temps, car les tâches documentaires sont particulièrement chronophages et doivent s'inscrire dans la vision finale du projet technique.

III Etude préalable

L'étude préalable au projet s'inscrit dans la stratégie globale de l'école. Elle établit précisemment le volume annuel de stages concernés et recueille les besoins auprès des formateurs et de l'administrateur du réseau dédié à la formation.

III.1 Stratégie de l'école

Le général MAURICE, commandant le COMSIC et le général ADLOFF, commandant l'ETRS, ont élaboré une carte stratégique pour l'École des Transmissions.

Elle s'appuie sur 4 axes :

Figure 4 Carte stratégique 2015-2016 de l'ETRS

Le projet de plateforme de Cloud de Formation s'inscrit dans l'axe stratégique (voir axes en rouge en figure 4) :

- D, visant à "positionner l'École comme pôle d'excellence TRANS sur les scènes terre, interarmées et interministérielle". Il contribue plus particulièrement au levier d'action D6 qui a pour objet de "développer la capacité en plateformes de formation et d'entraînement" et au levier D3 en faisant la "promotion de l'expertise sur la Numérisation de l'Espace de Formation" ;
- A, visant à "appuyer la montée en puissance du COMSIC", en fournissant un environnement de travail adapté (levier A4).

L'École des Transmissions n'échappe pas aux restrictions de budget et à la déflation de personnel, tout en continuant d'assumer ses missions de formation dans le domaine des SIC. Pour assurer ces cours à la fois techniques et complexes, l'école a choisi la voie de la Numérisation de l'Espace de Formation (NEF).

III.2 La programmation des stages

La programmation des stages est relativement cyclique et donc définie à l'avance.

La démarche d'étude a consisté, pour cet aspect, à analyser le nombre de stagiaires présents simultanément, suivant un des cursus des cours systèmes ou PRSI, pour l'année scolaire courante.

Ainsi, le schéma ci-dessous permet d'estimer, sur l'année scolaire 2016-2017 et pour les deux cours, qu'ils accueilleront au maximum 120 stagiaires durant la même période. Cette capacité est exceptionnellement atteinte une fois cette année et durant seulement 2 jours.

Au final, l'étude retiendra un maximum de 96 stagiaires utilisant simultanément les ressources informatiques ; ce qui, comme nous allons le voir dans la suite de l'étude, a des conséquences sur le choix des techniques à déployer et sur le dimensionnement des installations.

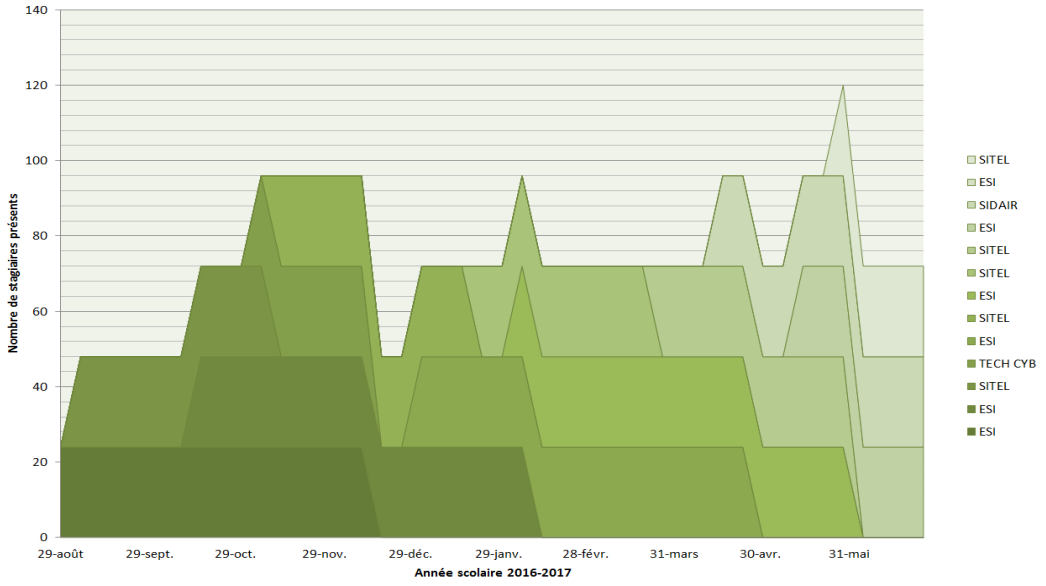


Figure 5 Stages et nombre de stagiaires présents aux cours systèmes et PRSI (année scolaire 2016-2017)

III.3 Recueil des besoins

Cette phase, incluant les travaux initialement menés ainsi que les besoins correspondants aux objectifs de l'école, va permettre de définir précisément l'ampleur du projet, tant sur le plan des problématiques à résoudre, qu'au sujet des exigences à spécifier en phase suivante (phase étude).

III.3.1 Actualisation de l'expression du besoin (2016)

L'expression initiale ayant été effectuée en 2014, il est indispensable de réaliser une actualisation de ces exigences auprès des formateurs actuels.

Une réunion de présentation des possibilités d'une plateforme IAAS est effectuée le 4 mai 2016, au profit des formateurs du cours systèmes (Windows, Services et Linux), Programmation PRSI et réseau.

Cet exposé a permis de sensibiliser les formateurs à la nécessité de se projeter, d'imaginer les concepts de demain et d'appréhender au mieux le changement de paradigme à venir :

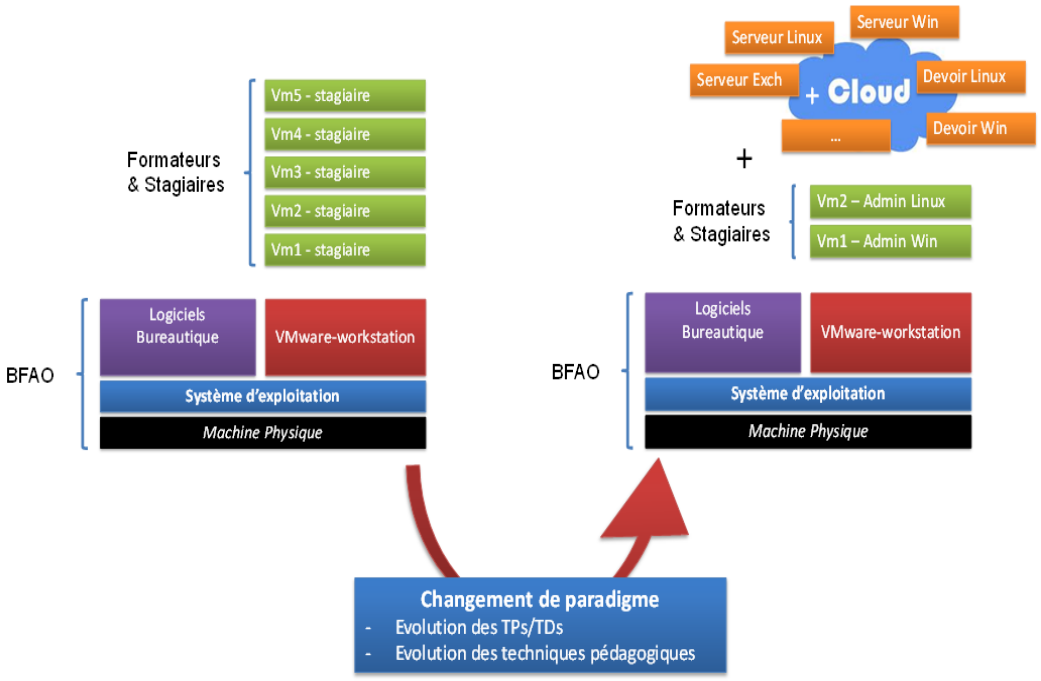


Figure 6 Le changement de paradigme amené par le Cloud Formation.

Les échanges passionnés à la fin de la séance ont mis en évidence que les différentes cellules n'ont pas les mêmes attentes, notamment au niveau du cloisonnement des VM sur le plan de la sécurité.

En effet, il en ressort que les besoins sont totalement différents selon les matières enseignées (développement, système Linux, système Windows) et selon les niveaux de formation des stagiaires (niveau 1 : utilisation de service, niveau 2 : administration du serveur).

III.3.2 Problématiques et charge de travail des formateurs

D'un point de vue formation, le CAN manque d'un environnement mettant à disposition des infrastructures réseaux et des serveurs ; ce qui permettrait aux futurs administrateurs du Ministère de la Défense de travailler dans des conditions plus proches du réel. Dans un tel environnement, ces serveurs sont déployés et supprimés à l'initiative du formateur ou du stagiaire.

Problématiques des formateurs

La virtualisation des serveurs s'est rapidement démocratisée en entreprise et est devenue une réalité incontournable. Toutefois, l'investissement en RAM et en puissance CPU nécessaire sur l'ensemble du parc pour la solution VMware Workstation n'est plus efficient. La virtualisation sur le poste de formation a ainsi trouvé ses limites dans les usages qui en sont faits par les stagiaires ou par les formateurs :

- Le stagiaire du cours systèmes fait fonctionner simultanément jusqu'à 5 machines virtuelles. Les postes de formation ne peuvent assumer cette charge sans faire l'objet d'une course à la puissance. L'exécution de ces machines virtuelles doit être déportée, permettant l'allongement de la durée de vie des postes de formation et la réduction du besoin de performance.

Déporter l'exécution des machines virtuelles (VM) rend les instructeurs dépendant de la disponibilité de la nouvelle plateforme, ce qui représente la crainte numéro une chez les formateurs. Toutefois, certains problèmes récurrents rencontrés par les formateurs, comme la corruption des VM à l'extinction des postes ou à l'éjection des supports amovibles, ne se produiront plus.

- Offrir un accès à ces ressources en dehors des heures de travail depuis la zone d'hébergement est également envisagé, ce qui est impossible avec la solution actuelle.
- Impossibilité pour le formateur de laisser sa machine virtuelle fonctionner au profit des élèves en dehors des heures de formation, ce qui est contraignant dans le cadre de cours sur les services réseaux ;
- Nécessité de copier les VM ou les données des VM à travers le réseau (risque de surcharge) ou sur clé USB (risque SSI) ;
- Les postes formateurs et stagiaires sont sur deux réseaux différents. Les scripts de correction automatique des machines d'évaluation doivent donc être adaptés en fonction de l'endroit d'où ils sont exécutés.

Charge de travail des formateurs

La priorité actuelle de la cellule Windows est à la consolidation de ses cours existants, à l'accueil des nouvelles populations de stagiaires et à la préparation de l'arrivée de la nouvelle plateforme de formation STCIA (Socle Technique Commun Interarmées). Ces nombreuses tâches limitent leurs disponibilités pour tester ce nouvel outil, mais aussi pour assumer la charge de travail induite par l'adaptation des cours (modification des cahiers de travaux pratiques, adaptation des procédures d'évaluation du stagiaire).

Les débuts de la plateforme de cloud privé coïncident avec l'arrivée des premiers stagiaires de la nouvelle filière ESI (Emploi des Systèmes d'Information) de l'Armée de Terre. Cette action de formation regroupe les spécialistes (de niveau 1 dans un premier temps, puis de niveau 2 en 2017) de l'administration des systèmes d'exploitation. Depuis plusieurs années, l'Armée de Terre ne formait plus les jeunes engagés sur le système Linux. La cellule concernée voit son volume de travail multiplié par deux depuis septembre 2016 et doit s'adapter à cette nouvelle population.

Le cours systèmes est composé de personnels expérimentés dans leur domaine d'expertise. Tous sont au moins "Brevetés Supérieurs" (niveau de formation militaire généralement reconnu au RNCP de niveau III), voir pour certains "Brevet de Maîtrise" ou "Diplômés Techniques" pour le personnel officier. La rotation du personnel induite par la mobilité géographique inhérente au métier de militaire est conséquente, surtout pour des postes de formateurs qui nécessitent à la fois une période d'apprentissage au métier de pédagogue et aux outils associés, en plus de l'assimilation technique du contenu des cours à dispenser.

La conduite du changement, dans ces conditions, est un aspect essentiel du projet. Les solutions mises en œuvre doivent impérativement répondre à un besoin réel, à des problématiques actuelles et n'ont pas pour objet d'apporter des fonctionnalités supplémentaires redondantes ou non pertinentes. La plateforme ne doit pas être un outil "en plus", générant une charge supplémentaire de travail au formateur pour préparer l'arrivée de ses stagiaires. Au contraire, elle doit offrir des solutions automatisées à des problèmes rencontrés ou des processus perfectibles connus des formateurs.

Il est primordial d'inventer les concepts d'utilisation, d'accompagner le changement de paradigme auprès des formateurs les plus anciens. Il faut également leur laisser du temps quant à l'adaptation des cours et pour qu'ils s'appuient sur toutes les nouvelles possibilités.

III.3.3 Besoins relatifs aux machines virtuelles d'examen

La gestion des machines virtuelles de devoir est effectivement un point noir dans le processus actuel de formation.

Afin d'assurer les corrections, les formateurs ou les stagiaires effectuent une copie de sauvegarde de leur devoir sur le réseau ou via un disque externe pour permettre une correction et un archivage « a posteriori ». Pour faciliter les transferts, ces VM sont compressées avec un utilitaire type 7zip, ce qui demande de la puissance processeur. Ce processus augmente le temps d'attente en fin de devoir et le risque de corruption des données durant la compression de la machine.

Pour corriger les machines virtuelles issues des travaux pratiques ou des examens, les formateurs perdent encore un temps important à copier les sauvegardes des machines de devoir sur leur poste de formateur.

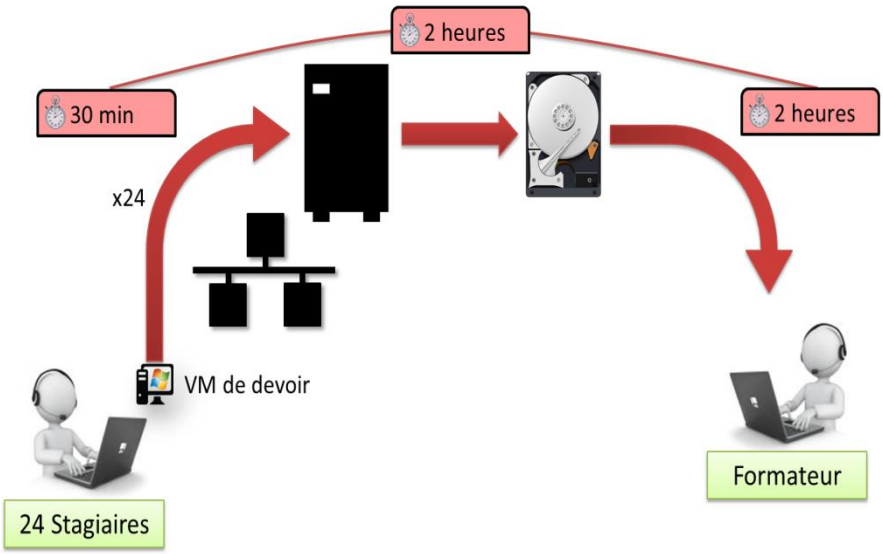


Figure 7 Processus de correction des machines virtuelles Windows de devoir.

Le passage au format Cloud des machines virtuelles de devoir répond à des besoins très importants, solutionnant les problématiques décrites précédement :

- un contrôle de ces machines virtuelles (déploiement, lancement, puis arrêt des VM à la fin du devoir) par le formateur, rendant la consultation de la VM de devoir par le stagiaire impossible en avance de phase ou sa modification a posteriori ;
- la correction des devoirs par démarrage des machines virtuelles au moment opportun, décidé par le formateur ;
- un archivage pendant 1 année des machines virtuelles "facilité" pour les formateurs ;
- une réduction du risque de corruption des données durant le transfert.

III.3.4 Expression des besoins par cellule

Cellule Linux

La cellule Linux exprime son besoin ainsi :

- Les travaux pratiques traitant de l'installation d'une station se font sur une machine virtuelle locale. L'administration des serveurs distants se fait ensuite depuis cette station.
- Les travaux pratiques portant sur la mise en œuvre de services comme apache, postfix, squid et bind sont effectués à distance sur une machine virtuelle du cloud. La gestion des ressources est de la responsabilité du stagiaire.
- Les devoirs "administration", "apache" et "postfix" se font sur une machine virtuelle disponible le temps du devoir et archivée ensuite pendant une année.
- Les formateurs Linux disposent de machines virtuelles qui permettent la création d'une hiérarchie de services avec les stagiaires. Une machine virtuelle de supervision et une autre d'hébergement de services java (pour le cours "Répartition de charge") sont démarrées lorsqu'elles sont nécessaires. Ce service vient en remplacement du SAAS StartTUX. Ce socle technique mettant à disposition des formateurs des services pour la formation a été mis en place en 2016 par la cellule Soutien PFI-ENT.

Cellule Windows

La cellule Windows exprime son besoin ainsi :

- Les travaux pratiques traitant de l'installation d'une station se font sur une machine virtuelle locale. Le stagiaire bascule ensuite sur une VM du cloud pour continuer sa formation Station de Travail puis Serveur.
- Les devoirs Windows 7 et Windows 2008 serveur nécessitent deux machines virtuelles qui sont ensuite archivées. A l'issue du devoir, les VM sont arrêtées. Chaque VM est relancée par le correcteur puis arrêtée à l'issue de son travail de notation.
- Les 6 formateurs disposent de machines virtuelles qui permettent de faire la correction des Travaux Dirigés en Face à Face Pédagogique (FAFP).

Cellule Services

La cellule Services exprime son besoin ainsi :

- Le suivi du cursus des cours Services nécessite une station cliente qui reste au niveau du poste de formation.
- Pour le cours Exchange, chaque stagiaire dispose d'un serveur qu'il intègre dans une architecture existante mise en place par le formateur. L'espace disque nécessaire est limité (30 Go) mais le serveur doit être relativement puissant.
- Le cours IIS nécessite quant à lui des serveurs plus modestes.
- En plus du serveur installé durant le cours Exchange, les cours Lync

nécessitent un serveur frontal et un backend SQL.

- Durant le temps de formation, l'ensemble des serveurs des stagiaires doivent communiquer entre eux mais également avec le serveur du formateur. Durant les devoirs, les serveurs ne communiquent plus entre eux, mais uniquement avec le serveur du formateur. Cette dernière restriction n'est pas mise en place à ce jour.
- La mise en place des devoirs sur l'espace de formation Cloud nécessite 24 serveurs isolés, un serveur formateur et un serveur pour l'infrastructure Active Directory. A l'issue des devoirs, le formateur ne doit pas redémarrer les serveurs pour leur correction comme c'est le cas pour les devoirs Linux et Windows.

Refaire les modèles des machines virtuelles n'est pas un problème. Il n'est pas nécessaire de prévoir une migration de l'existant.

La programmation des devoirs liés à la cellule Services étant prévue à la toute fin du stage, il est impossible de la décaler ou de la reprogrammer. Une solution de contournement est la bascule vers un devoir théorique type QCM.

La taille nécessaire des disques est estimée à 30 Go par serveur.

Cours PRSI

Les besoins du cours PRSI, sensiblement différents de ceux du cours systèmes, viennent compléter le périmètre de l'étude et permettront d'affiner l'architecture de la solution retenue.

Le cours PRSI ne faisait pas partie de la cible initiale de 2014.

Exigences liées aux VM

Actuellement, à cause des limitations imposées par la politique de sécurité sur les postes informatiques des salles de cours, chacun de nos stagiaires dispose d'une VM de travail configurée avec tous les outils nécessaires à l'ensemble de sa formation. Les stagiaires peuvent stocker cette VM en local sur leur poste mais il leur est conseillé de la stocker sur un support amovible (Clé USB ou disque dur) afin de pouvoir l'utiliser sur leur ordinateur personnel en dehors des heures de services.

Pour conserver leur environnement de travail de salle en salle, les formateurs du cours PRSI disposent également de leur VM, identique à celle des stagiaires, sur un support amovible.

Ces habitudes de travail présentent des risques pour la sécurité (virus lors des échanges sur clés USB) et n'offrent pas les performances attendues : les temps de lecture/écriture sur un périphérique USB ne permettent pas encore ce genre de pratique.

Ces VM sont celles qui requièrent le plus de puissance (1 à 2 CPU et 4 Go de RAM). Elles nécessitent des postes de formation disposant d'au moins 2 voir 4 CPU et 8 Go de RAM. Toutes les PFI ne sont pas à ce niveau.

Exigences liées aux postes de dévéloppement

Le besoin principal du cours PRSI est de permettre aux stagiaires et formateurs de

disposer d'une VM "poste de développement" accessible "graphiquement" à distance depuis les salles de cours (PFI Internet), la zone hébergement de l'ETRS et depuis Internet.

- Cette VM "poste de développement" basée sur Linux nécessite 4 Go de RAM avec 1 ou 2 CPU et 20 Go d'espace disque (50 Go pour les formateurs).
- En moyenne 60 VM (max. 80) pourraient s'exécuter en simultané.
- Un autre intérêt au "cloud ETRS" est de pouvoir proposer des VM supplémentaires aux stagiaires lors de leur projet de fin de cursus (frontal web, serveur d'appli, SGBD, serveur de mail…). Les exigences en ressources pour ces VM sont plus raisonnables. Une vingtaine maximum de ces VM sont provisionnées pour une durée assez courte (4 à 5 semaines) avant d'être archivées.

Les VM "Dev" des stagiaires et des formateurs ainsi que la VM "Services PRSI" sont soumises à une très forte disponibilité (99%) entre 7h30 et 23h00.

Expression du besoin de la cellule soutien PFI-ENT

Les besoins de la cellule soutien PFI-ENT s'articulent autour de 3 axes :

Administration de la plateforme

- La solution doit s'appuyer sur le serveur d'authentification CAS et sur l'annuaire LDAP pour importer les comptes et les droits.
- La solution doit être facilement administrable, ne doit pas nécessiter de compétences particulières.
- Les tâches d'administration doivent être automatisables par scripts.
- La mise en œuvre de cette plateforme ne doit pas perturber les autres services en production.
- Les procédures d'administrations doivent être rédigées, compréhensibles et testées par les futurs administrateurs.

Evolutivité de la plateforme

- La montée en puissance de la plateforme à venir doit être souple, nécessiter du matériel standard et si possible la configuration des nœuds doit être automatisée.
- L'ETRS ne doit pas s'enfermer dans une technologie propriétaire et risquer des dépenses futures non contrôlées.

Prise en compte de la SSI

- La sécurité de la plateforme doit être renforcée, en respectant au minimum les règles SSI du CAN/ENT en s'appuyant sur les services existants par des protocoles sécurisés.
- Les documents relatifs à la sécurité doivent être mis à jour :
  - FEROS (Fiche d'Expression Rationnelle des Objectifs de Sécurité),
  - PES (Politiques de Sécurité des Systèmes d'Information).
- Un audit de sécurité sera mené par une équipe externe à l'établissement dans le cadre d'une actualisation de l'homologation du système d'information CAN-ENT.

III.3.5 Etude quantitative en VM

Les besoins exprimés par les différentes cellules sont regroupés dans le tableau suivant qui les standardisent sous forme de type de ressources (offre S, M, L, XL, XXL, 2XL).

Tableau 2 Définition des offres de machines virtuelles

Offre	vCPU	RAM
S	1 x 1 Ghz	1
M	1 x 1 Ghz	2
L	1 x 1.5 Ghz	2
XL	1 x 2 Ghz	4
XXL	1 x 2 Ghz	8
2XL	2 x 2 Ghz	4

Les exigences de chaque celllule sont synthétisées dans les tableaux ci-dessous :

Tableau 3 Les exigences en VM de la cellule Linux.

Besoin	Nombre	Durée	Offre	Archivage
VM Admin	24 / stage	6 semaines	S	Non
VM Serveur	24 / stage	6 semaines	S	Non
VM Devoir Admin	24 / stage	3 jours	S	Oui
VM Devoir Apache	24 / stage	3 jours	S	Oui
VM Devoir Postfix	24 / stage	3 jours	S	Oui
VM Formateurs	5		M	Non
VM Supervision + Hebergement Java	2		S	Non

Tableau 4 Les exigences en VM de la cellule Windows.

Besoin	Nombre	Durée	Offre	Archivage
VM Windows 7	24 / stage	6 semaines	S	Non
VM Serveur	24 / stage	6 semaines	S	Non
VM Formateurs	6		M	Non
VM Infrastructure	6		L	Non
VM Devoir	48 / stage	2 semaines	L	Oui

Tableau 5 Les exigences en VM de la cellule Services.

Besoin	Nombre	Durée	Offre	Archivage
VM Exchange stagiaire	24 / stage	2 semaines	XXL	Non
VM Exchange formateur	3		XXL	Non
VM IIS	24 / stage	2 semaines	XL	Non
VM Frontal Link	24 / stage	2 semaines	XXL	Non
VM Backend Link	24 / stage	2 semaines	XXL	Non
VM Devoir	24 / stage	2 jours	XXL	Oui
VM Devoir Formateur	1 / stage	2 jours	XXL	Non
VM Devoir AD Formateur	1 / stage	2 jours	XL	Non

Tableau 6 Les exigences en VM du cours PRSI.

Besoin	Nombre	Durée	Offre	Archivage
VM "Dev" Stagiaire	24 / stage	6 mois	2XXL	Non
VM "Projet" Stagiaire	20 / stage	5 semaines	2XXL	oui
VM "Dev" Formateur	10		2XXL	oui
VM "Services PRSI"	2		M	oui

La synthèse des besoins de toutes les cellules du cours systèmes permet de définir l'allocation maximale de puissance de calcul à autoriser par stagiaire :

Tableau 7 Puissance de calcul maximale par stagiaire

Nom de la VM	Offre	Utilisation maximale concurrente	Puissance de calcul maximale
VM Linux Admin	S	2x S	2x 1 Ghz
VM Linux Serveur	S		
VM Linux Devoir Admin	S		
VM Linux Devoir Apache	S		
VM Devoir Postfix	S		
VM Windows 7	S	2x L	2x 1,5 Ghz
VM Windows Serveur	S		
VM Devoir Windows Serveur 1	L		
VM Devoir Windows Serveur 2	L		
VM Exchange stagiaire	XXL	3x XXL	3x 2 Ghz
VM IIS	XL		
VM Frontal Link	XXL		
VM Backend Link	XXL		
VM Devoir Exchange	XXL		
		Total :	**11 Ghz**

Lors de l'étude préalable, il a été confirmé que le projet de Cloud Formation s'inscrivait parfaitement dans la stratégie de l'école, dans sa volonté de Numérisation de l'Espace de Formation et de pédagogie moderne. L'actualisation de l'expression des besoins de 2014 a été l'occasion de présenter le projet aux formateurs et de recueillir leurs nouvelles exigences. Enfin, Une évaluation de la quantité de stagiaires potentiels fixe les ressources maximales nécessaires.

L'étude et la conception de la plateforme de Cloud Formation peuvent débuter.

IV Etude du projet

La phase d'étude du projet commence par dresser un état de l'art employé dans le domaine du « Cloud » pour proposer ensuite des solutions.

Une discussion autour des options possibles amène au choix de la plateforme retenue.

Enfin, l'étude du projet s'achève par l'étude des risques, étape indispensable pour tout projet du ministère de la Défense ouvert sur internet.

IV.1 Etat de l'art

L'état de l'art des technologies « Cloud » est restitué en commençant par le domaine strict de la virtualisation, se poursuit par les techniques du monde de l'informatique en nuage : le "Cloud Computing", pour finir par les technologies de stockage.

Une version plus détaillée est disponible en annexe 3.

IV.1.1 La virtualisation

La virtualisation a pour objectif de faire fonctionner sur une seule plateforme matérielle plusieurs systèmes d'exploitation ou plusieurs applications, d'augmenter le taux d'utilisation des éléments essentiels comme la mémoire ou le temps processeur, d'abaisser les coûts par mutualisation du stockage et réduire la facture énergétique.

Les deux principales méthodes de virtualisation sont :

La virtualisation de niveau 1

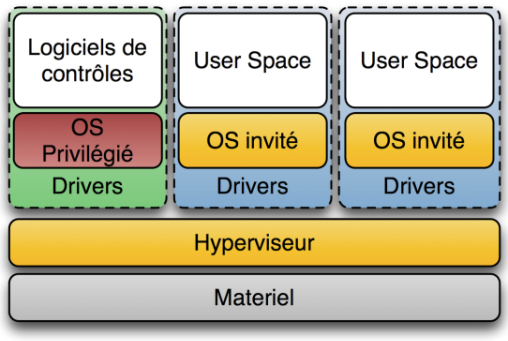


Figure 8 La virtualisation de niveau 1 (source wikipedia)

- S'appuie sur un micro noyau
- Utilise la paravirtualisation ou la virtualisation matérielle

La virtualisation de niveau 2

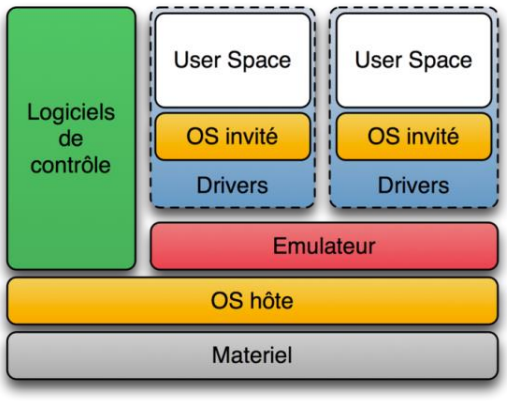


Figure 9 La virtualisation de niveau 2 (source wikipedia)

- Virtualisation logicielle sur système d'exploitation existant
- Emulation du matériel, adaptation du code

- Propose des services de haute disponibilité, de répartition de charge, d'élasticité.
- Plus performante que la virtualisation de niveau 2 mais elle est plus onéreuse
- Exemple d'hyperviseurs : VMware Esx, Citrix XenServer, KVM, Microsoft Hyper-V

binaire à la volée

- Gourmande en ressources
- Exemple d'hyperviseurs : VMware Workstation ou Server, Oracle Virtual Box, Microsoft Virtual PC

IV.1.2 Le cloud

L'informatique en nuage s'appuie généralement sur la virtualisation pour offrir une **informatique « à la demande »**. Il devient possible de louer un serveur virtuel comme un espace de stockage pour un temps donné et n'être facturé qu'en fonction de l'utilisation réelle.

Pour le NIST, dans sa définition du cloud [NIST], les logiciels dédiés aux plateformes de cloud computing doivent avoir les 5 caractéristiques suivantes :

- accès à la demande ;
- large bande passante ;
- réserve de ressources ;
- redimensionnement rapide ;
- facturation en fonction de l'utilisation des ressources.

Différents niveaux de services sont définis dans le terme « cloud » :

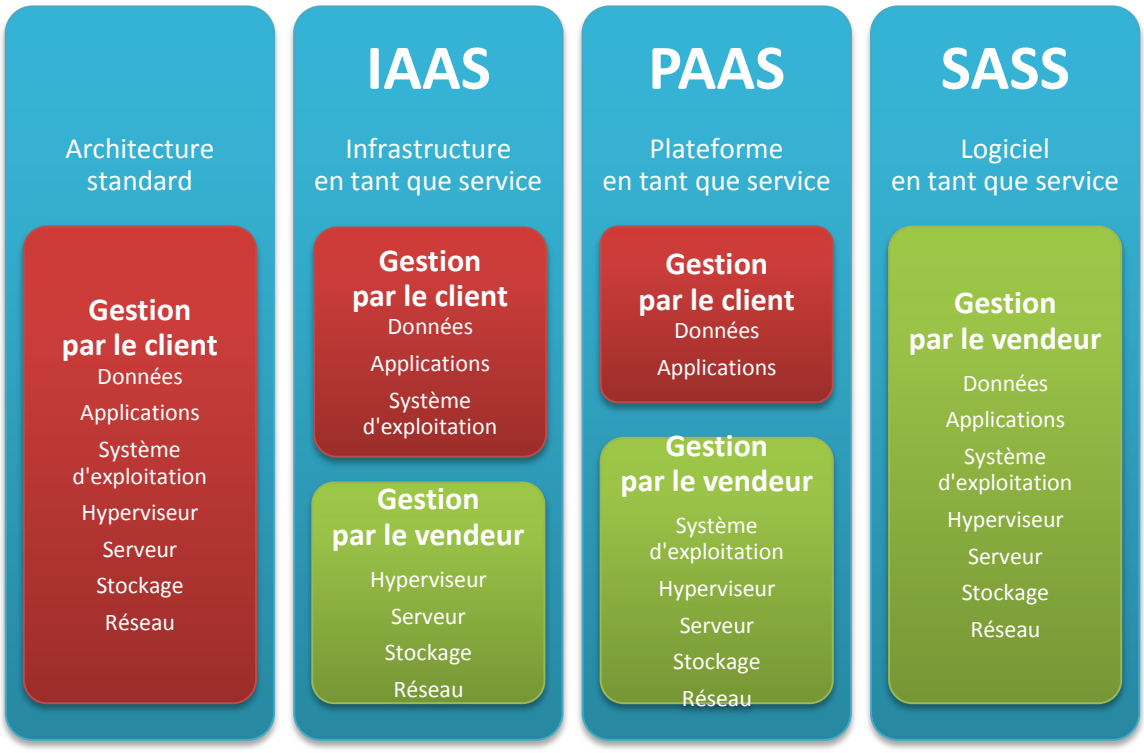


Figure 10 Les offres de services Cloud

IV.1.3 Le stockage

Le stockage fait partie intégrante de tout projet cloud. C'est un facteur important en termes d'espace de stockage mais également du point de vue des performances : quantité d'entrées/sorties possibles (IOPS).

Il existe, en plus du traditionnel espace de stockage local, deux technologies principales de stockage en réseau :

- la technologie NAS (Network Attached Storage) ;
- la technologie SAN (Storage Area Network).

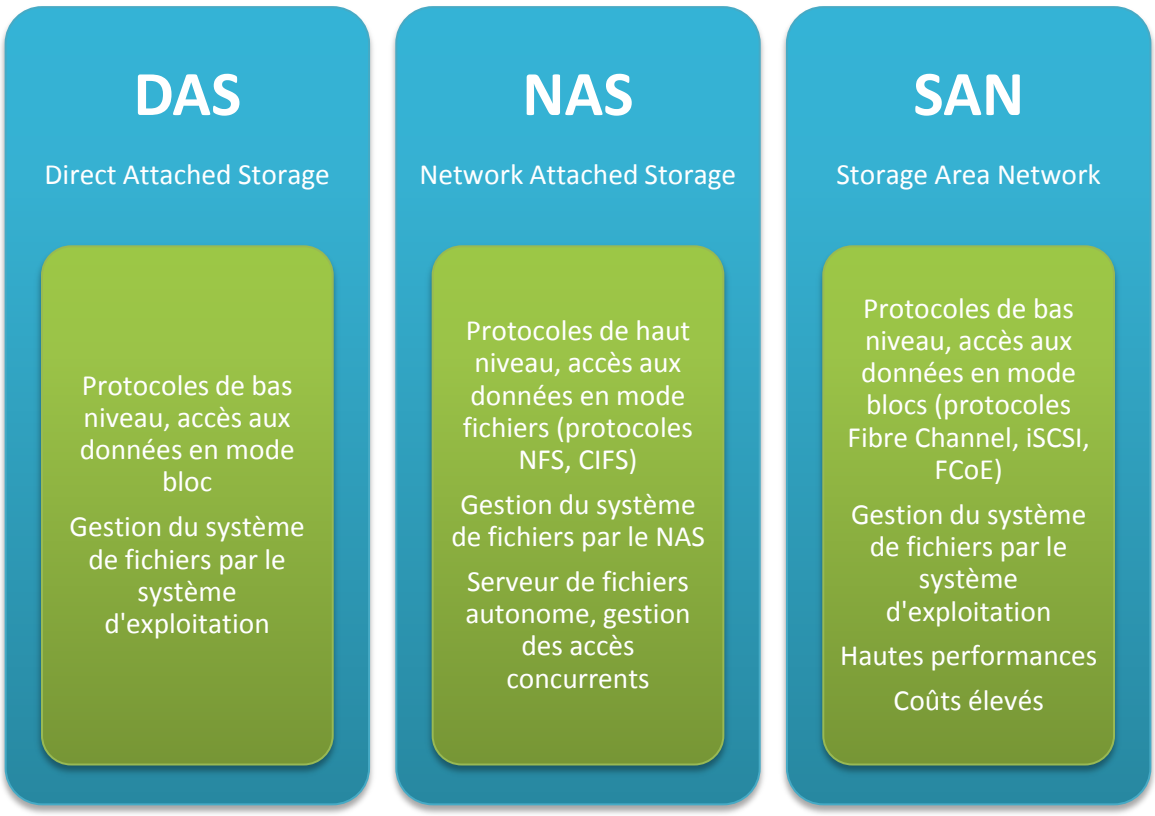


Figure 11 Différences entre DAS/NAS/SAN

Ainsi, l'état de l'art fait le point des technologies du domaine de la virtualisation, du stockage et de l'informatique en nuage mises en œuvre dans un projet de cloud privé. Les termes et définitions présentés sont les éléments de vocabulaire nécessaires pour aborder l'étude du projet.

Une étude des solutions existantes est maintenant nécessaire pour faire un choix éclairé de plateforme IAAS ainsi que de l'hyperviseur à privilégier.

IV.2 Solutions proposées

Nous allons nous intéresser successivement à ces deux points :

1. la plateforme de Cloud ;
2. l'hyperviseur.

IV.2.1 Les plateformes de gestion de Cloud

Les plateformes de gestion de cloud sont de véritables orchestrateurs de centre de données (Datacenter Orchestrator) et fournissent les fonctionnalités de :

- gestion du stockage ;
- gestion des identités ;
- gestion du réseau ;
- répartition de la charge ;
- gestion des médias d'installation et des modèles de machines virtuelles ;
- gestion du firewall et des VPN.

Le tout bien évidemment accessible en self-service depuis un portail internet pour correspondre à la philosophie de l'informatique « à la demande ».

Une présentation plus détaillée des plateformes IAAS du marché est fournie en Annexe 4.

Tableau 8 Les principales solutions de plateformes Cloud

CloudStack	OpenStack	Vcloud Director
Plateforme clé en main Opensource, licence Apache 2.0 Géré par la fondation Apache comme un Top Level Project Pérennité, stabilité, qualité du code API native, interface web Utilisé par de nombreux FAI dont Ikoula	Opensource, licence Apache API, Interface web Architecture très modulaire, nombreux projets corrélés Utilisé par de nombreux FAI dont OVH et les clouds souverains Cloudwatt et Numergy	Propriétaire, VMware Soumis à licence Basé sur VMware Vsphere Elasticité, scalabilité API ouverte Contrôle de la consommation des ressources

Tableau 9 Solutions de plateformes Cloud alternatives

OpenNebula	Eucalyptus
Plateforme clé en main Opensource, licence Apache 2.0 Existe depuis 2005	Opensource, licence BSD Cloud Hybride compatible Amazon Web Service (AWS) Remplacée par OpenStack sur les distributions Ubuntu Rachetée par Hewlett-Packard

IV.2.2 Les hyperviseurs disponibles sur le marché

Un hyperviseur est une couche d'abstraction logicielle. Il assure les tâches de bas niveau, comme l'ordonnancement du CPU et l'isolation de la mémoire utilisée par les machines virtuelles. L'hyperviseur rend le matériel abstrait pour les VM, il est le seul à avoir la connaissance du réseau, du stockage ou des ressources graphiques. Les VM sont ainsi indépendantes de la plateforme physique.

Le choix de l'hyperviseur est crucial. Il déterminera les fonctionnalités de la plateforme et les performances des machines invitées.

L'éventail dans le domaine est large, allant de l'offre propriétaire très onéreuse à la solution opensource.

ESXi (VMware)	XenServer (Citrix)	KVM
Micro-noyau Encombrement à 150 Mo Surface d'attaque très réduite Sous licence pour activer les fonctionnalités avancées	Hyperviseur Xen opensource Intégré au noyau linux Optimisation des systèmes Linux et BSD Librement téléchargeable	Kernel-based Virtual Machine Fonctionnalité du noyau linux Bien intégré aux solutions opensource Très bien soutenu de la communauté

Une présentation plus détaillée des hyperviseurs du marché est fournie en Annexe 5.

IV.2.3 Solutions d'externalisation

Avant de déployer une architecture de cloud pour la formation en interne, il peut être interessant de comparer les solutions de cloud privé avec les solutions d'externalisation.

Quelles sont les types d'offres existants sur Internet ?

Des prestataires de services (comme OVH ou Ikoula) proposent :

- la location de serveurs privés virtuels, correspondant à des instances dans leurs architectures cloud :
  - OpenStack-KVM pour OVH ;
  - CloudStack-Xen pour Ikoula.
- la gestion de « clouds privés dédiés ou infogérés ».

IV.2.3.1 Les serveurs virtuels privés

L'hébergeur OVH [3] est un leader du marché. Il propose plusieurs gammes de VPS (Virtual Private Server), dont la gamme VPS SSD qui est leur entrée de gamme. Son offre est détaillée ci-dessous [4] :

Tableau 10 Prix de la gamme VPS SSD de chez OVH

VPS SSD 1	VPS SSD 2	VPS SSD 3
KVM OpenStack	KVM OpenStack	KVM OpenStack
1 vCPU 2,4 Ghz	1 vCPU 2,4 Ghz	2 vCPU 2,4 Ghz
2 Go RAM	4 Go RAM	8 Go RAM
SSD 10 Go	SSD 20 Go	SSD 40 Go
3,59€ TTC / mois	7,19€ TTC / mois	14,39€ TTC / mois

L'avantage de la solution est de se libérer totalement du travail d'administration, des pics de charge et donc des contraintes d'élasticité.

IV.2.3.2 Le cloud dédié

Ces clouds sont prêts à l'emploi, disponibles en 30 minutes. Ils s'appuient sur VMware Vsphere (la licence est incluse) avec comme avantages :

- administration système minimale ;
- pas de maintenance matérielle (changement d'un hôte défecteux en 15 minutes) ;
- haute disponibilité ;

3 OVH : http://www.ovh.com
4 https://www.ovh.com/fr/vps/vps-ssd.xml

- élasticité de la solution.

Caractéristique d'un hôte L+[5] :

Tableau 11 Caractéristiques d'un hôte L+ du cloud dédié OVH

Caractéristique	Valeur
Coeur/Thread	16 / 16
Fréquence	3.1 Ghz
RAM	128 Go
Coût	503, 51€ TTC
Puissance processeur totale	49.6 Ghz

L'infrastructure propose 2x300 Go d'espace de stockage, 1,5 Gbit/s de bande passante en sortie, un réseau avec 4000 vLAN.

Un hôte L+, avec un facteur de surallocation processeur de 2, peut ainsi accueillir 100 VM 1 vCPU / 1 Go RAM (sans surallocation de RAM).

2 types d'externalisation s'offrent donc à l'ETRS, avec chacune leurs avantages et leurs inconvénients. Nous ne retenons toutefois pas ces solutions, car la formation est le cœur de métier de l'École. Elle doit garder la maîtrise de ses outils de formations : une entreprise n'externalise pas son cœur de métier !

- Que se passe t'il pour l'ETRS si l'hébergeur décide de mettre fin à l'offre ou d'augmenter fortement ses tarifs ?
- En cas de coupure Internet (panne, attaque DDOS), nous pouvons poursuivre les formations avec la solution de cloud privé.

Le monde de la virtualisation et du cloud computing est un monde complexe, riche en solutions élaborées dont certaines parmi les meilleures appartiennent au monde de l'open source.

L'état de l'art ayant défini les différentes options offertes à l'ETRS, le choix de la solution et de l'hyperviseur associé peut être effectué.

[5] https://www.ovh.com/fr/dedicated-cloud/hosts.xml

IV.3 Discussions et solution retenue

L'ETRS met en œuvre plusieurs configurations VMware ESXi et Vcenter au profit de ses plateformes de formation informatique (PFI).

Malgré la qualité indéniable des solutions VMware et les fonctionnalités avancées de ces produits, le coût particulièrement élevé des licences tant dans l'achat initial que dans leur maintien à niveau amène les responsables informatiques à explorer d'autres solutions techniques.

Compte tenu du besoin estimé pour le Cloud Formation en mémoire, processeurs et espace de stockage, la solution Vwware Vcloud Director s'avère prohibitive sur le plan budgétaire, le coût des licences dépassant le coût du matériel.

La solution VMware Vcloud Director est donc écartée du projet pour des raisons financières.

A partir de l'enveloppe budgétaire, le choix a été fait de privilégier l'achat d'équipements incontournables (stockage, serveurs, commutateurs) en recherchant l'adoption d'un cloud opensource sans écarter l'assistance d'une prestation d'une SSII spécialisée pour la construction de l'architecture.

En fonction du retour d'expérience sur le projet Cloud Formation, les choix techniques confirmés seront étendus à d'autres plateformes de formation (CAN-ENT par exemple) en remplacement des licences VMware.

Les deux solutions OpenNebula et Eucalyptus sont des projets dont le soutien principal est effectué par des sociétés. Leur pérénité à long terme et leurs perspectives d'évolutions sont plus incertaines que pour les deux grands acteurs actuels du domaine que sont CloudStack et OpenStack.

Pour ces raisons liées à la maintenabilité, les solutions OpenNebula et Eucalyptus sont également écartées du projet.

IV.3.1 Le choix de la solution : OpenStack ou CloudStack ?

Ces deux plateformes logicielles open-source de gestion de cloud privé offrent les mêmes services et ciblent les mêmes types d'entreprises [Jacobs-2015].

La longue liste de membres de la fondation OpenStack fait penser que ce projet dispose de nombreux soutiens. A contrario, la fondation Apache ne propose pas de listes de sociétés contributrices, bien qu'elle annonce tout de même une centaine d'organisations ayant déployé CloudStack en production, il est donc difficile de se faire une idée du poids d'un projet par rapport à l'autre.

Lorsqu'un contributeur participe à un développement, pour la fondation Apache, c'est son nom qui doit être cité et non celui de la société qui l'emploi, ce qui explique l'absence d'une telle liste de sociétés contributrices. Citrix en affiche tout de même certaines sur son site, comme Brocade, Cisco, Juniper Networks ou PuppetLabs.

OpenStack semble suivre un rythme de développement plus soutenu. Le fait que des hébergeurs comme OVH appuient leurs stratégies sur cet outil font de lui un choix de

poids. Toutefois sa mise en œuvre est beaucoup plus complexe que CloudStack, comme évoqué par Juliette Paoli dans son récent article [Paoli-J], malgré les efforts des éditeurs, comme RedHat ou Ubuntu, afin de proposer des solutions packagées. Son évolution rapide est également le signe du manque de maturité et de stabilité du projet, ce qui rend les opérations de mises à jour plus complexes. Il est peut être prématuré de le mettre en production.

La communication autour de CloudStack se fait plus discrète qu'autour d'OpenStack. Ce projet est géré comme un TLP par la fondation, ce qui est tout de même un gage de stabilité et de pérennité. J'ai tout de même demandé à un contributeur du projet CloudStack la raison de ce manque de communication. Sa réponse a été courte : « C'est une histoire de course au budget marketing perdue d'avance… »

Contrairement à OpenStack, pour qui chaque brique de l'infrastructure doit être installée puis configurée pour que l'ensemble fonctionne, CloudStack est une plateforme « clé en main », censée fonctionner tout de suite après son installation.

Le choix d'une plateforme par rapport à l'autre a fait l'objet de nombreux articles sur les blogs de l'Internet :

- Pour certains dont David Linthicum [linthium-2014], CloudStack a déjà perdu face à OpenStack : *« CloudStack est une bonne alternative à OpenStack, qui a gagné le marché des plateformes cloud open source. Bien entendu, « gagner » est un terme relatif […] »* face aux fournisseurs de cloud commerciaux publics comme Microsoft, Google ou Amazon Web Services.
- D'autres comme Simon Phipps, pensent le contraire [phipps-2014]. Dans son article, il cite Giles Sirett : « CloudStack est un produit (utilisateurs) ; OpenStack est une boîte à outils (vendeurs). » Ce n'est pas étonnant qu'il y ait une différence dans le bruit fait par chacun... Il cite également Rohit Yadev de la société ShapeBlue « CloudStack fonctionne, alors c'est ennuyeux ; OpenStack nécessite une grosse équipe, beaucoup de claviers pour le faire fonctionner. »
- Pour Xavier Buche, dans son mémoire « Cloud universitaire avec OpenStack » [buche-2015], « OpenStack est LA solution de cloud IaaS sujet de toutes les discussions ». Il estime que « Cet ensemble logiciel a acquis une telle popularité que «cloud privé» est désormais presque synonyme d'«OpenStack» ». Pour lui, c'est la modularité qui est le principal avantage d'OpenStack par rapport à ses concurrents. « Elle permet à chaque opérateur de créer sa propre architecture, parfaitement adaptée à son environnement et ses cas d'utilisation ».

  Sa conclusion est toutefois plus mitigée : « Je comparerai la mise en production d'OpenStack à un long chemin parsemé d'obstacles, jonché de pièges, parcouru d'entraves plus incertaines les unes que les autres. J'ai perdu le compte du nombre de fois où je pensais, à tort, toucher au but. »

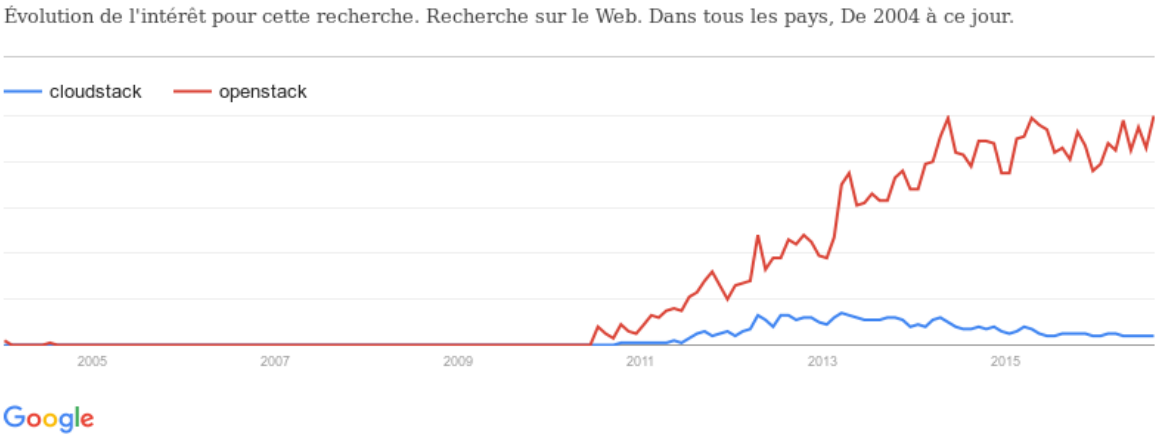


Figure 12 Nombre de recherches contenant les mots CloudStack et OpenStack sur le moteur de recherche Google.

Comme le montre la courbe précédente issue de Google Trends, l'intérêt du public pour la solution OpenStack est supérieur à celui pour le CloudStack. Elle va dans le sens de l'analyse de Xavier Buche.

Alors, quel est le bon choix pour la plateforme de l'ETRS ?

Nous avons recensé au sein du tableau ci-dessous les avantages et les inconvénients de chaque plateforme, sachant que les deux proposent l'ensemble des fonctionnalités qui correspondent à nos besoins :

Tableau 12 Avantages et inconvénients des 2 plateformes

Plateforme	OpenStack	CloudStack
Pour	Déploiement en production plus fréquent	Installation clé en main
	Communauté très active	Stabilité du projet
	Documentation abondante	Projet Apache Software Foundation (ASF)
		Déjà connu du personnel de l'école
		Administration plus aisée
	Technologies de bases connues (CentOS 7, NFS) et fiables	
	Compatibilité avec l'existant donc transition maîtrisable	
	Pas de grosse rupture ou de saut technologique	
Contre	Plus complexe à mettre en œuvre	Documentation en Anglais
	Briques interdépendantes	Evolution moins rapide
	Projet plus jeune, moins mature	
	Evolue (trop) vite ?	

Nous avons également, avec la cellule soutien PFI-ENT, recensé les impératifs de la cellule :

Tableau 13 Les impératifs de la cellule Soutien PFI-ENT.

Impératif	Pondération OpenStack	Pondération CloudStack
Simplicité d'administration	5	10
Elasticité de la solution	10	10
Haute disponibilité	10	10
Fonctionnalités de la plateforme	10	10
Documentation d'administration	8	6
Rythme des évolutions	8	10
Notoriété de la solution	10	8

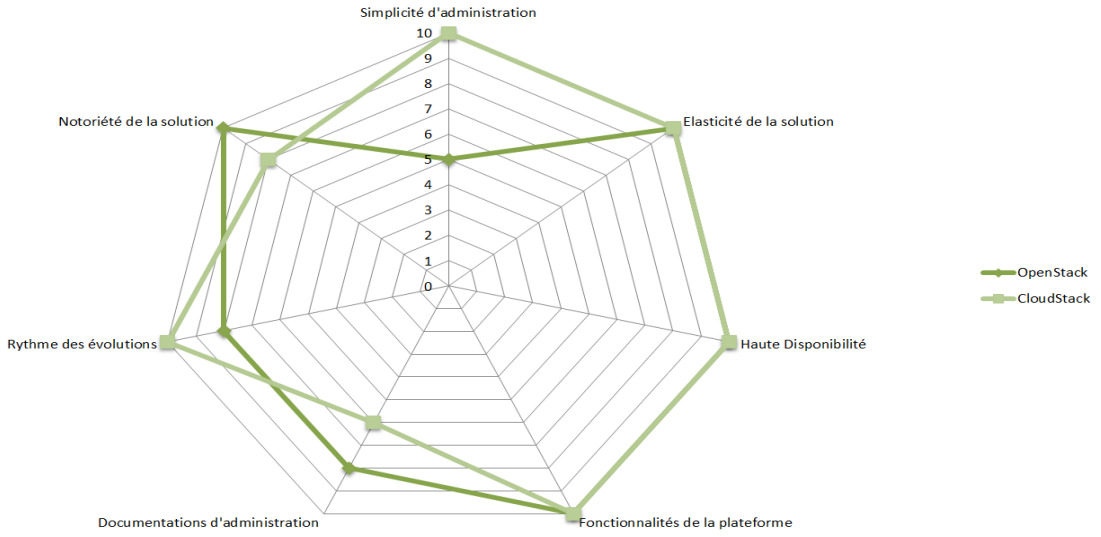


Figure 13 Choix de la solution selon les impératifs de la cellule Soutien PFI-ENT.

- La cellule Soutien PFI-ENT n'est pas dimensionnée pour maintenir un système complexe supplémentaire, le principe de solution « clé en main » et la simplicité d'installation de CloudStack font pencher la balance en sa faveur.
- Le POC de la société APX s'étant appuyé sur CloudStack, la solution est déjà un peu connue du personnel de l'équipe d'administration, ce qui limite l'appréhension d'un nouveau système supplémentaire à maîtriser.
- L'argumentaire de Xavier Buche est tout à fait juste. OpenStack est en train de s'imposer comme le standard de fait du Cloud Computing. CloudStack sera certes l'outsider de ce secteur, mais il sera un concurrent de qualité pour les années à venir. La solution CloudStack a encore de belles années devant elle. Le rythme de mises à jour (tous les 6 mois) vient d'être relancé après un petit temps de flottement au sein du comité d'administration.

L'ensemble des participants au projet, connaissant les tenants et les aboutissants de ce choix, sont d'accord sur le choix technique de la plateforme CloudStack. Il faut à présent choisir l'hyperviseur qui supportera les machines virtuelles.

IV.3.2 Choix de l'hyperviseur

La plateforme CloudStack supporte les principaux types d'hyperviseurs :

Tableau 14 Tableau récapitulatif des principales solutions existantes d'hyperviseur niveau 1.

Nom	Société	Plateforme	OS	OS invité	Licence
XenServer	Citrix	x86_64	XenServer	Linux, Windows, …	GNU GPL v2
ESXi	VMware	x86_64	ESXi		Propriétaire
KVM	RedHat	x86_64	Linux		GNU GPL v2

La cellule Soutien PFI-ENT maitrisant déjà l'environnement CentOS 6 et le logiciel KVM, le choix de ces derniers est tout indiqué (soutien de la communauté, pas de licence, simplicité de mise en œuvre).

Il convient de vérifier que l'ensemble des fonctionnalités techniques requises pour le projet sont supportées par CloudStack :

Tableau 15 Tableau comparatif des fonctionnalités réseaux et stockage des principaux hyperviseurs de niveau 1 prises en charge par CloudStack.

Fonctionnalités	XenServer	ESXi	KVM – RHEL
Groupes de sécurité dans les réseaux basiques	Oui	Non	Oui
iSCSI	Oui	Oui	Oui
FibreChannel	Oui	Oui	Oui
DAS	Oui	Oui	Oui
HA	Oui	Oui (Natif)	Oui
Snapshots des disques locaux	Oui	Oui	Oui
Données sur disques locaux	Oui	Non	Oui
Répartition de charge	Non	DRS	Non
Migration de VM	Oui	Oui	Oui

Tableau 16 Tableau comparatif des fonctionnalités de stockage primaire des principaux hyperviseurs de niveau 1 prises en charge par CloudStack.

Type de stockage	XenServer	vSphere	KVM – RHEL
Format des disques, modèles et snapshots	VHD	VMDK	QCOW2
Support iSCSI	CLVM	VMFS	Oui par point de montage
Support Fiber Channel support	Oui	VMFS	Oui par point de montage
Support NFS	Oui	Oui	Oui
Support du stockage local	Oui	Oui	Oui
Surallocation du stockage	NFS	NFS et iSCSI	NFS
SMB/CIFS	Non	Non	Non

IV.5 Etude des risques

L'Ecole est un organisme militaire, son réseau accessible depuis Internet, le CAN/ENT fait l'objet de tentatives d'attaques régulières. Dans ce contexte de cyberdéfense, l'étude des risques SSI doit évidement faire l'objet d'une attention particulière. L'Agence Nationale de la Sécurité des Systèmes d'Information est dans ce domaine force de recommandations.

Plus pragmatique, une étude des risques liés au projet, au niveau du formateur et de l'administrateur, est également effectuée. Cette démarche permettra de prendre en compte toutes les problématiques liées à ce nouvel environnement de travail. Il en découlera les mesures nécessaires pour répondre à ces risques.

IV.5.1 Problématique SSI en environnement virtuel : recommandations de l'ANSSI

L'aspect virtualisation doit faire l'objet d'une attention particulière, comme le met en garde l'organisme ANSSI dans une de ses recommandations SSI :

> *La virtualisation introduit aussi de nouveaux risques, aussi bien techniques qu'organisationnels, qui viennent s'ajouter aux risques des systèmes d'nformations classiques* [ANSSI-2013].

Par la note technique DAT-NT-011/ANSSI/SDE de l'ANSSI « Problématiques de sécurité associées à la virtualisation des systèmes d'information », l'agence fait des recommandations pour des plateformes comme la notre. Les risques identifiés dans ce document sont résumées dans la liste ci-dessous :

Tableau 17 Risques liés à la virtualisation identifiés par l'ANSSI et solutions

N°	Risques	Solutions
1	Risque accru de compromissions des systèmes	Diminuer au maximum la surface d'attaque Défense en profondeur Durcissement des systèmes invités
2	Accroissement du risque d'indisponibilité	Diminuer au maximum la surface d'attaque Défense en profondeur Durcissement des systèmes invités Utiliser des machines dédiées pour les applications plus sensibles
3	Fuite d'information par manque de cloisonnement	Isolation par réseaux physiques Mécanismes de confidentialités et de contrôle d'intégrité des données
4	Complexification de l'administration et de la mise en oeuvre	
5	Complexification de la supervision	
6	Prolifération non souhaitée des données et des systèmes	
7	Incapacité à gérer voire à comprendre les erreurs	Mettre en place une centralisation et une corrélation des journaux sur l'ensemble des systèmes
8	Investigations post incident plus difficiles	

L'ANSSI recommande ainsi de prendre en compte les éléments suivants :

1. La politique de sécurité du système faisant l'objet d'une démarche de virtualisation doit être mise à jour pour qu'y soient inclus certains items spécifiques à la technologie de virtualisation employée.
2. Un processus de veille des vulnérabilités propres aux technologies de virtualisation utilisées au sein de l'organisme doit être mis en place.
3. Réduire la surface d'attaque de la solution de virtualisation.
4. Concevoir une architecture respectant le principe de cloisonnement.
5. Utiliser des matériels gérant le cloisonnement.
6. Mettre à jour le plan de reprise ou de continuité d'activité.
7. Dédier une équipe d'administration à la solution de virtualisation distincte de celle des systèmes invités.
8. Prévoir une équipe d'administration des machines virtuelles (systèmes invités) indépendante de l'équipe d'administration de la solution de virtualisation.
9. Former les équipes d'administration, d'audit et de supervision aux techniques de virtualisation.

De ces 9 recommandations, les points suivants seront appliqués :

- Mise à jour de la documentation de sécurité ;
- Mise en place des outils de veille, de supervision et d'agrégation des logs ;
- Installation minimale des systèmes d'exploitation, durcissement de la configuration ;
- Séparation physique des réseaux ;
- Sensibilisation des responsables de cours sur les problématiques liées à la plateforme : droits d'administration des plateformes, prolifération des systèmes, gestion des mots de passe des machines virtuelles.

IV.5.2 Démarche AMDEC simplifiée des risques liés au processus de formation

En complément de l'étude des risques SSI, une analyse au niveau du processus de formation est nécessaire. La plateforme de Cloud apporte également dans ce domaine sa part de nouveaux risques. Afin de les déceler et de mettre en œuvre les outils permettant de les limiter, une étude des risques a été menée Celle-ci a été effectuée en suivant une démarche simplifiée de type **AMDEC** (Analyse des Modes de Défaillances, de leurs Effets et de leur Criticité).

Une étude menée avec les formateurs des différents cours a permis de dresser une liste exhaustive des risques :

- Accès frauduleux aux VM de devoirs
- Incompatibilité de la plateforme avec les nouveaux systèmes
- Incomptabilité des cours avec la plateforme
- Indisponibilité de la plateforme pendant les cours
- Indisponibilité de la plateforme pendant les devoirs
- Indisponibilité du serveur CAS
- Manque de ressources
- Manque de réactivité de l'affichage
- Mauvais cloisement VLAN
- Perte du lien internet
- Réactivité du service soutien.

Je leur ai ensuite demandé de classer ses risques en fonction de leur criticité et de la probabilité qu'ils surviennent. Le résultat de ce travail est résumé dans le tableau ci-dessous :

Tableau 18 Impact et probabilité des risques sur le Cloud Formation selon les formateurs

Risque	Impact	Probabilité
Accès frauduleux aux VM de devoirs	Critique	Faible
Incompatibilité de la plateforme avec les nouveaux systèmes	Elevé	Moyen
Incomptabilité des cours avec la plateforme	Important	Faible
Indisponibilité de la plateforme pendant les cours	Elevé	Faible
Indisponibilité de la plateforme pendant les devoirs	Critique	Moyen
Indisponibilité du serveur CAS	Moyen	Faible
Manque de ressources	Moyen	Faible
Manque de réactivité de l'affichage	Moyen	Faible
Mauvais cloisement VLAN	Elevé	Faible
Perte du lien internet	Faible	Faible
Réactivité du service soutien	Important	Moyenne

En établissant le tableau des valeurs AMDEC suivant, nous avons pu établir une matrice de risques à appliquer au projet Cloud Formation :

Tableau 19 Tableau des valeurs AMDEC

Valeur AMDEC	Impact faible	moyen	important	élevé	critique
Classement	**C**	**C**	**C**	**B**	**A**

A : Haute criticité B : Criticité importante C : Criticité faible

Tableau 20 La matrice des risques du projet Cloud Formation

Impact / Probabilité	Impact faible	moyen	important	élevé	critique
faible	**C**	**C**	**C**	**B**	**A**
moyenne	**C**	**C**	**B**	**B**	**A**
importante	**C**	**C**	**B**	**A**	**A**
élevée	**B**	**B**	**B**	**A**	**A**
critique	**A**	**A**	**A**	**A**	**A**

En appliquant la matrice de risques, nous avons pu classer les risques selon leur criticité :

Tableau 21 Classement des risques en fonction de leur criticité.

Risque	Criticité
Indisponibilité de la plateforme pendant les devoirs	A
Accès frauduleux aux VM de devoirs	A
Réactivité du service soutien	B
Incompatibilité de la plateforme avec les nouveaux systèmes	B
Mauvais cloisement VLAN	B
Indisponibilité de la plateforme pendant les cours	B
Incomptabilité des cours avec la plateforme	C
Indisponibilité du serveur CAS	C
Manque de réactivité de l'affichage	C
Manque de ressources	C
Perte du lien internet	C

La mise en place de la démarche AMDEC souligne les aspects critiques à prendre en compte lors de la conception :

- Possibilité de Haute Disponibilité et redondance des moyens. Le matériel utilisé en phase 1 fera l'objet d'un recyclage pour assurer la haute disponibilité dès la phase 2.
- Sécurisation de l'accès aux moyens de gestion des VM, gestion d'un profil Formateur disposant d'accès moins restrictifs que les accès du profil Stagiaire.

De cette matrice des risques, les points suivants seront appliqués :

- Mise en œuvre d'une solution de redondance, dès que les capacités matérielles seront suffisantes pour rendre possible la haute disponibilité ;
- Mise en place de profils avec des droits différents pour les formateurs et les stagiaires. Le processus de gestion des devoirs prendra en compte l'impossibilité de modifier a posteriori un devoir par le stagiaire.

La mise en place d'une plateforme de cloud privé est un choix technique qui répond aux attendus de l'ETRS, sous contrainte des exigences de sécurité informatique et de stabilité de son infrastructure système et réseaux.

Après avoir débattu des avantages et inconvénients de chaque solution parmi celles présentées et validé les capacités d'administration de la section soutien PFI-ENT tout en prenant en compte les impératifs de gestion, les différents acteurs du projet estiment que les solutions CloudStack et l'hyperviseur KVM sont aujourd'hui les plus adaptées au besoin et sont donc choisies pour la suite du projet.

Il faudra garder à l'esprit durant la phase de conception que le Cloud Formation doit être conçue en ménageant une capacité d'adaptation des ressources (mémoire, processeur, espace de stockage) mais aussi des services (l'augmentation des besoins par rapport aux actuels est inexorable), en particulier si la plateforme s'ouvre aux autres groupements de l'ETRS (systèmes de communications, cyberdéfense et guerre électronique).

L'élasticité (augmentation ou réduction des capacités) de la plateforme et la simplicité d'administration sont identifiées comme des exigences critiques pour la section Soutien PFI-ENT tandis que la haute disponibilité de la plateforme est un élément majeur pour les formateurs, notamment durant le déroulement des devoirs.

La sécurisation de la plateforme, de part l'aspect militaire du projet, est à intégrer dans toute la démarche de conception et de réalisation à venir.

V Conception

En se basant sur l'analyse des solutions existantes, Apache CloudStack est retenue comme plateforme de cloud privé, pour sa simplicité d'installation et d'administration, son élasticité, ses fonctionnalités de haute disponibilité et pour la stabilité de son développement.

Une analyse plus approfondie de la solution est maintenant nécessaire pour s'assurer que la plateforme répond à la totalité du besoin des clients.

Il faut choisir le matériel et définir la topologie du réseau.

Une étude financière est également effectuée durant cette étape de conception.

La gestion des machines virtuelles des devoirs et la reprise de l'existant font l'objet d'une démarche spécifique.

V.1 Définition des phases de déploiement

Le bon de commande pour le matériel nécessaire à la plateforme ayant été accepté par la DIRISI centrale (janvier 2016), le projet de cloud a été relancé. Le matériel tardant a être finalement commandé et livré, le projet a été scindé en plusieurs phases :

La phase 1 de déploiement :

Durant la phase 1, il est prévu de :

- Mettre en production la plateforme avec du matériel existant et les 2 NAS qui ont été livrés ;
- Evaluer les capacités existantes et nécessaires ;
- Péréniser l'infrastructure ;
- Former les administrateurs et les formateurs ;
- Créer les modèles de machines virtuelles.

La phase 2 de déploiement :

Le lancement de la phase 2 est prévu dès la réception du matériel commandé :

- Intégration des serveurs dans la plateforme ;
- Validation de l'élasticité ;
- Mise en place de la redondance et de la haute disponibilité ;
- Début de l'exploitation par les stagiaires ;

La phase 3 de déploiement :

La phase 3 s'inscrit dans une démarche sur le long terme. Les investissements requis seront justifiables par la réussite de la phase 2.

- Dimensionnement de la plateforme en fonction des moyens, des besoins, et des nouvelles opportunités (classes virtuelles ou formation à distance).

V.2 La plateforme CloudStack

V.2.1 Les fonctionnalités de la plateforme

CloudStack apporte une plateforme d'orchestration de cloud ouverte et flexible pour créer un cloud privé :

- CloudStack est basé sur Java, il est constitué d'un serveur de gestion et d'agents pour les hyperviseurs ;
- il fonctionne avec les hyperviseurs XenServer, KVM, Hyper-V et VMware ESXi ;
- dispose une interface Web de gestion ;
- présente une API native (rendant possible l'automatisation des tâches) ;
- assure le stockage des instances fonctionnant sur les hyperviseurs, les modèles de machines virtuelles, les snapshots et les images ISO ;
- propose des services réseaux depuis la couche 2 du modèle OSI jusqu'à certains protocoles de la couche 7 comme le DHCP, le DNS, le NAT, le firewall et le VPN ;
- gère les identités des utilisateurs ;
- orchestre le provisionnement automatique des machines virtuelles ;
- procure un accès aux consoles de gestion des serveurs ;
- permet de transformer une machine virtuelle en modèles (via un instantané) ;
- met en œuvre deux types de configuration (basique ou avancée basée sur les VLANs).

V.2.2 Vocabulaire et éléments constituants de la plateforme

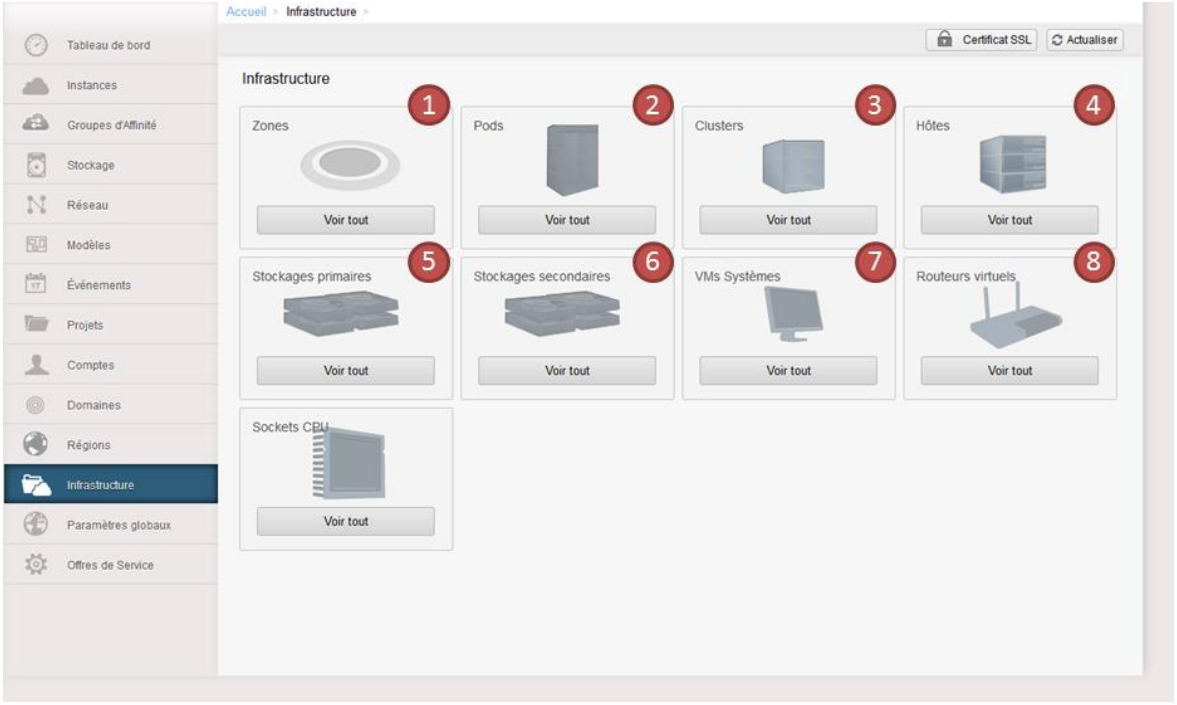


Figure 14 Configuration de l'infrastructure dans l'interface de gestion de CloudStack

Un schéma simplifié d'une architecture CloudStack avec le minimum de composant ressemble à :

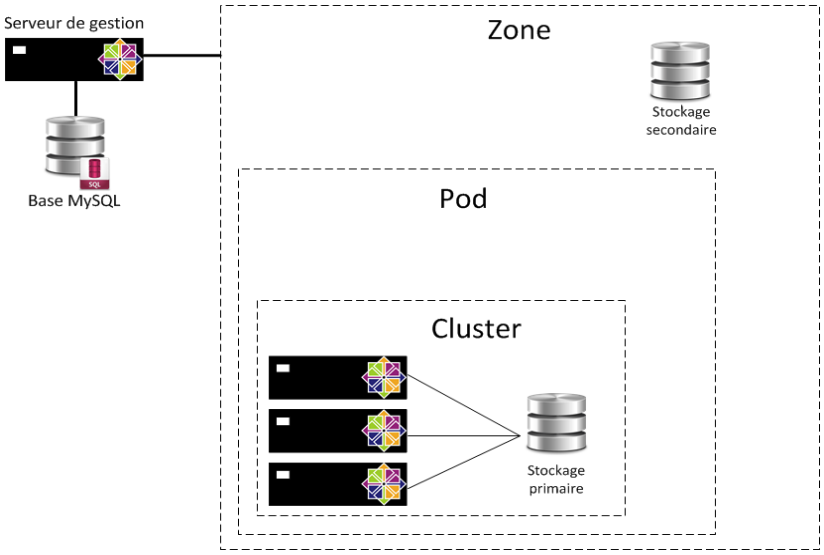


Figure 15 Schéma conceptuel d'un déploiement CloudStack simple

Les zones

Une **zone**[1] est la plus grande unité organisationnelle dans CloudStack et correspond typiquement à un centre de données.

Une zone est constituée :

- d'un ou plusieurs pods[2] ;
- d'un serveur de stockage secondaire[6].

2 types de zones sont disponibles :

1) La zone basique s'articule autour d'un réseau physique unique, partagé par tous les composants de CloudStack. Chaque instance de machine virtuelle se voit attribuer une adresse IP publique. L'isolation des invités est assurée par l'application de groupes de sécurité (filtrage de l'adresse IP source qui est autorisée à se connecter à un port ou à un groupe de ports) ;
2) La zone avancée est conseillée pour des topologies de réseau plus sophistiquées :
   - ce modèle de réseau apporte plus de flexibilité dans la définition des réseaux d'invités,
   - propose des offres personnalisées telles que le support de pare-feu, le VPN ou l'équilibrage de charge,
   - les machines virtuelles sont interconnectées entre elles par des réseaux privés, ce qui les isole des réseaux extérieurs et améliore leur sécurité,
   - l'accès aux machines virtuelles depuis l'extérieur de la plateforme se fait par des règles de transmissions de port (NAT statique ou dynamique) ou par VPN.

Chaque zone doit avoir au moins un serveur de stockage secondaire. Le stockage secondaire entrepose les modèles, les supports ISO et les images disques des volumes des machines virtuelles. Ce serveur est accessible par tous les hôtes de la zone.

Le réseau

Au sein d'une zone basique, un seul réseau physique, correspondant à une carte réseau sur l'hyperviseur, peut être paramètré. Ce réseau comporte plusieurs types de trafic :

Tableau 22 Séparation du trafic réseaux dans CloudStack

Nom du réseau	Observations
Réseau d'administration	Réservé à l'administration de la plateforme.
Réseau invité	Accès public aux invités de la plateforme.
Réseau de stockage	Facultatif. Optimise l'accès aux ressources des partages NFS.

Chaque réseau dispose de son propre libellé.

Le **réseau invité** supporte la communication entre les utilisateurs et leurs machines virtuelles. Il est donc accessible depuis l'extérieur de la plateforme. Une plage d'adresses IP que CloudStack pourra assigner aux machines virtuelles lui est réservé.

Le **réseau de stockage** assure le trafic entre les ressources internes de CloudStack, incluant tous les composants qui communiquent avec le serveur de stockage primaire, comme les hyperviseurs mais aussi les machines virtuelles si elles utilisent un partage NFS.

Au sein d'une zone avancée, plusieurs réseaux physiques, correspondant à autant de cartes réseaux sur l'hyperviseur, peuvent être paramètrés. Ces réseaux comportent plusieurs types de trafic :

Tableau 23 Séparation du trafic réseaux dans une zone avancée de CloudStack

Nom du réseau	Observations
Réseau d'administration	Réservé à l'administration de la plateforme.
Réseau public	Accès public aux éléments actifs (routeurs, répartiteurs de charge) de la plateforme.
Réseau de stockage	Facultatif. Optimise l'accès aux ressources des partages NFS.
Réseaux invités	Connectivité réseau entre les machines virtuelles. Les réseaux des clients peuvent être cloisonnés par la mise en place de groupes de sécurité ou par des VLAN.

Les pods

Chaque zone contient un ou plusieurs **pods**[2]. Un pod contient les **hôtes**[4] et les serveurs de **stockage primaire**[5]. Une plage d'adresses IP est réservée pour le trafic de gestion interne de CloudStack. Elle doit être unique pour chaque zone dans le nuage.

Un pod peut être vu comme une représentation logique d'une baie informatique physique.

Les clusters

Chaque pod contient un ou plusieurs clusters[3]. Un cluster est un regroupement d'hôtes. Les hôtes exécutent :

- le même hyperviseur ;
- sur du matériel identique ;
- ils sont dans le même sous-réseau ;
- ils accèdent au même stockage partagé.

Chaque cluster comprend un ou plusieurs cœurs et au minimum un serveur de stockage primaire.

Les hôtes

Chaque cluster contient au moins un hôte (hyperviseur) pour exécuter des machines virtuelles invitées. Avant de pouvoir l'intégrer au sein de la plateforme CloudStack, un logiciel type hyperviseur doit être installé ainsi que l'agent CloudStack.

Un hôte est donc un calculateur sous hyperviseur de niveau 1 offrant ses capacités de calcul et de mémoire.

Le stockage des données

Le stockage des données de la plateforme est effectué par un serveur de stockage supportant les protocoles NFS, CIFS (protocole disponible uniquement pour le stockage secondaire) ou ISCSI.

Le stockage primaire

Primary Storage 5 : centralise les données nécessaires aux VM et leurs snapshots.

Le stockage secondaire

Secondary Storage 6 : regroupe les données nécessaires au provisionning : images ISO d'installation ou modèles des machines virtuelles.

Le serveur de gestion (Management Server)

Ce serveur coordonne les multiples fonctionnalités de la plateforme.

Le logiciel CloudStack est installé sur une distribution CentOS 6 ou 7, environnement préconisé par la cellule Soutien PFI-ENT.

Il est développé par la communauté CloudStack en Java. Le serveur applicatif préconisé pour son installation est le serveur applicatif Tomcat (la version 7 est supportée).

Le serveur de gestion CloudStack est à l'écoute sur le port 8080. Un serveur web amont (reverse-proxy) sera nécessaire pour utiliser le port standard 80.

Des dépôts sont gérés par la communauté pour simplifier le déploiement du serveur. Ils sont disponibles pour les distributions CentOS et Debian.

L'agent CloudStack

L'agent CloudStack, installé sur chacun des hyperviseurs, gère les échanges avec le serveur de gestion pour le contrôle des VM.

Le fichier de configuration de l'agent :

- se situe sous : */etc/cloudstack/agent/agent.properties* ;
- regroupe l'ensemble des informations nécessaires à la configuration du logiciel (réseaux physiques, commutateurs virtuels, identifiant des zones, pods) ;
- le script cloudstack-setup-agent simplifie sa configuration.

Le fichier de log, situé sous */var/log/cloudstack/agent/setup-agent.log*, trace l'intégration de l'hyperviseur dans la plateforme.

V.2.3 Schémas conceptuels

Une architecture plus évoluée nécessite la mise en œuvre de plusieurs Pods et Clusters :

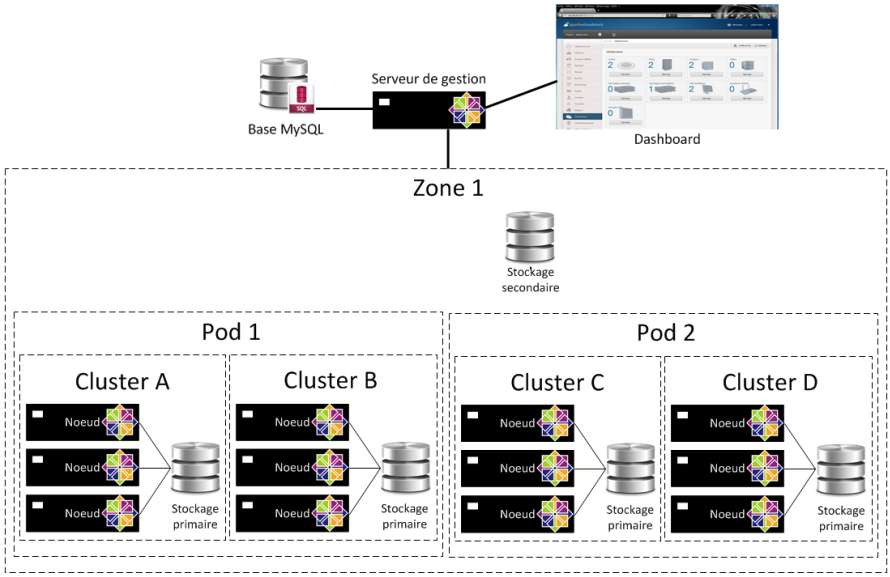


Figure 16 Architecture globale générique d'un système CloudStack

L'administration des composants d'une zone s'effectue à partir d'une interface simple :

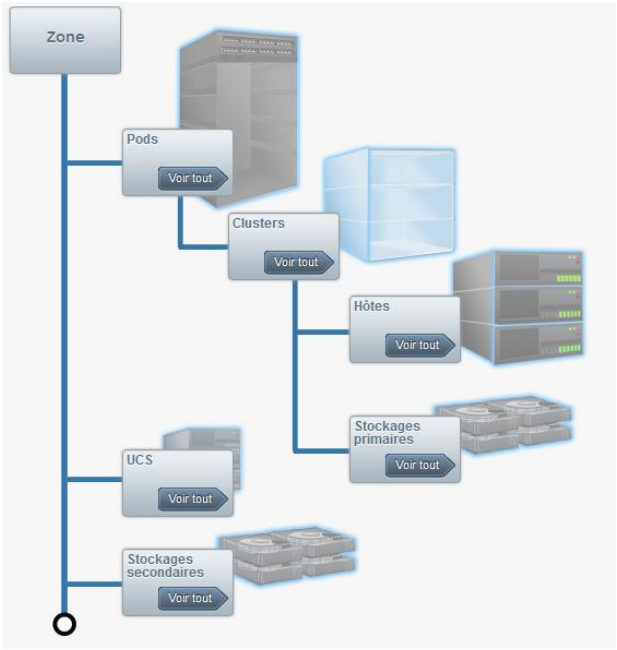


Figure 17 Panneau d'administration d'une Zone dans CloudStack

CloudStack procure une interface de gestion des élements le constituant. Ci-dessous une visualisation de l'infrastructure en phase 1 :

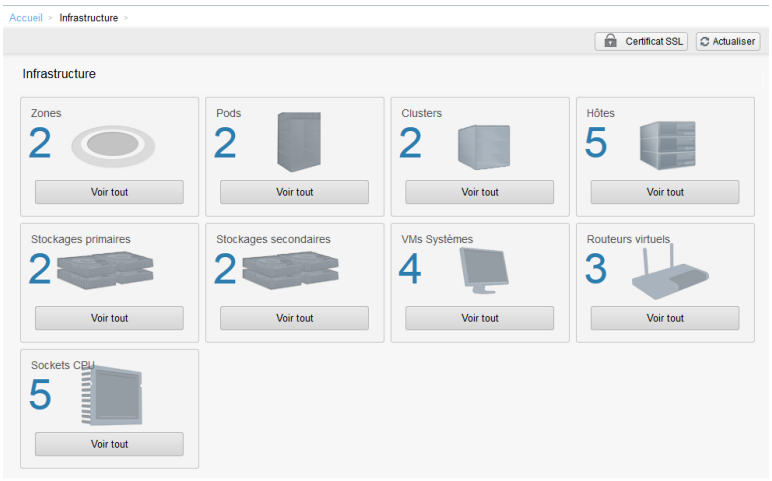


Figure 18 Panneau d'administration de l'infrastructure CloudStack finale

La vision et l'accès aux composants de l'infrastructure sont limités en fonction du profil de l'usager (administrateur, formateur ou stagiaire).

La navigation dans l'interface de gestion est facilitée par la connaissance des termes utilisés pour désigner les différents éléments constituant une infrastructure.

V.2.4 Le réseau virtuel

Les hyperviseurs KVM présentent à leurs invités un commutateur virtuel de niveau 3, créé grâce à la librairie **libvirt**.

Libvirt est utilisée entre autres par KVM, XEN, VirtualBox et VMware. Elle contient des APIs, des outils et un démon pour orchestrer la virtualisation.

Libvirt est l'implémentation native sous Linux des commutateurs virtuels, OpenVswitch est une alternative.

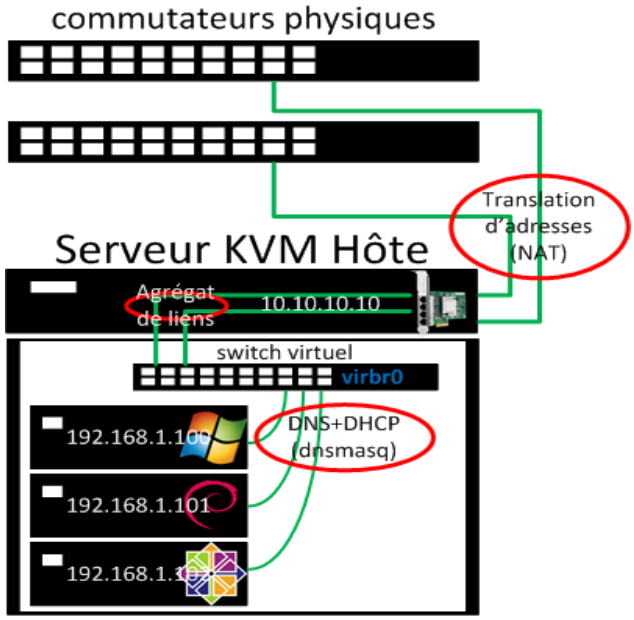


Figure 19 Schéma de fonctionnement d'un commutateur virtuel

Avec translation d'adresse

Par défaut, un commutateur virtuel fonctionne en mode NAT (avec une translation d'adresse), il utilise la technique de *masquerading* (l'adresse IP du commutateur est utilisée comme adresse externe). Les systèmes invités peuvent joindre l'extérieur, mais un serveur placé à l'extérieur du réseau physique de l'hôte ne peut pas initier de connexion vers les systèmes invités.

Le commutateur virtuel dispose d'une plage d'adresses IP, qu'il distribue aux invités via le service DHCP.

Avec un réseau par pont

Un commutateur virtuel peut également être configuré en mode « pont ». Dans ce mode, toutes les machines virtuelles disposent de leur propre adresse. Au sein de CloudStack, une machine virtuelle système, la VRVM (Virtual Routeur Virtual Machine), est dédiée au routage des paquets à destination d'une adresse IP publique vers les adresses IP de ces commutateurs virtuels.

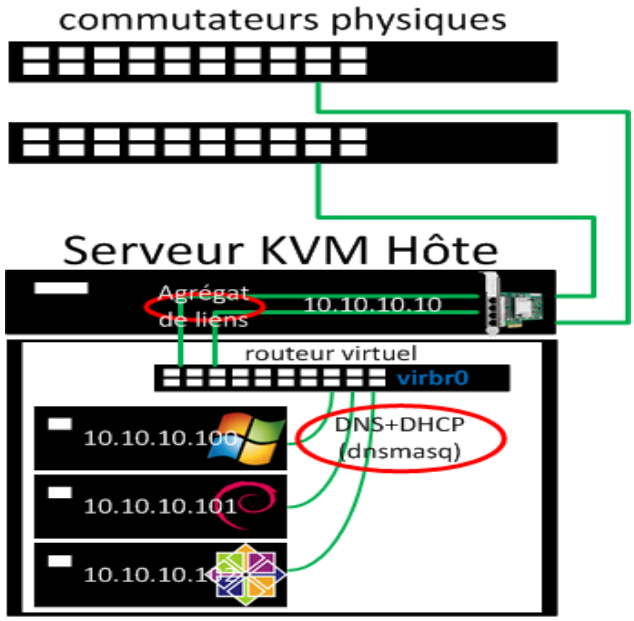


Figure 20 Schéma de fonctionnement d'un routeur virtuel

V.2.5 Architecture réseau

Le fonctionnement des commutateurs virtuels au sein d'un nœud de la plateforme ne disposant que de deux interfaces réseaux est schématisé dans la figure ci-dessous[6] :

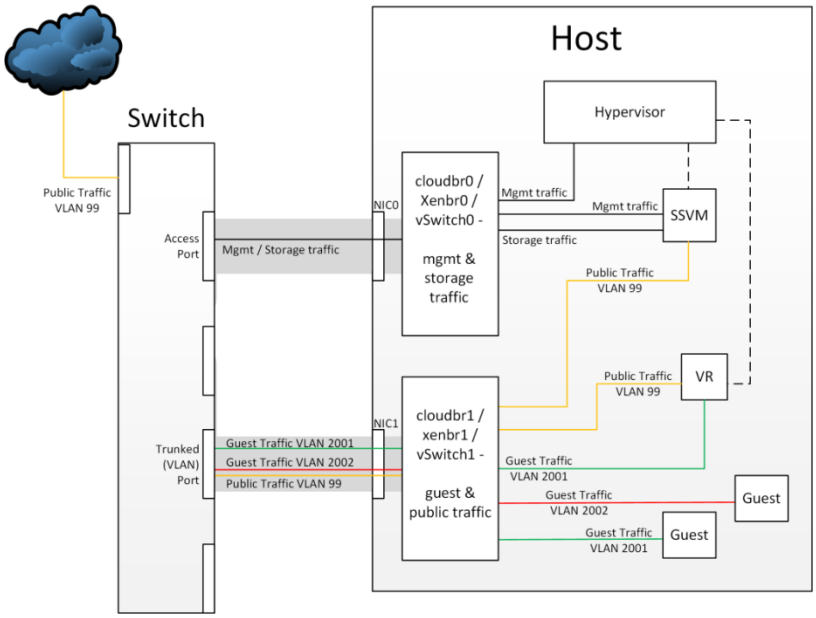


Figure 21 Fonctionnement des commutateurs virtuels au sein d'un nœud

[6] Source : http://www.shapeblue.com/understanding-cloudstacks-physical-networking-architecture/

Chaque interface implémente un commutateur virtuel.

Lorsque le cloisonnement des réseaux invités est recherché (dans le cas d'une zone avancée uniquement), il est nécessaire de mettre en place un agrégat de VLAN (trunk) au niveau du commutateur physique.

Les exigences SSI imposent le cloisonnement physique des réseaux. Ce cloisonnement est recherché dès la phase 1. Les serveurs utilisés n'étant alors équipés que de deux interfaces, les flux ont été séparés conformément au schéma précédent. La commande de 6 cartes réseaux à 2 interfaces gigabits a par la suite rendu possible l'isolation du réseau de stockage sur le commutateur virtuel cloudbr2 et les réseaux invités sur le commutateur virtuel cloudbr3.

La sécurité de la plateforme a été améliorée (trafic invité isolé physiquement du trafic public et du réseau de gestion ; isolation physique des NAS et du trafic client) et les flux optimisés (isolation du trafic de stockage).

La configuration du réseau retenue est la suivante :

Tableau 24 Architecture du réseau retenue

Flux	VLAN	Interface/Commutateur virtuel
Administration	Prod	eth0/cloudbr0
Stockage	Stor	eth1/cloudbr1
Public	Pub	eth2/cloudbr2
Invités	500 à 600	eth3/cloudbr3 uniquement en zone avancée. Trunk de VLAN au niveau du commutateur physique.

V.2.6 Les machines virtuelles (VM) systèmes

Le serveur de gestion CloudStack peut déployer 3 types de machines virtuelles : une première pour gérer les espaces de stockage (copies des modèles, des ISO, des instantanés), une seconde pour gérer les connexions aux consoles des machines virtuelles via VNC (Virtual Network Computing – « informatique virtuelle en réseau ») et une troisième pour le routage virtuel. La connaissance du fonctionnement de ces 3 machines virtuelles systèmes est un pré-requis au bon déroulement de l'installation et de la configuration de la plateforme.

Durant le déploiement, il est d'ailleurs parfois nécessaire de se connecter directement à ces machines virtuelles pour analyser les logs (voir Annexe 5 – Rappels techniques Linux).

La VM proxy CPVM

CloudStack procure la prise de contrôle d'une machine virtuelle grâce à VNC. VNC est un logiciel client/serveur qui transmet les saisies du clavier et les mouvements de la souris depuis un client (la visionneuse) vers le serveur dont le contrôle a été pris.

Le protocole VNC n'est pas un protocole sécurisé par défaut : pas d'authentification, pas de chiffrement des données.

Libvirt s'appuie sur QEMU-KVM qui est capable de rediriger la sortie graphique standard d'une machine virtuelle vers son serveur VNC, pour en prendre le contrôle à distance.

L'utilisateur de la plateforme accède à sa VM via une inteface web AJAX présentée par le serveur de gestion. Cette interface se connecte à la VM CPVM (Console Proxy Virtual Machine) par son adresse IP publique. La CPVM fait ensuite office de mandataire vers l'hôte gérant la VM cible sur le port qui lui est dédié (dans l'interval 5900 à 6100) sur le réseau des invités.

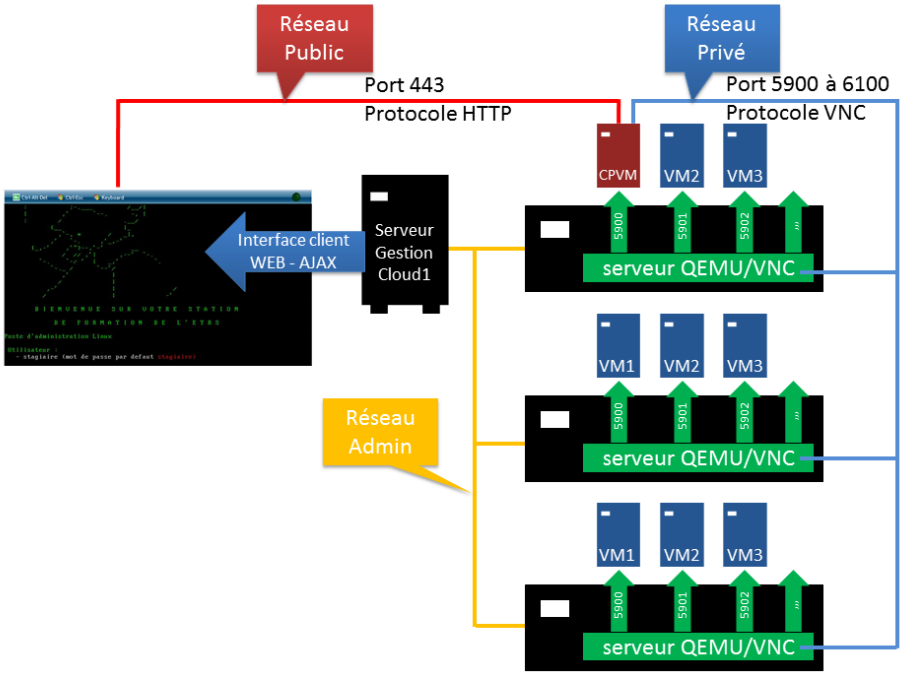


Figure 22 Principe de fonctionnement de la CPVM

La VM de gestion du stockage SSVM

La Secondary Storage Virtual Machine est chargée du déploiement des modèles et primaires. Cette copie à lieu lors de la première utilisation de la ressource (création d'une instance, montage d'un CD-ROM) si celle-ci n'est pas déjà disponible sur le stockage primaire.

La SSVM est également responsable de la copie des instantanés depuis le serveur de stockage primaire vers le serveur de stockage secondaire et de la suppression des ressources non utilisées sur le stockage primaire à l'issue de la période de rétention définie dans les paramètres globaux de CloudStack.

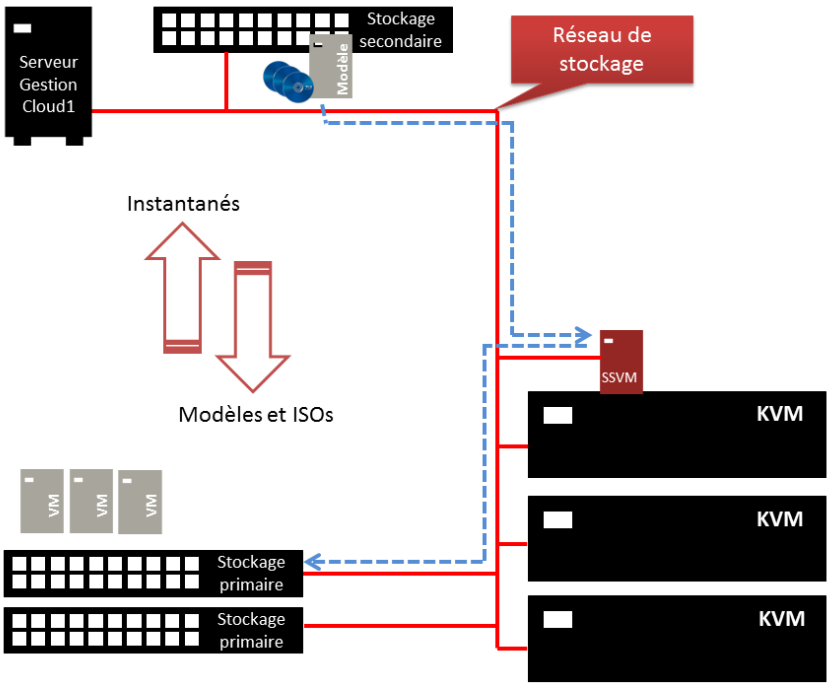


Figure 23 Principe de fonctionnement de la SSVM

La VM Routeur Virtuel VRVM

Chaque machine virtuelle de l'infrastructure CloudStack nécessite un ou plusieurs accès aux réseaux disponibles. Cette connectivité est obtenue grace à la mise en œuvre sur chacun des hôtes d'un ou plusieurs commutateurs virtuels. Ces équipements actifs sont gérés grâce à libvirt.

Dans une zone simple, la machine virtuelle du client dispose d'une adresse IP publique routable vers internet. Dans le cas d'une zone avancée, une adresse IP du réseau des invités est attribuée au serveur, elle n'est pas accessible depuis l'extérieur.

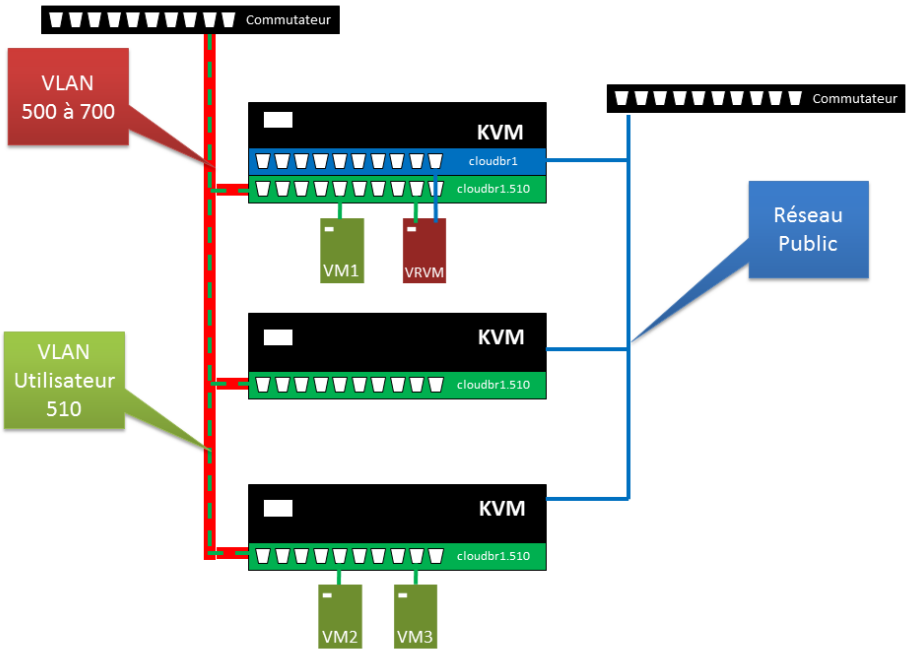


Figure 24 Schéma de fonctionnement de la VRVM dans une zone avancée avec cloisonnement par VLAN utilisateur.

Flux sortants

Pour offrir la connectivité vers l'extérieur aux machines virtuelles, le routeur virtuel effectuera une translation d'adresses sources (NAT SOURCE).

Flux entrants

Pour accèder depuis l'extérieur à une de ses VM, le client pourra au choix :

- se connecter à son réseau via le serveur VPN (Virtual Private Network) de la VRVM ;
- rediriger un port d'une adresse IP publique vers un port d'une adresse du réseau des invités (NAT Dynamique) ;
- rediriger l'ensemble des ports d'une adresse IP publique vers une adresse du réseau des invités (NAT Statique) ;
- utiliser un répartiteur de charge, pour rediriger un port d'une adresse IP publique vers plusieurs machines virtuelles. Les routeurs virtuels hébergent un service de répartition de charge des protocoles se basant sur TCP. Le serveur utilisé est HAProxy. Les règles de répartition de charge sont définies dans l'infrastructure de CloudStack puis appliquées par

l'agent au routeur virtuel.

La configuration de ces possibilités se fait depuis l'interface de gestion de CloudStack :

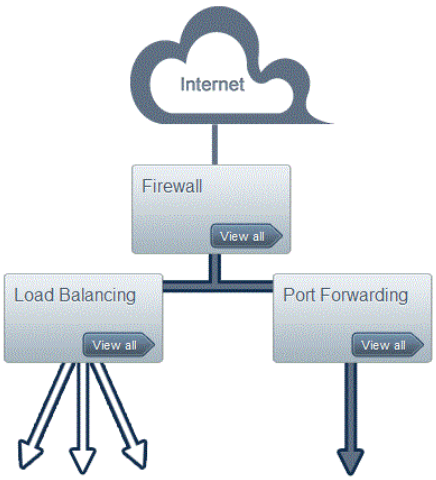


Figure 25 La gestion de l'accès aux VM de la zone avancée depuis l'interface CloudStack.

En résumé, les possibilités pour accéder à des VM de la zone avancée appartenant à un réseau isolé sont multiples et s'adaptent à des besoins variés :

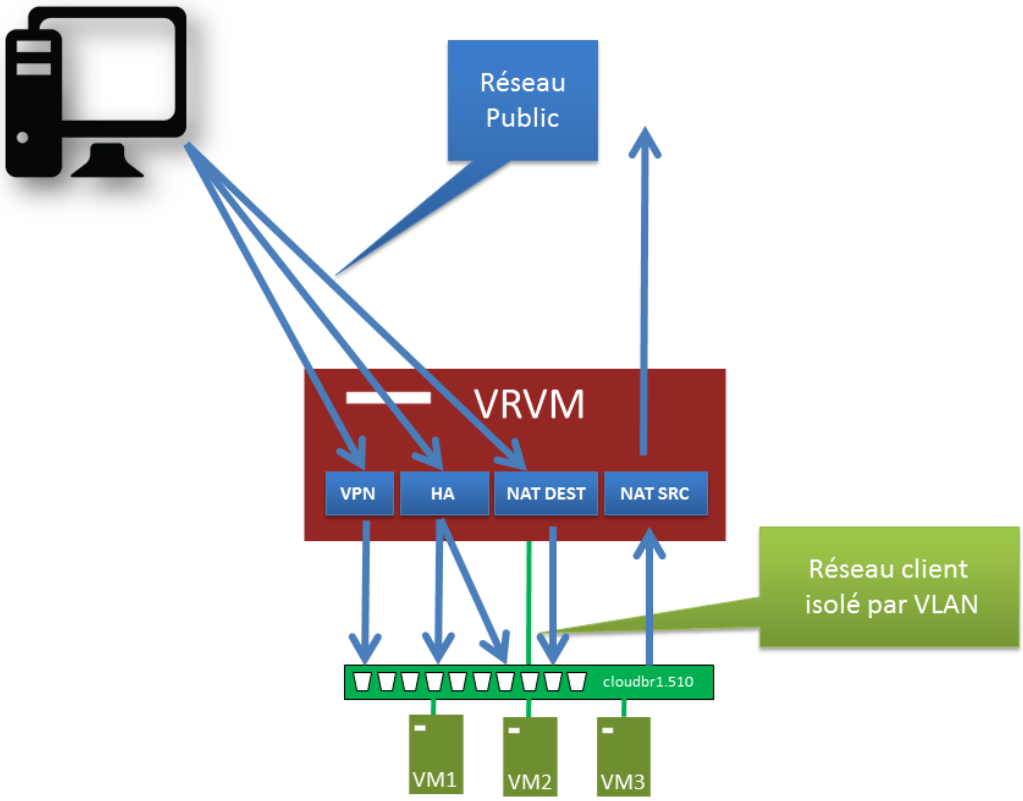
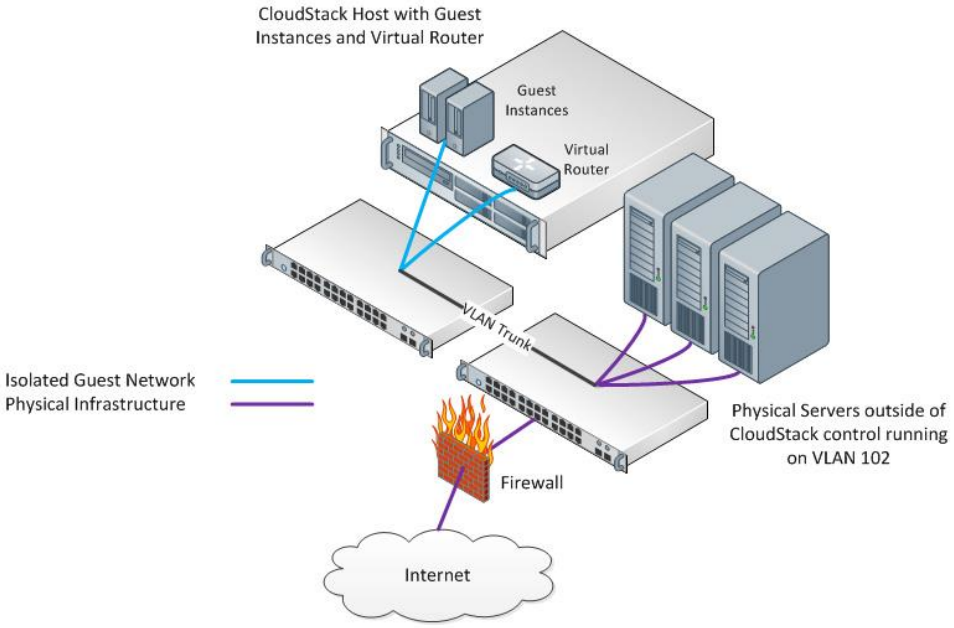


Figure 26 Accès externe à une VM d'une zone avancée.

Ces différentes méthodes isolent totalement le système d'information ce qui augmente sensiblement sa sécurité. L'accès depuis l'extérieur n'est seulement possible que vers un seul port d'une adresse IP publique.

Le choix d'une zone avancée offre des perspectives techniques très intéressantes, illustrées par la figure ci-dessous, issue du site ShapeBlue.com[7] :



[7] ShapeBlue est le plus grand intégrateur indépendant de la technologie CloudStack. http://www.shapeblue.com/using-the-api-for-advanced-network-management/

V.2.7 Présentation du matériel

Les achats de matériels sont centralisés par la DIRISI dans le cadre d'un marché public global. Ils font l'objet d'une validation par la DRHAT (Direction des Ressources Humaines de l'Armée de Terre).

La plateforme en phase 2 sera composée de :

8 serveurs IBM 3550 :

Figure 27 Le serveur IBM x3550 M4

Les 8 calculateurs commandés pour le projet disposent des caractéristiques suivantes :

- serveur 1U IBM x3550 M4 ;
- 2x Intel Xeon QuadCore E5-2603v2 1,8 Ghz 10 Mo de cache (supporte jusqu'à 2 processeurs de 24 cœurs et 48 threads) ;
- 64 Go RAM (supporte jusqu'à 768 Go de mémoire avec des barrettes de 32 Go LRDIMMs) ;
- 2x 500 Go SAS-NL 7200 tpm;
- 5 ports réseaux 1 Gb (dont 1 port admin).

Nombre total de cœurs : 2 procs x 4 cœurs x 8 calculateurs = 64 cœurs

Nombre total de mémoire vive : 64 Go x 8 calculateurs = 512 Go

2 NAS NetGear RN2120v2 :

Figure 28 Le serveur Netgear Ready NAS RN2120v2

Les caractéristiques matérielles de ces NAS sont les suivantes :

- processeur Marvell Armada XP dual core 1.6 Ghz ;
- 2 Go de mémoire ;
- 4 baies de disques de 2 To (capacité maximale de 16 To) ;
- 2 ports Ethernet Gigabit avec agrégation de lien et failover.

Ces NAS sont équipés des disques Toshiba DT01ACA200 2 To ;

- vitesse de rotation 7200 tours par minute ;
- taille du cache à 64 Mo.

1 commutateur HP 5120, assurant l'interconnexion des éléments actifs. Il est administré par l'opérateur unique du ministère de la défense : la DIRISI.

Figure 29 Le commutateur HP 5120

V.2.8 Choix du système d'exploitation

La fondation Apache maintient à jour une matrice de compatibilité[8].

Avant de commencer le déploiement, il est important de vérifier que les choix des systèmes d'exploitation sont compatibles avec le logiciel CloudStack.

V.2.8.1 Versions des systèmes d'exploitation supportés pour le serveur de management

L'installation du serveur de gestion CloudStack est supportée pour :

- RHEL versions 5.5, 6.2, 6.3 et 6.4 ;
- CentOS versions 6.3, 6.4 et 6.5 et ultérieures ;
- Ubuntu 12.04 LTS.

[8] http://cloudstack-release-notes.readthedocs.io/en/latest/compat.html

V.2.8.2 Versions des Hyperviseurs supportés

CloudStack supporte 4 familles d'hyperviseurs : XenServer avec XAPI, KVM VMware avec le Vcenter et Hyper-V.

- Windows Server 2012 R2 (avec le role Hyper-V d'activé) ;
- CentOS 6.2 avec KVM ;
- Red Hat Enterprise Linux 6.2 avec KVM ;
- XenServer versions 6.1 et 6.2 SPI à jour des patches ;
- VMware versions 5.0, 5.1 et 5.5.

CloudStack peut également provisionner des hôtes physiques Baremetal (sans hyperviseur) sous les systèmes d'exploitation suivant :

- RHEL or CentOS, v6.2 or 6.3;
- Fedora 17 ;
- Ubuntu 12.04.

La matrice de compatibilité n'étant pas suffisament précise pour le cas de KVM sur la distribution CentOS 7, il a fallu chercher cette information sur la liste de diffusion des utilisateurs de CloudStack, qui confirme la possibilité de déployer l'infrastructure CloudStack complète sur une CentOS 7.

V.3 Aspect financier

V.3.1 Coût de la plateforme

Une analyse du coût de la plateforme donne une valeur financière à une VM standard. De cette valeur, la rentabilité de la plateforme pourra être comparée avec les offres existantes sur le marché des clouds publics.

V.3.1.1 Coût matériel

Tableau 25 Coût des serveurs de la plateforme Cloud Formation

Type	Nombre	Prix HT	Total HT
Serveur IBM 3550 M4 2x Intel Xeon QuadCore E5-2603v2, 64 Go RAM, 2x 500 Go SAS 7200 trs 5x 1 Gb Ethernet	8	1 289,85	10 318,80
Prestation atelier	8	157,57	1260,56
Livraison sur site	8	6,59	52,72
Garantie	8	201,74	1613,92
Installation sur site	8	65,35	522,80

Tableau 26 Coût des éléments actifs de la plateforme Cloud Formation

Type	Nombre	Prix HT	Total HT
ReadyNAS RN2120v2 8 TB	2	1 550	3 100
Commutateur HP 5500-48G	1	1 320,39	1 584,47

Le coût en matériel est de 18 453,27€ HT (22 143,93 TTC). L'amortissement des serveurs au ministère de la défense se fait sur une durée de 8 ans. Le coût d'amortissement mensuel de la plateforme CloudStack revient à 230,67€ TTC.

La consommation d'énergie n'est pas prise en compte dans le calcul des coûts de la plateforme.

V.3.1.2 Coût en personnel

Pour administrer la plateforme, il est prévu de mandater :

- un Technicien Supérieur d'Etudes et Fabrication (TSEF) sur la moitié de son temps de travail ;
- un Ingénieur d'Etudes et Fabrication (IEF) sur 10 à 20% de son temps de travail.

L'estimation du montant du coût salarial est basé sur le document du SGA *Mémento des coûts moyens du personnel civil 2014* [SGA-2015] :

- IEF :
  - coût moyen par an : 44 363,52€ ;

- coût pour la plateforme par mois : 739,392€ (sur la base de 20% du temps de travail).

- TSEF 2ème classe :
  - coût moyen par an : 36 797,96€ ;
  - coût pour la plateforme par mois : 1 533,25€ (sur la base de 50% du temps de travail).

Coût global par mois pour le personnel d'administration : **2 272,64€**.

V.3.1.3 Capacité d'accueil

Tableau 27 Les processeurs « CloudStack ETRS »

Caractéristique	Proc CloudStack ETRS
Type	E5-2603V2
Cache	10 MB
Nb. De cœurs	4
Nb. De threads	4
Fréquence de base	1,8 GHz
Technologie Intel® Hyper-Threading	Non
Prix de vente recommandé[9]	202 $

Chaque serveur de la plateforme étant équipé de 2 processeurs de ce type, ils offriront une puissance de calcul de 2 x 4 x 1,8= 14,4 Ghz.

La puissance de calcul de la plateforme complète sera de 115,2 Ghz, moins les ressources nécessaires aux hyperviseurs. L'objectif de la virtualisation étant de centraliser la consommation de ressource afin de profiter des possibilités de surallocation, on peut estimer être en mesure d'accueillir **230** machines virtuelles avec **1 vCPU cadencé à 1 Ghz et un facteur de surallocation de 2**.

D'un point de vue RAM, la plateforme dispose d'un volume de 512 Go RAM. Elle peut attribuer plus **de 2 Go de RAM par vCPU à 1 Ghz** sans surallocation.

[9] http://ark.intel.com/fr/products/76157/Intel-Xeon-Processor-E5-2603-v2-10M-Cache-1_80-GHz

Du matériel supplémentaire étant en cours de commande pour l'année 2017, les capacités de la plateforme pourront être rapidement multipliées par 2, permettant de se rapprocher de l'objectif final :

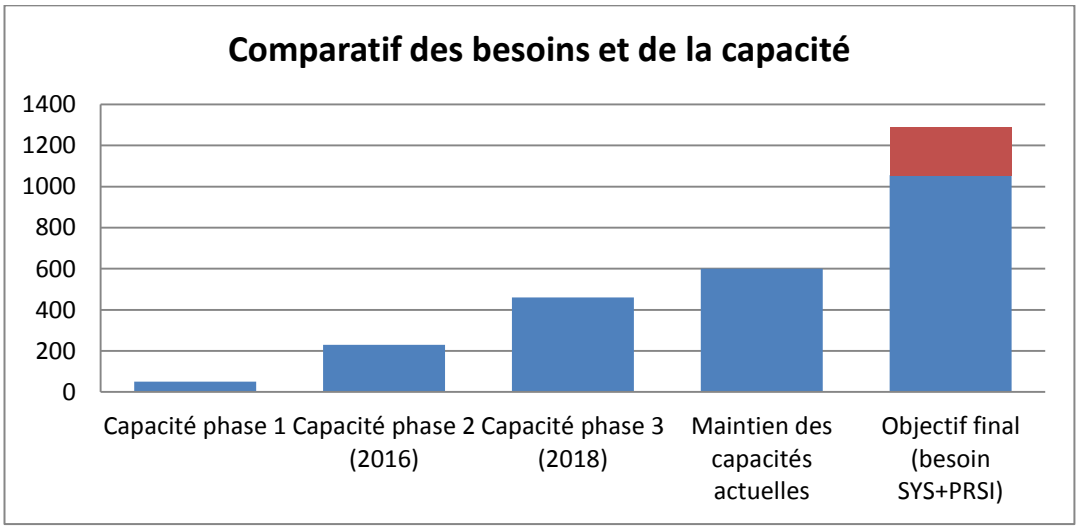


Figure 30 Schéma comparatif des besoins et de la capacité d'accueil de la plateforme (cible 2017)

V.3.1.4 Coût estimé d'un VM Cloud Formation

Il apparaît que le matériel commandé pour la plateforme ne permettra pas de répondre à la volumétrie nécessaire, même en seconde phase : la capacité d'accueil de 230 VM est déjà inférieure à l'expression du besoin d'origine. Il faudra donc commander du nouveau matériel pour rapidement gonfler les capacités d'accueil.

La plateforme sera dans un premier temps utilisée à plein rendement, le besoin étant supérieur à la capacité, ce qui permet de calculer au plus juste le coût d'une VM :

L'amortissement matériel calculé s'élève à **230,67€** par mois.

Le coût de la masse salariale est estimé à **2272,64€**.

La plateforme devrait héberger **230** VM à 1 vCPU 1 Ghz.

Le coût d'une VM 1 vCPU 1 Ghz est de (230,67 + 2272,64) / 230 = **10,88€**

Le tableau des offres du cloud définies précédement peut être complété avec le coût estimé par type d'offre. :

Tableau 28 Coût d'une VM par type offre.

Offre	vCPU	RAM	Coût
S	1 x 1 Ghz	1	10€88
M	1 x 1 Ghz	2	10€88
L	1 x 1.5 Ghz	2	16€32
XL	1 x 2 Ghz	4	21€76
XXL	1 x 2 Ghz	8	21€76
2XL	2 x 2 Ghz	4	43€52

Une puissance maximale de 11 Ghz a été calculée (voir étude quantitative) comme nécessaire pour satisfaire les besoins d'un cursus standard. Dans un cloud privé, il est possible de limiter l'allocation de puissance disponible à un stagiaire.

Dans le cas d'un cursus standard, un stagiaire pourrait être limité à 11 Ghz, soit un coût de 11 x 10€88 = **119€68**.

L'analyse de la programmation des stages nous apprend qu'il faut s'attendre à avoir au maximum 4 cursus en même temps au cours systèmes et PRSI.

Les besoins d'un stagiaire PRSI étant inférieurs à ceux d'un stagiaire système, pour faciliter les calculs, la valeur de 11 Ghz de puissance maximale par stagiaire est retenue.

La plateforme de Cloud Formation devrait être dimensionnée pour accueillir 11 Ghz x 96 stagiaires ; soit une puissance de calcul de **1056 Ghz**, ce qui est largement au dessus des **230 Ghz** estimés pour la plateforme avec le matériel actuellement commandé.

V.3.1.5 Comparatif avec les solutions d'externalisation

Le projet de Cloud Formation a pour périmètre une PFI traitant de données « Non protégées », ce qui laisse la possibilité d'envisager un cloud hybride. Mais si l'ETRS souhaite installer un autre « Cloud Formation » sur l'Intradef, le savoir faire acquis avec le Cloud Formation Internet est transposable.

V.3.1.5.1 Les serveurs virtuels privés

Dans le cadre de l'utilisation de serveurs VPS, les possibilités pour limiter la consommation de ressources sont plus limitées. Il faudrait prévoir la réutilisation de VPS d'un devoir à l'autre, ce qui semble difficilement gérable. L'achat d'un serveur se fait donc pour le mois.

Tableau 29 Coût global d'un cursus standard en VPS.

Nom de la VM	Type VPS	Durée	Coût
VM Linux Admin	SSD 1	2 mois	7,18€
VM Linux Serveur	SSD 1	1 mois	3,59€
VM Linux Devoir Admin	SSD 1	1 mois	3,59€
VM Linux Devoir Apache	SSD 1	1 mois	3,59€
VM Devoir Postfix	SSD 1	1 mois	3,59€
VM Windows 7	SSD 1	2 mois	7,18€
VM Windows Serveur	SSD 1	1 mois	3,59€
VM Devoir Windows Serveur 1	SSD 2	1 mois	14€38
VM Devoir Windows Serveur 2	SSD 2	1 mois	14€38
VM Exchange stagiaire	SSD 3	1 mois	14,39€
VM IIS	SSD 2	1 mois	14€38
VM Frontal Link	SSD 3	1 mois	14,39€
VM Backend Link	SSD 3	1 mois	14,39€
VM Devoir Exchange	SSD 3	1 mois	14,39€
Total :			**89,87€**

Le coût global d'un cursus standard revient dans ce cas à 89,87€, mais avec des fonctionnalités moindres : pas de solution de sauvegarde, pas d'instantanés, pas de gestion de modèles.

V.3.1.5.2 Le cloud dédié

Un hôte L+, avec un facteur de surallocation processeur de 2, peut accueillir 100 VM 1 vCPU / 1 Go RAM (sans surallocation de RAM).

Une VM 1 vCPU / 2 Go RAM chez OVH sur un hôte L+ avec une surallocation de 2 à un coût de : 503,51€/100=**5, 03€**.

V.3.1.5.3 Comparatif des offres

Nous pouvons comparer le coût des différentes offres :

Tableau 30 Comparatif des caractéristiques matérielles OVH/ETRS

Offre	Coût	Description	Observation
CloudFormation	10,88€	1 vCPU 1 Ghz 2 Go RAM	
VPS OVH	3,59€	1 vCPU 2,4 Ghz 2 Go RAM	Fonctionnalités limitées.
Cloud Dédié OVH	5,03€	1 vCPU 1 Ghz 1 Go RAM	Le coût de l'administration, même simplifié, n'est pas inclus. Surallocation de la RAM

Le coût de l'externalisation du Cloud Formation ne prend pas en compte le coût de l'administration que nous pouvons estimer à un ¼ du temps de travail d'un TSEF, soit 766,625€ par mois.

V.3.1.6 Comment devenir rentable ?

Le coût d'une VM du cloud formation est 2 fois supérieur à l'offre du cloud dédié d'OVH. Quelles solutions envisager pour réduire cet écart de prix ? Comment devenir rentable ?

Tableau 31 Comparatif des caractéristiques matérielles d'un hôte OVH/ETRS

Caractéristique	OVH	ETRS
Proc / Thread / Fréquence	16 / 16 / 3.1 Ghz	8 / 8 / 1.8 Ghz
RAM	256	64
Capacité VM mono CPU	100	28

La quantité de RAM sur la plateforme ETRS est légèrement surdimensionnée au vue des caractéristisques de ses processeurs.

Un investissement peut être fait pour changer les processeurs des hyperviseurs par des plus puissants sans devoir ajouter de nouveaux hôtes :

Tableau 32 Comparatif des processeurs « OVH » et « CloudStack ETRS »

Caractéristique	Processeurs de changement	Processeurs livrés
Type	E5-2690V2	E5-2603V2
Cache	25 Mb	10 Mb
Nb. De cœurs	10	4
Nb. De threads	20	4
Fréquence de base	3 Ghz	1.8 Ghz
Technologie Intel® Hyper-Threading	Oui	Non
Prix de vente recommandé[10]	2061,00$	202,00$

Ainsi, pour le remplacement des 16 processeurs de la plateforme, un investissement de **35 949,37€ TTC** (30 058€ HT ou 32 976$) permettrait de multiplier la puissance de calcul par 8. Il faudrait alors doubler la capacité en RAM et acheter 14 serveurs NAS supplémentaires (14x1 550€ HT soit 25 953€ TTC).

L'amortissement du coût de remplacement des processeurs et des NAS sur 8 ans ferait augmenter l'amortissement matériel de 644€82 (hors coût d'achat de la RAM) par mois soit au total 875€49 (ce qui reste bien en-dessous du coût de la masse salariale). Ansi, en hébergeant 1840 VM, **le coût estimé d'une VM 1 vCPU 1 Ghz serait de (875,49€ + 2272,64€) / 1840 = 1,71€.**

Une deuxième possibilité est d'augmenter notre capacité d'accueil en achetant de nouveaux serveurs. Pour pouvoir héberger les 1056 Ghz estimés lors de l'étude quantitative, sachant que chaque calculateur peut offrir 28,8 Ghz de puissance processeur avec un facteur de 2, il faudrait 36 calculateurs, soit 4,5 fois l'investissement de départ (36 calculateurs, 9 NAS, 4 commutateurs). Dans ce cas, **le coût estimé d'une VM 1 vCPU 1 Ghz serait d'environ (230,67€ x 4,5 + 2272,64€) / (230 x4,5) = 3€20.**

[10] http://ark.intel.com/fr/products/75279/Intel-Xeon-Processor-E5-2690-v2-25M-Cache-3_00-GHz

Le tableau ci-dessous récapitule les coûts de chaque solution en fonction du nombre de VM.

Tableau 33 Grille des coûts par type de solution

Nombre de VM	Cloud Formation	VPS	Cloud dédié
100		1125,625	1269,625
200		1484,625	1772,625
230	2503,31	1592,325	
300		1843,625	2275,625
400		2202,625	2778,625
460	2733,98	2418,025	
500		2561,625	3281,625
600		2920,625	3784,625
690	2964,65	3243,725	

Le cloud formation deviendra rentable pour l'ETRS dès qu'il aura atteint la capacité d'héberger plus de 690 VM. Le coût de la VM sera alors d'environ **(230,67€ x 3 + 2272,64€) / (230 x3) = 4€30.**

V.3.1.7 Impact sur l'investissement lié au parc informatique des PFI

La solution de virtualisation VMware Workstation implique une course à la puissance des ordinateurs des PFI : processeurs puissants et augmentation de la RAM.

Les PFI peuvent être équipées par différentes offres de PC :

- La configuration « UC de bureau – configuration standard (conf 1.1F) », coûtant 380€ TTC , équipée de 4 Go de RAM ;
- La configuration « Configuration fixe – hautes performances (conf 3.3F) », coûtant 1 750€ TTC, équipée de processeurs plus puissants et de 8 Go de RAM.

La configuration « Hautes Performances » est actuellement la référence pour l'équipement des 400 postes des salles de cours. Le passage au format Cloud des formations changera in fine la politique de renouvellement du parc, l'ETRS réalisant ainsi 1 300€ (quasiment le prix d'un serveur Cloud) d'économies par poste informatique (avec ajout de 4 Go de RAM sur les configurations standards).

V.4 Archivage des devoirs

Les VM de devoirs doivent être archivées pour une durée légale d'un an. Un espace de stockage conséquent doit être dédié à cet effet.

Grâce aux techniques d'allocation granulaire de capacité (provisionning dynamique ou thin provisioning), l'espace requis sur le NAS est généralement inférieur à l'espace provisionné à la création de la VM. La taille du disque de la VM augmente uniquement en fonction de la consommation réelle de l'espace.

Tableau 34 Espace nécessaire au stockage des VM de devoirs.

Devoirs	Espace estimé
Linux Admin	3 Go
Linux Apache	3 Go
Windows Serveur 1	8 Go
Windows Serveur 2	8 Go
VM Exchange	12 Go
Total :	**38 Go**

L'archivage des VM de devoirs pour les 312 stagiaires annuels (24 stagiaires x 13 stages) représente un espace de stockage de **11,856 To**. Cet espace n'est pas disponible actuellement.

V.5 Stratégie de la reprise de l'existant

La première expérimentation de 2014 prévoit d'examiner si les modèles utilisés dans VMware Workstation peuvent être transférés dans le Cloud.

Cette activité est cruciale et peut s'avérer extrêmement complexe dans certains cas. Des outils existent permettant de transformer une machine virtuelle du format « vmdk » (le format des disques sous VMware) vers le format utilisable par KVM : le format qcow2. Les tests réalisés se sont montrés concluants.

Avant de reprendre le travail déjà effectué, chaque cellule a été de nouveau interrogée pour connaitre plus précisement son besoin de migration. Il s'est avéré que :

- la cellule Windows n'utilise pas ou peu de modèles déjà configurés. Le stagiaire installe lui-même son système d'exploitation ;
- la cellule Linux est celle qui fait le plus grand usage des modèles. Le stagiaire dispose de deux machines virtuelles pré-configurées pour ses cours, et de deux autres pour les devoirs. Les machines étant régulièrement entièrement réinstallée, ce processus est très bien maîtrisé.

  Pour un formateur, créer de nouveaux modèles est une des rares occasions de pratiquer sur son système d'exploitation et de conserver son niveau de technicité. C'est aussi un moyen pour les nouveaux formateurs de valider les nouvelles compétences acquises.

  La cellule met également en place des outils de gestion de configuration (puppet et scripts bash) qui automatisent la tâche.

- la cellule Services utilise des images très basiques des systèmes d'exploitation Windows 7 et Windows Serveur. Le processus de migration prendrait plus de temps que la création de nouveaux modèles.
- le cours PRSI utilise des outils en constante évolution. Ce cours maîtrise également la création de ses modèles.

La possibilité de migrer les modèles existants vers le format qcow2 se révèle dans les faits une fausse nécessité, rassurant pour le décideur qui ne veut pas voir son personnel perdre du temps dans la migration, mais totalement inutile ou presque dans les faits du point de vue des formateurs.

Les fonctionnalités de l'environnement CloudStack répondent aux besoins de l'ETRS, comme l'a démontré la phase de conception. Après une première étude des procédures d'installation, une liste exhaustive des technologies à maîtriser par les futurs administrateurs a été établie et chacun des points analysés (voir Annexe 5).

Ne disposant pas d'un budget directement alloué, et n'étant pas maître du processus d'achat, la conception de la plateforme se voit limitée aux matériels présents et à ceux qui seront livrés sous peu. La montée en puissance de la plateforme se fera progressivement jusqu'à atteindre une capacité suffisante et devenir rentrable.

La solution de virtualisation actuelle n'étant pas abandonnée, l'ETRS pourra, en cas de pics de charge, se tourner vers :

- l'ancienne solution VMware Workstation pour des besoins basiques : formations Windows 7, formation Administrateur Linux ;
- une offre de cloud hybride : migrer certains stages vers une plateforme publique ;
- l'investissement dans plus de matériels pour la plateforme Cloud Formation, ce qui aura également pour effet de réduire le coût à la VM.

Nous sommes à présent en mesure de réaliser une solution technique adaptée pour répondre aux exigences identifiées.

VI Réalisation

Les choix de plateforme, des fonctionnalités à mettre en œuvre et d'architecture réseau ayant été validés. La phase de réalisation débute par une période d'appropriation (recommandée par la fondation Apache elle-même), nécessaire pour comprendre le fonctionnement interne du logiciel, pour rédiger les premières procédures d'installation et de configuration, pour se former aux dépannages et à l'adaptation de l'environnement (présence d'un proxy, VLANs de l'ENT).

La plateforme est ensuite définitivement mise en œuvre et les fonctionnalités progressivement configurées et validées.

VI.1 Installation du matériel

En 2015, après la première expérimentation, du matériel a été commandé pour mettre en œuvre le Cloud Formation.

La réception des 2 NAS en janvier 2016 relance le projet. Dans un premier temps (phase 1), avant la réception des nouveaux serveurs, nous avons profité de la mise à la réforme de 6 serveurs pour monter la plateforme avec des hyperviseurs provisoires.

Ces 6 serveurs ont des caractéristiques assez similaires :

- 2 processeurs bi-coeurs (9,31 Ghz) ;
- 22 Go de RAM ;
- 300 à 500 Go de disque dur en RAID 5.

Ils sont en mesure d'héberger environ 50 machines virtuelles.

Le réseau internet de l'école n'est pas administré par la cellule Soutien-PFI-ENT. Une réunion avec l'opérateur unique de la défense (la DIRISI) a été organisée le 3 mai durant laquelle nous avons présenté le projet et le besoin. Pour pouvoir commencer les travaux indépendamment de leur intervention, nous disposons du commutateur utilisé pendant la première expérimentation. Il dispose déjà des VLANs nécessaires.

Le montage de la baie a commencé au début du mois de juillet. En compagnie de l'IEF Fabrice Pollet, nous avons :

- Déplacé le commutateur vers sa nouvelle baie et branché le commutateur au coeur du réseau ;
- Positionné les 2 NAS et procédé à leur configuration ;
- Installé physiquement les 6 serveurs dans la baie ;
    - Configuré le RAID 5 des serveurs,
    - Installé le système d'exploitation Linux CentOS.

Bien que sans réelle valeur ajoutée, cette opération a nécessité deux journées de travail. Elle marque le début de la mise en œuvre concrête de notre projet.

Figure 31 La baie Cloud Formation

Figure 32 Le commutateur d'interconnexion de la baie Cloud Formation

VI.2 Validation de la solution CloudStack

VI.2.1 Plateforme virtuelle

Pour saisir toutes les subtilités de l'installation d'une solution aussi complexe que CloudStack, malgré son caractère « clé en main », il est nécessaire de procéder étape par étape, pour assurer une montée en compétence progressive.

La phase d'appropriation du logiciel s'est faite en installant des plateformes de plus en plus élaborées et en demandant davantage de puissance :

- une première plateforme mono-serveur en environnement virtuel VMware Workstation proposant un réseau simple : une seule machine virtuelle pour assurer l'ensemble des rôles de la plateforme (serveur de fichiers, serveur de base de données, serveur CloudStack, hyperviseur KVM) ;
- une seconde plateforme en environnement virtuel VMware Workstation comportant un serveur de gestion, deux serveurs NAS et 4 noeuds : un seul réseau physique supportant une plage d'adresses unique ;
- une troisième plateforme sur du matériel physique avec :
  - ✓ un réseau simple,
  - ✓ un réseau avancé avec 3 plages d'adresses : une plage d'adresses réservée à l'administration, une pour le réseau public et une pour le réseau des invités. Pour cette plateforme, chaque élément de CloudStack dispose de 2 interfaces réseaux.

VI.2.1.1 Première prise en main

Installation d'une seule VM avec l'ensemble des fonctionnalités de la plateforme.

Durée de l'expérimentation :

- 2 jours.

Bilan de l'expérimentation :

- se familiariser avec l'environnement, avec le vocabulaire et début de la rédaction de la documentation technique ;
- l'installation de la plateforme semble à première vue assez simple. De nombreux logiciels entre en jeu avec parfois des configurations particulières ;
- à cause du manque de ressources, il n'a pas été possible d'explorer plus en avant certains aspects techniques, mais cette étape était indispensable pour se familiariser avec l'environnement.

L'expérimentation a surtout permis de découvrir l'aspect commutateur virtuel de la librairie libvirt.

Points bloquants :

- le manque de ressources de la plateforme, ce qui est normal à cette étape ;
- le proxy de la DMZ en place à l'école, qui empêche le téléchargement des modèles et des images ISO depuis l'Internet.

Point contraignant pour les futurs administrateurs :

- la documentation est exclusivement en anglais. Un travail de traduction des pages les plus importantes est à envisager.

VI.2.1.2 Plateforme complète virtuelle

Installation d'une plateforme CloudStack complète sur plusieurs machines virtuelles VMware. La disponibilité d'une salle de formation permettant d'attribuer des ressources conséquentes à chacun des éléments : 6 Go Ram + 4 vCPU a été mise à profit.

Tableau 35 Composants de la plateforme virtuelle complète.

Nom de la VM	Adresse IP	Fonctionnalités	Observations
cloudstack	xxx.xxx.xxx.150/20	CloudStack Management + CloudDB	CentOS 6
nas1	xxx.xxx.xxx.210/20	Primary Storage	Serveur FreeNAS
nas2	xxx.xxx.xxx.211/20	Secondary Storage	Serveur FreeNAS
kvm1	xxx.xxx.xxx.200/20	Hyperviseur KVM	CentOS 6
kvm2	xxx.xxx.xxx.201/20	Hyperviseur KVM	CentOS 6
kvm3	xxx.xxx.xxx.202/20	Hyperviseur KVM	CentOS 6

Si l'installation de cette plateforme (serveur de gestion, NAS, hôtes) et sa configuration (création de la zone, du cluster et intégration des hyperviseurs) a été rapide (moins de 4 heures), il se trouve qu'après la phase de configuration, le déploiement des images ISO ou des modèles de machines virtuelles, et donc la création d'une nouvelle instance, sont impossibles.

Afin de résoudre cela, il a fallut se connecter à la SSVM (Secure Storage Virtual Machine) responsable de la copie des données entre le stockage primaire et secondaire pour obtenir une piste de dépannage. L'information permettant de résoudre la panne a été trouvée dans la documentation anglaise de CloudStack.

- Les VM systèmes doivent être détruites pour quelles soient recréées automatiquement par le manageur CloudStack et ainsi prendre en compte les modifications de la configuration globale.
- La fonctionnalité d'ip.forwarding doit être activée sur l'ensemble des éléments constituant la plateforme.
- Le montage des partages NFS primaire et secondaire se fait automatiquement sur les hyperviseurs. Il doit être fait manuellement sur le manageur avant le téléchargement et le déploiement des VM systèmes depuis l'Internet.

Le bon fonctionnement de cet essai confirme la faisabilité du projet. L'interface est présentée aux formateurs qui la découvraient et les évolutions à ceux qui la connaissaient déjà.

Les premiers éléments d'optimisation apparaîssent : à ce stade, la durée de session de l'environnement web est détectée comme trop courte. Le verrouillage des postes de travail après une trop longue inactivité sécurise déjà le stagiaire d'un vol de session. Un délai plus long peut être envisagé, en trouvant un équilibre correct entre confort d'utilisation et sécurité du système.

La procédure de configuration fait l'objet d'une modification pour prendre en compte cet élément.

VI.2.2 Plateforme physique

Le matériel étant prêt et la phase d'appropriation de la plateforme étant achevée, tout les pré-requis sont rassemblés pour enfin pouvoir déployer la plateforme sur le matériel qui lui est destiné et valider l'architecture du réseau.

VI.2.2.1 Validation de la zone simple

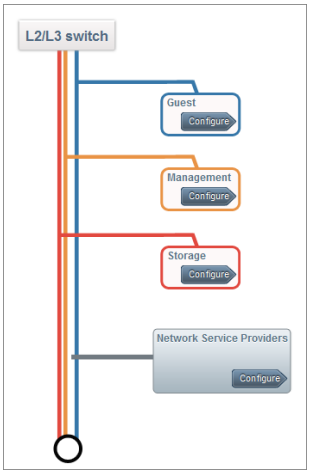


Figure 33 Le réseau physique d'une zone simple.

Avant de commencer l'installation logicielle, les enregistrements DNS nécessaires ont été ajoutés au domaine de l'école.

Le serveur de gestion de CloudStack est déployé sur le premier serveur, appelé Cloud1. Nous avons gardé la possibilité d'ajouter un deuxième serveur de gestion pour assurer la tolérance de panne lorsque les nouveaux serveurs auront été reçus (phase 2).

Dans un premier temps, la plateforme repose sur un système CentOS 6, environnement maîtrisé par les administrateurs.

Une zone simple a été configurée, afin de tester le bon fonctionnement et d'explorer les fonctionnalités en situation réelle. Dans le cadre d'une zone simple, le réseau invité doit être routable depuis l'extérieur de la plateforme. Le réseau Invité/Public est ainsi confondu.

Cette expérimentation ayant été un succès, une seconde installation en CentOS 7 a été testée. En effet, la version 6 de cette distribution commence à être un peu ancienne et après concertation, nous avons trouvé dommage de lancer un nouveau service sur un ancien système. Nous ne voulions toutefois pas être confrontés, en phase de validation, à des problèmes liés à un système d'exploitation que nous ne maîtrisions pas totalement, ce qui explique ce choix de double installation.

Après présentation de la zone simple aux différents acteurs du projet, nous avons décidé d'installer la plateforme avec une zone avancée, afin de pouvoir étudier toutes les fonctionnalitées étendues offertes et qui ne sont pas disponibles en zone simple.

VI.2.2.2 Validation de la zone avancée

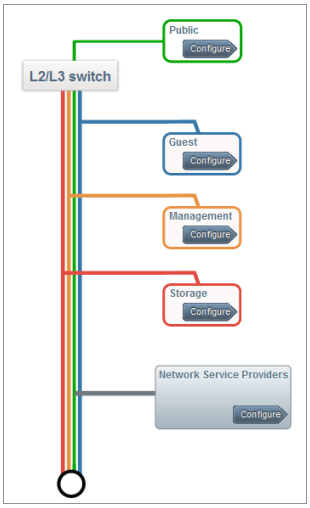


Figure 34 Le réseau physique d'une zone avancée.

Pour évaluer les fonctionnalités évoluées du réseau dans une zone avancée, la plateforme est une nouvelle fois installée.

Dans ce type de zone, la machine virtuelle se voit attribuer une adresse IP invitée. Cette adresse IP est totalement isolée du réseau extérieur. La mise en place d'une translation d'adresses réseaux (NAT) statique (une IP pour une IP) ou dynamique (un couple IP/port pour un couple IP/port) est nécessaire afin d'offrir un accès à la VM depuis le réseau public. Le client peut, depuis l'interface CloudStack, réclamer une adresse IP du réseau public pour la faire correspondre à une adresse IP du réseau invité. Une alternative à cette solution est de définir comme plage d'adresses IP pour le réseau invité de la zone avancée une plage d'adresses routables depuis l'extérieur de la plateforme. Les VM sont ainsi directement accessibles depuis leur adresse IP obtenue via CloudStack (comme c'est le cas pour le réseau simple).

Cette dernière possibilité n'a pas été vérifiée, puisqu'elle nécessite un sous-réseau complet que nous n'avions pas à disposition.

Une réunion a été organisée pour faire le point sur les possibilités offertes par ces deux types d'architecture. La zone simple convient parfaitement à certains cours qui ne mettent en œuvre qu'un ou deux serveurs sans interconnexion de réseaux complexes. La zone avancée propose un cloisonnement des réseaux intéressant dans le cadre de projet plus complexes ou pour l'hébergement sécurisé de service. La plateforme Cloud Formation pourrait dans l'avenir être le support des serveurs du CAN-ENT et la zone avancée offre un environnement de qualité.

La zone simple est plus accessible pour un nouvel utilisateur du cloud. Les fonctionnalités avancées semblent trop complexes pour les stagiaires. Nous pensons que l'utilisation de la zone avancée se fera au fur et à mesure de l'utilisation de la plateforme par les formateurs, qui s'approprieront progressivement les fonctionnalités offertes. La migration d'une zone à l'autre se fera progressivement et naturellement dans le temps.

Nous avons donc décidé d'installer la plateforme définitive avec deux zones pour profiter à terme du meilleur des deux offres. 3 hyperviseurs sont dédiés à la zone simple, 2 hyperviseurs à la zone avancée. En cas de nécessité, ou en fonction de l'usage du Cloud, il est possible a posteriori de répartir différemment les ressources de calcul.

VI.2.3 Bilan de la phase de validation

L'expérience acquise durant les précédentes mises en œuvre des plateformes virtuelles puis physiques a été capitalisée sous forme de procédures d'installation, de configuration et de dépannage (voir annexes 9 et 10). Les différentes topologies réseaux testées durant cette phase ont été présentées pour qu'un choix éclairé puisse être fait.

Cette phase a également permis d'obtenir un premier référentiel en matière de fonctionnement du système : caractéristiques nominales, valeurs critiques et valeurs maximales, marges d'évolutions possibles, niveau technique et moyens nécessaires pour assurer le MCO.

Les procédures et les résultats ayant été écrits durant la phase d'essais, la faisabilité du projet est dorénavant une chose acquise. Il est temps d'installer et de configurer la plateforme définitive.

VI.3 Mise en œuvre

VI.3.1 Installation de la plateforme définitive

Fort de l'expérience acquise durant les 3 mois précédents, l'installation de la plateforme et la configuration des 2 zones, appelées zone simple et zone avancée ont été très rapides. Il aura fallu 2 demi-journées pour obtenir un outil fonctionnel.

Le déploiement avait été initialement prévu début juillet pour laisser à chacun le temps de se familiariser avec le Cloud Formation durant la période creuse de l'été. Le retard pris par l'attente de la configuration du commutateur réseau et la réception des nouveaux serveurs n'a pas permis de respecter ce délai. L'installation est tout de même finie avant la fermeture d'août et son bon fonctionnement validé.

VI.3.1.1 Etapes d'installation de CloudStack

Le déploiement réussi d'une plateforme CloudStack respecte ces 9 grandes étapes :

1. Installation de l'hôte pour le serveur de management (CentOS) ;
2. Configuration du réseau, des adresses IP, du commutateur virtuel (Bridge) ;
3. Installation des paquets cloudstack-management et cloudstack-common ;
4. Installation et configuration du serveur de base de données MySQL server ;
5. Configuration des partages de stockage primaires et secondaires NFS ;
6. Téléchargement des modèles de VM système en fonction de l'hyperviseur retenu ;
7. Préparation du premier hôte KVM et installation du paquet cloudstack-agent ;
8. Configuration du pare-feu ;
9. Premier lancement de la plateforme et lancement de l'assistant de configuration.

VI.3.1.2 Montée de version de la plateforme

La fréquence des sorties des nouvelles versions de CloudStack a été ralentie cette année à cause de changement au niveau du comité directeur du projet.

Le projet CloudStack a annoncé la sortie de la version 4.9 le 25 juillet 2016. C'est l'occasion de tester les outils de montée de version et la faisabilité en condition réelle.

Lors de la procédure, le service du serveur de management doit être arrêté, le nouveau dépôt configuré, la mise à jour des paquets effectuée, puis le service relancé.

Chaque hôte doit ensuite être mis en maintenance, l'agent CloudStack arrêté, le paquet mis à jour et le service relancé.

Le processus de mise à jour de la version 4.9 modifie le fichier de configuration de l'agent et supprime un retour chariot, ce qui corrompt la connexion au serveur MySQL.

Un rapport de bug ayant été émis, une recherche sur Internet a rapidement permis de trouver la solution pour rétablir la situation. En production, cette mésaventure prouve qu'il ne faut pas se précipiter sur une procédure de mise à jour, même sur un projet de l'envergure de CloudStack.

VI.3.1.3 Intégration de la plateforme dans l'annuaire LDAP du CAN/ENT

L'interface de CloudStack propose des champs pour configurer l'authentification des utilisateurs via LDAP.

Cette intégration de CloudStack avec le serveur OpenLDAP du CAN/ENT est une exigence du service Soutien PFI-ENT et un pré-requis à l'intégration dans le CAS.

Avec l'administrateur système du CAN, nous avons donc configuré les paramètres relatifs à OpenLDAP dans l'interface de CloudStack pour s'appuyer sur notre serveur LDAP.

Les utilisateurs CloudStack s'authentifient dorénavant avec leurs comptes LDAP du CAN-ENT. Au sein de l'interface, l'administrateur dispose d'un assistant d'importation des comptes depuis l'annuaire.

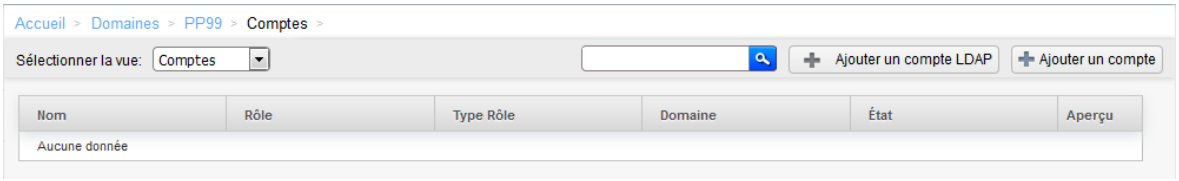


Figure 35 Importation d'un ou de plusieurs comptes LDAP depuis l'interface CloudStack

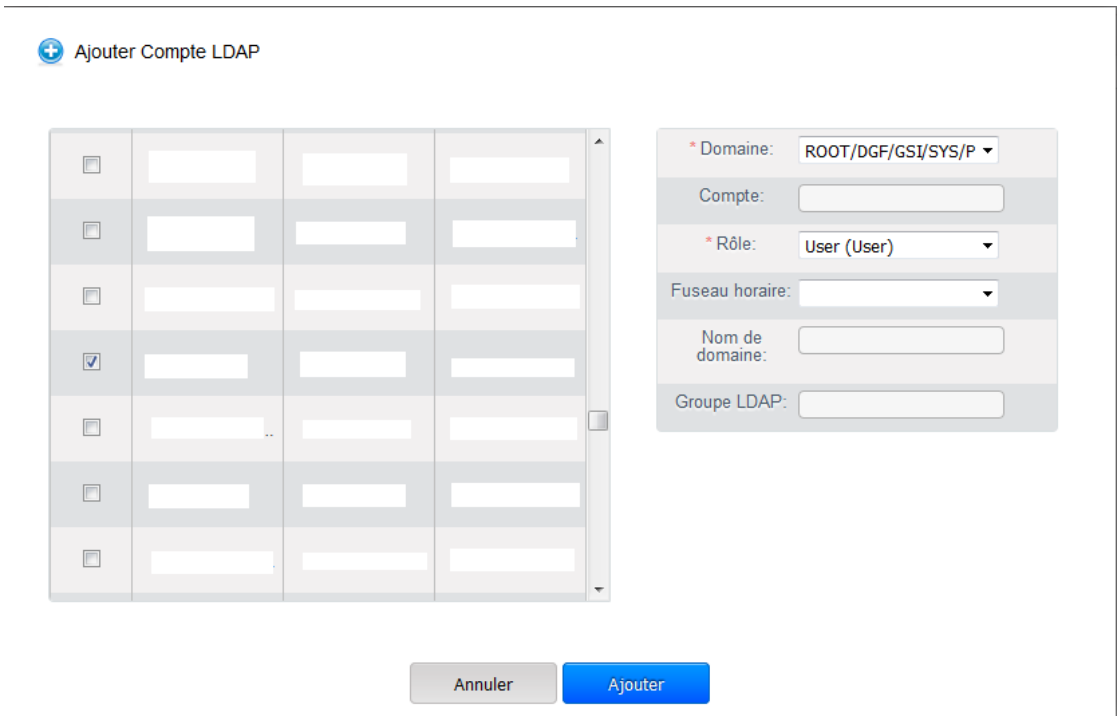


Figure 36 L'assistant "Ajouter Compte LDAP".

Une procédure dans le wiki a été rédigée au profit des futurs administrateurs de la plateforme.

Pour faciliter les actions de configuration de la plateforme, la page de documentation du guide d'administration CloudStack avait été préalablement traduite.

VI.3.1.4 Intégration dans le portail ENT

L'ENT représente le point d'accès unique à l'ensemble des ressources disponibles. Le portail s'appuie sur la solution java ESUP-PORTAIL.

Un lien vers l'interface du Cloud Formation a naturellement été configuré dans la zone d'administration du portail :

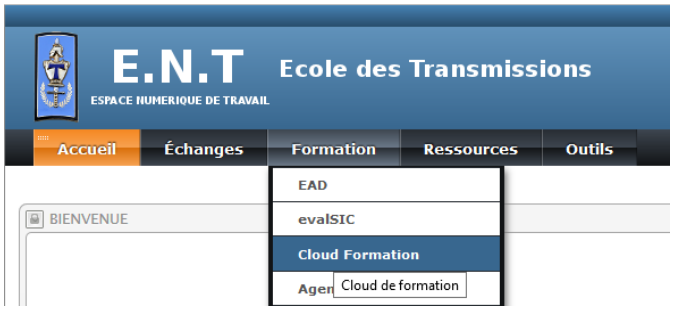


Figure 37 Accès à l'interface CloudStack via l'ENT

VI.3.1.5 Utilisation de la plateforme par les formateurs Linux

Depuis le 6 septembre 2016, les formateurs du cours Linux ont déployé individuellement une VM d'administration. Ils s'y connectent via le protocole SSH ou RDP pour les démonstrations et la correction des TP durant leurs formations.

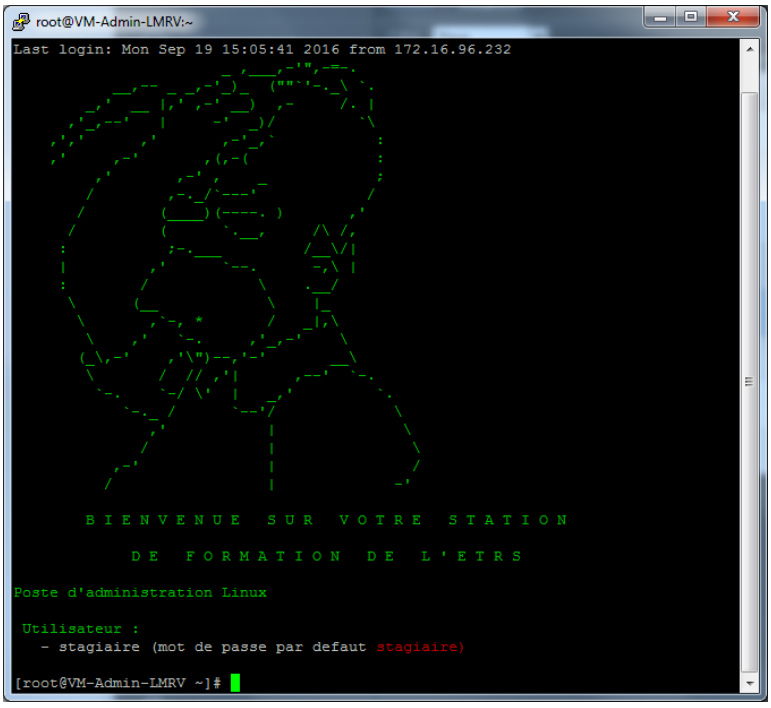


Figure 38 Accès SSH aux serveurs des formateurs Linux.

L’utilisation du Cloud Formation leur évite de devoir lancer avant chaque début de cours une VM créée localement sur leur poste de formation. La plateforme permet un gain de temps pour la préparation en début de cours.

VI.3.1.6 Optimisation des transferts vers le NAS

Lors de la création d’une nouvelle instance, la VM système SSVM copie le modèle du stockage depuis le stockage secondaire vers le stockage primaire. Le modèle est ensuite créé par recopie du modèle. Ce modèle est conservé sur le stockage primaire pendant une période de temps configurable avant d’être supprimé par la SSVM.

La première création d’une même instance est donc plus longue que les suivantes, le temps que le modèle soit copié du stockage secondaire vers le stockage primaire.

Les temps d’attentes étaient trop longs pour que la plateforme soit exploitable. L’installation depuis une image ISO d’un système windows 7 prenait plusieurs heures, contre 16 minutes sur les postes de travail actuels.

Une analyse des débits réseaux a été décidée le 5 septembre 2016. Le débit moyen mesuré entre un hôte et le NAS lors de la copie d’un fichier d’1 Go est de 13,94 Mbit/s (**1.7425** Mo/s).

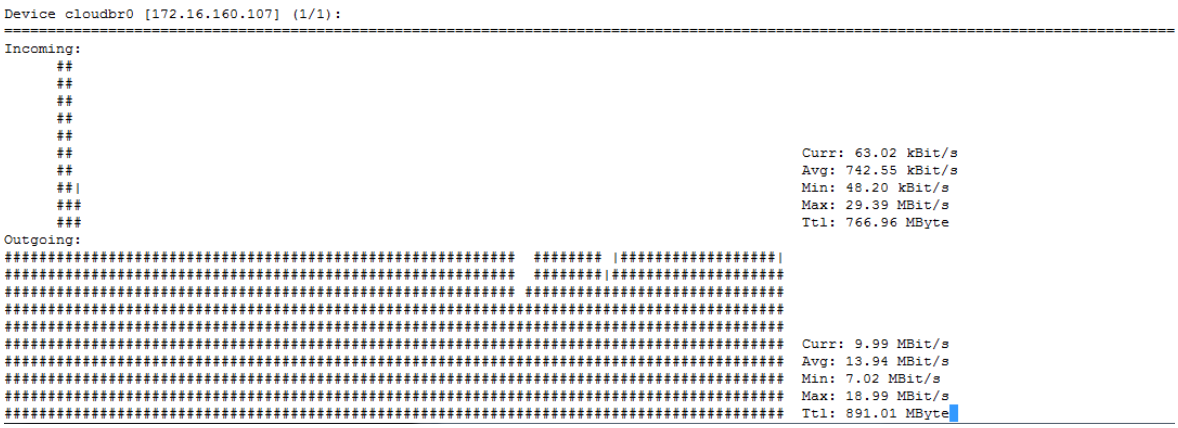


Figure 39 Débit réseau entre un hôte CloudStack et le NAS

L’option **async** du serveur NFS n’a pas été activée à la configuration des NAS. Cette option permet au serveur NFS d’acquitter la copie des données avant leur écriture effective sur le disque. Cette option est dangereuse en cas de coupure brutale du NAS car elle entraîne la corruption des données. Les NAS étant branchés sur un circuit électrique avec onduleur, les risques sont limités et maîtrisés.

L’analyse du débit après activation de l’option au niveau du NAS donne des débits plus de 30 fois supérieurs à ceux initialement mesurés :

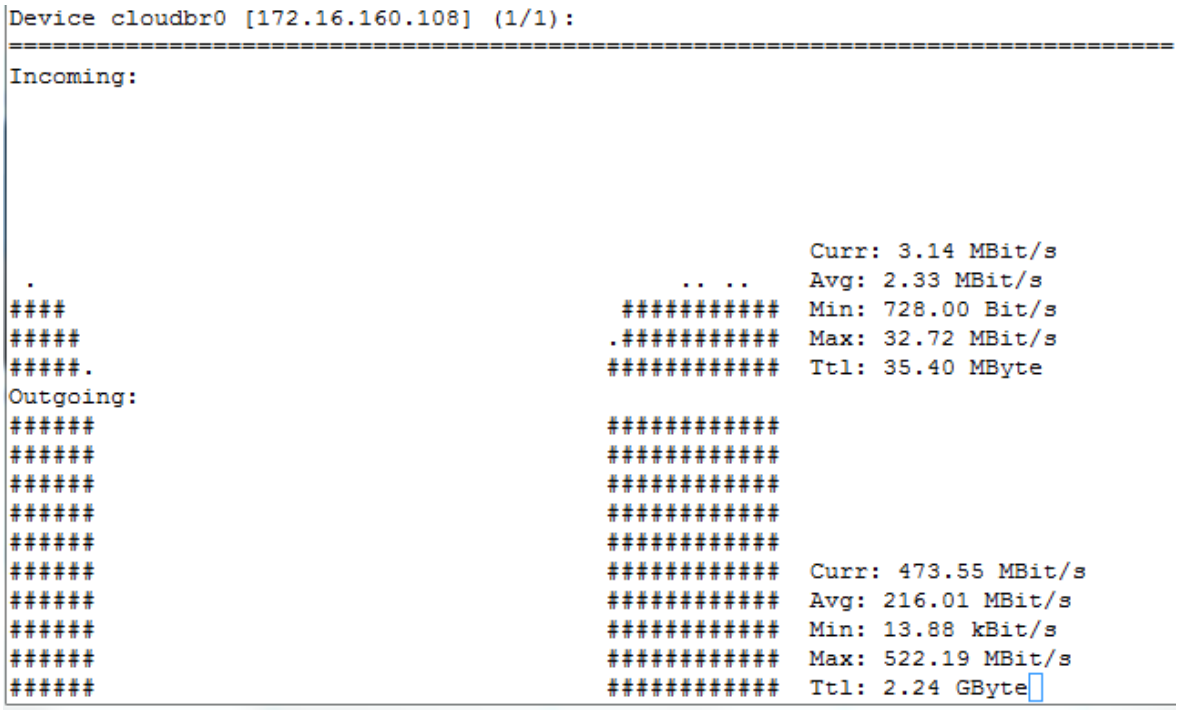


Figure 40 Activation de l'option NFS async et impact sur le débit réseau

L'installation d'une VM Windows 7 depuis l'image ISO prend dorénavant moins de 20 minutes, ce qui semble acceptable dans le cadre des TP d'installation Windows, et le provisionning d'une VM type Linux moins d'une minute et trente secondes.

VI.3.1.7 Sécurisation TLS

Par défaut, la plateforme CloudStack ne sécurise plus l'interface Web avec un certificat auto-signé.

La procédure pour le déploiement du certificat est assez compliquée, elle a donc également été traduite en français.

La procédure prévoit :

- la configuration du serveur Apache pour utiliser le certificat signé par l'autorité de certification ;
- la configuration de CloudStack lui-même pour qu'il injecte un certificat générique (qui répond à toutes les URL du domaine .mondomaine.com) dans les VM systèmes, dont la VM permettant l'accès aux consoles VNC. Cette procédure nécessite l'enregistrement de toutes les adresses IP publiques de la plateforme dans le DNS, ce qui peut être relativement long. L'exportation du certificat doit respecter le format standard PKCS#8.

Le vendredi 9 septembre 2016, une première tentative a été faite. Seul le site est sécurisé. La VM CPVM n'accepte pas le certificat chiffré.

Une seconde tentative est effectuée le lundi 24 octobre :

- l'ensemble des adresses IP publiques de la plateforme sont inscrites dans le DNS (400 enregistrements) ;

- les certificats sont de nouveau exportés au format requis par CloudStack en utilisant l'outil openssl puis importés dans la plateforme ;
- la configuration globale du serveur de gestion est modifiée, celui-ci est ensuite redémarré ;
- les 2 CPVM sont arrêtées puis redémarrées pour que les certificats soient pris en compte : un simple redémarrage ne suffisant pas.

Les tests de validation sont concluants : accès à la console, copie de modèles entre les 2 zones.

VI.3.1.8 Test de montée en charge

Afin de tester la montée en charge de la plateforme, les comptes d'un stage complet ont été importés depuis l'annuaire LDAP. Le 12 septembre 2016, ces militaires ont été mis à contribution pour un test de montée en charge.

Ils se sont connectés en même temps à l'interface de gestion pour déployer une VM depuis un modèle avec une offre S (vCPU 1 Ghz et 1 Go RAM). La présentation de l'environnement, le déploiement des 24 stations et la connexion en SSH a mis moins de 10 minutes.

Ressources				Util. CPU «				Util. Mém. «			Util. Réseau «	
Nom	État	Status Alimentation	Instances	Cores	Total	Utilisé	Alloué	Total	Utilisé	Alloué	Lecture	Écriture
node1-cloud			12 / 12	4	9.31 Ghz (x2)	1.02 G hz	8.94 G hz	22.38 GB (x 2)	8.85 G B	10.00 GB	126.47 GB	72.07 G B
node2-cloud			0 / 0	2	3.19 Ghz (x2)	0.00 G hz	0.99 G hz	22.39 GB (x 2)	1.89 G B	1.50 G B	16.25 G B	5.72 GB
node3-cloud			0 / 0	4	9.31 Ghz (x2)	0.00 G hz	0.47 G hz	22.38 GB (x 2)	0.92 G B	0.25 G B	17.80 G B	3.87 GB
node4-cloud			7 / 7	4	9.31 Ghz (x2)	2.79 G hz	6.42 G hz	22.38 GB (x 2)	5.45 G B	7.50 G B	98.33 G B	42.97 G B
node5-cloud			12 / 12	4	9.31 Ghz (x2)	1.68 G hz	14.99 Ghz	16.64 GB (x 2)	13.16 GB	19.75 GB	123.60 GB	70.46 G B

Figure 41 Les métriques CloudStack lors du test de montée en charge.

Au moment du test, comme le montre les métriques ci-dessus, la plateforme accueille 31 VMs sur les 3 nœuds 1, 4 et 5 (qui composent la zone simple). La charge processeur et RAM reste faible, bien que le facteur de surallocation sur le nœud 5 soit presque atteint. Il faut en déduire que la puissance en processeur et RAM de l'offre de service utilisée (ici l'offre S) dans le cadre des tests est supérieure au besoin réel.

- Il faut très certainement créer une offre XS moins puissante. La valeure initiale semblait pourtant tout à fait raisonnable (1 Ghz de puissance CPU ne semble pas être particulièrement exagérée), celle-ci a tout de même été surévaluée.
- Les VM déployées lors de ce test ont été laissées à disposition des stagiaires qui ont pu continuer à les utiliser durant leur cursus. Les retours quant à cette utilisation ont été très favorables.

VI.3.2 Création des modèles

Pour faciliter l'adoption de la plateforme et faire accepter le changement, la mise à disposition de modèles est un atout majeur.

En effet, le déploiement de VM depuis un modèle est très rapide. Il répond à un besoin de tous les formateurs.

Plusieurs modèles ont ainsi été créés :

- CentOS 6 pour la cellule Linux ;
- XUbuntu avec serveur RDP pour le cours PRSI ;
- Windows 7 et 2008R2 pour la cellule Windows.

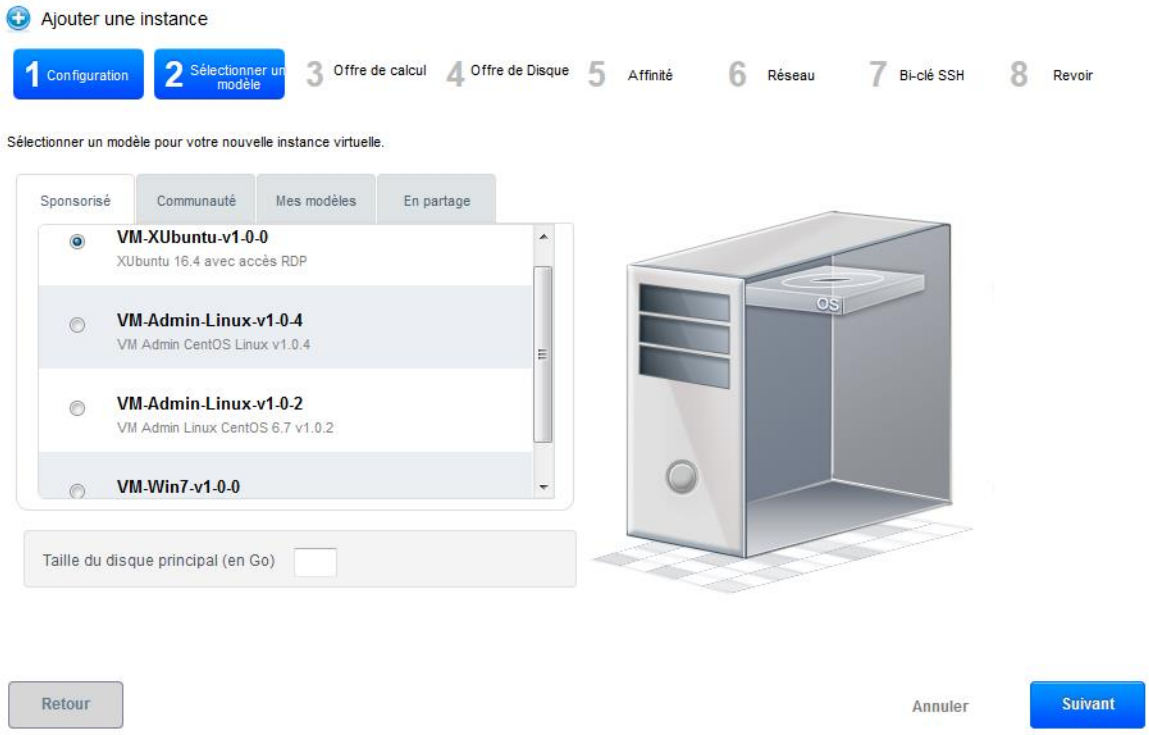


Figure 42 Les modèles proposés à la création d'une nouvelle instance

Le 16 septembre 2016, le modèle XUbuntu a été présenté aux acteurs du cours PRSI, la création de leurs comptes a été initiée, un compte administrateur de leur domaine a été configuré et le chargé du projet a été formé pour qu'il puisse accompagner ses collègues durant leurs tests.

Disposer d'un catalogue de VM « types » est réellement pertinent dans le cadre de la formation. La procédure de création d'une instance fait économiser du temps. Le déploiement d'une VM pour tous les stagiaires se fait en 10 minutes environ contre 20 à 25 minutes avec la solution VMware (lorsque tout se déroule correctement : accès au partage de fichiers, la copie de 24 fois le même fichier encombre le réseau, la décompression du fichier nécessite parfois plus d'espace que ce qui est disponible).

VI.3.3 Rédaction des procédures

Etant acteur du projet à tous les niveaux (administrateur, formateur et parfois en tant que stagiaire), il est temps pour moi de rédiger les procédures et transmettre les compétences techniques.

Le wiki de l'école semble être l'endroit idéal pour les déposer.

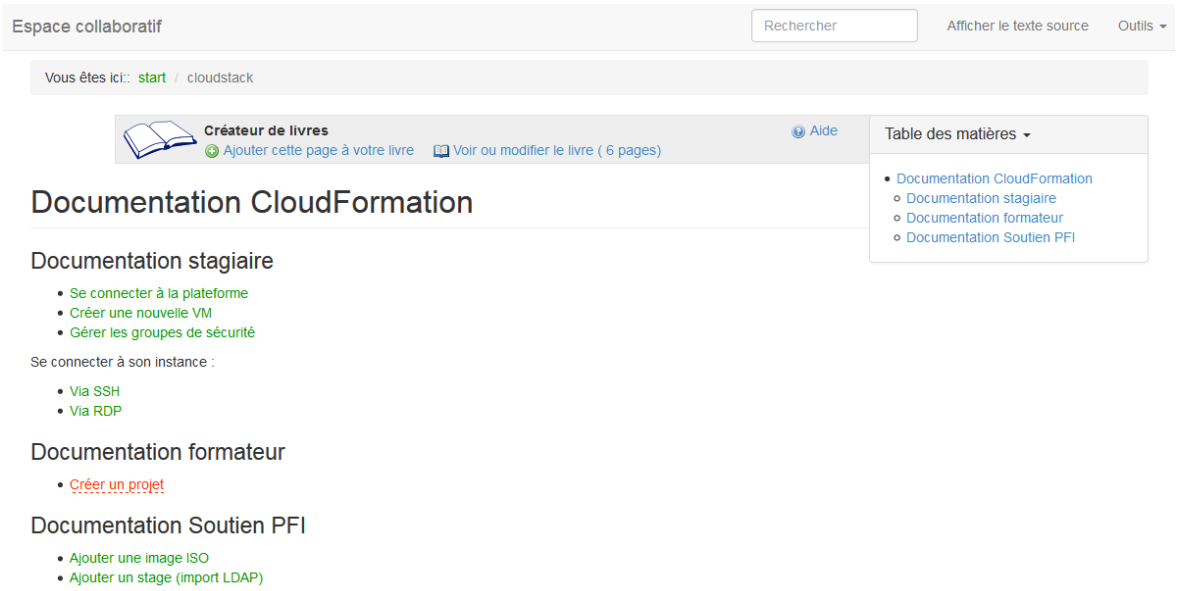


Figure 43 Les procédures dans le wiki de l'école.

Les premières procédures sont déjà écrites et concernent :

- le stagiaire :
  - se connecter à la plateforme ;
  - créer une nouvelle VM ;
  - gérer les groupes de sécurité ;
  - se connecter via SSH ;
  - se connecter via RDP.
- les formateurs :
  - création d'un modèle Linux ;
  - création d'un modèle Windows ;
  - configuration du serveur RDP sous Linux ;
  - configuration du serveur RDP sous Windows.
- les administrateurs :
  - ajouter une image ISO (admin) ;
  - ajouter un stage (import LDAP) (admin).

VI.3.4 Sécurisation de la plateforme

La fermeture de l'école durant les vacances de la Toussaint est un créneau idéal pour la mise en conformité de la plateforme avec les directives SSI idoines, permettant la mise à l'arrêt complet de la plateforme.

Durant la semaine du 24 au 28 octobre, nous avons sécurisé chaque nœud, conformément aux procédures internes de la cellule Soutien PFI-ENT :

- Interdire l'utilisation de la commande su ;
- Sécurisation du serveur openSSH :
  - Compte root interdit ;
  - Connexion sans mot de passe interdit ;
  - Limitation de l'utilisation du SSH aux seuls comptes administrateurs de l'ETRS (en plus du mien) ainsi qu'aux adresses IP des postes d'administration associés ;
  - Ajout d'un avertissement aux logs lors d'une tentative de connexion non autorisée.
- Changement du mot de passe de l'utilisateur root ;
- Redirection des logs
- Redirection des e-mails du système
- Sécurisation de la base de données MySQL ;

La communication entre les VM systèmes ayant déjà fait l'objet d'une configuration spécifique (passage au format TLS), les réseaux publics et invités étant séparés physiquement du réseau d'administration et de stockage, les calculateurs du cloud n'étant pas accessible depuis le réseau public (ne disposant pas d'adresses configurées pour ce réseau), l'ensemble de la plateforme est en conformité avec les règles SSI nécessaires.

VI.3.5 Accès depuis la zone « Vie »

L'accès aux VM de formation depuis la zone « vie » ou depuis le réseau « wifi » déployé sur la base est un besoin essentiel de la part des stagiaires. En effet, ces derniers doivent accéder aux salles de classe le soir pour continuer leur formation ou pour réviser. Cela implique également la mise en place de rondes de sécurité et de fermeture des batiments à des horaires tardifs de la part du service de sécurité de la base. Il arrive parfois que les stagiaires demandent l'accès aux salles de classe le week-end ou a des horaires plus tardifs durant les projets de fin de stages. Ces exceptions ont des conséquences sur l'organisation du service des militaires de garde.

La plateforme ayant fait l'objet d'une sécurisation globale et d'un durcissement des hôtes, les règles d'accès sur les pare-feu des différentes zones sont appliquées pour permettre l'accès distant.

Les différents tests effectués valident le bon fonctionnement et le débit réseau est suffisant à la prise de contrôle des invités par le protocole RDP.

VI.3.6 Travail communautaire

Mes différents travaux et recherches m'ont amenés à m'investir dans la communauté CloudStack à deux niveaux :

- au niveau du code du script de configuration setup-cloudstack-agent, qui utilise une commande non disponible sur CentOS 7. J'ai donc proposé un correctif qui devrait être intégré dans la prochaine version ;
- au niveau de la documentation. En effet, la documentation anglaise n'est traduite qu'en tchèque. Un début de traduction française avait été initié il y a plusieurs années, mais la documentation a depuis été beaucoup modifiée. Après avoir pris contact avec des responsables du projet, j'ai repris ce travail de traduction et je contribue régulièrement à son avancement.

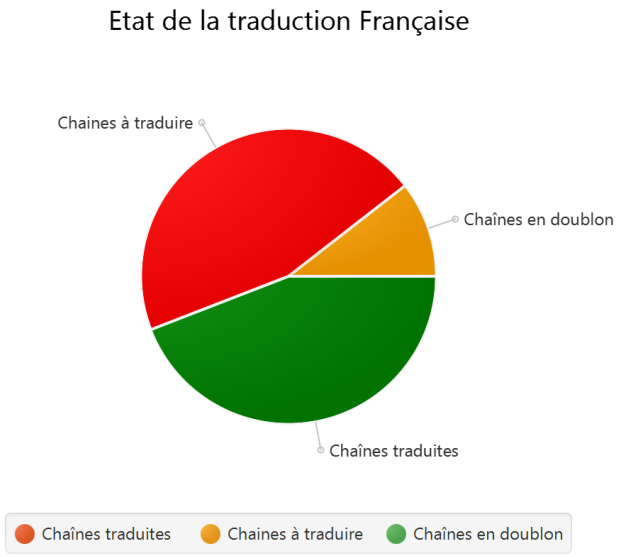


Figure 44 Etat de la traduction Française

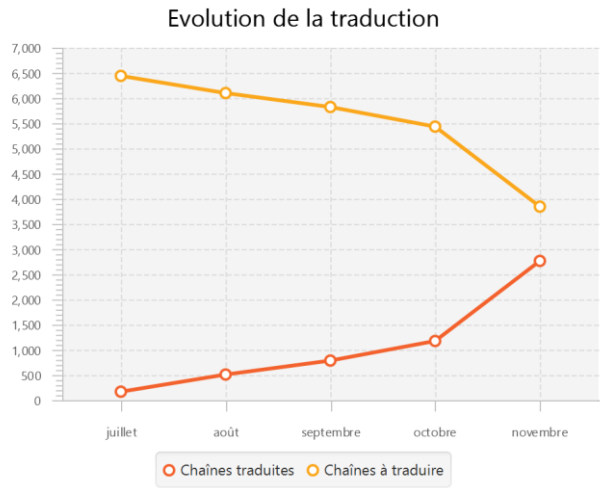


Figure 45 Evolution de la traduction

En attendant que la traduction française soit un peu plus avancée et qu'elle puisse être officiellement intégrée à la version officielle, j'ai temporairement créé un site internet dédié à l'hébergement de cette documentation en cours de traduction. Ce site est déjà référencé par Google et sera supprimé lorsque la copie du dépôt GitLab dédié à la traduction sera fusionnée avec l'officiel.

Figure 46 Le site internet de la documentation CloudStack en français.

L'ossature de la plateforme CloudStack définitive (le serveur de gestion, le commutateur et les NAS) est installée et configurée, prête à accueillir de nouveaux calculateurs. Les premiers stagiaires utilisent la plateforme dans le cadre d'actions de formation qui ne nécessitent pas trop de ressources. Les formateurs, quand à eux, s'en servent déjà intensivement. L'objectif initial principal du projet est donc atteint. Il reste encore des possibilités qui n'ont pas été explorées mais qui le seront au fur et à mesure de la montée en puissance de la plateforme. Ce qui n'est pas encore réalisable aujourd'hui le sera après l'intégration des nouveaux serveurs.

VII Evaluation et retour d'expérience

VII.1 Réponses aux problématiques

Administration du poste de formation

Le Cloud Formation ne nécessite pas l'installation de nouveaux logiciels, le système d'exploitation Windows 7 déployé sur le parc proposant nativement un client RDP. La solution VMware Workstation continuera à être déployée durant la phase de montée en puissance du Cloud Formation. Le coût des licences étant raisonnable, elle fera office de solution de secours dans un second temps.

Le gestionnaire du parc prévoit un allongement de la durée de vie des postes en place, notamment ceux de la gamme « hautes performances » puis un remplacement par des postes moins performants, le tout représentant des économies significatives qui pourront être ré-investies dans le matériel du Cloud Formation.

La programmation des stages sera également assouplie, la contrainte de puissance des postes étant supprimée lors de l'attribution des salles de classes aux différentes formations.

Souplesse de la solution

Les premiers retours d'expériences sont très positifs :

- pour le formateur :
    - qui accède à distance à sa station lors des travaux pratiques. Il peut reprendre là où il s'était arrêté à la fin du cours précédent ;
    - qui peut mettre en place une hiérarchie de services avec ses stagiaires et laisser le service en ligne durant plusieurs jours. Il est obligé de couper le service à la fin cours avec la solution VMware ;
    - pour qui la nouvelle solution représente un gain de temps non négligeable dès le début des cours : gain de temps de déploiement (le temps mesuré pour le déploiement d'une VM linux est de 1 minute et 30 secondes), simplicité de la solution, il n'a plus besoin de lancer des VM depuis des clés USB.
- pour le stagiaire :
    - qui peut continuer son travail en dehors des heures de cours depuis la zone vie ;
    - qui peut déployer une nouvelle station depuis l'interface web en fonction d'un catalogue de modèles, (sans devoir copier un modèle depuis le réseau, le dézipper et l'importer dans le logiciel VMware WorkStation, opération qui s'avère être fastidieuse).

Comparaison des solutions

CloudStack dispose des mêmes fonctionnalités que celles utilisées par les formateurs sur le logiciel VWware : création d'instantanés avant les travaux pratiques, déploiement de plusieurs VM et création de réseaux isolés.

La convivialité de l'interface web de CloudStack concurrence largement la

simplicité de l'interface de VMware.

La mise à disposition de modèles pour les stagiaires est largement améliorée sur le nouveau système. La création de modèle depuis une VM stoppée directement dans l'interface de CloudStack est une avancée significative et fait gagner du temps au formateur. Un script est également présent dans toutes les machines virtuelles Linux qui permet d'automatiser la préparation d'une VM pour devenir un modèle.

Gestion des comptes des stagiaires

L'importation des comptes par l'interface CloudStack directement depuis le serveur LDAP est rapide et accessible pour n'importe quel formateur.

La cellule soutien PFI-ENT tient toutefois à développer un script qui automatisera cette importation.

VII.2 Evaluation SSI

L'offre de service apportée par le Cloud Formation s'intègre dans l'espace numérique de travail destiné aux stagiaires et formateurs. Cet outil de formation a fait l'objet d'une démarche d'homologation, en suivant le guide de l'ANSSI [ANSSI-2014]. La possibilité offerte à un stagiaire ou un formateur de créer et d'administrer des systèmes virtualisés implique de considérer l'impact potentiel de ses nouvelles capacités sur l'architecture en place.

La prise en compte la sécurité durant toute la durée du projet a donc été un impératif de premier ordre. Suivre les recommandations de l'ANSSI [ANSSI-2013] nous a semblé être la meilleure solution pour respecter la dimension virtualisation de la SSI et ses nouvelles problématiques.

Nous avons répondu à toutes les recommandations de la note technique de 2013 :

- les documents relatifs à la politique de sécurité du site (FEROS, PES utilisateur, PES Administrateur) ont été mis à jour pour prendre en compte les problèmatiques liées à la solution Cloud Formation, et notamment le fait que les stagiaires disposent in fine des droits d'administration sur leurs machines virtuelles. Un audit de sécurité est programmé au 2nd trimestre 2017 ;
- les systèmes hôtes utilisent une version minimale de la distribution CentOS 7 à jour des dernières mises à jour de sécurités,
- le système d'exploitation de l'hôte est correctement configuré : l'authentification des administrateurs se fait via le serveur LDAP, l'accès en SSH est restreint aux postes d'administration et aux administrateurs, les journaux et les messages systèmes sont renvoyés vers les serveurs centraux ;
- les modèles de machines virtuelles sont configurées pour appliquer les mises à jour (configuration des dépôts et du proxy). Lors du déploiement, un nouveau mot de passe est généré pour le compte root par CloudStack ;
- l'administrateur du CAN/ENT est formé aux spécificités de la virtualisation et de la solution CloudStack. Il est abonné à la liste de diffusion announce@cloudstack.apache.org ;
- les logiciels CloudStack sont à jour ;

- les réseaux d'administration et de stockage sont physiquement séparés des réseaux publics et invités. Dans l'avenir, les 4 réseaux seront physiquements séparés, ce qui nécessite 4 interfaces réseaux et deux nouveaux commutateurs. Les hôtes sont isolés du réseau public.
- les formateurs entretiennent une solution de secours en cas d'indisponibilité de la plateforme ;
- un correspondant de chaque cellule cliente du projet est responsable du maintient en condition de sécurité de ses modèles et des VM ;
- des quotas sont mis en place pour restreindre l'utilisation des ressources par les clients de la plateforme ;
- la solution CloudStack cloisonne les systèmes invités par l'application de groupes de sécurité (pare-feu) ou par la création de VLAN ;
- la date et l'heure des hôtes sont synchronisées, leurs journaux sont centralisés ;
- des procédures sont disponibles pour aider à la création des modèles de machines virtuelles.

VII.3 Evolution de la plateforme

Le retard dans la livraison des serveurs a été la problématique la plus difficile à gérer. La demande de matériel ayant été validée, il devrait arriver. Mais quand ? Nous avons alors fait le choix d'utiliser le matériel déjà en notre possession, quitte à sacrifier certaines possibilités offertes, tout en concervant la possibilité de faire évoluer la plateforme vers la cible initiale.

Notre stratégie a donc été d'atteindre les objectifs essentiels, de laisser le temps rendre légitime l'outil, et d'y ajouter dès que possible le plus de puissance et de possibilités d'utilisations possibles.

La sauvegarde

Bien que nous ne disposions pas à l'heure actuelle du NAS destiné à accueillir les sauvegardes des VM de devoirs, un scénario a déjà été imaginé.

Un hyperviseur de l'ancienne génération sera concervé et intégré à la plateforme au sein d'un cluster qui lui sera dédié. Le NAS lui sera exclusivement rattaché.

Ainsi la sauvegarde d'une VM de devoir consistera à migrer la VM de son cluster d'origine vers le cluster de sauvegarde.

Le NAS est commandé, il sera livré en décembre 2016.

Montée en puissance

Dès la reception des nouveaux serveurs, ces derniers seront installés avec la distribution CentOS 7, durcis et intégrés dans le cluster actuel de CloudStack. Aucune configuration ne sera nécessaire du côté serveur de gestion.

Dès lors, l'utilisation de la plateforme Cloud pourra s'intensifier et l'achat de nouveaux matériels se justifiera.

A terme, l'ETRS pourra proposer de nouvelles formations en classes virtuelles ou en formations à distance tout en fournissant les outils nécessaires aux stagiaires via le cloud.

Gestion des devoirs

La migration des devoirs vers le Cloud est très attendue des formateurs. Il faut toutefois que la plateforme dispose de plus de puissance et que sa stabilité soit approuvée auprès des formateurs pour acquérir leur adhésion.

Ce cas d'usage est celui qui fera gagner le plus de temps aux formateurs. Pour qu'il puisse être réalisé, il faudra automatiser le déploiement d'une VM de devoir par stagiaire. Plusieurs solutions sont possibles, soit en utilisant simplement le logiciel CloudMonkey[11], l'interface en ligne de commande de la solution CloudStack, soit par la mise en place du logiciel d'automatisation Ansible[12], qui a la particuliarité de s'appuyer sur le protocole SSH pour automatiser les tâches.

Informatique responsable

La mise en place d'outils d'automatisation, comme Ansible, couplée avec la supervision des capacitées de la plateforme, devrait aboutir à une gestion intelligente des nœuds en fonctionnement au sein de la plateforme. En limitant leur nombre au juste besoin, notamment durant les périodes de vacances scolaires, l'ETRS devrait pouvoir mettre en place une véritable démarche d'informatique responsable.

Nouveaux usages

Lorsque la puissance de la plateforme sera suffisante, de nouveaux cas d'usages vont naturellement apparaître. Alors que les formateurs Linux utilisaient essentiellement l'interface en ligne de commande pour leurs démonstrations, ils utilisent dorénavant la plateforme CloudStack pour se connecter à leurs VM via le protocole RDP en environnement graphique, signe que les mentalitées évoluent.

Il y a fort à parier que d'autres changements vont encore apparaître, comme le déploiement d'appliances de serveurs applicatifs Java, la virtualisation applicative avec Docker qui devrait particulièrement intéresser le cours PRSI, l'utilisation de la plateforme pour les stages de fin de cursus ou la création d'une zone dédiée aux serveurs du CAN/ENT et leurs migrations depuis la solution VMware actuelle.

Poste de développement

Les tests effectués avec le Lieutenant Migeon ne sont pas concluants. Si le temps de lancement de la plateforme de développement Eclipse est correct, dans certaines conditions, l'autocomplétion des directives de programmation n'est pas assez réactive. Le logiciel firefox est également très long à démarrer. Une solution envisagée pour résoudre ces lenteurs est d'activer le stockage local de l'hyperviseur au profit de ce type de VM. Des analyses plus approfondies seront effectuée en phase 2.

[11] https://cwiki.apache.org/confluence/display/CLOUDSTACK/CloudStack+cloudmonkey+CLI
[12] https://docs.ansible.com/ansible/guide_cloudstack.html

VII.4 Bilan personnel

Durant le projet Cloud Formation, je suis intervenu à chaque étape de la gestion de projet, de la phase d'analyse à la réalisation en passant par la conception. J'ai pu mettre à profit mon expérience de la virtualisation, acquise au centre de données de Suresnes et des technologies opensource pour réaliser le projet de plateforme de cloud de formation avec des logiciels libres.

J'ai réalisé la phase d'étude pour proposer plusieurs solutions techniques à mes clients. Après avoir choisi ensemble la solution CloudStack, j'ai installé le matériel, mis en œuvre la solution, résolu les problèmes de configuration, optimisé les flux de données. De plus, j'ai assuré la mise aux normes SSI, ainsi que la promotion de la plateforme et accompagné les formateurs dans le changement d'outils. En parallèle, j'ai également rédigé la documentation d'exploitation et d'administration.

C'est ainsi que j'ai ainsi acquis l'expérience de la gestion d'un projet complet. J'ai appris à organiser des réunions, présenter nos travaux, rédiger une documentation technique et faire des choix non plus basés sur l'émotion ou le vécu mais sur la réflexion. J'ai eu l'occasion de prendre du recul, d'aller au bout de ma curiosité, de sortir de mes habitudes de technicien pour endosser le rôle d'un ingénieur, et surtout de travailler en équipe avec M. Pollet pour ensemble mener le projet à terme.

Côté technique, faire fonctionner la plateforme CloudStack s'est avéré être relativement complexe. Techniquement parlant, j'ai pu :

- capitaliser l'expérience acquise lors de l'installation des plateformes de tests ;
- appréhender de nouvelles technologies que je ne connaissais pas, notamment la partie virtualisation du réseau ;
- persévérer face aux difficultés, optimiser les flux du réseau, rechercher dans la documentation anglaise ;
- sécuriser les noeuds de la plateforme ;
- adapter rapidement les modèles, trouver des solutions techniques répondant aux besoins des clients ;
- optimiser les ressources disponibles ;
- prévoir la montée en puissance de la plateforme et l'intégration de nouvelles ressources.

Durant la phase d'étude, j'ai rencontré chez certains formateurs de la réticence quant à l'arrivée de la nouvelle plateforme.

C'est pour cette raison que j'ai axé mes efforts sur la communication et l'accompagnement du changement, en préparant par exemple des modèles de machines virtuelles spécifiques à la demande et dans des délais réduits.

L'aspect humain a été pour moi la partie essentielle de la réussite de ce projet. Dès les premières démonstrations, d'autres formateurs ont immédiatement saisi les nouvelles opportunités offertes et ont commencé à évaluer les capacités de la plateforme, puis à l'utiliser. A partir de là, l'adoption de la plateforme et la généralisation de son utilisation sont d'ores et déjà acquises.

Conclusion

L'École des Transmissions (ETRS) utilise depuis 12 ans VMware Workstation pour ses actions de formation. Cette technologie a trouvé ses limites en matière d'économies matérielles et dans son adéquation au domaine de la formation. L'ETRS désire désormais centraliser ses ressources et investir dans une solution de type « cloud » mettant en jeux 230 machines virtuelles sur 8 serveurs physiques.

La problématique à résoudre était de trouver une plateforme logicielle qui optimiserait les processus de formation, ouvrirait de nouvelles perspectives, moderniserait les actions de formations, s'intégrerait parfaitement dans l'existant tout en réalisant des économies budgétaires.

En adoptant une gestion cycle en V du projet, j'ai pu réaliser une expression des besoins, étudier différentes possibilités pour proposer des solutions, aider les acteurs du projet à faire leur choix, concevoir la plateforme, la mettre en œuvre, la configurer, la sécuriser et la valider, puis enfin accompagner le changement vers ce nouvel outil auprès des formateurs.

En début de projet, le choix de la solution s'est avéré être délicat : choisir une plateforme clé en main ou une plateforme en devenir ? La plateforme CloudStack a été retenue, car représentant le meilleur compromis au regard des besoins : stabilité et simplicité, sans sacrifier les aspects fonctionnalités et financiers.

En matière de gestion de projet informatique, la résistance au changement a nécessité le choix de techniques de communication adaptées, y compris au sein des groupes de formateurs : réunions, présentations, démonstrations personnalisées ; et avec le temps, la plateforme a trouvé sa place parmi les outils pédagogiques du formateur, modernisant nos actions de formation.

La solution mise en place n'est pas encore optimale, mais elle aura déjà permis un gain de temps au niveau des formateurs et leur aura ouvert de nouvelles perspectives pédagogiques.

A court terme, le nouveau matériel est attendu avec impatience pour intensifier son utilisation.

A moyen terme, les bénéfices de la solution vont apparaître dès que la plateforme aura atteint une certaine capacité d'hébergement. La programmation des salles sera alors plus souple, le renouvellement du parc informatique moins onéreux. Mais surtout de nouvelles perspectives s'ouvriront à l'école, que ce soit dans le domaine de la formation à distance ; ou pourquoi pas dans le domaine de l'hébergement, en mettant la plateforme (ou le retour d'expérience associé) à disposition des autres écoles du ministère de la Défense, dans le cadre d'un cloud communautaire.

Enfin, ce projet démontre que les technologies de virtualisation du monde libre sont fiables, performantes et permettent des économies non négligeables. Les administrateurs de l'ETRS s'intéressent à l'optimisation du poste de travail, qui pourrait s'inspirer de l'exemple de l'université Paris Descartes et de son projet de « Virtualisation avancée de stations de travail Windows sous Linux KVM » [liger-2015].

Bibliographie et références

Livres

[taoup] Eric Steven Raymond. 'The Art of Unix Programming'. Addison-Wesley. ISBN 0-13-142901-9.

[walsh-muellner] Norman Walsh & Leonard Muellner. 'DocBook - The Definitive Guide'. O'Reilly & Associates. 1999. ISBN 1-56592-580-7.

[tim-201608] Terre Information Magazine, 'Le commandement SIC des forces', août 2016.

[apache-admin-guide] Contributeurs CloudStack. 'Apche CloudStack 4.5 Administration Guide. Samurai Media Limited. ISBN 9888381830. 2015.

[goasguen-recipes-cloudstack] Sebastien Goasguen. '60 recipes for Apache CloudStack : using the CloudStack Ecosystem'. O'Reilly. ISBN 1491910135. 2014.

[apache-cloudstack-cloudcomputing] Navin Sabharwal - Ravi Shankar. 'Apache CloudStack Cloud Computing'. PACKT PUBLISHING. ISBN 1782160108. 2013.

[hennion-2012] Romain Hennion. 'Cloud computing : Décider, concevoir, piloter, améliorer'. Eyrolles. ISBN 2212134045. 2012.

Rapports et notes

[Jaouen-2014] IDEF Jaouen - IEF Gouriou - IEF Pollet. 'Rapport d'expérimentation CLOUD-Formation'. 2014.

[buche-2015] Xavier Buche. 'Cloud universitaire avec OpenStack - Mémoire d'ingénieur du CNAM'. 2015. [En ligne].

Disponible sur : http://www.fil.univ-lille1.fr/~buche/doc/os/memoire_cnam.pdf.

[SGA-2015] SGA. 'Mémento des coûts moyens du personnel civil 2014'. 2015.

[ANSSI-2013] ANSSI. 'Problématiques de sécurité associées à la virtualisation des systèmes d'information'. Note technique DAT-NT-011/ANSSI/SDE. Septembre 2013.

[ANSSI-2014] ANSSI, 'L'homologation de sécurité en 9 étapes simples'. Août 2014.

Disponible sur : https://www.ssi.gouv.fr/uploads/2014/06/guide_homologation_de_securite_en_9_etapes.pdf

[Cigref-2013] Rapport Cigref. 'Fondamentaux du Cloud Computing : Le point de vue des Grandes Entreprises'. mars 2013. [En ligne]

Disponible sur : http://images.cigref.fr/Publication/2012-2013-Fondamentaux-Cloud-Computing-Point-de-vue-grandes-entreprises.pdf.

[DGSIC-2013] Note N°768/DEF/DGSIC/SDAU du 12/07/2013. 'Evolutions technologiques du monde actuel et de l'informatique du ministère'. 2013.

[MINDEF-2014] MINDEF. 'Politique de l'informatique en nuage'. Février 2014.

[liger-2015] Jean-Marc Liger - Julien Joubin. 'Virtualisation avancée de stations de travail Windows sous Linux KVM'. 2015. [En ligne]

Disponible sur : https://2015.rmll.info/IMG/pdf/virtualisation_avancee_de_stations_de_travail_windows_en_environnement_libre_avec_linux_kvm-v2.pdf

Vidéos

[Deppierraz-2014] F. Deppierraz. 'Déployer son propre cloud avec OpenStack'. [En ligne]

Disponible sur : https://www.youtube.com/watch?v=_Eqdeog4cD4 (consulté le 22/02/2016).

Blogs

[Jacobs-2015] D. Jacobs. 'OpenStack ou Cloustack, quelle est la meilleur approche ?'. [En ligne]

Disponible sur : http://www.lemagit.fr/article/OpenStack-ou-CloudStack-quelle-est-la-meilleure-approche (consulté le 22/02/2016).

[SearchStorage-2007] SearchStorage TechTarget. 'LUN Management at the heart of SAN configuration'. [En ligne].

Disponible sur : http://searchstorage.techtarget.com/feature/LUN-management-at-the-heart-of-SAN-configuration (consulté le 05/03/2016).

[StorageReview-WDRED] Storage Rewiew. 'Western Digital Red NAS Hard Drive Review'. [En ligne].

Disponible sur http://www.storagereview.com/western_digital_red_nas_hard_drive_review_wd30efrx.

[linthium-2014] David Linthium. 'CloudStack, losing to OpenStack, takes its ball and goes home'. 2014. [En ligne].

Disponible sur : http://www.infoworld.com/article/2608995/openstack/cloudstack—losing-to-openstack—takes-its-ball-and-goes-home.html (consulté le 22/02/2016).

[phipps-2014] Simon Phipps. 'No, Citrix did not kill CloudStack'. 2014. [En ligne].

Disponible sur http://www.infoworld.com/article/2682557/open-source-software/open-source-software-no-citrix-did-not-kill-cloudstack.html (consulté le 22/02/2016).

[Paoli-J] Juliette Paoli. 'Cloud privé OpenStack : du succès, mais difficile à implémenter'. 2016. [En ligne].

Disponible sur : http://www.solutions-numeriques.com/cloud-prive-openstack-du-succes-mais-difficile-a-implementer/ (consulté le 22/02/2016).

[NIST] Nist. 'Cloud Computing'. [En ligne]

Disponible sur : https://www.nist.gov/itl/cloud-computing

Guides

[Sysfera] Sysfera. 'Analysis of Six Distributed File Systems'. [En ligne].

Disponible sur : https://hal.inria.fr/file/index/docid/789086/filename/a_survey_of_dfs.pdf.

[RHEL-Virtu7] RedHat. 'Guide de déploiement et d’administration de la virtualisation sour RHEL 7'. [En ligne]

Disponible sur : https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Virtualization_Deployment_and_Administration_Guide/index.html.

[dell-2014] Jose De la Rosa - Dell Linux Engineering. 'La virtualisation KVM sous RHEL 7 rendue simple'. 2014. [En ligne]

Disponible sur :

https://linux.dell.com/files/whitepapers/KVM_Virtualization_in_RHEL_7_Made_Easy.pdf
.

[RHEL-Demarrage-Virtu7] RedHat. 'Guide de démarrage de la virtualisation'. [En ligne].

Disponible sur : https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Virtualization_Getting_Started_Guide/index.html.

[RHEL-Secu-Virtu7] RedHat. 'Guide la sécurité de la virtualisation'. [En ligne].

Disponible sur : https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Virtualization_Security_Guide/index.html.

[Sudhansu-2015] Sudhansu Sahu. 'Cloudstack Tuning'. CloudStack Collaboration Conference Europe. 2015. [En ligne].

Disponible sur : http://events.linuxfoundation.org/sites/events/files/slides/CloudSTack-Tuning-Collab-2015.pdf.

Table des annexes

Annexe 1
Le Commandement SIC des forces

Extrait de Terre Information Magazine [tim-201608]

Le Commandement des systèmes d'information et de communication est créé le 1er juillet 2016 à Cesson-Sevigné, par dissolution de la division SIC d'appui au commandement du CFT (Commandement des Forces Terrestres) et de l'état-major de la brigade de transmissions et d'appui au commandement (BTAC) et l'intégration de la direction des études et prospective (DEP) et de l'École des Transmissions (ETRS).

Il constitue une capacité unifiée de commandement SIC pour l'Armée de Terre. Il permet de pourvoir et de générer des architectures de commandement performantes et protégées tout en mutualisant des moyens et des compétences rares, en anticipant l'évolution des technologies de l'information. Chargé de la collaboration opérationnelle des unités SIC, il prépare leur engagement et en garantit l'aptitude opérationnelle. Responsable de la gestion des capacités SIC, il appuie l'entraînement des états-majors opérationnels dans les exercices.

Subordonné au CFT, le COMSIC est :

- autorité organique des unités subordonnées ;
- tête de chaîne SIC pour l'ensemble de l'Armée de Terre.

Le COMSIC est constitué :

- D'un **état-major** articulé en :
    - une division Opérations composée du centre opérationnel des réseaux SIC Terre et de cybersécurité (CORTECS) ;
    - Une division Emploi, experte de l'emploi des SIC et chargée de la doctrine, des études capacitaires, de l'appropriation des nouveaux systèmes, de l'anticipation, de l'adaptation réactive et du retour d'expérience ;
    - Une **division formation composée d'une école**, l'ETRS, chargée de la formation SIC, Cyber et GE (guerre électronique) du personnel sur un périmètre interarméees voir ministériel.
- **5 régiments** en mesure d'armer les groupements de transmissions (GTRS) et d'intégrer des modules SIC interarmées en opération ;
- 1 compagnie de **combat de cyberdéfense** (807° CT), spécialisée dans la lutte informatique défensive ;
- 1 centre de **formation initiale** des militaires du rang (CFIM) à Dieuze.

Le COMSIC représente 4900 femmes et hommes, dont 4750 militaires et 150 civils.

Annexe 2
Le domaine de la formation

Former des administrateurs systèmes est un processus complexe. Il nécessite des plateformes informatiques (réseaux et serveurs) qui sont, avec les techniques de formation standards, installées, configurées et détruites régulièrement manuellement. Des droits spécifiques sont accordés (les stagiaires sont de facto administrateurs de leurs serveurs et de leurs commutateurs). Ces moyens représentent un investissement financier important (coûts des éléments actifs, de l'espace disque, des processeurs ou de la RAM). Cette méthode présente de nombreux facteurs de risques et nécessite souvent que les plateformes soient déconnectées du réseau du campus.

Il faut rappeler que l'ETRS propose des stages de cursus (stages longs obligatoires pour tous les militaires d'une même spécialité) et des stages courts d'adaptation à l'emploi. Les formateurs du cours systèmes interviennent uniquement durant les stages de cursus, ce qui implique que la plateforme Cloud soit dans un temps utilisé dans ce cadre. Cependant, la capacité d'assurer des stages d'adaptation à l'emploi doit être prise en compte.

Parmi les Technologies de l'Information et de la Communication pour l'Education (TICE), le formateur peut, pour atteindre son objectif pédagogique, faire appel à des environnements :

- d'enseignement à distance (EAD) ;
- de classe virtuelle (FOAD - Formation Ouverte et/ou A Distance).

ou à des outils :

- d'enseignement assisté par ordinateur (EAO - CAL : Computer Aided Learning) ;
- de simulation.

L'Enseignement A Distance (EAD) et les classes virtuelles

L'enseignement à distance est une forme d'enseignement sans présence physique d'un formateur et s'effectue à l'extérieur de l'établissement scolaire.

Plus spécifique, la classe virtuelle réunit à distance des stagiaires et un formateur en même temps et sur une durée définie.

L'essentiel de l'offre de l'ETRS porte sur l'EAD dans le cadre de la préparation des cursus ou de la remise à niveau des stagiaires avant leur arrivée à l'école. L'interaction entre le stagiaire et le formateur reste assez marginale et les contraintes du métier limitent les possibilités des classes virtuelles (présence synchrone). Des tests sont faits en ce sens pour des classes virtuelles en formation d'adaptation par le Major Desnos (Cours PRSI).

Ces cours sont suivis à distance : le stagiaire travaille dans son régiment sur son temps de travail.

L'Enseignement Assisté par Ordinateur (EAO) et les outils de simulation

L'EAO et les outils de simulation sont utilisés dans le cadre des cours en

présentiel.

> *L'E-Learning est l'utilisation des nouvelles technologies multimédias de l'Internet pour améliorer la qualité de l'apprentissage en facilitant d'une part l'accès à des ressources et à des services, d'autres part les échanges et la collaboration à distance.*
>
> *— Définition de l'Union Européenne*

L'EAO est une spécialité de l'informatique qui regroupe les logiciels permettant l'aide à l'apprentissage et les outils utilisés pour les créer. L'EAO implique que les ressources soient réparties sur chaque poste de formation (coût matériel et course à la puissance) et que les outils soient déployés et maintenus à jour (coût de maintenance).

Pour réduire ces coûts, une centralisation des ressources est nécessaire et l'élasticité de la solution doit être recherchée :

- avec un accès direct à la ressource qui limite les possibilités de sécurisation ;
- avec un accès par rebond à la plateforme (protocoles SSH, RDP ou VPN). L'accès est possible depuis l'extérieur dans le cadre de l'EAD.

Le Campus Area Network

Le campus numérique CAN (Campus Area Network) a pour fonction première d'offrir une infrastructure destinée à l'enseignement répondant au besoin global de partage de la connaissance.

Le CAN représente l'interconnexion de l'ensemble des réseaux de l'école, zone vie comprise[13].

L'Espace Numérique de Travail

Au sein de ce campus numérique, un portail internet offre un accès centralisé à l'ensemble des ressources pédagogiques disponibles sous la forme d'un Environnement Numérique de Travail (ENT - VLE : Virtual Learning Environnement). Ce dispositif fédère un ensemble de services dédiés à la formation tel que des classes virtuelles, des outils de visioconférence, des wikis.

L'ETRS utilise le portail ESUP Portal, qui est une solution Open Source soutenue par le consortium universitaire ESUP-Portail [14]. Ce portail propose notamment un serveur d'authentification central (CAS - Central Authentication Service) qui procure les fonctionnalités d'authentification unique SSO (Single Sign On) et de fournisseur d'identité [15] intégré à la fédération RENATER.

---

13 La majorité des stagiaires sont hébergés sur le site de l'école.
14 ESUP-Portail: https://www.esup-portail.org
15 IDP : Identity Provider : https://services.renater.fr/federation/participate/idp

Annexe 3
Etat de l'art

L'état de l'art s'intéresse d'abord au domaine strict de la virtualisation et du stockage pour ensuite étudier le monde de l'informatique en nuage : le "Cloud Computing".

La virtualisation

La virtualisation a pour objectif de faire fonctionner sur une seule plateforme matérielle plusieurs systèmes d'exploitation ou plusieurs applications.

Les avantages de cette technologie sont multiples :

- réduction de la facture énergétique (Green IT - Informatique responsable) ;
- augmentation du taux d'utilisation des éléments essentiels comme la mémoire ou le temps processeur ;
- réduction des coûts par mutualisation du stockage.

Un système d'exploitation étant conçu pour exploiter directement le matériel qu'il contrôle, il n'est normalement pas possible de faire fonctionner deux systèmes sur une même plateforme. La virtualisation nécessite des logiciels spécifiques.

L'étude ne prend pas en compte les systèmes de type **Isolateurs** qui permettent de faire tourner des applications différentes dans des contextes séparés. Cette technologie émergente prend de plus en plus d'ampleur, notamment avec le phénomène Docker. La virtualisation applicative ne correspond pas au besoin premier des formateurs. L'école attend une virtualisation système, bien que la virtualisation applicative puisse être un prolongement au projet de Cloud Formation.

La virtualisation de niveau 2

Un hyperviseur de type 2 est un logiciel qui s'installe sur un système d'exploitation existant (Windows, Linux, Mac, …). Une partie émulation du matériel permet d'héberger des systèmes d'exploitation, appelés « invités », directement "au-dessus" du système d'exploitation "hôte". Techniquement, l'hyperviseur adapte les instructions binaires du système invité à la volée et éventuellement il peut en remplacer certaines.

Même si cette solution nécessite généralement beaucoup de ressources, elle reste plus performante qu'un émulateur. Le système invité accède directement, dans la limite fixée par l'hyperviseur, au matériel (CPU, RAM).

Un émulateur est un logiciel se substituant à un matériel informatique.

Exemples d'hyperviseurs de niveau 2 : VMware Workstation ou Server, Oracle Virtual Box, Microsoft Virtual PC.

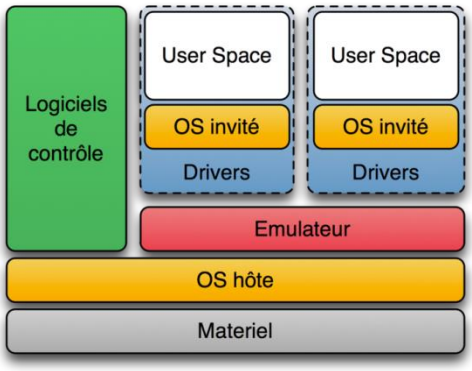


Figure 47 La virtualisation de niveau 2 (source wikipedia[16])

La virtualisation de niveau 1

Un hyperviseur de niveau 1 est un système d'exploitation très léger, spécialisé dans la virtualisation, qui offre l'environnement nécessaire aux systèmes d'exploitation invités pour s'adresser aux ressources matérielles. Cette technique de virtualisation est la plus performante, notamment dans le cas de la paravirtualisation (le système d'exploitation a conscience qu'il fonctionne sur une plateforme virtuelle), mais elle est aussi beaucoup plus onéreuse. Lorsque le système invité n'a pas été spécifiquement modifié pour la paravirtualisation, l'hyperviseur utilise dans ce cas les capacités de virtualisation du matériel, comme les technologies Intel VT-x ou AMD-V des processeurs, maintenant des performances proches d'un environnement classique.

Exemples d'hyperviseurs de niveau 1 : VMware Esx, Citrix XenServer, KVM, Microsoft Hyper-V.

Des fonctionnalités avancées permettent aux plateformes de virtualisation de niveau 1 d'offrir des services de haute disponibilité, de répartition de charge, d'élasticité. Des logiciels sont alors nécessaires pour contrôler plusieurs hyperviseurs regroupés en « grappes » ou en « cluster » : VMware Vcenter, Citrix XenCenter, Proxmox, Microsoft SCVMM.

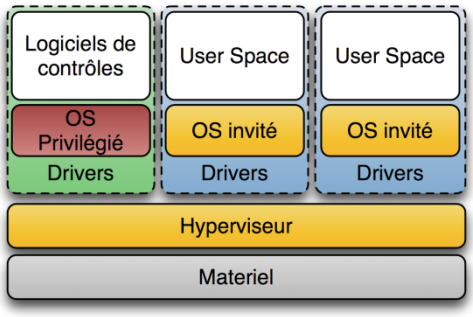


Figure 48 La virtualisation de niveau 1 (source wikipedia[17])

[16] https://fr.wikipedia.org/wiki/Virtualisation

Virtualisation et informatique en nuages (Cloud)

La virtualisation et l'informatique en nuage sont souvent confondus.

- La virtualisation a permis la consolidation des moyens informatiques et la mise en place des grands centres de données (DataCenter).
- L'informatique en nuage s'appuie généralement sur la virtualisation pour offrir une **informatique à la demande**. Il devient possible de louer un serveur virtuel comme un espace de stockage pour un temps donné et n'être facturé qu'en fonction de l'utilisation réelle.

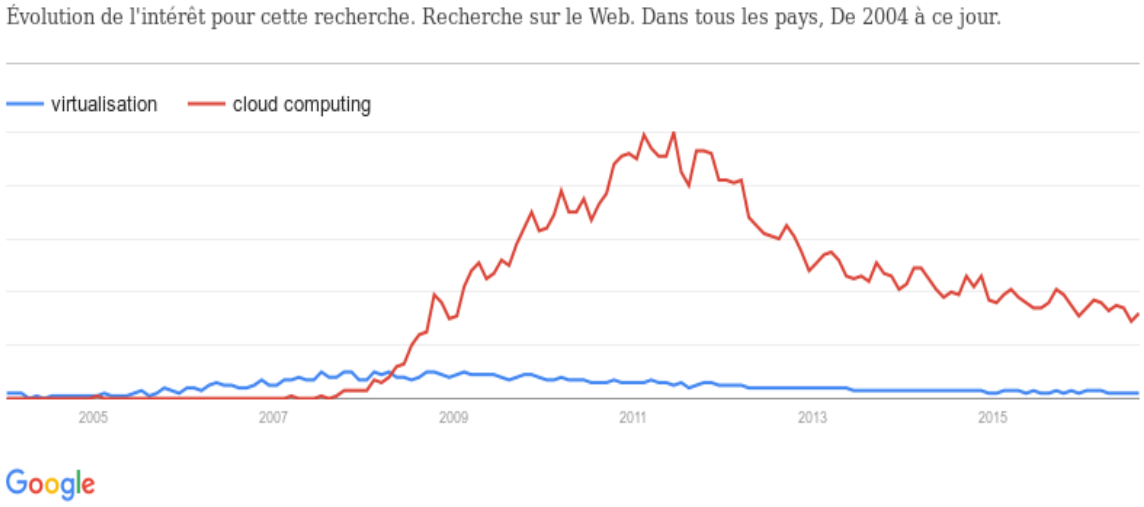


Figure 49 Evolution du nombre de recherches contenant les mots Virtualisation et Cloud Computing sur le moteur de recherche Google.

Comme le montre la courbe précédente issue de Google Trends, l'intérêt du public pour la virtualisation est apparu sur Internet bien avant celui pour le Cloud Computing.

Le NIST (National Institute of Standards and Technology) définit la technologie d'informatique en nuage ainsi [NIST] :

> *Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics (On-demand self-service, Broad network access, Resource pooling, Rapid elasticity, Measured Service); three service models (Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS), Cloud Infrastructure as a Service (IaaS)); and, four deployment models (Private cloud, Community cloud, Public cloud, Hybrid cloud).*
>
> — *NIST*

---

[17] https://fr.wikipedia.org/wiki/Virtualisation

Des logiciels sont nécessaires pour assurer toute la partie de mise à disposition des capacités demandées depuis la commande de la ressource jusqu'à sa mise à disposition et cela de manière totalement automatique et transparente pour l'utilisateur. Cette phase s'appelle le « provisionning ». Dans l'absolu, l'usager n'a pas conscience que sa ressource est hébergée sur l'un ou l'autre Datacenter de son fournisseur.

Pour le NIST, les logiciels dédiés aux plateformes de cloud computing doivent avoir les 5 caractéristiques suivantes :

- accès à la demande ;
- large bande passante ;
- réserve de ressources ;
- redimensionnement rapide ;
- facturation en fonction de l'utilisation des ressources.

Ces logiciels sont en mesure de gérer :

- des plateformes privées ;
- des plateformes communautaires ;
- des plateformes publiques : Amazon ECS, Microsoft Azure, ;
- des plateformes hybrides : privées et publiques.

Ces environnements procurent des connecteurs afin de piloter les différents hyperviseurs existants et présentent aux utilisateurs des API permettant de créer des interfaces de gestion personnalisés.

Le niveau d'abstraction de ces logiciels est tel que l'hébergement d'une nouvelle ressource se fait en toute transparence sur le plan géographique, matériel ou en type d'hyperviseur utilisé.

Les termes « informatique en nuage » et « à la demande » sont indisociables. La virtualisation n'est donc pas le cloud, tandis que le cloud s'appuie généralement sur la virtualisation.

Les différentes offres de Cloud

Différent niveaux de services sont définis dans le terme « cloud » :

SAAS

Les plateformes de « logiciel en tant que service » (Software As A Service) offrent l'accès à des logiciels installés sur des serveurs distants plutôt que locaux. Le service est payé à l'utilisation par un abonnement et non plus comme traditionnellement à la version.

Pour le service informatique d'une entreprise, ce modèle lui permet d'externaliser une partie (ou la totalité) de son système d'information. Une société choisit de s'appuyer par exemple sur les offres de Google ou de Microsoft pour la gestion de son domaine de messagerie. Les coûts d'investissement pour acheter et maintenir une plateforme de messagerie sont remplacés par des frais de fonctionnement (abonnement à la plateforme) en fonction de l'usage constaté.

PAAS

Les « plateformes en tant que service » (Plateform As A Service) offrent aux entreprises la capacité à se concentrer sur la configuration logicielle, tout le reste étant géré par le fournisseur de la solution. Cela permet le déploiement rapide des logiciels incompatibles avec les offres SAAS.

IAAS

Les plateformes du type « infrastructure en tant que service » (Infrastructure As A Service) ouvrent aux entreprises la perspective d'externaliser toute l'infrastructure physique de leur informatique, comme les serveurs mais également le stockage, le réseau et les moyens de sauvegarde.

Reste à la charge du service informatique de l'entreprise la configuration du système d'exploitation et du logiciel.

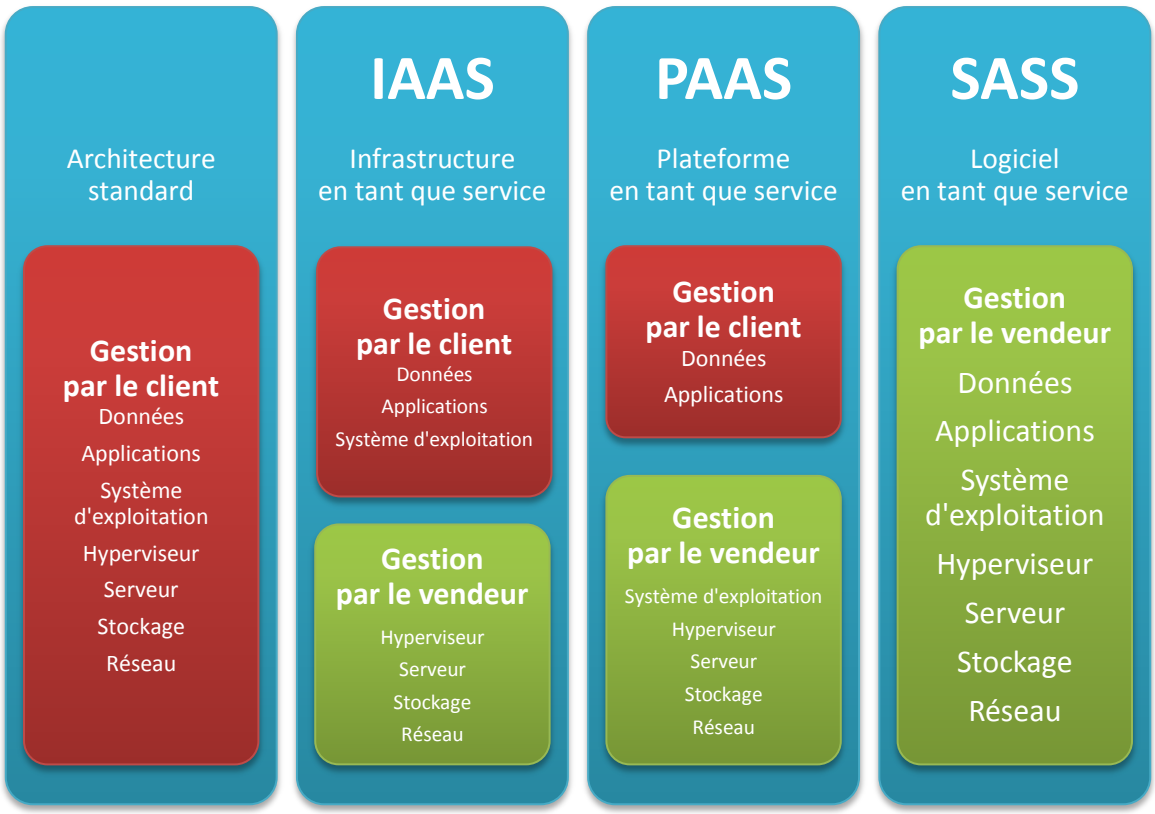


Figure 50 Les offres de services Cloud

Le stockage

Le stockage fait partie intégrante de tout projet cloud. C'est un facteur important en termes d'espace de stockage mais également du point de vue des performances : quantité d'entrées/sorties possibles (IOPS).

Pour un environnement de stockage de données froides (données non accédées depuis plus d'un an en écriture), la performance en lecture est intéressante. Une grosse capacité à bas prix sera recherchée.

Pour un environnement plus exigeant, comme le stockage des données d'une base

de données, la performance en écriture et en lecture est impérative. Dans de tels environnements, il est parfois nécessaire de sacrifier l'espace de stockage pour augmenter le nombre d'IOPS disponibles.

Une supervision standard vérifie logiquement l'espace disque disponible d'un espace de stockage. Une réaction s'imposera lorsque le seuil de 80% de remplissage d'un disque dur est atteint. Dans des environnements plus exigeants, ce sont les indicateurs de performances en lecture ou en écriture des disques qui seront surveillés. Lorsqu'un espace de stockage, composé de plusieurs disques, arrive à saturation en opérations de lectures ou d'écritures, l'ajout d'un ou de plusieurs disques sera pertinent pour augmenter les capacités d'entrées/sorties, sans se préoccuper d'optimiser les taux d'occupation de l'espace disque.

Comme le montre le graphique ci-dessous, extrait du résultat de l'analyse du disque Caviar Red [StorageReview-WDRED], les disques n'ont pas les mêmes performances :

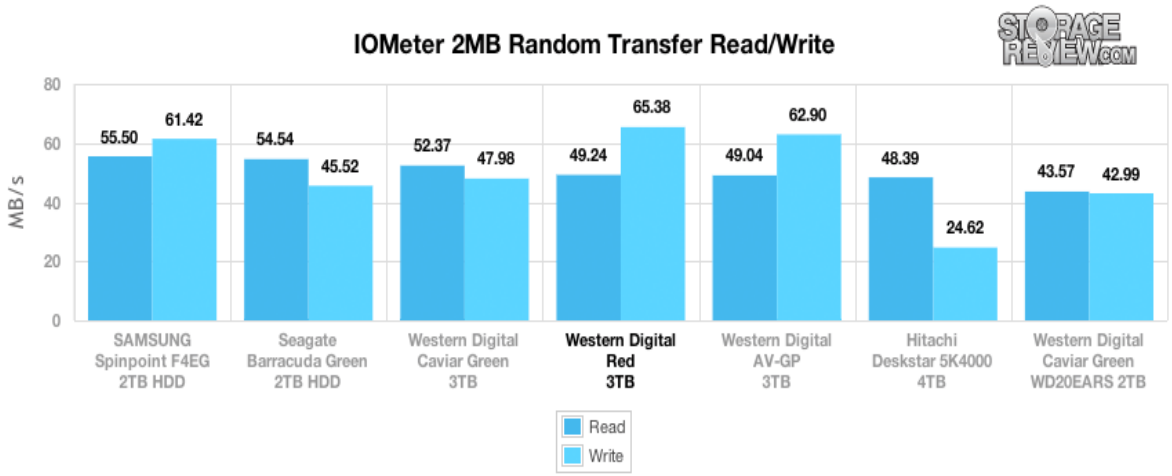


Figure 51 Comparatif des performances du disque Caviar Red 3TB avec d'autres disques du commerce.

Dans l'exemple précédent, le disque objet du test permet plus d'opérations d'entrées/sortie que le disque Hitachi. Il est donc très important de sélectionner avec précaution les disques destinés au stockage dès leurs achats pour garantir une efficacité maximale au serveur de stockage. Il est également judicieux d'acheter des disques du même modèle mais dans des séries différentes pour limiter les risques de défauts de fabrication (anomalies qui impactent une série) et éviter les pannes disques à répétitions (les disques de même série ont une probabilité plus élevée de tomber en panne en même temps).

Il existe deux technologies principales de stockage en réseau :

- la technologie SAN ;
- la technologie NAS.

La différence entre un stockage de type SAN (Storage Area Network) et de type NAS (Network Attached Storage) est le mode d'accès qui ne se fait pas en mode fichiers, mais en mode bloc.

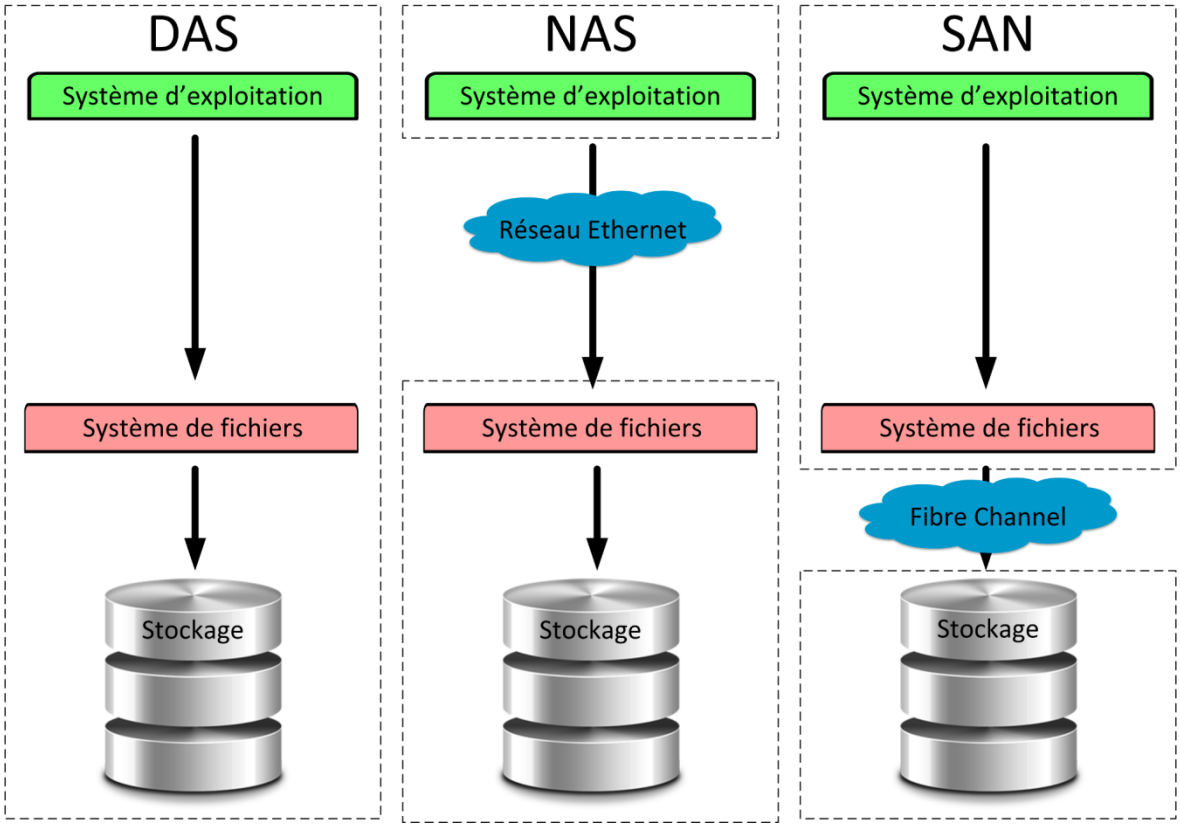


Figure 52 Différences entre DAS/NAS/SAN

Le schéma précédent illustre la différence entre l'attachement direct du disque (la technologie DAS) et les technologies de stockage en réseau.

- Dans le cas du NAS, le système de fichiers est géré par le serveur de stockage. Sur le réseau ne transitent que des protocoles de haut niveau de partage de fichiers (CIFS ou NFS par exemple).
- Dans le cas du SAN (qui se rapproche du fonctionnement du DAS), c'est le système d'exploitation qui gère le système de fichiers, comme si l'espace de stockage lui était directement rattaché. Sur le réseau, des protocoles de bas niveau offrent des accès de type bloc vers les disques.

Technologies SAN

Les technologies SAN (Storage Area Network) centralisent et mutualisent les ressources de stockage.

L'accès à leur espace de stockage par les clients se fait de manière très similaire aux accès à des disques locaux, sauf que les appels de bas niveaux sont envoyés sur le réseau, très souvent dédié et en fibre optique.

La mise en œuvre d'un réseau dédié en fibre optique permet d'offrir des performances incomparables, mais le prix est très élevé. Une interface fibre optique (voir deux pour la redondance) est nécessaire sur l'ensemble des serveurs devant accéder au stockage. Le protocole Fibre Channel est alors mis en œuvre et permet d'atteindre des débits supérieurs à 10 Gbit/s.

Pour réduire les coûts, il est possible d'utiliser un réseau IP dédié ou un réseau

commun avec les données de production pour faire transiter les accès disques. Les protocoles iSCSI (commandes SCSI sur TCP/IP) ou FcoE (Fibre Channel Over Ethernet) sont alors mis en œuvre, mais n'atteignent pas les mêmes performances.

Les espaces mis à disposition des serveurs sont appelés LUN (Logical Unit Number). Ils sont présentés à un ou plusieurs serveurs par une configuration appelée zoning. Un espace mis à disposition d'un système informatique est ensuite formaté et utilisé comme s'il était local.

Bien évidemment, plusieurs machines peuvent partager le même LUN, mais il faut alors formater les partitions avec un système de fichiers adaptés (OCFS2 – Oracle Cluster File System, VMFS – VMware File System, GFS2 – RedHat Global File System).

Chaque équipement constitutif d'un SAN dispose d'un identifiant unique : le World Wide Name (WWN).

L'ensemble des commutateurs du réseau est appelé **fabrique**.

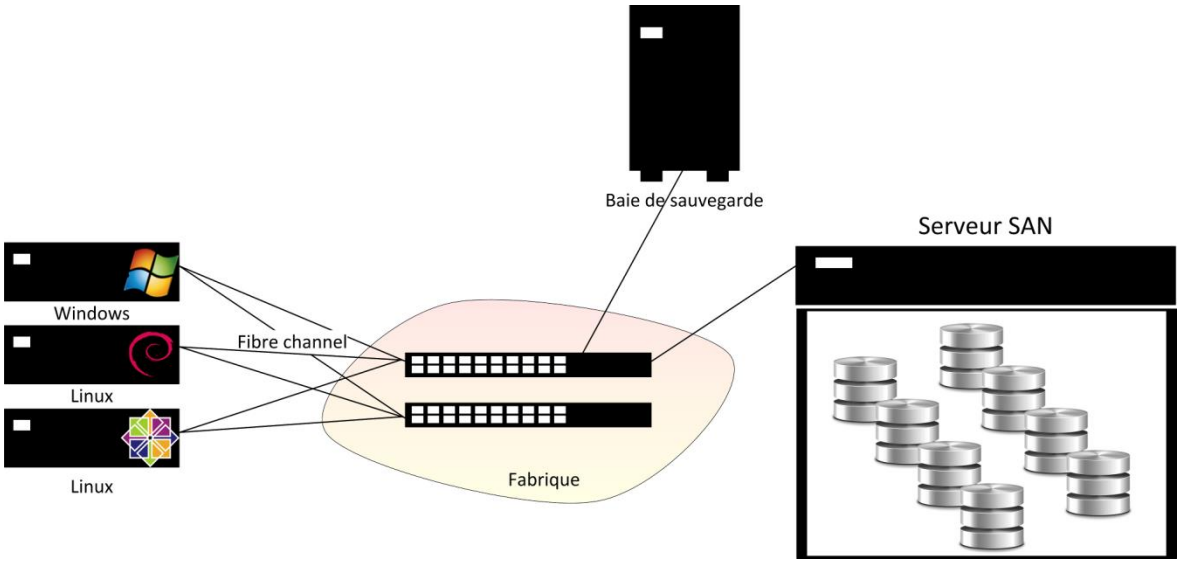


Figure 53 Schéma de fonctionnement d'un SAN

Technologies NAS

Un serveur NAS (Network Attached Storage) est un serveur de fichiers autonome. Il présente sur le réseau des espaces de données partagés basés sur des protocoles réseaux comme NFS, CIFS ou AFP.

Les données ne sont plus transmises par blocs de données, mais fichiers par fichiers. Les accès concurrents des clients sont gérés par le NAS. Le client n'a pas besoin de formater de partition. Le partage est directement utilisable par le système d'exploitation client.

Un NAS peut utiliser le LUN d'un SAN comme support de stockage pour le présenter au réseau sous forme de partages de fichiers.

DAAS

Les plateformes de « Données en tant que service » (Data as a service) mettent à la disposition de leurs clients un espace de stockage distant à la demande.

La définition du NIST ne prévoit pas cette offre de cloud. Elle a pourtant su s'imposer avec les offres types DropBox ou OneDrive.

Les systèmes de fichiers à disques partagés

Chaque nœud accède au même espace de stockage (par exemple via un SAN), le système de fichiers est monté sur l'ensemble des nœuds et gère un système de verrous pour empêcher les accès concurrents aux données.

Systèmes de fichiers distribués

Les systèmes de fichiers distribués (DFS) proposent deux grandes familles architecturales.

- Les systèmes de fichiers basés sur une architecture client/serveur : plusieurs serveurs gèrent et stockent à la fois les métadonnées et les données du stockage et forment un espace de nommage global. En ajoutant un serveur, les capacités de stockage et d'interrogation par les clients augmentent.
- Les systèmes de fichiers basés sur une architecture en cluster : les données et les métadonnées sont découplées. Les métadonnées sont centralisées ou totalement distribuées.

Les données sur les systèmes de fichiers distribués peuvent être parallélisées, cœurs être présentes sur plusieurs nœuds, pour augmenter leur disponibilité.

Les systèmes de fichiers distribués les plus usités sont :

- Hadoop Distributed File System (Apache Software Foundation), un système de fichiers distribué centralisé ;
- Ceph (Sage Weil), un système de fichiers totalement distribué ;
- GlusterFS (Gluster Core Team) qui fonctionne en client/serveur avec métadonnées distribuées.

L'état de l'art a fait le point des technologies du domaine de la virtualisation, du stockage et de l'informatique en nuage mises en œuvre dans un projet de cloud privé. Les termes et définitions présentés sont les éléments de vocabulaire nécessaires pour aborder l'étude du projet.

Annexe 4
Etude des plateformes IAAS du marché

Les plateformes de gestion de cloud sont de véritables orchestrateurs de centre de données (Datacenter Orchestrator) et fournissent les fonctionnalités de :

- gestion du stockage ;
- gestion des identités ;
- gestion du réseau ;
- répartition de la charge ;
- gestion des médias d'installation et des modèles de machines virtuelles ;
- gestion du firewall et des VPN.

Le tout bien évidemment accessible en self-service depuis un portail internet pour correspondre à la philosophie de l'informatique à la demande.

Apache CloudStack

Apache CloudStack est une plateforme logicielle « clé en main » opensource assurant la mise en œuvre d'une infrastructure informatique IAAS (Infrastructure As A Service). Cette technologie permet la gestion d'un cloud privé, publique ou hybride, le déploiement et la gestion de nombreux réseaux de machines virtuelles et autorise l'augmentation des capacités d'hébergement (élasticité-scalabilité).

Histoire du projet

Développée à l'origine par la société Cloud.com, rachetée par Citrix en 2011, CloudStack est depuis 2012 gérée par la fondation Apache. Le code est disponible sous licence Apache 2.0, ce qui est un certain gage de pérennité, de stabilité et de qualité du code.

Hyperviseurs supportés

CloudStack supporte les principaux hyperviseurs :

- VMware ESXi via VMware Vcenter ;
- KVM ;
- Citrix Xen via le XenServer ;
- Microsoft Hyper-V.

Fonctionnalités

CloudStack prend en charge l'ensemble des fonctionnalités attendues pour un cloud IAAS :

- orchestration des machines virtuelles ;
- gestion du réseau ;

- gestion des utilisateurs et de leurs comptes de gestion ;
- une API native et une interface de gestion internet permettant aux utilisateurs de gérer leurs machines virtuelles.

Sociétés ou communautés soutiens du projet

Ce projet est utilisé par de nombreux FAI (fournisseur d'accès à Internet) pour des offres publiques et par des sociétés privées pour leurs clouds privés. En Cœurs, CloudStack est utilisée par Ikoula (hébergeur de plus de 40 000 sites et infogère aujourd'hui plus de 5 000 serveurs dédiés et VPS) pour son offre de cloud privé.

CloudStack est considéré par la fondation apache comme un projet « TLP » (Top Level Project). Il est géré par son propre comité de management PMC (Project Management Commitee).

OpenStack

OpenStack est une autre plateforme logicielle de gestion de cloud privé ou public. Elle gère les nombreuses ressources (serveurs, stockages, réseaux) d'un datacenter via une interface web (le dashboard) ou via ses APIs et fonctionne avec les principales technologies actuelles, qu'elles soient propriétaires ou libres.

Histoire du projet

Le projet débute en juillet 2010 lorsque la société Rackspace Hosting et la NASA lancent conjointement un nouveau projet de Cloud open source qu'ils appellent OpenStack.

Le code d'OpenStack est disponible sous licence Apache.

Hyperviseurs supportés

OpenStack supporte les principaux hyperviseurs :

- VMware ESXi via VMware Vcenter,
- KVM,
- Citrix Xen via le XenServer,
- Microsoft Hyper-V.

Fonctionnalités

Son architecture est très modulaire, composée de nombreux projets corrélés comme par exemple : Nova pour la gestion des ressources, Swift pour le stockage des objets, Cinder pour le stockage, Neutron pour le réseau, Keystone pour la gestion des identités, Glance pour le service d'image.

OpenStack prend ainsi en charge l'ensemble des fonctionnalités attendues pour un cloud IAAS :

- orchestration des machines virtuelles ;
- gestion du réseau ;
- stockage des données et des objets ;

- gestion des identités ;
- gestion des images ;
- gestion de la télémétrie ;
- une API native et une interface de gestion internet permettant aux utilisateurs de gérer leurs machines virtuelles.

Sociétés ou communautés soutiens du projet

OpenStack est soutenue par la fondation OpenStack.

Les sociétés ayant rejoint la fondation OpenStack sont nombreuses, notamment OVH, Canonical, Red Hat, Cisco, Dell, HP, IBM, Orange, Cloudwatt, EMC, VMware, Intel, NetApp.

Les 2 clouds souverains Cloudwatt (Orange/Thalès) et Numergy (SFR/Bull) du projet Andromède (création d'un Cloud Souverain sécurisé pour les entreprises et les administrations françaises) de 2011 sont tous les deux basés sur OpenStack.

OpenNebula

OpenNebula procure une plateforme clé en main de cloud privé, public ou hybride.

Le code d'OpenNebula est disponible sous licence Apache 2.

Histoire du projet

OpenNebula est né d'un projet de 2005 et sa première version publique est sortie en mars 2008.

Hyperviseurs supportés

OpenNebula intègre les hyperviseurs :

- KVM ;
- ESXi ;
- ou XenServer.

Fonctionnalités

OpenNebula gère le stockage, le réseau, la virtualisation, la supervision et la sécurité pour déployer des services et des infrastructures distribuées.

Il propose les outils nécessaires au cloud pour :

- sa gestion ;
- son expansion ;
- sa sécurité ;
- la gestion des comptes utilisateurs.

Sociétés ou communautés soutiens du projet

La plateforme est gérée par la société internationale **OpenNebula Systems** et la communauté de développeurs.

VMware Vcloud Director

Vcloud est le projet de plateforme de cloud privé de VMware, se basant sur

VMware Vsphere. Comme pour les solutions précédentes, la création de nouveaux serveurs hôtes est très rapide, ce qui permet à l'infrastructure de s'adapter en taille au fur et à mesure des besoins.

Vcloud est un système propriétaire soumis à licence.

Histoire du projet

Le projet a été annoncé à la conférence 2008 de Vmworld à Las Vegas.

Hyperviseurs supportés

VMware Vcloud Director supporte les hyperviseurs suivants :

- VMware ESXi ;
- KVM ;
- Citrix Xen ;
- Microsoft Hyper-V.

Fonctionnalités

- VMware Vcloud Director gère des ressources virtualisées de calcul, réseau, stockage et sécurité qui peuvent être provisionnées en quelques minutes.
- Une API ouverte,
- Un contrôle de la consommation des ressources.

Eucalyptus

Eucalyptus est une plateforme opensource sous licence BSD pour la création d'un cloud hybride compatible avec Amazon Web Service (AWS).

Histoire du projet

Elle est intégrée à la distribution Ubuntu Enterprise Cloud (UEC) dès la version 9.04 mais est remplacée deux ans plus tard par OpenStack à l'occasion de la sortie de la version 11.10 (oneiric – Ubuntu Cloud Infrastructure). En septembre 2014, Eucalyptus est racheté par Hewlett-Packard et devient HPE Helion Eucalyptus.

Hyperviseurs supportés

- KVM sur RedHat/CentOS.

Fonctionnalités

- API compatible avec AWS ;
- gestion des machines virtuelles ;
- gestion des utilisateurs ;
- gestion du réseau et du stockage.

Annexe 5
Etat des hyperviseurs du marché

Un hyperviseur est une couche d'abstraction logicielle. Il assure les tâches de bas niveau, comme l'ordonnancement du CPU et l'isolation de la mémoire utilisée par les machines virtuelles. L'hyperviseur rend le matériel abstrait pour les VM, il est le seul à avoir la connaissance du réseau, du stockage ou des ressources vidéo. Les VM sont ainsi indépendantes de la plateforme matérielle.

Le choix de l'hyperviseur est crucial. Il déterminera les fonctionnalités de la plateforme et les performances des machines invitées.

L'éventail dans le domaine est large, allant de l'offre propriétaire très onéreuse à la solution opensource.

Tout hyperviseur nécessite un processeur dont la virtualisation matérielle a été activée.

ESXi Hypervisor (VMware)

VMware ESXi (Elastic Sky X) est un hyperviseur de type 1 développé par VMware, qui inclut son propre micro-noyau : le VMKernel. Les fonctionnalités de gestion de l'hyperviseur bare-metal ESXi sont intégrées directement au Vmkernel, ce qui réduit son encombrement à 150 Mo. Ainsi, sa surface d'attaque très réduite pour les logiciels malveillants et les menaces réseau, améliore la fiabilité et la sécurité.

Un microkernel est un noyau présentant le code minimum pour mettre en œuvre les mécanismes nécessaires d'un système d'exploitation. Les services du système d'exploitation sont placés à l'extérieur du noyau (en espace utilisateur)

L'hyperviseur ESXi est en libre téléchargement. Il n'est pas nécessaire d'acquérir de licence pour pouvoir le mettre en œuvre. Dans ce cas, certains services avancés sont inopérants.

L'installation d'un serveur VMware Vcenter permet d'activer ces fonctionnalités avancées (migration de VM, répartition de charge, haute disponibilité, tolérance de panne, migration du stockage) mais dans ce cas, il faudra s'acquitter d'une licence.

Les limitations imposées par l'infrastructure VMware (version 6) sont assez élevées :

- mémoire par invité : 4 TB ;
- mémoire par hyperviseur : 6 TB (voir 12 TB sur certaines plateformes) ;
- processeurs par invité : 128 ;
- processeurs par hyperviseur : 480 ;
- vCPU par CPU physique : 32 ;
- invité par hyperviseur : 1024.

L'intégration des hyperviseurs VMware dans une infrastructure CloudStack implique l'installation d'un serveur VMware Vcenter (soumis à licence payante).

XenServer

Citrix XenServer utilise l'hyperviseur de type 1 et open source Xen.

L'hyperviseur Xen est en partie intégré au noyau Linux depuis la version 3.0. Les systèmes d'exploitation type Linux ou BSD ont « conscience » de fonctionner sur un hyperviseur Xen ce qui optimise leur fonctionnement. Pour les systèmes propriétaire comme Microsoft Windows, l'hyperviseur s'appuie sur les fonctionnalités de virtualisation du processeur.

L'hyperviseur Xen est librement téléchargeable.

Les limitations de l'hyperviseur Xen sont :

- mémoire par invité : < 1 TB ;
- mémoire par hyperviseur : 16 TB ;
- processeurs par invité : 512 ;
- processeurs par hyperviseur : 4095.

XenServer est spécialement conçu pour une gestion efficace des machines virtuelles Windows et Linux et garantit une consolidation rentable des serveurs. Il offre les meilleures performances de sa catégorie pour la virtualisation des postes de travail.

KVM

Le système KVM (Kernel-based Virtual Machine) est une fonctionnalité du noyau linux, introduite dans le noyau 2.6.20 en 2007. Ce module permet d'utiliser n'importe quel noyau Linux, sur du matériel disposant de la virtualisation matérielle, comme hyperviseur. Il est donc naturellement un peu moins performant qu'un hyperviseur de type 1 dédié disposant d'un micronoyau comme c'est le cas pour un hyperviseur ESXi.

KVM est compatible avec un grand nombre de systèmes d'exploitation invités, dont Windows et Linux. Des logiciels graphiques permettent la gestion des VM.

Anaconda, le logiciel gérant l'installation d'une distribution RedHat/CentOS propose une option d'installation et de configuration d'un hyperviseur KVM.

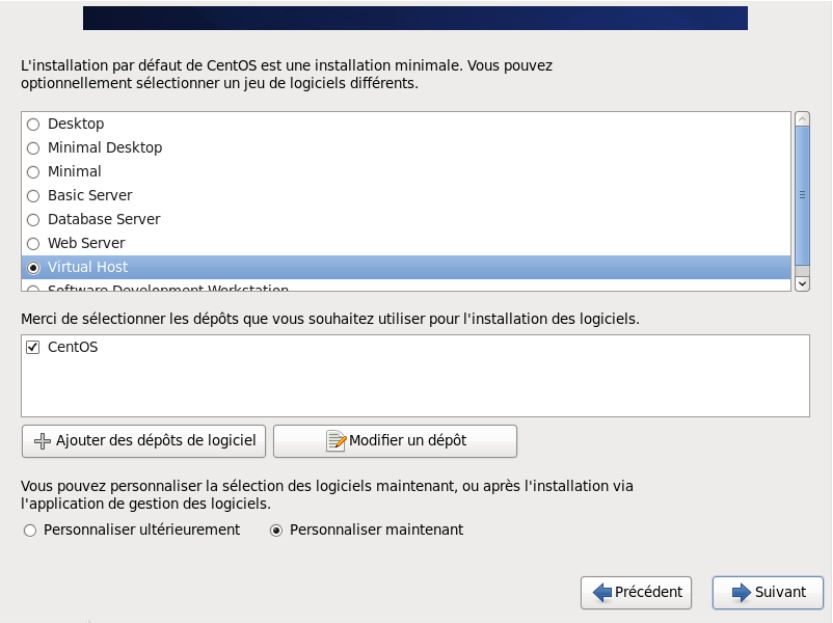


Figure 54 Anaconda propose une option d'installation d'un hyperviseur KVM.

Les limitations d'un hyperviseur KVM sont :

- mémoire par invité : < 4 TB ;
- mémoire par hyperviseur : 64 TB ;
- processeurs par invité : 240 ;
- processeurs par hyperviseur : 5120 ;
- vCPU par CPU physique : 8.

KVM étant une fonctionnalité du noyau Linux, il est très bien intégré aux solutions OpenSource et souvent très bien soutenu par la communauté d'utilisateurs, comme c'est le cas d'OpenStack, de CloudStack mais aussi de Proxmox.

Les annexes suivantes sont issues de notre expérience sur la plateforme CloudStack.

Elles serviront aux futurs administrateurs de la plateforme et toute personne amenée à installer une plateforme technique y trouvera des informations intéressantes pour faciliter son travail.

Annexe 6
Recueil des bonnes pratiques du déploiement de CloudStack

Déployer un cloud privé est un challenge. CloudStack est suffisamment flexible pour pouvoir être adapté à de nombreux besoins. Il est toutefois nécessaire de faire de nombreux choix technologiques, de les combiner et d'adapter la configuration de CloudStack au cas d'usage.

Voici un extrait de quelques recommandations (Best Practices) de la communauté CloudStack, que nous avons essayé de suivre dès la phase de conception :

Déploiement

- Avoir un environnement de développement. Ce n'est malheureusement pas possible dans l'état actuel de nos moyens physiques. Lorsque les nouveaux serveurs seront arrivés, une partie de l'ancienne plateforme pourra alors avoir cette vocation.
- Commencer par déployer un environnement beta, pour apprendre le fonctionnement du système. L'installation se fera avec une configuration basique, qui ne devrait prendre que quelques heures. L'installation avec un réseau plus complexe prendra plusieurs jours et le temps s'allongera en fonction de la complexité et de l'expérience sur la plateforme CloudStack. Pour un environnement complet en production, il faut compter au moins de 4 à 8 semaines pour un fonctionnement correct en ayant résolu tous les problèmes rencontrés lors de la phase d'intégration. Cette recommandation a été appliquée comme nous l'avons vu précédement lors de la mise en œuvre des différentes plateformes de tests.

Configuration

- Chaque hôte du système devrait être configuré pour n'accepter que des connexions issues d'autres éléments reconnus du système.
- Le point de montage du stockage primaire NFS ou le LUN ne devrait pas dépasser les 6 TB d'espace de données. Il est préférable d'avoir plusieurs petits espaces de stockage primaire par cluster qu'un seul gros. Protéger les points d'accès NFS en restreignant la plage d'adresses IP autorisée à se connecter.
- Faire appel à des agrégats de lien pour accroitre la bande passante et implémenter la tolérance aux pannes. Il peut être nécessaire d'utiliser des liens à 10G lorsque les besoins de la plateforme augmentent.
- Il est possible de faire de la surallocation de vCPU ou d'espace de stockage. Il est fortement déconseillé de faire de même avec la RAM.

Maintenance

- Superviser l'espace disque. La plupart des erreurs sur les VM ont lieu à cause d'un espace rempli par des logs sans système de rotation.
- Superviser le nombre total de VM par cluster et désactiver la possibilité de faire de nouvelles allocations lorsque l'hyperviseur est proche de la saturation, tout en conservant une marge de sécurité pour assurer la

répartition des VM en cas de panne d'un hyperviseur. Respecter les préconisations de l'éditeur de l'hyperviseur pour connaitre la valeur maximum à allouer par hyperviseur dans les options globales de CloudStack.

Le suivi de ces quelques recommandations permet de lancer le projet avec de bonnes bases.

Annexe 7
Rappels techniques Linux

Cette annexe traite des technologies mises en œuvre dans le cadre d'une plateforme CloudStack basée sur un hyperviseur KVM. Pour chacune des technologies, un rappel des notions et des options fondamentales est fait. L'administrateur, avant de se lancer dans l'installation de plateformes d'essais, pourra s'appuyer sur ce document pour vérifier qu'il dispose des compétences nécessaires à sa tâche.

Sudo - utilisateur administrateur

Par mesure de sécurité SSI, le compte root ne doit pas être utilisé pour l'administration des systèmes. Un compte d'administration doit être crée, disposant des droits suffisants. Il faut pour cela configurer la commande sudo.

Lorsqu'une instruction lancée nécessite les privilèges d'administration, elle est préfixée de la commande sudo.

L'utilisateur utilisé pour nos besoins sera l'utilisateur "pupitre".

```
[root]# useradd pupitre
```

Il doit appartenir au groupe "wheel".

```
[root]# usermod -aG wheel pupitre
```

Enfin le groupe wheel doit disposer des droits de sudo. Pour cela, éditer le fichier /etc/sudoers avec la commande visudo pour décommenter la ligne suivante :

```
[root]# visudo


...
%wheel  ALL = (ALL) ALL
...
```

L'utilisateur pupitre peut maintenant effectuer des tâches d'administration en préfixant les commandes avec **sudo**.

Configurer le firewall

CloudStack proposant des services réseaux, il faut configurer le pare-feu.

Ceci est nécessaire par exemple sur le serveur mysql si la base de données n'est pas sur le serveur de gestion, ou sur les noeuds, par exemple, pour autoriser la connexion au serveur de prise en main à distance VNC.

La configuration du pare-feu sous CentOS 7 se fait avec la commande firewall-cmd.

Le démon firewalld permet d'administrer dynamiquement le firewall avec la gestion de zones pour définir le niveau de confiance d'une connexion réseau ou d'une

interface.

Les configurations "en cours" et "permanente" sont séparées.

Utiliser la commande firewall-cmd

La commande firewall-cmd permet la gestion du firewall sous CentOS 7.

- Obtenir le status de firewalld

```
firewall-cmd --state
```

- Obtenir la liste des zones :

```
 firewall-cmd --get-zones
```

- Obtenir la liste des services supportés :

```
firewall-cmd --get-services
```

Important

Toute modification dans la configuration "en cours" sera perdue au prochain démarrage.

Autoriser un port/service dans une zone :

```
firewall-cmd [--zone=<zone>] --add-service=<service>
```

Autoriser un ensemble de port/service sur un protocole (TCP|UDP) :

```
firewall-cmd [--zone=<zone>] --add-port=<port>[-<port>]/<protocol>
```

Pour travailler sur la configuration permanente, il faut spécifier l'option *--permanent* à la commande firewall-cmd. L'option *--permanent* doit être la première de la liste des options.

```
firewall-cmd --permanent [--zone=<zone>] --add-service=<service>
```

Une règle doit donc être définie deux fois : pour la configuration "en cours" et pour la configuration "permanente".

Lire les logs

La mise au point de la plateforme nécessite de la part de l'administrateur de suivre les logs générés par les différents éléments de l'architecture CloudStack.

Différentes méthodes sont possibles.

Le suivi en temps réel

Le suivi des logs en temps réel se fait à l'aide de la commande tail et de son option -f.

```
$ tail -f /var/log/cloudstack/agent/cloud.log
```

Afficher les logs

Si la commande cat est bien connue de la plupart des administrateurs, elle n'est pas toujours pertinente pour le débuggage. Elle affiche en effet le contenu d'un fichier du début vers la fin. La pagination étant obtenue en passant la sortie de la commande à la commande less via un pipe.

La commande tactac permet d'afficher, comme sa grande soeur la commande cat, le contenu d'un fichier, en partant de la fin et en remontant vers le début. Cette version est particulièrement intéressante pour remonter dans l'histoire d'un fichier d'enregistrement.

```
$ tac /var/log/cloudstack/agent/cloud.log | less
```

Colorer les logs

La commande ccze permet de colorer les logs, ce qui facilite leur lecture.

```
$ tail -f /var/log/cloudstack/agent/cloud.log | ccze
```

Installer MySQL

CloudStack nécessite une base de données Mysql. Depuis la version 7 de CentOS, le serveur MariaDB a remplacé MySQL. Les deux serveurs de bases de données étant encore compatibles, le serveur installé ici est celui disponible par défaut : MariaDB.

Pour installer un logiciel sous CentOS 7, il faut utiliser le gestionnaire de paquet yum :

```
$ sudo yum install mariadb-server
```

Historiquement, la configuration de mysql se fait dans le fichier /etc/my.cnf. Il est aujourd'hui possible d'ajouter des options de configuration dans le répertoire /etc/my.cnf.d/.

Tout fichier dont le nom terminera par l'extension .cnf sera inclus dans la configuration de mysql.

Toute directive inclue dans une section [mysqld] de ces fichiers sera lue par le serveur mysqld, tandis qu'une directive dans une section [mysql] et [client] sera lue soit par le client mysql ou par tous clients mysql (dans le cas de [client]).

Les directives sont ajoutées selon le format variable=valeur sans espace de chaque côté du "=".

Pour afficher les directives prisent en compte par le serveur mysqld, il est possible d'utiliser la commande my_print_defaults :

```
$ sudo my_print_defaults mysqld
```

La documentation officielle de CloudStack demande d'ajouter quelques directives :

Directive	**Signification**
innodb_rollback_on_timeout	Le moteur InnoDB effectue par défaut un rollback de la dernière instruction d'une transaction qui est en timeout. Si la directive est positionnée à 1, dans ce cas, le moteur InnoDB

Directive	Signification
	effectue un rollback de la transaction complète.
innodb_lock_wait_timeout	Le temps en secondes durant lequel le moteur InnoDB attend qu'une transaction libère le verrou sur une ligne (pas sur une table) avant de renvoyer l'erreur ERROR 1205 (HY000) : Lock wait timeout exceeded ; try restarting transaction. Lorsque cela arrive, l'instruction (pas la transaction) fait l'objet d'un rollback. La transaction complète fait l'objet d'un rollback si la directive innodb_rollback_on_timeout est positionnée à 1.
max_connections	Le nombre de connexion clientes maximale. Il est possible de devoir augmenter cette variable en fonction de l'architecture de la plateforme.
log-bin	Pour activer les logs au format binaire.
binlog-format	Il y a trois formats de logs binaires : par instruction, par ligne ou mixte.

Directives à ajouter à mysqld

```
$ sudo vim /etc/my.cnf.d/cloudstack.cnf
[mysqld]
innodb_rollback_on_timeout=1
innodb_lock_wait_timeout=600
max_connections=350
log-bin=mysql-bin
binlog-format = 'ROW'
```

L'automatisation du démarrage et le premier lancement du service se font à l'aide de la commande systemctl :

```
$ sudo systemctl start mariadb
$ sudo systemctl enable mariadb
```

Après l'installation et la configuration de Mariadb, il est primordial de lancer le script de sécurisation de mysql :

```
$ sudo mysql_secure_installation
```

Se connecter en SSH

La connexion à distance à un serveur Linux se fait à l'aide de la commande ssh :

```
$ ssh utilisateur@host
```

La commande ssh dispose de nombreuses options dont voici celles qui vous seront utiles :

Option	commentaire
-p 2222	Se connecter au serveur ssh sur le port 2222
-i clé_prive	Spécifier un fichier contenant la clé privée pour s'authentifier avec une clé RSA ou DSA. Les clés sont généralement stockées dans le répertoire ~/.ssh/.

Options importantes de la commande ssh

Les machines virtuelles de gestion de CloudStack nécessitent une connexion sur le port 3922 et une authentification avec la clé /root/.ssh/id_rsa.cloud injectée par le serveur de management puis stockée sur chacun des noeuds. L'adresse IP utilisée est l'adresse IP de gestion interne de CloudStack, ce qui rend la connexion SSH impossible ailleurs que depuis l'hôte sur lequel fonctionne la machine virtuelle système.

Par exemple :

```
$ ssh -i /root/.ssh/id_rsa.cloud -p 3922 root@169.254.1.255
```

Les dépôts RPM

RedHat (et donc CentOS) utilise le format de paquet RPM (RedHat Packet Manager). Les paquets regroupés sous forme de dépôts peuvent être exploités grâce au logiciel yum (Yellow Dog Updater Modified). La commande yum gère les dépendances des paquets et les montées de versions.

Pour ajouter un dépôt, yum impose la présence d'un fichier dont l'extension est .repo dans le dossier /etc/yum.repos.d/. Chaque fichier décrit un ou plusieurs dépôts.

Chaque dépôt, représenté par son nom entre crochet [nom], est composé d'un nom, d'une URL d'accès à la racine du dépôt (protocole http, ftp, file) et d'une clé de signature gpg. Le dépôt ou la vérification de la signature peuvent être désactivés avec respectivement la directive enabled et gpgcheck.

Désactiver la vérification de la signature gpg reste une faille de sécurité.

Les dépôts pour CloudStack sont accessibles sur le site http://cloudstack.apt-get.eu. En navigant sur ce site, vous trouverez la racine du dépôt sous http://cloudstack.apt-get.eu/centos/7/4.9/.

Ces informations permettent de créer le fichier /etc/yum.repos.d/cloudstack.repo contenant :

```
[cloudstack]
name=Cloudstack
baseurl=http://cloudstack.apt-get.eu/centos/6/4.9/
enabled=1
gpgcheck=0
```

Le dépôt contient, entre autres, les paquets cloudstack-management pour installer le serveur de gestion et cloudstack-agent pour chaque noeud hébergant les machines virtuelles.

En fonction de la fonctionnalité ciblée, l'installation se fera avec la commande yum :

```
$ sudo yum install cloudstack-management
```

ou :

```
$ sudo yum install cloudstack-agent
```

Reverse proxy avec Apache

Le serveur de gestion CloudStack est une application développée en java, qui est gérée par le serveur applicatif tomcat (en version 7). Tomcat répond aux requêtes des clients sur le port 8080, qui n'est pas le port standard du protocole HTTP ni un port sécurisé.

Pour héberger de manière sécurisée (en https) sur le port standard (443), il faudra mettre en œuvre un mandataire inversé (reverse-proxy) au choix : apache ou haproxy.

Bien que plus rapide qu'Apache, haproxy est un projet plus jeune et actuellement en développement intensif.

La configuration ci-dessous est pour le serveur web Apache avec le module mod_http_proxy.

Installation

```
yum install httpd
systemctl enable httpd.service
systemctl start httpd.service
```

Configuration http

L'objectif est de faire prendre en compte par le serveur mandataire inverse une requête destinée à l'URL cloud.mondomainecloud.fr sur le port 80 et de la renvoyer vers le serveur tomcat en 8080.

```
NameVirtualHost 192.168.1.101:80

<VirtualHost 192.168.1.101:80>

  ServerName cloud.mondomainecloud.fr

  ProxyPreserveHost On
  ProxyVia On
  <Proxy *>
    Order deny,allow
    Allow from all
  </Proxy>

  ProxyPass /client/ http://localhost:8080/client/
  ProxyPassReverse /client/ http://localhost:8080/client/

</VirtualHost>
```

Pour rediriger toutes les requêtes dont le préfixe /client/ n'a pas été spécifié, il suffit d'ajouter :

```
  RewriteEngine on
  RewriteRule   "^/$"  "/client/"  [R]
```

Configuration https

L'objectif est d'héberger cette fois-ci CloudStack en https. Pour cela il faudra générer :

- une clé privée ;
- une clé publique dérivée de la clé privée ;
- une demande de signature de certificat ;
- la clé d'autorité de certification et son certificat ;
- signer la demande de certificat ;
- configurer apache.

Génération de la clé privée

```
openssl genrsa -out /etc/pki/tls/private/cloud.mondomainecloud.fr.key 2048
```

Génération de la clé publique

```
openssl req -new -key /etc/pki/tls/private/cloud.mondomainecloud.fr.key -out
/etc/pki/tls/certs/cloud.mondomainecloud.fr.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:FR
State or Province Name (full name) []:France
Locality Name (eg, city) [Default City]:Melesse
Organization Name (eg, company) [Default Company Ltd]:Ma compagnie
Organizational Unit Name (eg, section) []:IT
Common Name (eg, your name or your server's hostname) []:cloud.mondomainecloud.fr
Email Address []:antoine@mondomainecloud.fr

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Génération de la clé d'autorité et de son certificat

(requis ici pour les besoins de la démonstration)

```
openssl genrsa -out /etc/pki/CA/private/cakey.pem
Generating RSA private key, 1024 bit long modulus
.....................++++++
```

```
.........++++++
e is 65537 (0x10001)
openssl req -new -x509 -key /etc/pki/CA/private/cakey.pem -out
/etc/pki/CA/certs/cacert.pem -days 3650
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:FR
State or Province Name (full name) []:France
Locality Name (eg, city) [Default City]:Melesse
Organization Name (eg, company) [Default Company Ltd]:Ma compagnie
Organizational Unit Name (eg, section) []:IT
Common Name (eg, your name or your server's hostname) []:cloud.mondomainecloud.fr
Email Address []:antoine@mondomainecloud.fr
```

Signature de la demande de certificat

Configuration d'openSSL :

```
[ CA_default ]

dir             = /etc/pki/CA           # Where everything is kept
database        = $dir/index.txt        # database index file.
certificate     = $dir/certs/cacert.pem         # The CA certificate
serial          = $dir/serial           # The current serial number
private_key     = $dir/private/cakey.pem# The private key
```

Les deux fichiers suivants sont requis :

```
touch /etc/pki/CA/index.txt
echo '1000' > /etc/pki/CA/serial
openssl ca -in /etc/pki/tls/certs/cloud.mondomainecloud.fr.csr -out
/etc/pki/tls/certs/cloud.mondomainecloud.fr.crt
Using configuration from /etc/pki/tls/openssl.cnf
Check that the request matches the signature
Signature ok
```

Il faut protéger les certificats :

```
chmod 400 /etc/pki/tls/certs/cloud.mondomainecloud.fr.*
chmod 400 /etc/pki/tls/private/cloud.mondomainecloud.fr.key
chmod 400 /etc/pki/CA/certs/cacert.pem
chmod 400 /etc/pki/CA/private/cakey.pem
```

Configuration d'Apache

```
yum install -y mod_ssl
```

Le VirtualHost d'apache peut ressembler à ceci :

```
NameVirtualHost 192.168.1.101:443

<VirtualHost 192.168.1.101:443>

  ServerName cloud.mondomainecloud.fr

  SSLEngine on
  SSLCertificateFile /etc/pki/tls/certs/cloud.mondomainecloud.fr.crt
  SSLCertificateKeyFile /etc/pki/tls/private/cloud.mondomainecloud.fr.key

  RewriteEngine on
  RewriteRule   "^/$"  "/client/"  [R]

  ProxyPreserveHost On
  ProxyVia On
  <Proxy *>
    Order deny,allow
    Allow from all
  </Proxy>

  ProxyPass /client/ http://localhost:8080/client/
  ProxyPassReverse /client/ http://localhost:8080/client/

</VirtualHost>
```

Libvirt

Libvirt est un ensemble d'outils de gestion de la virtualisation.
Il est composé d'une bibliothèque, d'une API, d'un démon et d'outils logiciels.
Libvirt est utilisé par la majorité des hyperviseurs disponibles sur le marché.
Libvirt procure :

- la gestion à distance avec chiffrement TLS et certificats x509 ;
- la gestion à distance avec authentification kerberos et SASL ;
- la gestion des machines virtuelles, des réseaux virtuels et du stockage.

L'installation du démon libvirtd est obtenue par le paquet libvirt :

```
$ sudo yum install libvirt
```

Ce qui aura pour effet de télécharger et configurer libvirt et ses dépendances :

- libvirt-client ;

- libvirt-daemon ;
- libvirt-daemon-config-network ;
- libvirt-daemon-driver-interface ;
- libvirt-daemon-driver-network ;
- libvirt-daemon-driver-nodedev ;
- libvirt-daemon-driver-nwfilter ;
- libvirt-daemon-driver-qemu ;
- libvirt-daemon-driver-secret ;
- libvirt-daemon-driver-storage ;
- libvirt-daemon-kvm ;
- libvirt-daemon-config-nwfilter ;
- libvirt-daemon-driver-lxc ;

CloudStack utilise libvirt pour gérer à distance les machines virtuelles hébergées par les noeuds : démarrage, arrêt, migration.

Pour que CloudStack puisse correctement utiliser libvirt, il faudra sur chacun des noeuds :

- autoriser le démon libvirtd à écouter sur des connexions TCP non sécurisées et sans authentification ;
- refuser à libvirt de faire du DNS Multicast ;
- fixer le port tcp sur le numéro 16509.

La configuration du démon libvirtd se situe dans le fichier /etc/libvirt/libvirtd.conf :

```
$ sudo vim /etc/libvirt/libvirtd.conf
listen_tls = 0
listen_tcp = 1
tcp_port = "16509"
auth_tcp = "none"
mdns_adv = 0
```

Sans oublier de mettre le démon libvirtd à l'écoute du réseau en décommentant la ligne suivante :

```
$ sudo vim /etc/sysconfig/libvirtd
LIBVIRTD_ARGS="--listen"
$ sudo systemctl restart libvirtd
```

Il est possible de vérifier que le démon libvirtd est bien à l'écoute sur le réseau avec la commande netstat :

```
$ sudo netstat -tapn | grep 16509
tcp        0      0 0.0.0.0:16509           0.0.0.0:*           LISTEN
12306/libvirtd
```

```
tcp6       0      0 :::16509                :::*                    LISTEN
12306/libvirtd
```

ou avec la commande ss :

```
$ sudo ss -tuna | grep 16509
tcp    LISTEN     0      30         *:16509                 *:*
tcp    LISTEN     0      30        :::16509                :::*
```

Il ne faudra pas oublier d'autoriser l'ouverture du port 16509 dans le firewall avec la commande firewall-cmd :

```
firewall-cmd --zone=public --add-port=16509/tcp --permanent
```

VNC via QEMU.

Une machine virtuelle de gestion est dédiée à la gestion des consoles des VM dans une infrastructure CloudStack : la CPVM (Console Proxy VM). Elle permet à un client de prendre le contrôle de sa VM depuis l'interface web CloudStack via le protocole VNC.

Par défaut, le serveur VNC n'écoute pas les connexions provenant du réseau, mais uniquement celle provenant de l'adresse de loopback 127.0.0.1. Il est donc nécessaire de modifier ce comportement en décommantant la ligne suivante du fichier /etc/libvirt/qemu.conf :

```
$ sudo vim /etc/libvirt/qemu.conf
vnc_listen="0.0.0.0"
```

La documentation d'installation de CloudStack prévoit l'ouverture des ports de 5900 (le port par défaut de VNC) jusqu'au port 6100, soit 200 machines virtuelles maximum par noeud de l'infrastructure.

```
firewall-cmd --zone=public --add-port=5900-6100/tcp --permanent
```

Une machine virtuelle aura donc sa console accessible via la machine virtuelle de proxy VNC à l'adresse IP de son noeud suivi d'un numéro de port situé entre 5900 et 6100.

Configurer un commutateur virtuel

Chaque machine virtuelle de l'infrastructure CloudStack nécessite un ou plusieurs accès aux réseaux disponibles. Cette connectivité est obtenue grace à la mise en œuvre sur chacun des noeuds d'un ou plusieurs commutateurs virtuels.

Ces commutateurs sont gérés grâce à libvirt.

Avant de commencer la configuration d'un commutateur virtuel, il faut :

- désactiver netfilter (le pare-feu) sur le commutateur virtuel (bridge) ;
- activer le routage (forwarding) par le noyau.

La configuration du noyau se fait directement dans le fichier /etc/sysctl.conf ou dans un fichier .conf du dossier /etc/sysctl.d/. C'est cette deuxième solution qui est retenue :

```
$ sudo vim /etc/sysctl.d/cloudstack.conf
```

```
net.ipv4.ip_forward = 1
net.bridge.bridge-nf-call-ip6tables = 0
net.bridge.bridge-nf-call-iptables = 0
net.bridge.bridge-nf-call-arptables = 0
```

Le serveur doit être démarré pour que les modifications soient prises en compte.

CloudStack impose une restriction sur le nommage des commutateurs des hyperviseurs KVM. Les commutateurs doivent s'appeler cloudbr0, cloudbr1, cloudbrN, etc.

Pour créer un commutateur virtuel, il faut le déclarer dans un fichier ifcfg-cloudbrX du répertoire /etc/sysconfig/network-scripts/ :

```
$ sudo vim /etc/sysconfig/network-scripts/ifcfg-cloudbr0
DEVICE=cloudbr0
TYPE=Bridge
ONBOOT=yes
BOOTPROTO=none

$ sudo systemctl restart network
```

Les différents commutateurs virtuels peuvent être visualisés par la commande brctl du paquet bridge-utils :

```
$ sudo brctl show
bridge name     bridge id           STP enabled   interfaces
cloudbr0        8000.000000000000   no
virbr0          8000.52540065db1f   yes           virbr0-nic
```

Le commutateur que nous venons de créer ne dispose pas pour l'instant de connectivité vers le réseau physique. Pour cela, il faut lui attacher une interface :

```
$ sudo vim /etc/sysconfig/network-scripts/ifcfg-cloudbr0
TYPE=Ethernet
BOOTPROTO=none
DEFROUTE=yes
NAME=eth0
DEVICE=eth0
ONBOOT=yes
IPADDR=192.168.1.101
PREFIX=24
GATEWAY=192.168.1.254
DNS1=8.8.8.8
DNS2=8.8.4.4
...
BRIDGE=cloudbr0

$ sudo systemctl restart network
```

En procédant de la sorte, la commande brctl permet de constater que l'interface eth0 a été attachée au commutateur, mais que cette interface a perdu sa configuration IP :

```
$ sudo brctl show
bridge name     bridge id           STP enabled   interfaces
cloudbr0        8000.000000000000   no            eth0
virbr0          8000.52540065db1f   yes           virbr0-nic

$ sudo ip add sh
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast master
cloudbr0 state UP qlen 1000
    link/ether 00:1a:a0:46:b3:2b brd ff:ff:ff:ff:ff:ff
3: virbr0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN
    link/ether 52:54:00:65:db:1f brd ff:ff:ff:ff:ff:ff
    inet 192.168.122.1/24 brd 192.168.122.255 scope global virbr0
       valid_lft forever preferred_lft forever
4: virbr0-nic: <BROADCAST,MULTICAST> mtu 1500 qdisc pfifo_fast master virbr0
state DOWN qlen 500
    link/ether 52:54:00:65:db:1f brd ff:ff:ff:ff:ff:ff
7: cloudbr0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
    link/ether 00:1a:a0:46:b3:2b brd ff:ff:ff:ff:ff:ff
```

Important

Le serveur n'est donc plus accessible depuis cette interface bien que le commutateur virtuel peut continuer à transférer le trafic réseau des machines virtuelles vers le commutateur physique. Cette configuration sera retenue pour les interfaces des réseaux physiques publics, ce qui améliore la sécurité de l'hôte.

Pour une interface d'administration, la configuration IP de l'interface sera appliquée sur le commutateur directement de cette façon :

```
$ sudo vim /etc/sysconfig/network-scripts/ifcfg-cloudbr0
DEVICE=cloudbr0
TYPE=Bridge
ONBOOT=yes
BOOTPROTO=none
TYPE=Ethernet
ONBOOT=yes
IPADDR=192.168.1.101
PREFIX=24
GATEWAY=192.168.1.254
```

```
DNS1=8.8.8.8
DNS2=8.8.4.4
```

Après redémarrage du réseau, le commutateur devrait normalement disposer de sa propre configuration IP :

```
ip addr sh dev cloudbr0
7: cloudbr0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
    link/ether 00:1a:a0:46:b3:2b brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.101/24 brd 192.168.1.255 scope global cloudbr0
       valid_lft forever preferred_lft forever
    inet6 fe80::21a:a0ff:fe46:b32b/64 scope link
       valid_lft forever preferred_lft forever
```

Partage de fichiers NFS

Une infrastructure CloudStack nécessite deux types de partages : le stockage primaire et le stockage secondaire.

Sauf cas particulier (utilisation d'un système de fichiers distribué), les partages qui sont utilisés sur une plateforme CloudStack sont du type NFS, qui est le standard du partage de fichiers sous Linux.

Dans sa version 4, NFS nécessite que le domaine soit correctement fixé sur l'ensemble des noeuds de cette manière :

```
$ vim /etc/idmapd.conf
Domain = mondomainecloud.fr
```

Lors d'une mise en place d'infrastructure conséquente, des serveurs NAS devraient supporter ces partages de fichiers.

Il reste possible de se servir du serveur de gestion comme d'un serveur NFS.

Commencer par créer les 2 dossiers qui serviront de partage :

```
mkdir -p /export/primary
mkdir -p /export/secondary
```

Le paquet nfs-utils doit être installé :

```
yum install nfs-utils
```

La configuration des partages se fait dans le dossier /etc/exports :

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

Les ports utilisés par le serveur NFS doivent être fixés en décommentant les lignes adéquates :

```
$ sudo vim /etc/sysconfig/nfs
LOCKD_TCPPORT=32803
```

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

Les partages peuvent maintenant être activés :

```
$ sudo exportfs -a
```

Sans oublier d'ouvrir les ports NFS sur le firewall :

```
firewall-cmd --zone=public --add-port=111/tcp --permanent
firewall-cmd --zone=public --add-port=111/udp --permanent
firewall-cmd --zone=public --add-port=2049/tcp --permanent
firewall-cmd --zone=public --add-port=32803/tcp --permanent
firewall-cmd --zone=public --add-port=32769/udp --permanent
firewall-cmd --zone=public --add-port=892/tcp --permanent
firewall-cmd --zone=public --add-port=892/udp --permanent
firewall-cmd --zone=public --add-port=875/tcp --permanent
firewall-cmd --zone=public --add-port=875/udp --permanent
firewall-cmd --zone=public --add-port=662/tcp --permanent
firewall-cmd --zone=public --add-port=662/udp --permanent
```

Après avoir relancé le serveur, il est primordial de tester le bon fonctionnement des partages NFS depuis le serveur de gestion (qu'un serveur NAS soit utilisé ou non…) :

```
mkdir /primary
mount -t nfs 192.168.1.101:/export/primary
touch /primary/test ; rm /primary/test
umount /primary
mkdir /secondary
mount -t nfs 192.168.1.101:/export/secondary
touch /secondary/test ; rm /secondary/test
umount /secondary
```

SELinux

SELinux (Security-Enhanced Linux) permet de définir une politique de contrôle obligatoire aux éléments du système.

La documentation de CloudStack propose de positionner SELinux dans son mode permissif. Pour cela, il faut éditer le fichier /etc/sysconfig/selinux :

```
$ sudo vim /etc/sysconfig/selinux
SELINUX=permissive

$ sudo reboot
```

Désactiver SELinux nécessite de mettre en œuvre d’autres mesures de sécurité.

Annexe 8
Recueil des éléments techniques

La mise en œuvre des plateformes de test a permis de recueillir un ensemble d'éléments techniques à regrouper avant de commencer une installation CloudStack.

Avant de commencer une installation de CloudStack, vous pouvez préparer les éléments suivants :

- Pour configurer une zone, il faut saisir les informations suivantes :

Champ	Observations
Nom de la zone	
DNS1 IPV4	Adresse IP d'un serveur DNS utilisé par les VM de la zone. Les adresses IP **publiques** de cette zone doivent avoir une route vers ce serveur ;
DNS2 IPV4	
DNS Interne 1	Adresse IP d'un serveur DNS servant à CloudStack pour les VM système dans cette zone. Les adresses IP **privées** des pods doivent avoir une route vers ce serveur.
DNS Interne 2	
Hyperviseur	CloudStack supporte les hyperviseurs suivant : XenServer, HyperV, KVM, VMware, Baremetal, OVM, LXC, OVM3.
L'offre de réseau	A choisir entre DefaultSharedNetworkOfferingWithSGService, DefaultSharedNetworkOffering, DefaultSharedNetscalerEIPandELBNetworkOffering, QuickCloudNoServices,
Nom de domaine	
Dédié	oui/non
Activer le stockage local pour les VM utilisateur	Ne pas stocker les disques des VM sur le stockage secondaire. Améliore les performances mais la VM est perdue en cas de défaillance système de l'hôte.
Activer le stockage local pour les VM système	Ne pas stocker les disques des VM systèmes sur le stockage secondaire. Améliore les performances mais la VM est perdue en cas de défaillance système de l'hôte.

Informations de configuration d'une zone

- Pour configurer un pod, il faut saisir les informations suivantes :

Champ	Observations
Nom du pod	
Passerelle réservée Système	La passerelle utilisée par les hyperviseurs du pod.
Masque de sous-réseau réservé Système	Le masque de sous-réseau utilisé par les hyperviseurs du pod.
Adresse IP de début réservée Système	
Adresse IP de fin réservée Système	

Informations de configuration d'un pod - réseau d'administration

- Pour configurer le réseau invité, il faut saisir les informations suivantes :

Champ	Observations
Passerelle pour les invités	La passerelle utilisée par les machines virtuelles.
Masque de sous-réseau des invités	Le masque de sous-réseau utilisé par les machines virtuelles.
Adresse IP de début pour les invités	
Adresse IP de fin pour les invités	

Informations de configuration d'un pod - réseau d'invité

- Pour configurer le réseau de stockage, il faut saisir les informations suivantes :

Champ	Observations
Passerelle	
Masque de réseau	
VLAN	
Adresse IP de début	
Adresse IP de fin	

Informations de configuration d'un pod - réseau de stockage

- Pour configurer un hôte dans un cluster, il faut saisir les informations suivantes :

Champ	Observations
Le nom de l'hôte ou son adresse IP	Le système DNS doit pouvoir résoudre le nom de l'hôte.
L'identifiant de connexion	Généralement root, sinon il faudra penser à configurer le fichier sudoers.
Le mot de passe	Le mot de passe du compte root ou de l'utilisateur configuré dans le fichier sudoers.
Les étiquettes permettant de classer les hôtes	

Informations de configuration d'un hôte

- Pour configurer le stockage primaire, il faut saisir les informations suivantes :

Champ	Observations
L'adresse IP du serveur	Serveur NFS, SMB/CIFS, S3 ou Swift.
Le chemin d'export	Dans le cas d'un partage NFS.

Informations de configuration du stockage primaire

Annexe 9
Procédure d'installation du manager CloudStack

Installation du système

Installation du serveur depuis un CD-ROM d'installation (version minimale).

- Durant l'étape de partitionnement, supprimer toutes les anciennes données éventuellement présentes sur le disque ;
- Durant l'installation, configurer le nom d'hôte : **cloud1** ;
- Choisir l'option "Installation minimale" ;

Configuration du réseau

Après l'installation, il faut impérativement vérifier la bonne résolution du nom de machine :

```
$ hostname
cloud1
$ hostname -f
cloud1.etrs.terre.defense.gouv.fr
```

Pour que la résolution soit effective, il faut configurer le fichier /etc/hosts ou s'assurer de la bonne résolution DNS.

L'adresse IP doit être configurée. Modifier le fichier /etc/sysconfig/network-scripts/ifcfg-eth0 :

```
$ vim /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
NM_CONTROLLED=no
ONBOOT=yes
BOOTPROTO=none
IPADDR=XXX.XXX.XXX.101
NETMASK=255.255.240.0
GATEWAY=XXX.XXX.XXX.254
DNS1=XXX.XXX.XXX.XXX
DNS2=XXX.XXX.XXX.XXX
service network restart
```

SELinux

Mettre SELinux en permissif :

```
$ vi /etc/sysconfig/selinux
SELINUX=permissive
```

Configuration du proxy

L'école étant derrière un proxy, il faut le configurer pour yum et get :

```
$ vi /etc/yum.conf
proxy=http://proxy:8080
```

Configurer le proxy pour wget (utilisé pour télécharger les images systèmes) :

```
$ vi /etc/wgetrc
https_proxy = http://proxy:8080/
http_proxy = http://proxy:8080/
ftp_proxy = http://svrproxy.ent-etrs.net:8080/
use_proxy = on
$ vi /etc/profile.d/proxy.sh
export https_proxy = http://proxy:8080/
export http_proxy = http://proxy:8080/
export ftp_proxy = http://proxy:8080/
export no_proxy="localhost,127.0.0.1,…"
use_proxy = on
```

Installation de logiciels complémentaires

```
$ yum install ccze vim epel-release wget
```

NTP

Installation des logiciels :

```
$ yum install ntp
```

Configuration du fichier /etc/ntp.conf :

```
server XXX.XXX.XXX.XXX iburst
server XXX.XXX.XXX.XXX iburst
[...]
restrict default kod nomodify notrap nopeer noquery
restrict -6 default kod nomodify notrap nopeer noquery
restrict 127.0.0.1
restrict -6 ::1
```

- Automatiser le lancement de ntpd

```
$ chkconfig ntpd on
$ service ntpd start
```

CloudStack

Dépôt Cloudstack

Créer le fichier /etc/yum.repos.d/cloudstack.repo

```
[cloudstack]
name=Cloudstack
baseurl=http://cloudstack.apt-get.eu/centos/6/4.8/
enabled=1
gpgcheck=0
```

Configuration des services requis

```
$ yum -y install nfs-utils mysql-server
```

Configuration de NFS

Le serveur NFS sera utilisé uniquement en absence de serveur NAS.

```
$ vim /etc/sysconfig/nfs
LOCKD_TCPPORT=32803
LOCKD_UDPPORT=32769
MOUNTD_PORT=892
RQUOTAD_PORT=875
STATD_PORT=662
STATD_OUTGOING_PORT=2020
$ vim /etc/idmapd.conf
Domain = etrs.terre.defense.gouv.fr
```

Configuration de mysql-server

```
$ vim /etc/my.cnf
[mysqld]
...
innodb_rollback_on_timeout=1
innodb_lock_wait_timeout=600
max_connections=350
log-bin=mysql-bin
binlog-format = 'ROW'
$ service mysqld start
$ chkconfig mysqld on
```

Configuration du noyau

- Autoriser le forwarding IP V4

- Désactiver le netfilter sur le Bridge

```
$ vim /etc/sysctl.conf
net.ipv4.ip_forward = 1
net.bridge.bridge-nf-call-ip6tables = 0
net.bridge.bridge-nf-call-iptables = 0
net.bridge.bridge-nf-call-arptables = 0
```

Installation du manager CloudStack

Le serveur est prêt à recevoir Cloudstack (partie manager).

Ne pas hésiter à relancer le serveur pour que toutes les modifications soient prises en compte.

Definir le mot de passe de base de données !!!

```
$ yum -y install cloudstack-management
$ cloudstack-setup-databases cloudstack:password@localhost --deploy-as=root
$ cloudstack-setup-management
```

Avant de lancer l'installation des VM systèmes, le point de montage nfs vers le serveur NFS Secondaire doit être monté (ici dans /secondary).

```
$ mkdir /secondary
$ mount -t nfs nas2-cloud.etrs.terre.defense.gouv.fr:/secondary /secondary
$ /usr/share/cloudstack-common/scripts/storage/secondary/cloud-install-sys-tmplt
\
-m /secondary \
-u http://cloudstack.apt-get.eu/templates/4.7.1.0/systemvm64template-2016-05-18-
4.7.1-kvm.qcow2.bz2 \
-h kvm -F
```

Configuration du pare-feu

Des règles sont nécessaires pour laisser passer les requêtes réseaux :

- le port 22 est utilisé par le service SSH ;
- le port 8080 est utilisé par l'agent CloudStack et par les API;
- le port 8096 est utilisé par l'agent CloudStack et par les API (non authentifié).

Pour info :

- le port 3922 est utilisé pour la communication la communication avec l'agent CloudStack ;
- le port 8250 est utilisé pour communiquer avec les VM système.

```
$ vim /etc/sysconfig/iptables
-A INPUT -s XXX.XXX.XXX.XXX/20 -m state --state NEW -p tcp --dport 22 -j ACCEPT
-A INPUT -s XXX.XXX.XXX.XXX/20 -m state --state NEW -p tcp --dport 8080 -j ACCEPT
```

```
-A INPUT -s XXX.XXX.XXX.XXX/20 -m state --state NEW -p tcp --dport 8096 -j ACCEPT
$ service iptables restart
```

Script d'automatisation

```
$ sed -i --follow-symlinks 's/SELINUX=.*/SELINUX=permissive/g'
/etc/sysconfig/selinux
$ echo "proxy=http://proxy:8080" >> /etc/yum.conf
$ yum install -y vim-enhanced ccze epel-release

$ yum install -y wget
$ echo "https_proxy = http://proxy:8080/
http_proxy = http://proxy:8080/
ftp_proxy = http://proxy:8080/
use_proxy = on" >> /etc/wgetrc

$ echo "export https_proxy=http://proxy:8080/
export http_proxy=http://proxy:8080/
export ftp_proxy=http://proxy:8080/
export no_proxy="localhost,127.0.0.1, …"
use_proxy=on" >> /etc/profile.d/proxy.sh

$ yum install -y ntp
$ chkconfig ntpd on
$ service ntpd start

$ echo "[cloudstack]
name=Cloudstack
baseurl=http://cloudstack.apt-get.eu/centos7/4.9/
enabled=1
gpgcheck=0" >> /etc/yum.repos.d/cloudstack.repo

$ yum -y install nfs-utils
sed -i '/\#LOCKD_TCPPORT/s/^#//g' /etc/sysconfig/nfs
sed -i '/\#LOCKD_UDPPORT/s/^#//g' /etc/sysconfig/nfs
sed -i '/\#MOUNTD_PORT/s/^#//g' /etc/sysconfig/nfs
sed -i '/\#STATD_PORT/s/^#//g' /etc/sysconfig/nfs
sed -i '/\#STATD_OUTGOING_PORT/s/^#//g' /etc/sysconfig/nfs
echo 'RQUOTAD_PORT=875' >> /etc/sysconfig/nfs
egrep
'LOCKD_TCPPORT|LOCKD_UDPPORT|MOUNTD_PORT|RQUOTAD_PORT|STATD_PORT|STATD_OUTGOING_P
ORT' /etc/sysconfig/nfs



$ yum install mariadb-server mariadb
```

```
$ echo "[mysqld]
innodb_rollback_on_timeout=1
innodb_lock_wait_timeout=600
max_connections=350
log-bin=mysql-bin
binlog-format = 'ROW'" >> /etc/my.cnf.d/cloudstack.cnf

$ systemctl start mariadb
$ systemctl enable mariadb

# Gestion du domain NFS
sed -i '/\#Domain/s/^#//g' /etc/idmapd.conf
sed -i 's/Domain = .*/Domain = etrs.terre.defense.gouv.fr/g' /etc/idmapd.conf
grep Domain /etc/idmapd.conf

$ echo "net.ipv4.ip\_forward = 1
net.bridge.bridge-nf-call-ip6tables = 0
net.bridge.bridge-nf-call-iptables = 0
net.bridge.bridge-nf-call-arptables = 0" >> /etc/sysctl.d/10-cloudstack.conf

$ cloudstack-setup-databases cloudstack:qsmlybfhie@localhost --deploy-as=root
$ cloudstack-setup-management --tomcat7

$ systemctl enable cloudstack-management.service
```

Annexe 10
Procédure d'installation d'un hyperviseur KVM

Installation du système

Installation du serveur depuis un CD-ROM d'installation (version minimale) téléchargeable ici.

- Durant l'étape de partitionnement, supprimer toutes les anciennes données éventuellement présentes sur le disque ;
- Durant l'installation, configurer le nom d'hôte : kvmX ;
- Choisir l'option "Installation minimale" ;

Configuration du réseau

Après l'installation, il faut impérativement vérifier la bonne résolution du nom de machine :

```
$ hostname
node1-cloud
$ hostname -f
node1-cloud.etrs.terre.defense.gouv.fr
```

Pour que la résolution soit effective, il faut configurer le fichier /etc/hosts ou s'assurer de la bonne résolution DNS.

L'adresse IP doit être configurée. Modifier le fichier /etc/sysconfig/network-scripts/ifcfg-eth0 :

```
$ vim /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
NM_CONTROLLED=no
ONBOOT=yes
BOOTPROTO=none
IPADDR=XXX.XXX.XXX.107
NETMASK=255.255.240.0
GATEWAY=XXX.XXX.XXX.254
DNS1=XXX.XXX.XXX.XXX
DNS2=XXX.XXX.XXX.XXX
```

```
$ service network restart
```

SELinux

Mettre SELinux en permissif :

```
$ vi /etc/sysconfig/selinux
```

```
SELINUX=permissive
```

Configuration du proxy

L'école étant derrière un proxy, il faut le configurer pour yum et get :

```
$ vi /etc/yum.conf
proxy=http://proxy:8080
```

Configurer le proxy pour wget (utilisé pour télécharger les images systèmes) :

```
$ vi /etc/wgetrc
https_proxy = http://proxy:8080/
http_proxy = http://proxy:8080/
ftp_proxy = http://proxy:8080/
use_proxy = on
$ vi /etc/profile.d/proxy.sh
export https_proxy=http://proxy:8080/
export http_proxy=http://proxy:8080/
export ftp_proxy=http://proxy:8080/
export no_proxy="localhost,127.0.0.1,…"
use_proxy = on
```

NTP

Installation des logiciels :

```
$ yum install ntp
```

Configuration du fichier /etc/ntp.conf :

```
server XXX.XXX.XXX.XXX iburst
server XXX.XXX.XXX.XXX iburst
[...]
restrict default kod nomodify notrap nopeer noquery
restrict -6 default kod nomodify notrap nopeer noquery
restrict 127.0.0.1
restrict -6 ::1
```

- Automatiser le lancement de ntpd

```
$ chkconfig ntpd on
$ service ntpd start
```

Installation de logiciels complémentaires

```
$ yum install ccze vim epel-release wget
```

Installation de KVM

Installation des logiciels nécessaires :

```
$ yum install kvm qemu-kvm python-virtinst libvirt libvirt-python virt-manager
virt-viewer libguestfs-tools bridge-utils ntp
```

Configuration

Plusieurs configurations de fichiers sont nécessaires pour que CloudStack puisse intéragir avec KVM :

- Configuration de VNC (via QEMU)

  Décommenter la ligne suivante :

```
$ vim /etc/libvirt/qemu.conf
vnc_listen="0.0.0.0"
```

- Configuration de libvirt

Libvirt ne gère pas uniquement les commutateurs virtuels. Pour permettre la migration à chaud des machines virtuelles, CloudStack communique à travers le réseau avec l'agent libvirt situé sur les hyperviseurs.

S'assurer que libvirtd écoute les instructions de CloudStack sur le réseau :

```
$ vim /etc/libvirt/libvirtd.conf
listen_tls = 0
listen_tcp = 1
tcp_port = "16059"
auth_tcp = "none"
mdns_adv = 0
$ vim /etc/sysconfig/libvirtd
LIBVIRTD_ARGS="--listen"
$ service libvirtd restart
```

Configuration du pare-feu

Des règles sont nécessaires pour laisser passer les requêtes réseaux :

- le port 22 est utilisé par le service SSH ;

  le port 1798 est utilisé par l'agent CloudStack ;
- le port 16509 est utilisé par le service libvirtd ;
- les ports de 5900 à 6100 sont utilisés par les consoles VNC ;
- les ports de 49152 à 49216 sont utilisé pour la migration à chaud de libvirt ;

```
firewall-cmd --zone=public --add-port=5900-6100/tcp --permanent
firewall-cmd --zone=public --add-port=1798/tcp --permanent
firewall-cmd --zone=public --add-port=16509/tcp --permanent
```

```
firewall-cmd --zone=public --add-port=49152-49216/tcp --permanent
$ service iptables restart
```

CloudStack

Dépôt Cloudstack

Créer le fichier /etc/yum.repos.d/cloudstack.repo

```
[cloudstack]
name=Cloudstack
baseurl=http://cloudstack.apt-get.eu/centos/6/4.8/
enabled=1
gpgcheck=0
```

Configuration des services requis

```
$ yum -y install nfs-utils
```

Configuration de NFS

```
$ vim /etc/sysconfig/nfs
LOCKD_TCPPORT=32803
LOCKD_UDPPORT=32769
MOUNTD_PORT=892
RQUOTAD_PORT=875
STATD_PORT=662
STATD_OUTGOING_PORT=2020
$ vim /etc/idmapd.conf
Domain = etrs.terre.defense.gouv.fr
$ mkdir /secondary
$ mkdir /primary
$ chown nobody:nogroup /secondary
$ chown nobody:nogroup /primary
```

Configuration de la partie agent de CloudStack

Configuration du noyau

- Autoriser le forwarding IP V4
- Désactiver le netfilter sur le Bridge

```
$ vim /etc/sysctl.d/cloudstack.conf
net.ipv4.ip_forward = 1
net.bridge.bridge-nf-call-ip6tables = 0
net.bridge.bridge-nf-call-iptables = 0
net.bridge.bridge-nf-call-arptables = 0
```

Installation de l’agent CloudStack

Le serveur est prêt à recevoir l’agent Cloudstack.

Ne pas hésiter à relancer le serveur pour que toutes les modifications soient prises en compte.

```
$ yum -y install cloudstack-agent
```

Liste des figures

Liste des tableaux

Conception et réalisation d'une plateforme de cloud privé au profit de la formation des administrateurs systèmes.

Mémoire d'Ingénieur C.N.A.M., Bretagne 2016

RESUME

Ce mémoire traite de la mise en œuvre d'un cloud privé au sein de l'Espace Numérique de Formation de l'École des Transmissions de Cesson-Sévigné au profit des formateurs et stagiaires du Groupement des Systèmes d'Information de la Direction Générale de la Formation de l'école.

Cette plateforme offre les ressources nécessaires à la formation des futurs administrateurs systèmes du Ministère de la défense. Ils peuvent déployer, à leur initiative, les serveurs et les infrastructures réseaux nécessaires à leurs travaux pratiques.

Ce projet prend en compte les aspects SSI réglementaires, l'évolutivité et l'élasticité (montée en puissance) de la plateforme, l'identification des nouveaux usages pédagogiques, l'adaptation de la solution à la spécificité de la formation, l'automatisation du provisionnement et l'accompagnement du changement.

Mots clés : Cloud, Formation, CloudStack, Virtualisation.

SUMMARY

This memoir is about the implementation of a private cloud inside the Digital Space Formation of the "Transmissions de Cession-Sévigné" school for the benefit of the instructors and trainees of the school's Training Management Information System Group.

This platform offers the resources required to train tomorrow's system administrators of the Ministry of Defense. They can deploy, on their own, the servers and the network infrastructures needed for their hands-on training.

This project takes into consideration the ISS regulatory aspects, the evolution and resilience (load increase) of the platform, the identification of new teaching uses, the adaptation of the solution to the training specifics, the provisioning automation and the change support.

Key words : Cloud, Formation, CloudStack, Virtualisation.