

Sommaire

<i>Dédicace</i>	1
<i>Remerciements</i>	2
<i>Résumé</i>	3
<i>Liste des figures</i>	7
<i>Introduction générale</i>	11
Présentation d'organisme d'accueil	12
1.1 Présentation de l'entreprise	12
1.2 Les services	12
1.3 Infrastructure WAN CASTINFO	13
1.4 Parc technique de CASTINFO	14
1.5 Schéma de l'installation de réseau	15
Présentation et planification du projet de stage.....	16
2.1 Contexte.....	16
2.2 Problématique.....	16
2.3 Enjeux et objectifs	17
2.4 La démarche adoptée dans la réalisation du projet.....	17
2.5 Planification de projet	18
Etat de l'art sur Cloud Computing.....	19
3.1 Historique	19
3.2 Définition.....	21
3.3 Les différentes couches de service d'un cloud	21
3.4 Les différents niveaux de déploiement.....	23
3.5 Cloud Computing et clusters	24
3.6 Avantages et inconvénients Cloud Computing	26
3.7 Conclusion.....	27
Etudes Comparatives	28
4.1 Introduction	28
4.2 Solution open source	29
4.2.1 Openstack.....	29
4.2.2 Eucalyptus.....	30
4.2.3 OpenNubela.....	31

4.2.4	CloudStack	31
4.2.5	Etude comparative	32
4.3	Les serveurs d'application JEE	32
4.3.1	Apache Tomcat.....	33
4.3.2	GlassFish.....	33
4.3.3	JBOSS	33
4.3.4	Etude comparative	33
4.4	Les systèmes de gestion de base de données.....	34
4.4.1	MySQL.....	34
4.4.2	PostgreSQL	34
4.4.3	HSQLDB.....	35
4.4.4	Etude comparative	35
4.5	Les logiciels de supervision informatique.....	35
4.5.1	Nagios	36
4.5.2	Zenoss.....	36
4.5.3	Zabbix	36
4.5.4	Etude comparative	36
4.6	Les logiciels de sauvegarde informatique	37
4.6.1	Les différents types de sauvegarde.....	37
4.6.2	Etude comparative	37
4.7	Les firewalls	38
4.7.1	Firewall Pfsense	39
4.7.2	Firewall IPCop.....	39
4.7.3	Firewall Smoothwall	39
4.7.4	Comparaison.....	40
4.8	Conclusion.....	40
Architecture Technique et Logicielle		41
5.1	Architecture technique.....	41
5.1.1	Architecture du réseau	41
5.1.2	Architecture du système	51
5.2	Architecture logicielle.....	52
5.2.1	Pattern de conception.....	52
5.2.2	Pattern de couche	52
5.2.3	Frameworks et base de données utilisés	52

5.2.4	Les outils utilisés.....	53
	Analyse Et Conception.....	54
6.1	Phase d'inception	54
6.1.1	Diagramme de cas d'utilisation	55
6.2	Phase d'analyse	57
6.2.1	Diagramme de séquence.....	57
6.2.2	Diagramme de classes d'analyse	60
	Implémentation.....	62
7.1	Mécanismes de la sécurité.....	62
7.1.1	Java Simplified Encryption(Jasypt)	62
7.1.2	HyperText Transfer Protocol Secure(HTTPS).....	63
7.2	Application web de BusinessaaS.....	64
7.2.1	Front office de BusinessaaS.....	64
7.2.2	Back office de BusinessaaS.....	71
7.3	Application web des écoles privées (EcoleCloud)	73
7.3.1	Front office de l'application EcoleCloud.....	73
7.3.2	Back office de l'application EcoleCloud.....	77
	Annexe 1. Serveur Cloud	82
	Annexe 2. Serveur GlassFish	88
	Annexe 3. Cluster de Serveur GlassFish	90
	Annexe 4.Serveur MySQL cluster.....	94
	Annexe 5.Serveur Nagios.....	98
	Annexe 6.Serveur Backup(Bacula).....	105
	Annexe 7.Firewall (PfSense).....	113
	Annexe 8. SNORT.....	118
	<i>Bibliographie</i>	120

Liste des figures

Figure 1:	Schéma de l'infrastructure WAN CAST-INFO	13
Figure 2 :	Schéma illustrant le centre informatique	14
Figure 3 :	le processus suivi, lors de l'installation de réseau	15
Figure 4 :	Cycle en V	17
Figure 5 :	Intérêt pour le terme « cloud computing » sur Internet.....	20

Figure 6 : Évolution de l'informatique jusqu'au cloud computing.....	20
Figure 7 : Les couches du cloud computing.....	21
Figure 8 : Type de Cloud Computing.....	24
Figure 9 : Nuage du cloud computing.....	25
Figure 10 : étapes de déploiement	25
Figure 11 : Cluster Cloud Computing.....	26
Figure 12 : logo open stack	29
Figure 13 : Logo Eucalyptus.....	30
Figure 14 : logo OpenNebula.....	31
Figure 15 : logo CloudStack.....	31
Figure 16 : Représentation d'un firewall	38
Figure 17 : Architecture réseau du Cloud	42
Figure 18 : système Openstack.....	42
Figure 19 : Cluster GlassFish.....	44
Figure 20 : Architecture de MySQL Cluster	45
Figure 21 : La topologie du serveur cloud	45
Figure 22 : Dialogue entre le client et le serveur DHCP.....	46
Figure 23 : La configuration réseau du firewall	49
Figure 24 : Les règles de l'interface LAN.....	49
Figure 25 : Les règles de l'interface WAN	50
Figure 26 : Les règles de l'interface DMZ.....	50
Figure 27 : Exemple de machine malveillante bloqué par SNORT	51
Figure 28 : Architecture du système	52
Figure 29 : Diagramme de cas d'utilisation de société BusinessaaS.....	55
Figure 30 : Diagramme de cas d'utilisation de l'école.....	56
Figure 31 : Diagramme de classe d'analyse de BusinessaaS	60
Figure 32 : Diagramme de classe d'analyse des écoles.....	61
Figure 33 : Transfert de données non sécurisé, pas de certificat SSL	63
Figure 34 : Transfert de données sécurisé par certificat SSL :.....	63
Figure 35 : Page d'accueil de BusinessaaS.....	64
Figure 36 : Page des modules de BusinessaaS.....	65
Figure 37 : Formulaire de création le compte d'école	66
Figure 38 : Page d'activation du compte.....	66
Figure 39 : Page d'authentification des écoles	67
Figure 40 : Page de profil d'une école	68
Figure 41 : Page de choix des modules	69
Figure 42 : Page de confirmation de l'abonnement	70
Figure 43 : Page de paiement PayPal	70
Figure 44 : Espace de connexion de l'administrateur de BusinessaaS.....	71
Figure 45 : Page d'accueil administrateur de BusinessaaS	71
Figure 46 : Page de gestions de modules de BusinessaaS	72
Figure 47 : Page de lister des clients de BusinessaaS	72
Figure 49 : La page de choix le nom d'école	73
Figure 50 : Page d'authentification des utilisateurs de l'application des écoles	74
Figure 51 : La page d'accueil de l'application EcoleCloud	74

Figure 52: L'espace élève de l'application des écoles	75
Figure 53 : L'espace enseignant de l'application des écoles.....	76
Figure 54 : La page de surveillance de l'application des écoles	77
Figure 55 : Espace de connexion de l'administrateur de CloudEcole.....	77
Figure 56 : Page de gestion de la page d'accueil de l'application des écoles.....	78
Figure 57 : Page de gestion du module de gestion de l'application EcoleCloud	79
Figure 58 : Espace de gestion des enseignants d'application des écoles	79
Figure 59 : Page de configuration des caméras IP des salles	80
Figure 60 : Page de gestion du module de formation à distance d'EcoleCloud	80
Figure 61 : Interface web d'authentification Openstack Juno	83
Figure 62 : Tableau de bord d'Openstack Juno.....	83
Figure 63 : Création des réseaux sous openstack	84
Figure 64 : Création des routeurs sous openstack.....	84
Figure 65 : Ajout des interfaces réseaux à un routeur sous openstack.....	84
Figure 66 : Gestion des règles de la sécurité sous openstack.....	85
Figure 67 : Gestion les paires de clés sous openstack.....	85
Figure 68 : Gestion les types d'instance sous openstack.....	85
Figure 69 : Création des images sous openstack.....	86
Figure 70 : Lancement une instance sous openstack.....	87
Figure 71 : Topologie réseau de serveur cloud	87
Figure 72 : La page d'authentification de GlassFish.....	89
Figure 73 : L'interface d'administration de serveur GlassFish	89
Figure 74 : Création d'un nouveau nœud de cluster en utilisant la console d'administration.....	90
Figure 75 : Création d'un nouveau cluster en utilisant la console d'administration.....	91
Figure 76 : Interface pour la gestion des clusters dans la console d'administration	92
Figure 77 : Exemple de déploiement d'une application web	92
Figure 78 : les adresses d'une application déployée.....	93
Figure 79 : Interface web de Nagios.....	99
Figure 80 : Le fonctionnement de NRPE	99
Figure 81 : La fenêtre de l'état des services de la machine linux.....	103
Figure 82 : La fenêtre de l'état de service PING de routeur	104
Figure 83 : La fenêtre de l'état de service PING de switch	104
Figure 84 : Configuration module de Bacula	109
Figure 85 : Tableau de bord de Bacula.....	109
Figure 86 : création Backup client.....	110
Figure 87:Création la partie à sauvegarder	111
Figure 88 : Définir le calendrier de sauvegarde	111
Figure 89 : Création un travail de sauvegarde	111
Figure 90 : Démarrage le travail de sauvegarde	112
Figure 91 : Restauration.....	112
Figure 92 : La fenêtre d'authentification PfSense	116
Figure 93 : La fenêtre de user manager PfSense	117
Figure 94 : La fenêtre de configuration des interfaces de PfSense	117

Liste des tableaux

Tableau 1 : Les différents éléments matériels et logiciels du centre Informatique	14
Tableau 2 : La liste des tâches.....	18
Tableau 3 : Avantage et Inconvénient des services cloud	23
Tableau 4 : Etude comparative des systèmes de gestion de l'infrastructure du cloud	32
Tableau 5 : Etude comparative des serveurs d'application JEE.....	34
Tableau 6 : Etude comparative des systèmes de gestion de base de données	35
Tableau 7 : Etude comparative des logiciels de supervision informatique	36
Tableau 8 : Etude comparative des logiciels de sauvegarde	38
Tableau 9 : Etude comparative des firewalls.....	40
Tableau 10 : Framework java et base de données	53

Glossaire

D.A.L.I	Système de monitoring développé par Cast-Info
UP	Unified Project
MPM	Méthode des potentiels Métra
SaaS	Software as a service
PaaS	Platform as a service
IaaS	Infrastructure as a service
EC2	Elastic Compute Cloud
S3	Simple Storage Service
GNU GPL	GNU General Public License
CDDL	Common Development and Distribution License
JEE	Java Enterprise Edition, ou Java EE
EJB	Enterprise JavaBeans
JPA	Java Persistence API
JSF	Java Server Faces
JSP	Java Server Pages
Licence BSD	Berkeley software distribution license
CPU	central processing unit
DAO	Data Access Object
BO	Business Object
POJO	Plain Old Java Object

Introduction générale

Face à l'augmentation continue des coûts de mise en place et de maintenance des systèmes informatiques, les entreprises externalisent de plus en plus leurs services informatiques en les confiant à des entreprises spécialisées comme les fournisseurs de cloud.

L'intérêt principal de cette stratégie pour les entreprises réside dans le fait qu'elles ne paient que pour les services effectivement consommés.

Grâce au cloud computing, « l'informatique dans les nuages », les entreprises disposent aujourd'hui d'une puissance informatique considérable et modulable. Elles sont en mesure d'externaliser avec une souplesse inédite tout ou partie de leur système d'information (SI) postes de travail, serveurs, applications, stockage, etc.

Le but de ce projet de fin d'études est de concevoir une solution cloud pour les écoles privées. Nous proposons de mettre en place un système assurant la qualité des services demandés pour les écoles privées. Cette solution est générique, flexible, réutilisable et adaptable aux exigences des clients actuels et des clients potentiels.

Ce rapport se présente en sept chapitres à savoir : présentation de l'organisme d'accueil, présentation et planification du projet de stage, Etat de l'art de Cloud Computing, architecture technique et logicielle, analyse et conception, implémentation, conclusion et perspectives. Enfin, les annexes qui contiennent les phases d'installation et de configuration de chaque serveur de notre infrastructure viendront clôturer ce document.

1

Présentation d'organisme d'accueil

1.1 Présentation de l'entreprise

Cast-info a été créé en 1993, sa couverture nationale avec des centres à Madrid, Barcelone et Bilbao et expansion internationale : ouverture de trois antennes internationales ces cinq dernières années : Chili, Portugal et Maroc.

Cast-info présent dans les principaux secteurs économiques : Télécommunications, banque, assurances, administrations publiques, industrie, santé, services, TI et moyens de communication.

1.2 Les services

- **Service 7x24**

Cast-info offre des services d'administration de l'infrastructure de TI à ses clients dans un horaire sans interruption, 24x7, 365 jours par an. Ce service est complété par l'utilisation du système de monitoring D.A.L.I., développé par Cast-info et fondé sur Nagios.

- **Développement**

L'entreprise dispose d'une équipe de programmeurs spécialisés en JEE et en PHP, experts en développement.

L'entreprise est en voie de certification CMMI et est en mesure d'exécuter des projets avec les meilleures garanties quant au développement, aux tests de qualité, à la documentation, à la maintenance etc., avec l'économie de coûts que cela suppose pour le client.

- **Testing**

L'entreprise offre un service de test des logiciels créés par les développeurs, afin d'assurer leur fiabilité et le bon fonctionnement.

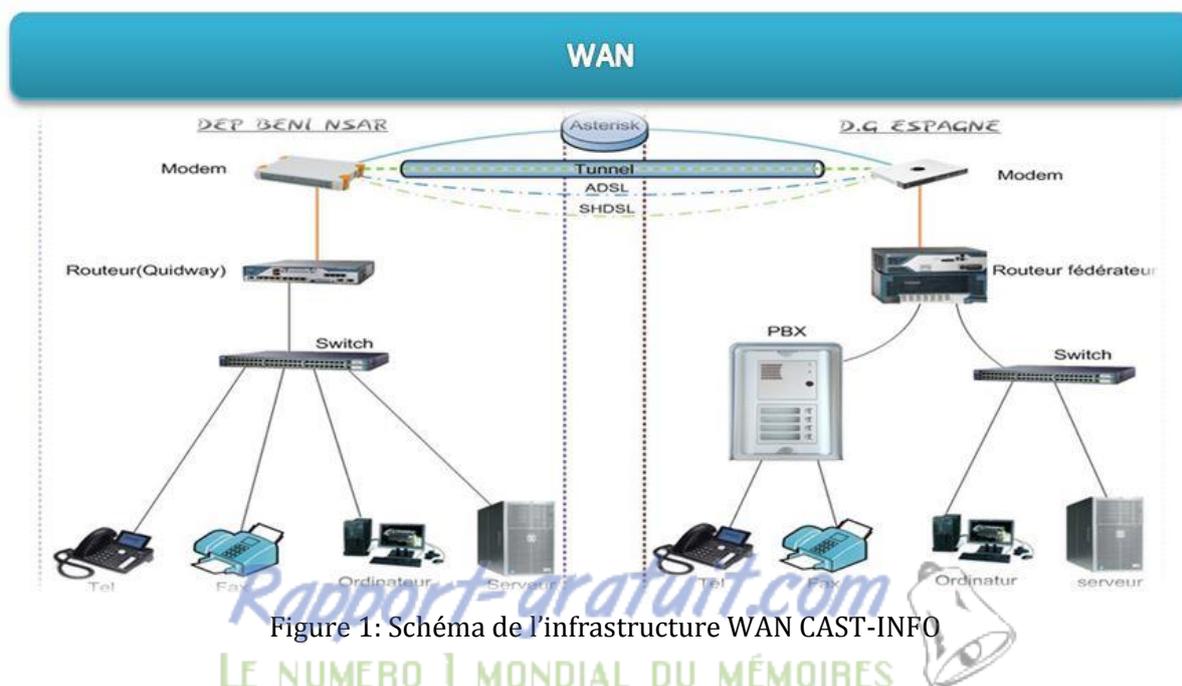
- **Emagister**

C'est l'un des services les plus importants, au sein de la société qui a pour but de collecter des informations sur les formations dispensées dans les universités du monde, dans diverses spécialités.

- **Panda**

Cast-info propose à sa clientèle un service de recommandation de l'antivirus PANDA. Ce service présente en ligne des solutions relatives à la configuration, à l'installation et à la mise à jour des produits.

1.3 Infrastructure WAN CASTINFO



Il est à signaler que le réseau local de CASTINFO est connecté à la Direction Générale via 4 Modem 'NTU KEYMILE' (ligne spécialisée LLPLUS à 2 Mb/S). « Les liaisons louées permettent aux grandes entreprises de raccorder leurs réseaux internes par le biais d'accès permanents, pour une utilisation intensive du réseau Internet. »

1.4 Parc technique de CASTINFO

Le centre informatique qui est situé au siège social, est équipé des éléments suivants :

Eléments Matériels	Eléments Logiciels
Quidway AR 28-11	VMware ESXi
OvisLink	Asterisk
SMCWBR14S-N2	Nagios
VPN KEYMILE	Thunderbird
Switch Cat.3560	My office
APC Smart-UPS	Sugar CRM
ProLiant ML110	Site-Scope
HP ProLiant ML310	
HP Workstation X2100	
Dell Poweredge 440	
Cisco call manager	

Tableau 1 : Les différents éléments matériels et logiciels du centre Informatique



Figure 2 : Schéma illustrant le centre informatique

1.5 Schéma de l'installation de réseau

Le schéma suivant désigne au sens concret « un ensemble de lignes entrelacées ». Il s'agit d'un ensemble d'appareils électroniques (ordinateurs, routeurs, Switch ...) géographiquement éloignés les uns des autres, interconnectés par des télécommunications généralement permanentes, qui permettent d'échanger et d'autoriser la circulation en mode continu ou discontinu de flux.



Figure 3 : le processus suivi, lors de l'installation de réseau

2

Présentation et planification du projet de stage

2.1 Contexte

Toutes les écoles se trouveraient ainsi en compétition et obligées de veiller à la qualité de leurs services pour garder leur « clientèle » et pour attirer de nouveaux clients.

Les écoles ne doivent plus seulement offrir un enseignement de qualité. Elles doivent innover et offrir des programmes variés et attrayants. Pour ce faire, la majorité de ces écoles s'orientent vers l'informatisation de leurs services.

2.2 Problématique

Les entreprises à des services communs comme les écoles privées ont les mêmes besoins et poursuivent la même finalité, nous proposons de mettre en place un système assurant la qualité des services demandés. Le système proposé est générique, flexible, réutilisable et adaptable aux exigences des clients actuels et des clients potentiels. La solution qui s'impose est un **Software as a Service** déployé dans notre cloud public payant.

2.3 Enjeux et objectifs

Notre solution BusinessaaS (**Software as a Service**) est un modèle de déploiement dans lequel **Cast-info** loue en main à ses clients (les écoles privées) en tant que service à la demande au lieu de leur facturer la licence du logiciel. De cette façon, l'utilisateur final n'a plus besoin d'installer le logiciel.

BusinessaaS permet de graduer le niveau d'externalisation : de l'hébergement du système d'information d'une école privée à l'externalisation complète en assurant les fonctions suivantes :

- Réduire les délais de déploiement d'une nouvelle application et d'acquisition de nouveaux matériels
- Réduire le coût des investissements informatique et de gestion de l'infrastructure
- Bénéficier d'une solution simple d'utilisation et avec des mises à jour automatiques et en temps réel
- Sécuriser et sauvegarder les données et informations avec une mutualisation des moyens pour une plus grande efficacité
- Accéder à l'information sans contraintes de lieux et de temps, via un simple navigateur Internet

2.4 La démarche adoptée dans la réalisation du projet

Le modèle que nous avons utilisé pour la réalisation de ce projet est le modèle du cycle en V. Son principe de base est l'association d'une phase de test à chaque phase de projet. A l'issue de chaque phase des livrables sont produits.

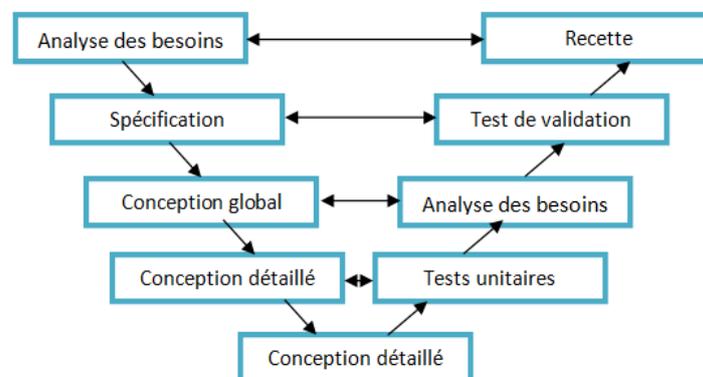


Figure 4 :Cycle en V

Nous avons adopté comme méthode de développement, la méthode UP.

2.5 Planification de projet

Afin d'organiser notre travail, la première étape que nous avons abordé est la planification du projet.

Nous avons choisi de gérer notre projet en fonction de tâches. Pour chaque tâche bien déterminée nous avons fixé une durée de réalisation, date de début et de fin ainsi que les prédécesseurs de chaque tâche. Le tableau suivant représente les différentes tâches de notre projet.

Tâches	Description	Durée (en jours)
1. Environnement	Etude de l'existant, les différents départements, les services, l'architecture	2j
2. Analyse de l'existant.	Cahier des charges, objectif de projet, planification ...	3j
3. Infrastructure	Préparation des serveurs, Installation et configuration des serveurs : cloud, DHCP, Nagios, Backup ...	25 j
4. Conception	Méthodes de conception, UML, use cas ...	20 j
5. Design	Interfaces graphiques	10 j
6. Développement	Formation des Frameworks (struts2 et Hibernate) JEE, développement des applications.	45 j
7. Test et validation	Test et validation des applications.	2 j
8. Déploiement et Hébergement	Déploiement et Hébergement des applications.	1 j
9. Rapport	Rédaction du rapport	15 j

Tableau 2 : La liste des tâches

3

Etat de l'art sur Cloud Computing

3.1 Historique

Techniquement, le concept de cloud computing est loin d'être nouveau, il est même présent depuis des décennies. On en trouve les premières traces dans les années 1960, quand John McCarty affirmait que cette puissance de traitement informatique serait accessible au public dans le futur. Le terme en lui-même est apparu plus couramment aux alentours de la fin du XXe siècle et il semblerait que Amazon.com soit l'un des premiers à avoir assemblé des data centres et fournit des accès à des clients. Les entreprises comme IBM et Google ainsi que plusieurs universités ont seulement commencé à s'y intéresser sérieusement aux alentours de 2008, quand le cloud computing est devenu un concept "à la mode".

Réalisant ce qu'ils pourraient faire de toute cette puissance, de nombreuses compagnies ont ensuite commencé à montrer un certain intérêt à échanger leurs anciennes infrastructures et applications internes contre ce que l'on appelle les " *pay per-use service* " (services payés à l'utilisation). [1].

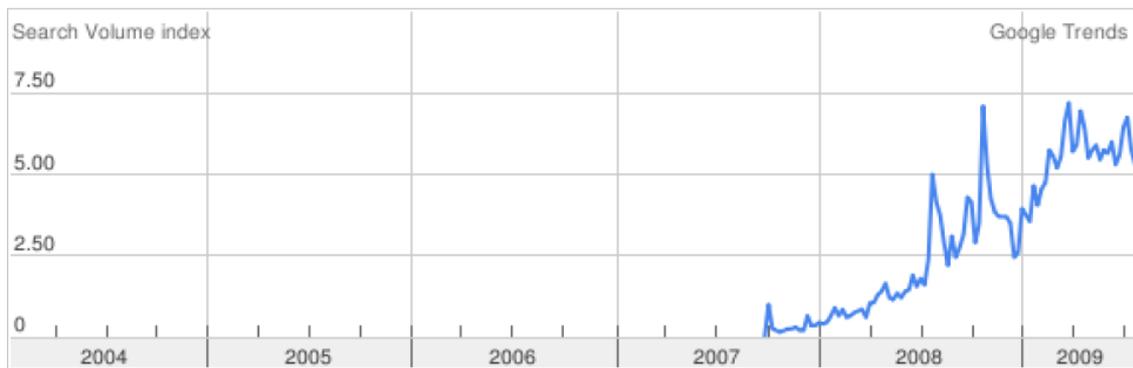


Figure 5 : Intérêt pour le terme « cloud computing » sur Internet

Aujourd'hui, le « Cloud Computing » compte plus de 10,3 millions d'entrées dans Google. Sa portée est passée de simples services d'infrastructure tels que les ressources de stockage et de calcul à la mise à disposition d'applications. Cela signifie donc que les précurseurs tels que les prestataires de services d'application et les logiciels-services sont dorénavant inclus dans le « Cloud Computing ».

Actuellement les experts sont convaincus que bientôt, nous utiliserons le cloud computing de la même manière que nous utilisons l'électricité, c'est à dire en payant uniquement ce que nous consommons sans même nous soucier des aspects techniques nécessaires au bon fonctionnement du système. Le principal facteur de développement restant le fait que toute cette puissance est à tout moment partagée par plusieurs utilisateurs et évité ainsi de perdre du "temps machine" à ne rien faire. Cela devrait également drastiquement réduire les couts de développements et donc les prix. [2]



Figure 6 : Évolution de l'informatique jusqu'au cloud computing

3.2 Définition

Le cloud computing se traduit littéralement par "informatique dans les nuages", faisant référence aux technologies d'internet qui est souvent représenté schématiquement par nuage. On peut considérer de manière générale, lorsque l'on parle de cloud computing, qu'il s'agit de rendre accessible et exploitable des données et des applications à travers un réseau. Ce terme désigne à la fois les applications en tant que services sur Internet et le matériel et logiciels qui permettent de fournir ces services [3].

A ce jour, il n'existe pas de définition officielle ou standardisée du Cloud Computing. Nous allons donc nous appuyer sur les définitions du NIST (National Institute of Standards and Technology) :

“Le Cloud Computing est l'ensemble des disciplines, pratiques, technologies et modèles commerciaux utilisés pour délivrer comme un service à la demande et par le réseau des capacités informatiques (logiciels, plateformes, matériels)”.

3.3 Les différentes couches de service d'un cloud

Le concept de cloud computing est utilisé pour désigner des services, on distingue trois "catégories" de services fournis :



Figure 7 : Les couches du cloud computing

1. IaaS : Infrastructure as a Service :

C'est le service de plus bas niveau. Il consiste à offrir un accès à un parc informatique virtualisé. Des machines virtuelles sur lesquelles le consommateur peut installer un système d'exploitation et des applications. Le consommateur est ainsi dispensé de l'achat de matériel informatique. [4]

Ce modèle permet au client de faire abstraction du modèle physique (gestion des serveurs physique, des éléments relatifs aux centres de données comme l'électricité, la climatisation, la sécurité physique). Dans ce modèle, le fournisseur contrôle le matériel et la couche de virtualisation. Au niveau des données, le contrôle est partagé au niveau de la machine virtuelle (qui est stockée et sauvegardée par le fournisseur de Cloud de type IaaS).

- **Avantage:** grande flexibilité, contrôle total des systèmes (administration à distance par SSH ou Remote Desktop, RDP), qui permet d'installer tout type de logiciel métier.
- **Inconvénient:** besoin d'administrateurs système comme pour les solutions de serveurs classiques sur site.

2 PaaS : Plateforme as service

Plateforme sur laquelle des développeurs ou éditeurs de logiciels peuvent déployer des applications. Le PaaS dispose d'environnements spécialisés au développement comprenant les langages, les outils et les modules nécessaires.

Le consommateur a le contrôle des applications et peut ajouter ses propres outils. La situation est analogue à celle de l'hébergement web où le consommateur loue l'exploitation de serveurs sur lesquels les outils nécessaires sont préalablement placés et contrôlés par le fournisseur. La différence étant que les systèmes sont mutualisés et offrent une grande élasticité - capacité de s'adapter automatiquement à la demande, alors que dans une offre classique d'hébergement web l'adaptation fait suite à une demande formelle du consommateur. [4]

- **Avantage:** le déploiement est automatisé, pas de logiciel supplémentaire à acheter ou à installer.
- **Inconvénient:** limitation à une ou deux technologies (ex. : Python ou Java pour Google AppEngine, .NET pour Microsoft Azure, propriétaire pour force.com). Pas de

contrôle des machines virtuelles sous-jacentes. Convient uniquement aux applications Web.

Les cibles sont les développeurs. Google App Engine est le principal acteur proposant ce genre d'infrastructures.

3 Saas : Software as a Service

Le client utilise une application standard selon un modèle de mise à disposition et paiement à l'usage et le fournisseur gère et contrôle les couches requises pour le service cloud. Les prestataires de solutions SaaS les plus connus sont : Google avec Gmail et Youtube ou encore les réseaux sociaux Facebook et Twitter. [5]

- **Avantage** : plus d'installation, plus de mise à jour (elles sont continues chez le fournisseur), plus de migration de données etc. Paiement à l'usage. Test de nouveaux logiciels avec facilité.
- **Inconvénient**: limitation par définition au logiciel proposé. Pas de contrôle sur le stockage et la sécurisation des données associées au logiciel. Réactivité des applications Web pas toujours idéale.

	Avantage	Inconvénient
SaaS	<ul style="list-style-type: none"> ▪ Pas d'installation ▪ Plus de licence ▪ Migration 	<ul style="list-style-type: none"> ▪ logiciel limité ▪ sécurité ▪ dépendance des prestataires
PaaS	<ul style="list-style-type: none"> ▪ Pas d'infrastructure nécessaire ▪ Pas d'installation ▪ Environnement hétérogène 	<ul style="list-style-type: none"> ▪ Limitation des langages ▪ Pas de personnalisation dans la configuration des machines virtuelles
IaaS	<ul style="list-style-type: none"> ▪ Administration ▪ Personnalisation ▪ Flexibilité d'utilisation 	<ul style="list-style-type: none"> ▪ sécurité ▪ besoin d'un administrateur système

Tableau 3 : Avantage et Inconvénient des services cloud

3.4 Les différents niveaux de déploiement

Le cloud computing peut être exploité à différents niveaux de déploiement suivant le réseau dans lequel les services sont disponibles. On parle alors de :

Types of Cloud

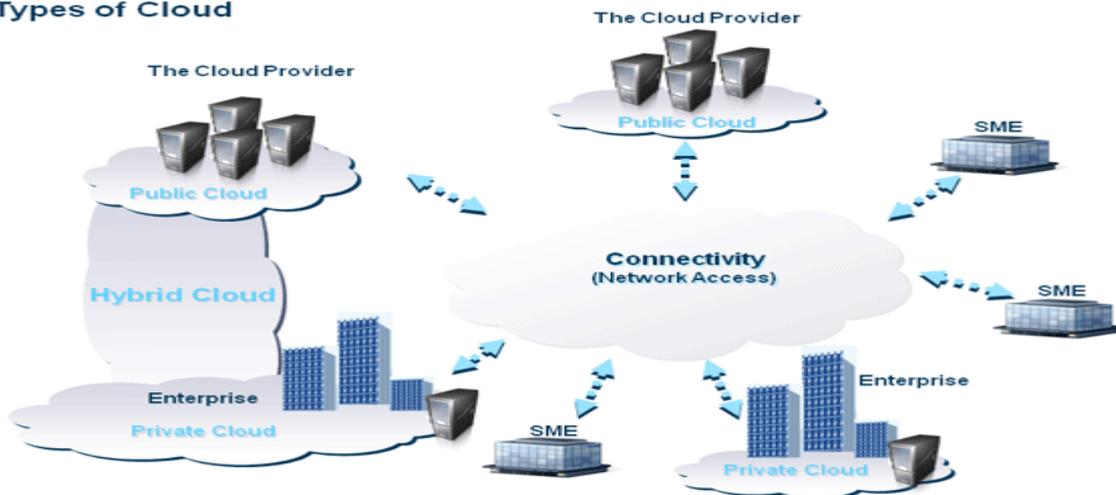


Figure 8 : Type de Cloud Computing

- **Cloud Privé :** L'infrastructure est dédiée à un seul et unique client. Habituellement un cloud privé est plutôt à l'intérieur de l'entreprise et tourne sur des équipements propres à cette même entreprise, mais il peut aussi tourner dans le data-centre d'un fournisseur.
- **Cloud Communautaire :** L'infrastructure Cloud est partagée par plusieurs organisations pour les besoins d'une communauté qui souhaite mettre en commun des moyens (sécurité, conformité, etc..). Elle peut être gérée par les organisations ou par une tierce partie et peut être placée dans les locaux ou à l'extérieur.
- **Cloud Public :** L'infrastructure cloud est ouverte au public ou à de grands groupes industriels. Cette infrastructure est possédée par une organisation qui vend des services Cloud. C'est le cas le plus courant. C'est celui de la plate-forme Amazon Web Services déjà citée.
- **Cloud Hybride :** L'infrastructure Cloud est composée d'un ou plusieurs modèles ci-dessus qui restent des entités séparées. Ces infrastructures sont liées entre elles par la même technologie qui autorise la portabilité des applications et des données. C'est une excellente solution pour répartir ses moyens en fonction des avantages recherchés.

3.5 Cloud Computing et clusters

Le but du cloud computing est de construire un nuage de clusters, c'est à dire d'interconnecter un ensemble de machines sur un réseau défini. Les utilisateurs peuvent ensuite déployer des machines virtuelles dans ce nuage, ce qui leur permet d'utiliser un certain

nombre de ressources. Par exemple de l'espace disque, de la mémoire vive, ou encore du CPU (processeur).

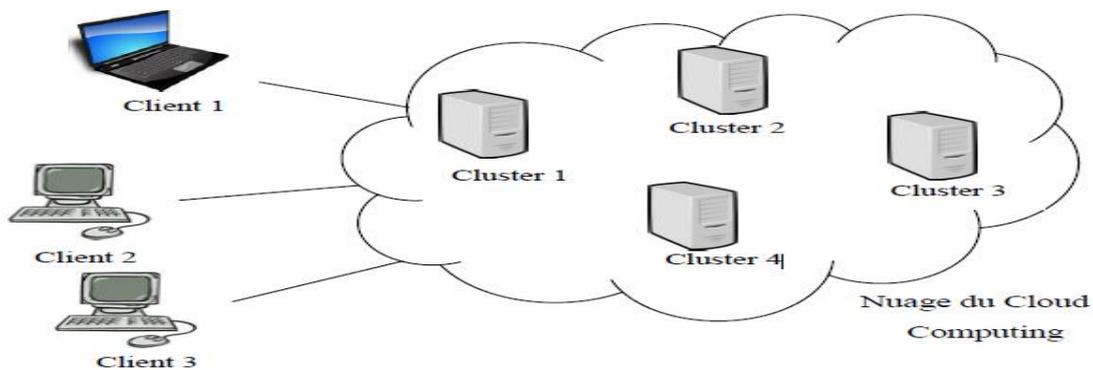


Figure 9 : Nuage du cloud computing

Cette infrastructure, en allant plus dans le détail, est constituée de clusters et de nœuds. Les clusters servent à gérer l'interface entre les nœuds et l'utilisateur. Ainsi, lorsqu'on déploie une machine virtuelle sur un cluster, le cluster va créer une instance, qui se matérialisera par l'utilisation des ressources dans les nœuds. Voici un schéma UML récapitulatif qui décrit les étapes de déploiement d'une image.

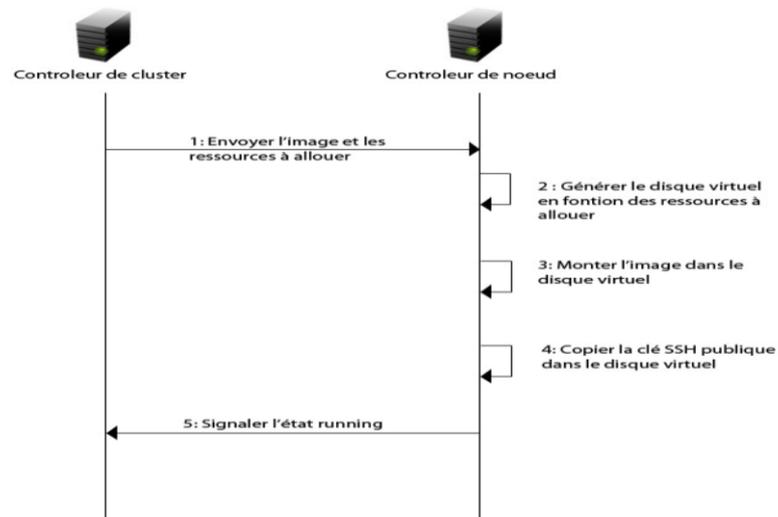


Figure 10 : étapes de déploiement

L'utilisateur final disposera enfin d'un accès SSH sur la machine virtuelle. Pour lui, l'utilisation des ressources sera transparente. Ce sont des administrateurs réseaux qui lui délivreront ses ressources en fonction de ses besoins.

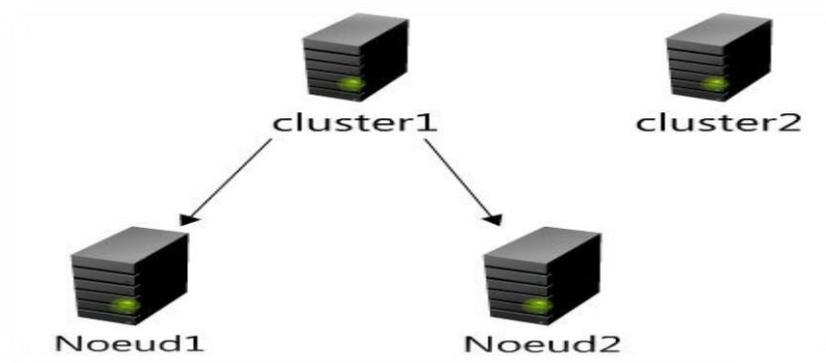


Figure 11 : Cluster Cloud Computing

3.6 Avantages et inconvénients Cloud Computing

Avantages

Les avantages du cloud computing sont nombreux. Nous allons en citer quelques-uns:

- Un démarrage rapide : Le cloud computing permet de tester le business plan rapidement, à coûts réduits et avec facilité.
- L'agilité pour l'entreprise : Résolution des problèmes de gestion informatique simplement sans avoir à vous engager à long terme.
- Un développement plus rapide des produits : Réduisons le temps de recherche pour les développeurs sur le paramétrage des applications.
- Pas de dépenses de capital : Plus besoin des locaux pour élargir vos infrastructures informatiques

Inconvénients

Il existe quelques inconvénients au cloud computing :

- La bande passante peut faire exploser votre budget : La bande passante qui serait nécessaire pour mettre cela dans le Cloud est gigantesque, et les coûts seraient tellement importants qu'il est plus avantageux d'acheter le stockage nous-mêmes plutôt que de payer quelqu'un d'autre pour s'en charger.
- Les performances des applications peuvent être amoindries : Un Cloud public n'améliorera définitivement pas les performances des applications.

- La fiabilité du Cloud : Un grand risque lorsqu'on met une application qui donne des avantages compétitifs ou qui contient des informations clients dans le Cloud,
- Taille de l'entreprise : Si votre entreprise est grande alors vos ressources sont grandes, ce qui inclut une grande consommation du cloud. Vous trouverez peut-être plus d'intérêt à mettre au point votre propre Cloud plutôt que d'en utiliser un externalisé. Les gains sont bien plus importants quand on passe d'une petite consommation de ressources à une consommation plus importante.

3.7 Conclusion

De l'informatique utilitaire des années 60, au service bureau des années 70, tout en passant par l'émergence d'Internet et des avancées de virtualisation, le Cloud Computing comme les chiffres nous le confirme, est promis à un bel avenir. Il reste encore beaucoup à faire notamment concernant la sécurité ou l'interopérabilité, mais aussi la mise en place de normes et de standards, qui permettront, comme c'était le cas lors du développement d'Internet, de constituer un ensemble de systèmes hétérogènes.

Au cours de cette partie, nous avons fourni une base théorique sur le Cloud Computing, en présentant ses types, ses services (IaaS, PaaS, SaaS) .ses avantages et inconvénients, afin d'appliquer ses concepts, spécifiquement le service SaaS à notre contexte.

4

Etudes Comparatives

4.1 Introduction

Le Cloud Computing représente un nouveau défi dans le monde informatique, Plusieurs solutions sont proposées : des solutions propriétaires et des solutions open source. Parmi les solutions propriétaires les plus connus on trouve :

- **VMwarevCloud** : Développé par la société VMware, l'un des leaders mondiaux dans le domaine de la virtualisation, ce logiciel sert tout aussi à créer son propre Cloud privé. Il donne la possibilité de créer des machines virtuelles ceci en fonction des besoins des utilisateurs.
- **Office 365** : Développé par la firme Microsoft, ce logiciel permet de créer un Cloud privé pour entreprise. La création et la configuration de nouveaux comptes utilisateurs se fait en quelques minutes. Il est idéal pour les entreprises de 25 employés ou moins.

Par la suite, Nous nous intéressons aux solutions open source, nous allons faire une étude comparative entre des différents, solutions open source au niveau IaaS, des serveurs d'application JEE, des systèmes de gestion de base de données, des logiciels de supervision, des logiciels de sauvegarde informatique et des firewalls. Cette étude comparative nous permettra d'adopter le système qui correspond à nos besoins afin de construire une infrastructure de cloud public.

4.2 Solution open source

Comme dans tous les domaines de l'informatique de nos jours, le Cloud Computing n'échappe pas à la règle du logiciel libre. Face à des solutions payantes et propriétaires, il existe des solutions libres et gratuites.

Ces logiciels sont développés en communauté, et font l'objet de mises à jour régulières. Ils peuvent être modifiés à volonté suivant l'utilisation que l'on veut en faire. Voici une liste non exhaustive de quelques logiciels libres pour créer son Cloud privé.

4.2.1 Openstack



Figure 12 : logo open stack

Créé en juillet 2010 par la NASA et l'hébergeur américain Rackspace, OpenStack est une offre d'IaaS 100% open-source. Ce n'est qu'en septembre 2012 qu'une fondation dédiée à Openstack a été créée, permet aux sociétés de développer leurs propres solutions d'infrastructure du Cloud Computing.

OpenStack est composé d'une série de logiciels et de projets au code source libre qui sont maintenus par la communauté incluant: OpenStack Compute (nommé Nova), OpenStack Object Storage (nommé Swift), et OpenStack Image Service (nommé Glance).

Il s'installe sur un système d'exploitation libre comme Ubuntu ou Debian et se configure entièrement en ligne de commande. C'est un système robuste et qui a fait ses preuves auprès des professionnels du domaine.

- **Code :**

- Ecrit en python
- Sous licence Apache 2.0

- **Versions :**

- Les versions sont cycliques et ont une durée de 6 mois
- La dernière version : juno

4.2.2 Eucalyptus



Figure 13 : Logo Eucalyptus

Eucalyptus est un outil, open source issue d'un projet de recherche de l'université de Californie. Est considéré parmi les solutions les plus connus, car elle est intégrée dans les distributions Ubuntu Server et Debian.

Permet de créer des Cloud IaaS de type privé ou hybride, son avantage majeur est le fait qu'il est compatible avec Amazon EC2 et S3.

Il possède également une version entreprise (Payante) de la société Eucalyptus Systèmes qui apporte de fonctionnalités supplémentaires comme le support de VMware [6].

- **Code :**

- Ecrit en Java, C et Python
- Sous licence GNE GPL v3

- **Versions :**

- Cycle de 4 mois
- La dernière version : Eucalyptus 4.0, le 30 Mai 2014

4.2.3 OpenNubela



Figure 14 : logo OpenNebula

Il s'agit d'une plateforme purement open source permettant de déployer des clouds privés, hybrides et publics.

OpenNebula est un projet de recherche commencé en 2005, publié en mars 2008 et financé par l'Union Européenne. Elle supporte les hyperviseurs Xen, KVM et VMware, le support de VirtualBox est prévu à partir de la version 4.0 de VirtualBox .

Cette solution propose une architecture complète pour la gestion de Datacenter et la création de services Cloud. [7]

- **Code :**

- Ecrit en C, C++, Ruby, Java, Shell script
- Sous licence Apache 2.0

- **Versions :**

- Cycle de 3 mois (mineur) et 12 mois (majeur)
- La dernière version : OpenNebula 4.4, le 03 décembre 2013.

4.2.4 CloudStack



Figure 15 : logo CloudStack

CloudStack est une plateforme informatique à la demande d'IaaS (infrastructure as a service) constituée de logiciels libre (open source). Permettant de déployer des clouds privés, hybrides et publics.

Elle support différents hyperviseurs du type VMware, Oracle VM ou encore KVM tout en étant également compatible avec le cloud public d'Amazon

Cloudstack a été fondé en Mai 2010 sous forme cloud.com. C'est en Juillet 2011 que le cloud.com a été racheté par la société Citrix.

- **Code :**

- Ecrit en Java et C
- Sous licence Apache 2.0

- **Versions :**

- Les versions sont cycliques et ont une durée de 4 mois
- La dernière version : Cloudstack 4.2.0 : 1 Octobre 2013

4.2.5 Etude comparative

Le tableau ci-dessous représente une étude comparative entre des différents systèmes de gestion de l'infrastructure du cloud computing.

	OpenStack	CloudStack	Eucalyptus	OpenNebula
Orientation	Cloud public, privé et hybride	Cloud public, privé et hybride	Cloud privé ou hybride	Cloud public, privé et hybride
Installation	Facile et automatisée	Facile	Facile mais difficile en environnement hétérogène	Manuelle et facile (sur les distributions supportées)
Sécurité	Très Bien	Bien	Bien	Neutre
Documentation	Excellente	Complète	Correcte	Complète

Tableau 4 : Etude comparative des systèmes de gestion de l'infrastructure du cloud

4.3 Les serveurs d'application JEE

Les serveurs d'applications sont des outils qui permettent l'exécution de composants Java côté serveur (servlets, JSP, EJB, ...) selon les spécifications de la plate-forme JEE.

Parmi les serveurs d'application les plus connus, et les plus utilisés (open source) à savoir : Apache Tomcat, GlassFish et JBoss.

4.3.1 Apache Tomcat

Apache Tomcat est une implémentation open source d'un conteneur web qui permet donc d'exécuter des applications web reposant sur les technologies servlets et JSP.

Apache Tomcat est l'un des serveurs d'applications Web les plus populaires et les plus puissants sur Linux. Tomcat est diffusé en open source sous une licence Apache.

Tomcat est un ensemble de plusieurs composantes ayant chacun un rôle. Il s'agit par exemple de : [8]

- **catalina** : un conteneur servlet qui implémente les spécifications de Sun pour les servlets et les JSP.
- **coyote** : un connecteur http qui écoute le trafic entrant, dirige les requêtes au moteur de Tomcat et renvoie la réponse au client.
- **jasper** : un moteur JSP qui compile les fichiers JSP en tant que servlets et est capable de détecter les modifications des fichiers et de les recompiler à la volée.

4.3.2 GlassFish

Né en juin 2005, Sun Glassfish Enterprise Server est le premier serveur Open source ayant implémenté totalement la norme JEE 5.

GlassFish est un serveur d'application développé par Sun Microsystems, implémente complètement la norme JEE (EJB, JPA, JSF, JSP et Servlet), et qui est maintenant maintenu par Oracle Corporation. Il est open source et distribué sous double licence CDDL et GPLv2. Il dispose de nombreux outils pour faciliter le développement, le déploiement et la maintenance d'application. [9]

4.3.3 JBOSS

JBoss est un serveur d'application Java EE, écrit en Java et distribué sous licence GNU LGPL. Étant donné qu'il est écrit en Java, JBoss Application Server peut être utilisé sur tout système d'exploitation fournissant une machine virtuelle Java (JVM). [10]

4.3.4 Etude comparative

	Apache Tomcat	GlassFish	JBoss
Prise en main	Rapide	Rapide	Lente
Sécurité	Faible	excellente	excellente
Performance	Moyenne	Elevée	Très élevé
Support/Communauté	Excellente	Existante	Correcte
Délai d'exécution du code	Rapide	Rapide	Lente

Tableau 5 : Etude comparative des serveurs d'application JEE

4.4 Les systèmes de gestion de base de données

Un système de gestion de base de données (abr. SGBD) est un logiciel système destiné à stocker et à partager des informations dans une base de données, en garantissant la qualité, la pérennité et la confidentialité des informations, tout en cachant la complexité des opérations. Un SGBD (en anglais DBMS pour database management system) permet d'inscrire, de retrouver, de modifier, de trier, de transformer ou d'imprimer les informations de la base de données.

Nous avons donc besoin d'un logiciel qui permet d'interagir avec une base de données grâce à un système de gestion de base de données (SGBD). Nous avons sélectionné trois SGBD: MySQL, PostgreSQL et HSQLDB, afin de réaliser une étude comparative et d'adopter celui qui correspond le plus à nos besoins.

4.4.1 MySQL

Est un système de gestion de bases de données relationnelles (SGBDR). Il est distribué sous une double licence GPL et propriétaire. Il fait partie des logiciels de gestion de base de données les plus utilisés au monde [11].

4.4.2 PostgreSQL

Est un système de gestion de base de données relationnelle et objet (SGBDRO). C'est un outil libre disponible selon les termes d'une licence de type BSD.

Ce système multi-plateforme est largement connu et réputé à travers le monde, notamment pour son comportement stable et pour être très respectueux des *normes ANSI SQL*.

4.4.3 HSQLDB

HSQLDB est un système de gestion de base de données relationnelle, développé en Java. Il est disponible sous une licence BSD.

4.4.4 Etude comparative

	MySQL	PostgreSQL	HSQLDB
Installation/configuration	Facile	Facile	Facile
Documentation	Excellente	Excellente	Existante
Taille de Base de données	Illimitée	Illimitée	8 Go
Délai d'exécution des requêtes	Rapide	Lente	Lente
Systèmes d'exploitation	Windows, Linux, MAC OS X	Windows, Linux, MAC OS X	Windows, Linux, MAC OS X

Tableau 6 : Etude comparative des systèmes de gestion de base de données

4.5 Les logiciels de supervision informatique

La gestion d'un parc de serveurs est un travail à temps réel. Un bon administrateur réseau doit savoir à tout moment l'état des différentes machines et des différents services. Cependant, l'administrateur ne peut pas se permettre de passer son temps devant un tableau avec des voyants verts en attendant qu'un voyant passe au rouge pour agir, son temps est occupé à d'autres tâches, donc il ne peut pas surveiller les statuts des machines en permanence.

L'examen quotidien des logs systèmes est un bon début, mais, si un problème survient, on s'en rend compte seulement le lendemain, ce qui peut être trop tard.

Pour simplifier leur travail, les administrateurs utilisent généralement des logiciels de surveillance et de supervision de réseaux.

La supervision est la « surveillance du bon fonctionnement d'un système ou d'une activité ». Elle permet de surveiller, rapporter et alerter les fonctionnements normaux et anormaux des systèmes informatiques.

Parmi les logiciels de surveillance et de supervision de réseaux open source les plus populaires on trouve : Nagios, Zenoss, Zabbix.

4.5.1 Nagios

Nagios (anciennement appelé **Netsaint**) est une application permettant la surveillance système et réseau. Elle surveille les hôtes et services spécifiés, alertant lorsque les systèmes ont des dysfonctionnements et quand ils repassent en fonctionnement normal. C'est un logiciel libre sous licence GPL.

4.5.2 Zenoss

Zenoss est une plate-forme d'administration et de supervision réseau. Sous licence GPL, il est construit avec Zope et Python.

Les principales fonctions de ce logiciel sont la supervision de l'activité du réseau, la gestion de la performance, d'évènements ainsi que des alertes. Les communications entre les clients et le serveur reposent essentiellement sur les protocoles SNMP, Telnet/SSH et WMI (Windows Management Instrumentation).

4.5.3 Zabbix

Créé en 2000 par **Alexel Vladishev**, Zabbix est une solution de supervision open source de classe Entreprise. Simple à installer, il est compatible avec les systèmes Linux, Windows et Unix.

Il permet de surveiller l'état de divers services réseau, serveurs et autres matériels réseau et produisant des graphiques dynamiques de consommation des ressources

4.5.4 Etude comparative

	Nagios	Zenoss	Zabbix
Environnements	Linux, Windows	Linux, Windows	Linux, Unix, Windows
Installation	Facile	Facile	Facile
Configuration	Pas facile	Facile	Problème de configuration sur le Switch
Ressources	Minimal	Plus gourmand en ressource machine	Selon les machines à surveiller (utilise Base de données pour stocker les données)
Licence	GNU GPL	GPL/version commerciale	GNU GPL

Tableau 7 : Etude comparative des logiciels de supervision informatique

4.6 Les logiciels de sauvegarde informatique

En informatique, la **sauvegarde** (*backup* en anglais) est l'opération qui consiste à dupliquer et à mettre en sécurité les données contenues dans un système informatique.

La perte de données peut être due à plusieurs facteurs (mauvaise manipulation, disque dur hors service, malveillance, vol, ...).

4.6.1 Les différents types de sauvegarde

La majorité des outils de sauvegarde proposent au moins trois types de sauvegardes à savoir :

- **Sauvegarde complète** : permet de sauvegarder toutes les données, les répertoires et les sous répertoires sélectionnés. C'est le type de sauvegarde le plus rapide, le plus simple, et le plus précis pour restaurer les données sans erreurs.
- **Sauvegarde différentielle** : permet de sauvegarder les données qui ont été modifiées ou ajoutées depuis la dernière sauvegarde complète. La sauvegarde différentielle permet comme la sauvegarde incrémentale de sauvegarder les données plus rapidement qu'avec une sauvegarde complète, mais prend plus de temps qu'une sauvegarde incrémentale.
- **Sauvegarde incrémentale** : permet de sauvegarder les données qui ont été modifiées ou ajoutées depuis la dernière sauvegarde complète ou incrémentale. La sauvegarde incrémentale permet de sauvegarder les dernières modifications sur les fichiers plus rapidement qu'avec une sauvegarde complète

4.6.2 Etude comparative

Le tableau ci-dessous représente une étude comparative entre des différents logiciels de sauvegarde informatique.

Nom	Sauvegarde complète	Différentielle	Incrémentale	Planification	Description
BackupPC	Oui	Oui	Oui	Oui	Outil puissant. Sauvegarder plusieurs clients (Linux ou Windows).

Bacula	Oui	Oui	Oui	Oui	Outil puissant. Installation et la configuration et l'utilisation très. simple.
Areca Backup	Oui	Oui	Oui	Non	Sauvegarde sur un disque local ou distant.
Sbackup	Oui	Non	Oui	Oui	Outil simple d'utilisation.
Backup-Manager	Oui	Oui	Oui	Non	Sauvegarde de fichier local sous forme d'archivages pouvant être exportés sur un serveur distant.

Tableau 8 : Etude comparative des logiciels de sauvegarde

4.7 Les firewalls

Toutes les entreprises possédant un réseau local disposent aussi d'un accès à Internet, afin d'accéder à la manne d'information disponible sur le réseau des réseaux, et de pouvoir communiquer avec l'extérieur. Cette ouverture vers l'extérieur est indispensable... et dangereuse en même temps. Ouvrir l'entreprise vers le monde signifie aussi laisser place ouverte aux étrangers pour essayer de pénétrer le réseau local de l'entreprise, et y accomplir des actions douteuses, parfois gratuites, de destruction, vol d'informations confidentielles, ...

Pour parer à ces attaques, une architecture sécurisée est nécessaire. Pour cela, le cœur d'une telle architecture est basé sur un **firewall**. Cet outil a pour but de sécuriser au maximum le réseau local de l'entreprise, de détecter les tentatives d'intrusion et d'y parer au mieux possible.

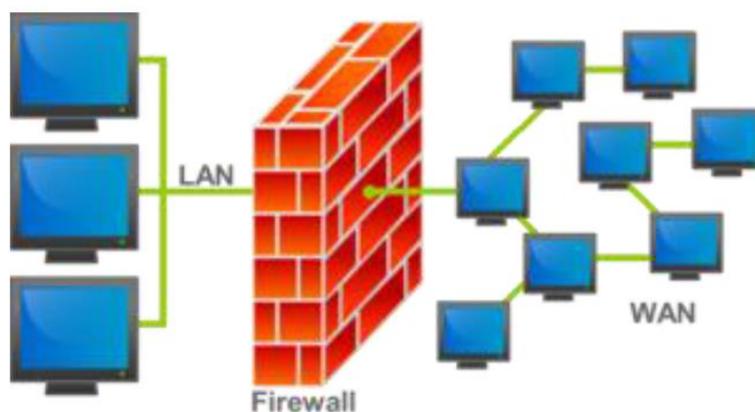


Figure 16 : Représentation d'un firewall

Un pare-feu (Firewall, en anglais) est un dispositif matériel et/ou logiciel qui implémente la fonction de sécurité de contrôle d'accès. Un pare-feu est donc un dispositif pour filtrer les accès, les paquets IP, les flux entrant et sortant d'un système.

Les firewalls sont nombreux, nous avons sélectionné seulement trois, à savoir Pfsense, IPCop et Smoothwall.

4.7.1 Firewall Pfsense

PfSense ou « *Packet Filter Sense* » est un routeur/firewall open source basé sur le système d'exploitation FreeBSD réputé pour son extrême stabilité et Monowall auquel il rajoute ses propres fonctionnalités.

Ce qui séduit chez Pfsense est sa facilité d'installation et de configuration des outils d'administration réseau. En effet est possible de configurer quasiment toutes les fonctionnalités de Pfsense via l'interface Gui PHP.

La distribution Pfsense met ainsi à la disposition de l'administrateur réseau une multitude d'outils open sources permettant d'optimiser ses tâches.

4.7.2 Firewall IPCop

Est un projet Open Source dont le but est d'obtenir une distribution GNU/Linux complètement dédiée à la sécurité et aux services essentiels d'un réseau. C'est une distribution linux faite pour protéger un réseau des menaces d'Internet et surveiller son fonctionnement.

Les principaux services offerts de base sont les suivants: DHCP, NTP (serveur de temps), PROXY, SSH, IDS (détection d'intrusions).

4.7.3 Firewall Smoothwall

Smoothwall est une distribution de firewall/routeur optimisé, paramétrable via une interface web et qui tourne sur n'importe quel vieux PC. Conçue pour être utilisée comme une source ouverte pare-feu. Elle comprenait également le système de détection d'intrusion Snort (IDS).

4.7.4 Comparaison

	Pfsense	IPCop	Smoothwall Express
Licence	BSD	GPL	GPL
Installation et configuration	Facile	Simple et rapide	Facile
Configuration minimale	133 Mhz/ 128 Mb de RAM/ 1Go de DD/ Cartes réseaux 100 Mbit/s	233 MHz/ 64Mo de RAM/ 800Mo de DD/ Cartes réseaux 10/100 Mbit/s	100 MHz/ 16Mo de RAM/200 Mo de DD/ Cartes réseaux 10 Mbit/s
VPN	IPSec, PPTP, L2TP, clés RSA, DES, 3DES, AES	IPSec, PPTP, clés RSA, DES, 3DES	IPSec, clés RSA, DES, 3DES, AES
Load Balance	Oui	Non	Non
Multi-WAN	Oui	Non	Non
Mises à jour automatique	Oui	Non	Non

Tableau 9 : Etude comparative des firewalls

4.8 Conclusion

Après les différentes études comparatives, nous allons adopter comme un système de gestion du cloud au niveau IaaS : Openstack, le serveur d'application JEE GlassFish, le système de gestion de base de données MySQL, le logiciel de supervision Nagios, le logiciels de sauvegarde informatique Bacula et le firewall Pfsense pour construire notre infrastructure du cloud public.

5

Architecture Technique et Logicielle

Ce chapitre est consacré à la présentation de L'architecture Technique qui permet de construire l'infrastructure de notre cloud ainsi que l'architecture logicielle qui contient les Framework utilisé pour construit notre application ainsi que l'organisation de code.

5.1 Architecture technique

Dans cette partie nous allons présenter l'infrastructure réseau de notre application BusinessaaS ainsi que architecture du système.

5.1.1 Architecture du réseau

L'infrastructure réseau de notre application BusinessaaS est composée d'un :

- routeur (20 MB et IP fixe)
- firewall (pfSense)
- Serveur DHCP
- Serveur de supervision (Nagios)

- Serveur de sauvegarde (Backup)

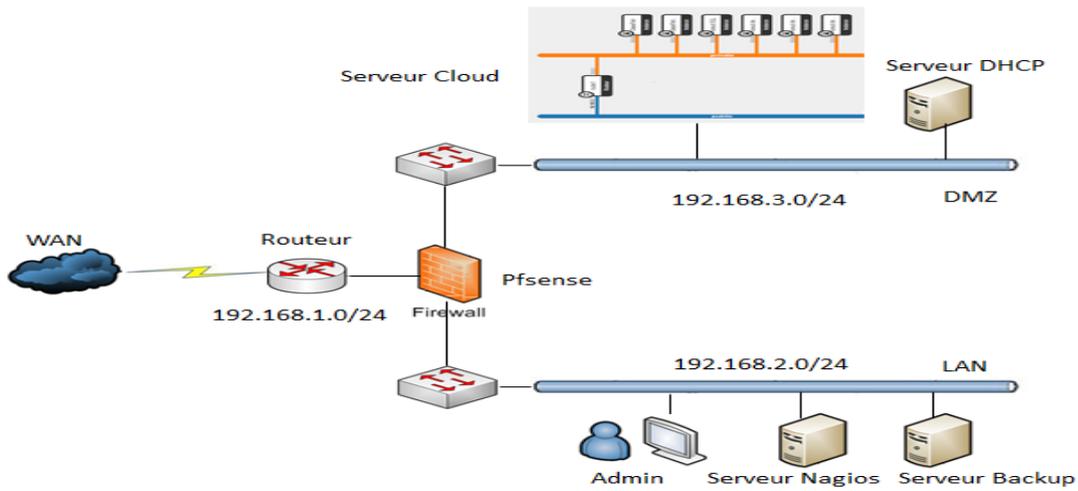


Figure 17 : Architecture réseau du Cloud

5.1.1.1 Serveur cloud (Open Stack)



OpenStack est un système d’exploitation de Cloud capable de contrôler de grand volume de calcul, de stockage et de ressources réseau au travers d’un data center virtuel, le tout géré par un tableau de bord offrant aux administrateurs le contrôle des utilisateurs et des ressources à disposition par le biais d’une interface web.

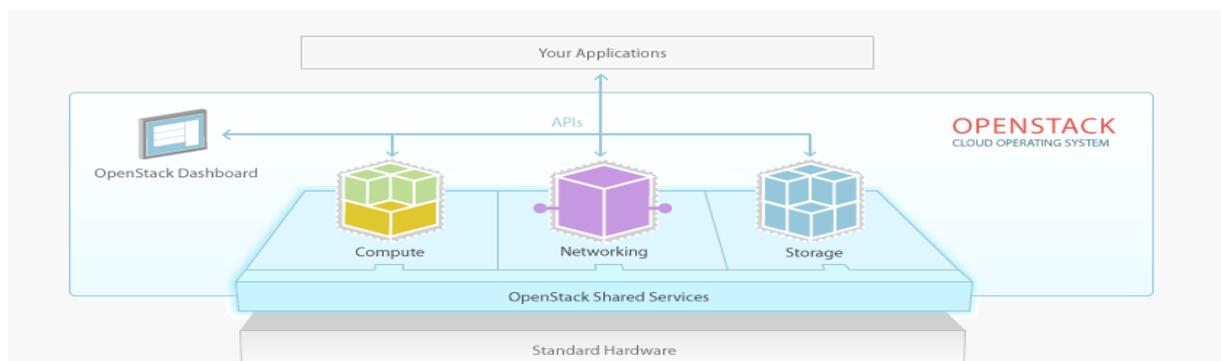


Figure 18 : système Openstack

Composantes d'OpenStack :

- **OpenStack Nova (Compute) :** provisionner et contrôler un large réseau de ressources virtuelles (machine, réseau, stockage).
- **OpenStack Swift (Object Storage) :** Plateforme de stockage de plusieurs Petabytes hautement disponible
- **Openstack Glance (Image Service) :** Gérer et organiser le catalogue d'images de machines
- **Keystone (Gestion des Identités) :** Unification et gestion centralisée des comptes pour l'ensemble des services
- **Horizon (Dashboad) :** Module pour construire vos interfaces Web (Django)
- **Quantum (Gestion de Réseau) :** bloc complet pour la gestion de réseaux complexes dans les infrastructures clouds
- **Cinder (Gestion d'interconnexion du stockage) :** Service de disques persistants pour les machines virtuelles
- **Ceilometer (Module de Mesure et De Facturation)**
- **Oslo (OpenStack common library) :** visionner et contrôler un large réseau de ressources virtuelles (machines, réseau, stockage)
- **Neutron :** Permet la connectivité réseau en tant que service pour d'autres services, tels qu'OpenStack Compute

Installation et Configuration d'OpenStack

Après installation et configuration d'OpenStack sous ubuntu14.04 (**voir l'Annexe1**), dedans nous avons créé des instances comme montre la figure ci-dessous, dans chaque instance nous avons installé et configuré un serveur virtuel :

- **Le serveur d'application « GlassFish » (voir l'Annexe2) :** GlassFish est un serveur d'application libre open source pour la plate-forme JEE.
- **Le cluster de serveur GlassFish (voir l'Annexe3) :** Le clustering est l'utilisation de plusieurs ordinateurs, typiquement PC ou stations de travail, plusieurs périphériques de stockage, et des interconnexions redondantes, pour former ce qui apparaît aux utilisateurs comme un système unique à haute disponibilité.

Utilité de Clustering

La technologie de cluster informatique, met grappes de systèmes ensemble pour offrir une meilleure fiabilité, disponibilité et les performances du système, aux clients du réseau.

Si l'un des serveurs du cluster GlassFish tombe en panne, un autre serveur prend le relais et le service n'est pas interrompu.

Dans la pratique, le cluster de GlassFish fonctionne de la manière suivante: chaque nœud du cluster doit avoir un serveur GlassFish installé au préalable, puis crée des instances dans les différents nœuds.

Notre cluster GlassFish est composé de deux nœuds, avec deux instances dans chacun et un nœud gère également le DAS (Domain Administration Server : est le serveur principal qui permet de configurer et de mettre en relation pour la première fois tous les nœuds. Dès que le cluster est démarré, le DAS peut tomber en panne sans que cela n'affecte les autres nœuds du cluster). La figure ci-dessous explique l'architecture du cluster GlassFish.



Figure 19 : Cluster GlassFish

- **Le serveur MySQL cluster (voir l'Annexe 4) :** MySQL cluster est un groupe de processus qui s'exécutent sur plusieurs serveurs MySQL, Il est conçu pour fournir une haute disponibilité et un débit élevé avec une faible latence.

MySQL cluster est constitué de trois composants principaux :

- Le nœud SQL: un nœud qui accède aux données du cluster.
- Le nœud de gestion: c'est lui qui supervise le cluster. Ses missions principales sont de répartir la charge lors des transferts de données et de maintenir à jour l'état du cluster.

- Le nœud de données : C'est le nœud où les données réelles du cluster sont stockées.

Notre cluster sera configuré comme suite :

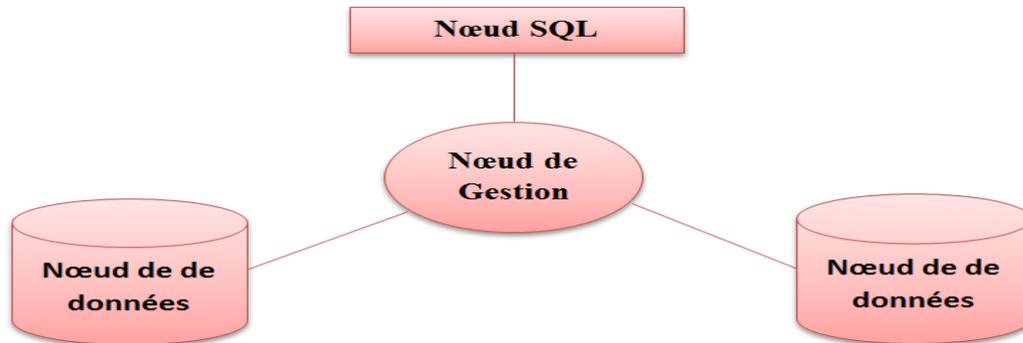


Figure 20 : Architecture de MySQL Cluster

Dans le serveur d'application, nous allons déployer l'application web de notre société BusinessaaS et l'application de nos clients : les écoles privées. Et au niveau du serveur de base de données, nous allons créer la base de données de notre société « BusinessaaS » et une base de données pour chaque client « école privée ».

La figure ci-dessous représente la topologie du serveur cloud.

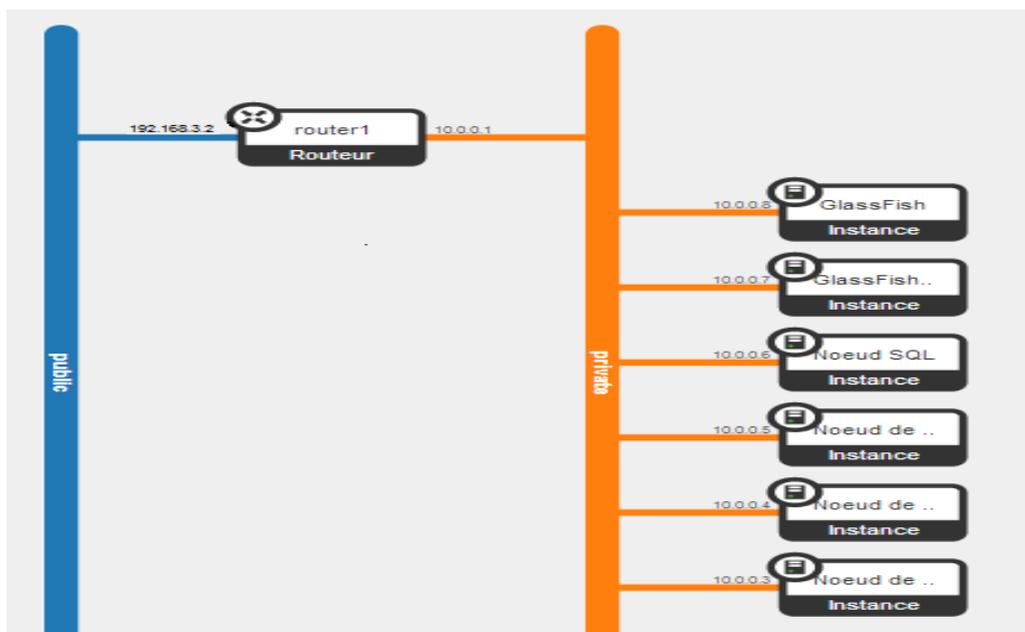


Figure 21 : La topologie du serveur cloud

5.1.1.2 Serveur DHCP (Dynamic Host Configuration Protocol)

Un serveur DHCP a pour rôle de distribuer des adresses IP à des clients pour une durée déterminée. Au lieu d'affecter manuellement à chaque machine une adresse statique, ainsi que tous les paramètres tels que serveur de noms DNS, passerelle par défaut, nom du réseau, un serveur DHCP alloue à chaque client un bail d'accès au réseau, pour une durée déterminée (durée du bail). Il passe en paramètres au client toutes les informations dont il a besoin. Tous les nœuds critiques du réseau (serveur de nom primaire et secondaire, passerelle par défaut) ont une adresse IP statique, en effet si celle-ci variait, ce processus ne serait réalisable.

Avantage de DHCP

- Le protocole DHCP offre une configuration de réseau TCP/IP fiable et simple, empêche les conflits d'adresses et permet de contrôler l'utilisation des adresses IP de façon centralisée.
- Economie d'adresse : ce protocole est presque toujours utilisé par les fournisseurs d'accès Internet qui disposent d'un nombre d'adresses limité.

Le fonctionnement de DHCP :

Le dialogue entre le client et le serveur DHCP est décrit comme illustré ci-dessous:

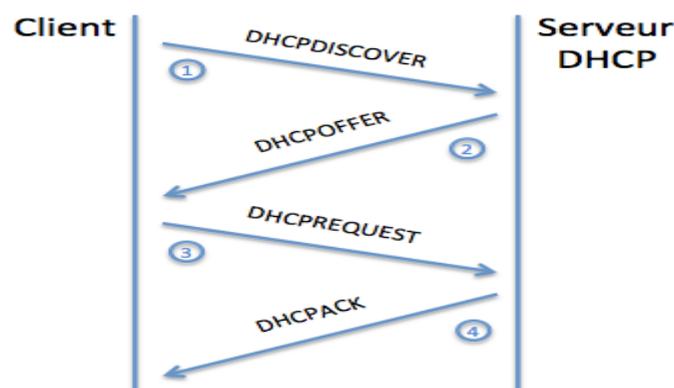


Figure 22 : Dialogue entre le client et le serveur DHCP

1. Lorsque le client DHCP démarre, il n'a aucune connaissance du réseau, il envoie donc une trame "**DHCPDISCOVER**", destinée à trouver un serveur DHCP.

2. **DHCPOFFER** : Le serveur DHCP le plus proche répond en unicast (uniquement à la machine voulue) en lui proposant une configuration DHCP (une adresse IP, un masque de sous réseau, l'adresse d'une passerelle par défaut et l'adresse d'un serveur DNS).
3. Le client répond alors par un **DHCPREQUEST** à tous les serveurs (donc toujours en "Broadcast") pour indiquer quelle offre il accepte.
4. Le serveur DHCP concerné répond définitivement par un **DHCPACK** qui constitue une confirmation du bail. L'adresse du client est alors marquée comme utilisée et ne sera plus proposée à un autre client pour toute la durée du bail.

5.1.1.3 Serveur de supervision (Nagios)



Pour surveiller et superviser notre infrastructure réseau nous avons choisi Nagios, Successeur de NetSaint, il est certainement le logiciel libre le plus connu dans le milieu de la supervision réseau. Appréciée des entreprises ainsi que des particuliers, cette application possède une très grande communauté qui participent activement au développement.

Nagios supervise la disponibilité d'actifs réseaux, de serveurs ou d'applications, suivre l'évolution des capacités disques ou la bande passante de carte réseau etc.

Nagios génère des alertes en fonction de l'état des matériels et services supervisés, ces alertes visualisées par une interface web. Cette interface web permet également l'administration (très partielle) du monitoring. Il existe quatre types d'états :

- **OK** : tout va bien.
- **WARNING** : le seuil d'alerte est dépassé.
- **CRITICAL** : le service a un problème.
- **UNKNOWN** : impossible de connaître l'état du service.

Veuillez trouver les phases d'installation et de configuration de Nagios dans « l'Annexe 5 ».

5.1.1.4 Serveur de sauvegarde (Bacula)



Pour sauvegarder les fichiers de configurations de notre réseau nous avons choisi Bacula qui est un système de sauvegarde libre extrêmement puissant. Le logiciel dispose d'un ensemble de fonctionnalités extrêmement intéressant, et d'une qualité professionnelle telle que certains logiciels propriétaires devraient suivre son exemple.

Veillez trouver les phases d'installation et de configuration dans « **l'Annexe 6** ».

▪ **Stratégie de sauvegarde :**

La stratégie que nous avons suivi pour sauvegarder les partitions des nœuds de données de MySQL cluster et les fichiers de configuration de chaque serveurs de l'infrastructure réseaux est comme suite :

Les fichiers de configuration de chaque serveur:

- Sauvegarde complète : chaque dimanche à 22 :00.

Les partitions des nœuds de données de MySQL cluster :

- Sauvegarde complète : chaque samedi à 23 :00.

- Sauvegarde incrémentale : chaque lundi, mardi, mercredi, jeudi, vendredi et dimanche à 23:00.

5.1.1.5 Firewall(PFSense)



Nous avons choisi comme firewall la distribution Linux PFSense (Packet Filter Sense) qui est un firewall open source reconnu comme l'un des plus puissants, sécurisé et fiable parmi les firewalls existant. Son succès est basé sur le fait qu'il est entièrement configurable via une interface web simple et intuitive.

Veillez trouver les phases l'installation et configuration de PFSense dans « **Annexe 7** ». Comme présenté dans l'architecture technique, nous avons attribué : au LAN le réseau 192.168.2.0/24, au DMZ le réseau 192.168.3.0/24 et au WAN le réseau 192.168.1.0/24. L'image suivante montre la configuration réseau du Firewall :



Figure 23 : La configuration réseau du firewall

▪ **Stratégie de sécurité :**

Nous avons choisi comme stratégie de sécurité les règles suivantes:

- Le Réseau LAN: peut accéder au Réseau WAN et DMZ.
- Le Réseau WAN: ne peut pas accéder au Réseau LAN.
- Le Réseau WAN: à un accès très restreint au réseau DMZ peut accéder au service (HTTPS, SFTP) de serveur d'application (192.168.3.201/24) et au serveur cluster GlassFish (192.168.3.202/24).
- Le Réseau DMZ: étant donné que le Réseau WAN a accès au Réseau DMZ, nous avons bloqué tout accès du DMZ vers le LAN pour remédier aux attaques par rebond.

Les images suivantes représentent l'implémentation de ces règles sous PfSense :

Firewall: Rules



Firewall: Rules										
Floating										
WAN LAN DMZ										
ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	
▶	*	*	*	LAN Address	80 22	*	*		Anti-Lockout Rule	⌵ ⌴
▶	IPv4 *	*	*	*	*	*	none		Default allow LAN to any rule	⌵ ⌴

Figure 24 : Les règles de l'interface LAN

Firewall: Rules



Firewall: Rules										
Floating WAN LAN DMZ										
ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	
<input type="checkbox"/>	IPv4 TCP/UDP	WAN net	*	192.168.3.99/24	443 (HTTPS)	*	none		wan_to_dmz_port_HTTPS	
<input type="checkbox"/>	IPv4 TCP/UDP	WAN net	*	192.168.3.100/24	443 (HTTPS)	*	none		wan_to_dmz_port_HTTPS	
<input type="checkbox"/>	IPv4 TCP/UDP	WAN net	*	192.168.3.99/24	22 (SSH)	*	none		wan_to_dmz_port_SFTP	
<input type="checkbox"/>	IPv4 TCP/UDP	WAN net	*	192.168.3.100/24	22 (SSH)	*	none		wan_to_dmz_port_SFTP	

Figure 25 : Les règles de l'interface WAN

Firewall: Rules



Firewall: Rules										
Floating WAN LAN DMZ										
ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	
<input type="checkbox"/>	IPv4 ICMP	DMZ net	*	WAN net	*	*	none			
<input type="checkbox"/>	IPv4 TCP/UDP	DMZ net	*	WAN net	*	*	none			
<input checked="" type="checkbox"/>	IPv4 ICMP	DMZ net	*	LAN net	*	*	none			
<input checked="" type="checkbox"/>	IPv4 TCP/UDP	DMZ net	*	LAN net	*	*	none			

Figure 26 : Les règles de l'interface DMZ

5.1.1.6 SNORT

SNORT est un outil open source de détection d'intrusions réseaux. SNORT est capable d'écouter sur une interface afin d'effectuer une analyse du trafic en temps réel, de logger les paquets IP, de rechercher des correspondances de contenu, le but étant de détecter une grande variété d'attaques connues.

SNORT peut fonctionner en quatre modes différents :

- SNIFFER : capture et affichage des paquets.
- PACKET LOGGER : capture et log des paquets.

- NIDS (Network Based Intrusion Detection System) : Détecter des tentatives d'intrusions réseaux d'après des règles.
- IPS (Intrusion Prevention System) : Empêcher les intrusions réseaux détectées, toujours d'après les mêmes règles.

Après l'installation et configuration de SNORT sous PfSense (voir l'annexe 8), nous allons lancer le logiciel Zenmap pour scanner le réseau afin de tester la détection d'une attaque.

Une fois SNORT détecte l'attaque, il va bloquer l'accès de l'intrus malveillants au réseau, comme indiqué ci-dessous.

The screenshot shows the 'Snort: Blocked Hosts' interface. At the top, there are tabs for 'Snort Interfaces', 'Global Settings', 'Updates', 'Alerts', 'Blocked', 'Whitelists', 'Suppress', and 'Sync'. Below the tabs, there is a 'Blocked Hosts Log View Settings' section with options to 'Download' (All blocked hosts will be saved), 'Clear' (Warning: all hosts will be removed), and 'Auto Refresh and Log View' (Save, Refresh, Default is ON, 500). Below this is a table titled 'Last 500 Hosts Blocked by Snort' with columns for '#', 'IP', 'Alert Description', and 'Remove'. The table contains one entry for IP 192.168.1.77 with several alert descriptions.

#	IP	Alert Description	Remove
1	192.168.1.77	ET SCAN Potential VNC Scan 5800-5820 - 08/27/14-09:27:33 ET SCAN Potential SSH Scan - 08/27/14-09:25:37 ET SCAN Nmap Scripting Engine User-Agent Detected - 08/27/14-09:23:24 (http_inspect) WEBROOT DIRECTORY TRAVERSAL - 08/27/14-09:23:24 (http_inspect) NO CONTENT -LENGTH OR TRANSFER 6ENCODING IN HTTP REPOSE -08/27/14-09:23:24	

Figure 27 : Exemple de machine malveillante bloqué par SNORT

5.1.2 Architecture du système

L'application de fournisseur « BusinessaaS » à un accès à la base de données de fournisseur, cette application utilisé par les écoles privée afin de s'abonner aux services offerts par le fournisseur cloud, et de même utilisée par l'administrateur cloud pour la gérer.

L'application à la demande, nommée « EcoleSaaS », à un accès à deux bases de données, une base de données commune entre toutes les écoles, c'est la base de données de BusinessaaS et une base de données propre à chacune. La base de données de BusinessaaS pour indiquer les modules bénéficiés et le nom de sa propre base de données. Elle est aussi utilisée par l'administrateur d'école pour la gérer.

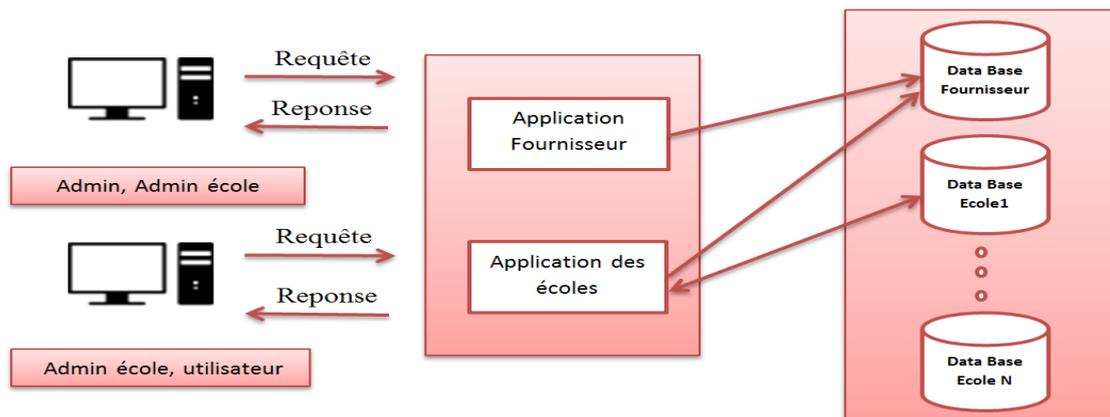


Figure 28 : Architecture du système

5.2 Architecture logicielle

5.2.1 Pattern de conception

Le Modèle-Vue-Contrôleur (en abrégé MVC, de l'anglais Model-View-Controller) est une architecture et une méthode de conception qui organise l'interface homme-machine (IHM) d'une application logicielle. Ce paradigme divise l'IHM en un modèle (modèle de données), une vue (présentation, interface utilisateur) et un contrôleur (logique de contrôle, gestion des événements, synchronisation), chacun ayant un rôle précis dans l'interface. Ce modèle d'architecture impose la séparation entre les données, la présentation et les traitements, ce qui donne trois parties fondamentales dans l'application finale : le modèle, la vue et le contrôleur.

5.2.2 Pattern de couche

Nous avons décomposé nos applications en quatre couches à savoir :

- **DAO** : s'occupe de l'accès aux données
- **Service** : La couche métier : représente le logique métier
- **Controller** : La couche de présentation : comprend des actions mettant la relation entre les modèles et les vues.
- **Business Object** : Cette couche représente le domaine du métier. Généralement sont des POJO représentent les tables de la base de données.

5.2.3 Frameworks et base de données utilisés

L'utilisation du Framework Hibernante permet de garantir l'accès à la base de données par des appels à des méthodes objet de haut niveau. Ainsi que Framework Struts2 permet la structuration d'une application Java sous forme d'un ensemble d'actions représentant des événements déclenchés par les utilisateurs de l'application.

Logo	Description
	Struts2 : est un Framework libre servant au développement d'applications web Java EE.
	Hibernate : est un Framework open source gérant la persistance des objets en base de données relationnelle.
	MySQL : est un système de gestion de base de données (SGBD). Il est distribué sous une double licence GPL et propriétaire. Il fait partie des logiciels de gestion de base de données les plus utilisés au monde.

Tableau 10 : Framework java et base de données

5.2.4 Les outils utilisés

- **Eclipse** : est un environnement de développement intégré (Integrated Development Environment) dont le but est de fournir une plate-forme modulaire pour permettre de réaliser des développements informatiques. Il est développé par IBM, est gratuit et disponible pour la plupart des systèmes d'exploitation.
- **Visual Paradigm For UML** : permet la création des diagrammes UML et des modèles qui en sont à l'origine. Ceux-ci peuvent alors générer du code dans un langage de programmation déterminé. Il propose également la création d'autres types de diagrammes, comme celui qui permet la modélisation des bases de données pouvant, lui aussi, générer des canevas d'applications basé sur des Framework et Pattern mais en plus, générer du code SQL qu'il peut ensuite déployer automatiquement dans différents environnements.
- **Jasper Reports** : est un outil de reporting Open source pour le langage Java. Il peut accéder aux données via JDBC, Table Models, JavaBeans, XML, Hibernate, CSV, Il génère des rapports au format PDF, RTF, XML, XLS, CSV, HTML, XHTML, texte, DOCX, et OpenOffice. Il peut être couplé à iReport pour faciliter la création des rapports au format .jrxml

6

Analyse Et Conception

Tout comme la construction d'une maison nécessite des plans à différents niveaux (vision extérieure, plan des différents étages, plans techniques...), la réalisation d'une application informatique ou d'un ensemble d'applications est basée sur plusieurs diagrammes.

Le formalisme UML s'est imposé comme l'outil de plus approprié pour ce projet. En effet, le langage de modélisation UML permet de mener la phase de conception tout en bénéficiant de la puissance et de la simplicité de ses diagrammes

Dans ce chapitre nous allons présenter, le diagramme de cas d'utilisation, le diagramme de séquence boîte noire et le diagramme de classes d'analyse.

6.1 Phase d'inception

Consiste à cadrer le projet et à définir son business case, en particulier en identifiant toutes les entités externes qui vont interagir avec le système, et en définissant la nature de cette interaction à haut niveau.

6.1.1 Diagramme de cas d'utilisation

Il permet d'identifier les possibilités d'interaction entre le système et les acteurs (intervenants extérieurs au système), c'est-à-dire toutes les fonctionnalités que doit fournir le système. Il permet aussi de délimiter le système.

Un cas d'utilisation représente une unité discrète d'interaction entre un utilisateur (humain ou machine) et un système. Il est une unité significative de travail. Dans un diagramme de cas d'utilisation, les utilisateurs sont appelés acteurs (actors), ils interagissent avec les cas d'utilisation (use cases).

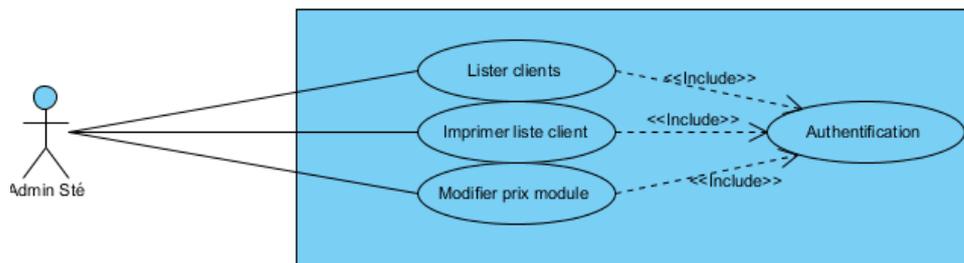


Figure 29 : Diagramme de cas d'utilisation de société BusinessaaS

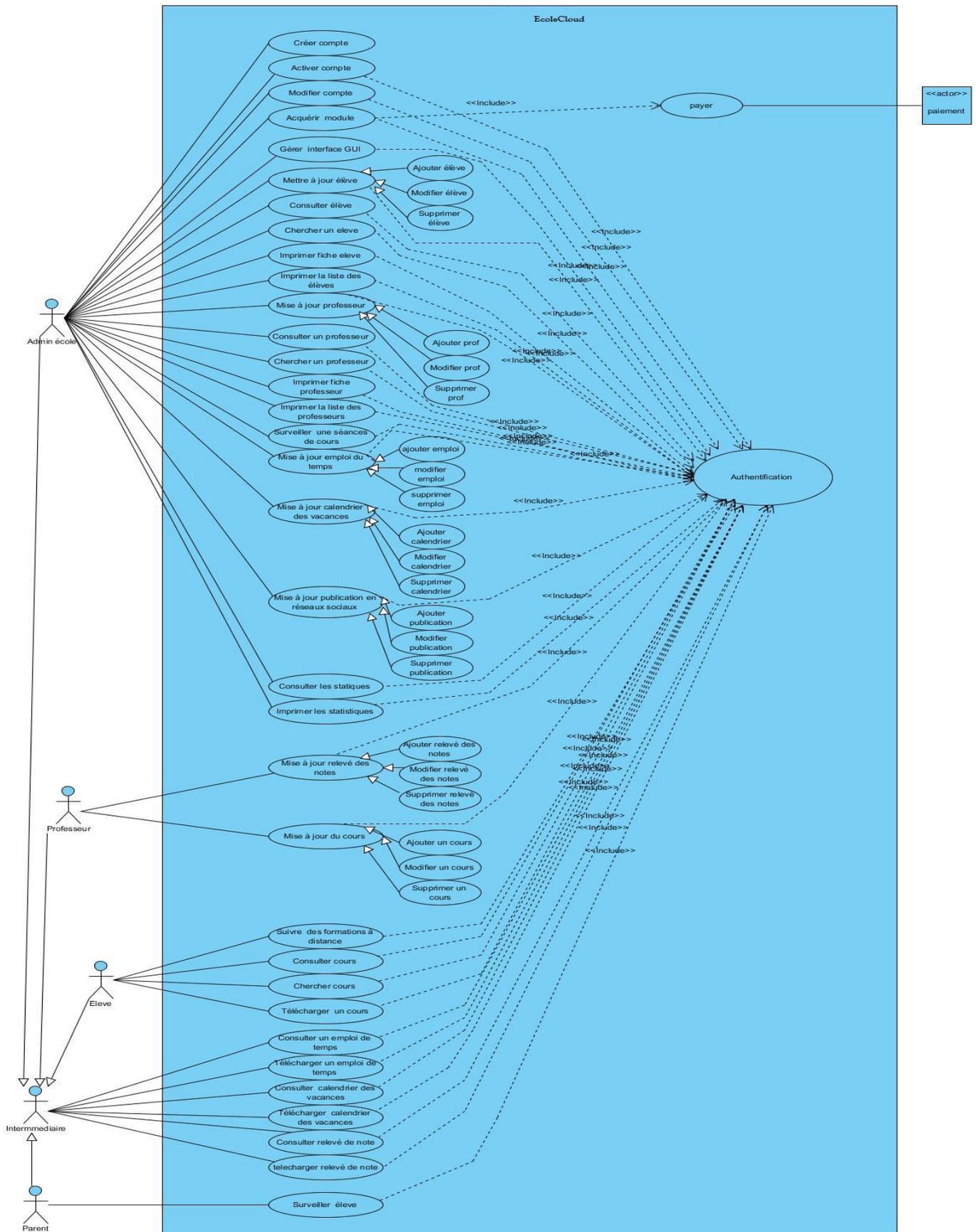


Figure 30 : Diagramme de cas d'utilisation de l'école

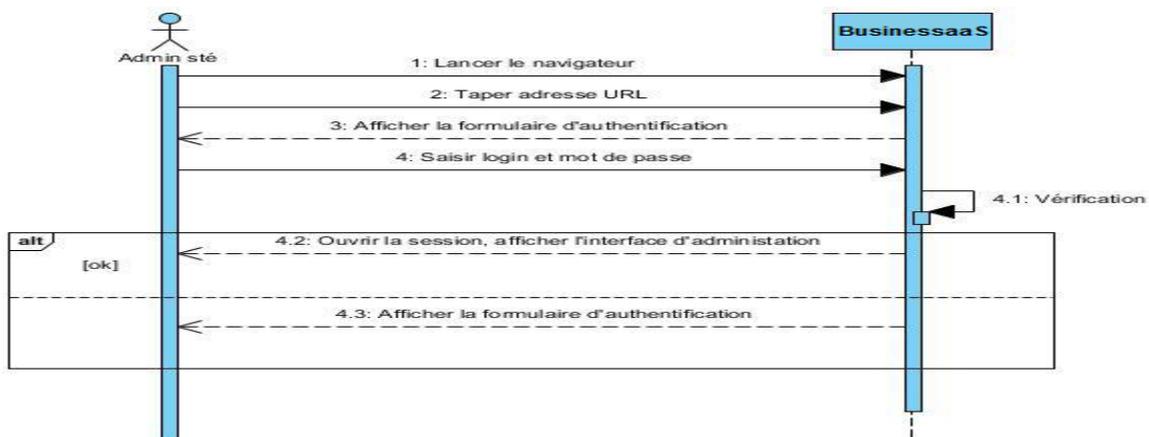
6.2 Phase d'analyse

La phase d'analyse sert à analyser l'environnement actuel du processus et à identifier les besoins. Il est aussi utilisé pour définir les exigences. Si des modifications ou corrections doivent y être apportées, alors le cycle recommence depuis la modélisation et ainsi de suite.

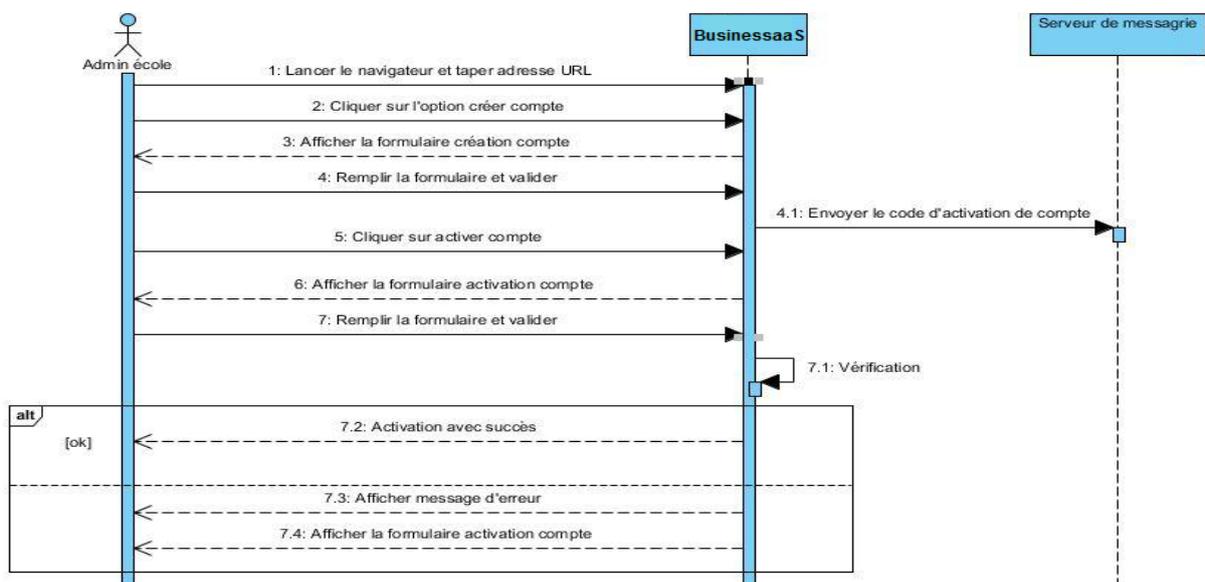
6.2.1 Diagramme de séquence

Les diagrammes de séquence : ils présentent la vue dynamique du système. L'objectif du diagramme de séquence est de représenter les interactions entre les objets en indiquant la chronologie des échanges. Cette représentation se réalise par cas d'utilisation.

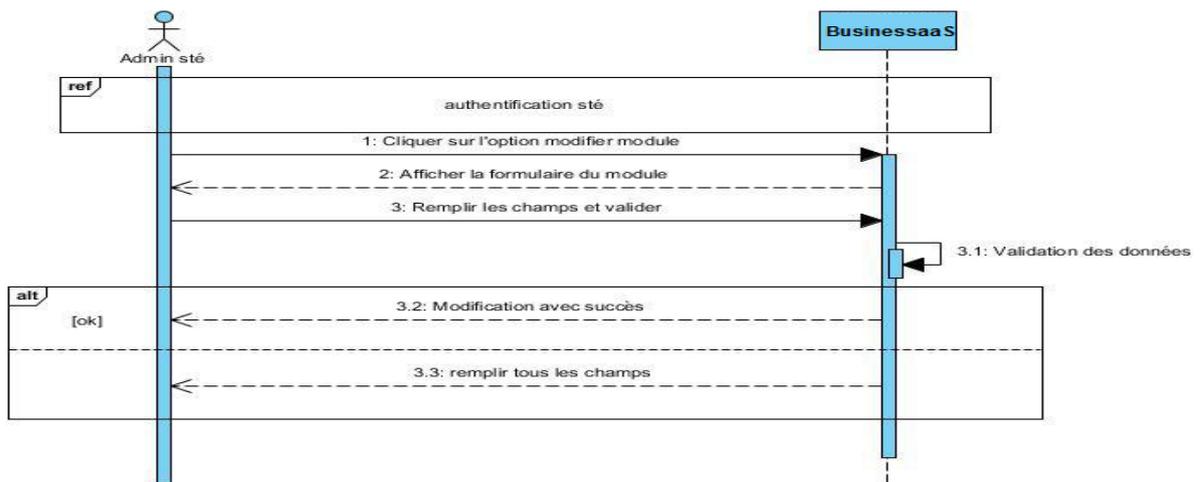
- **Diagramme de séquence d' « authentification » :**



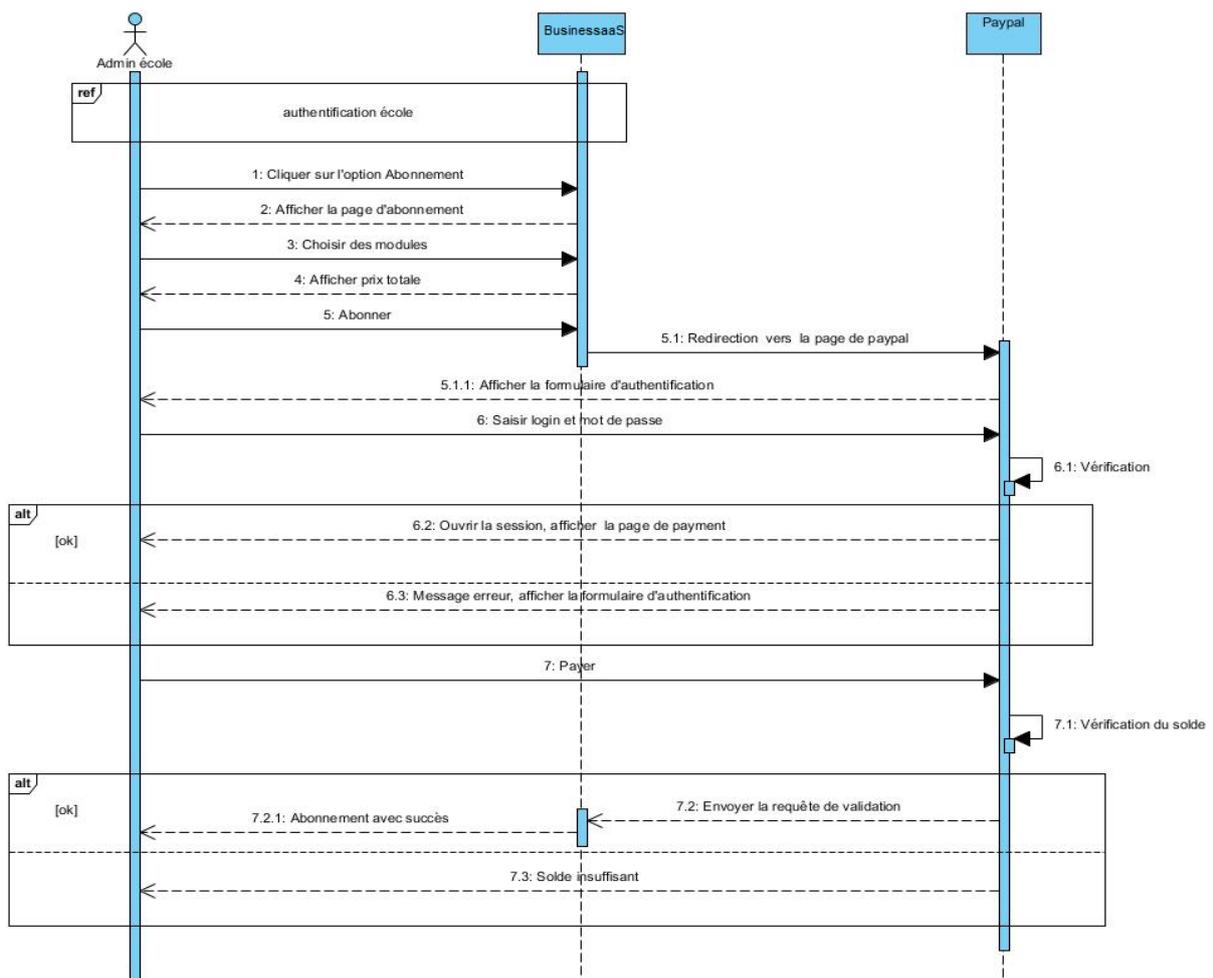
- **Diagramme de séquence « création compte de l'école » :**



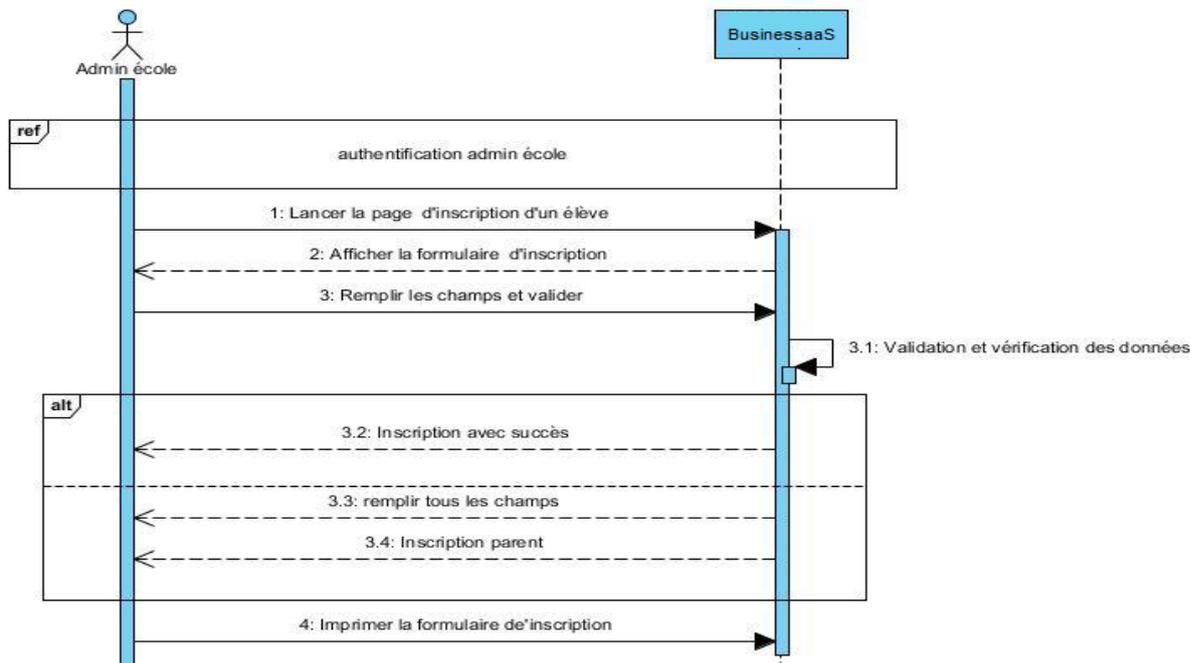
▪ Diagramme de séquence de « modification d'un module de BusinessaaS » :



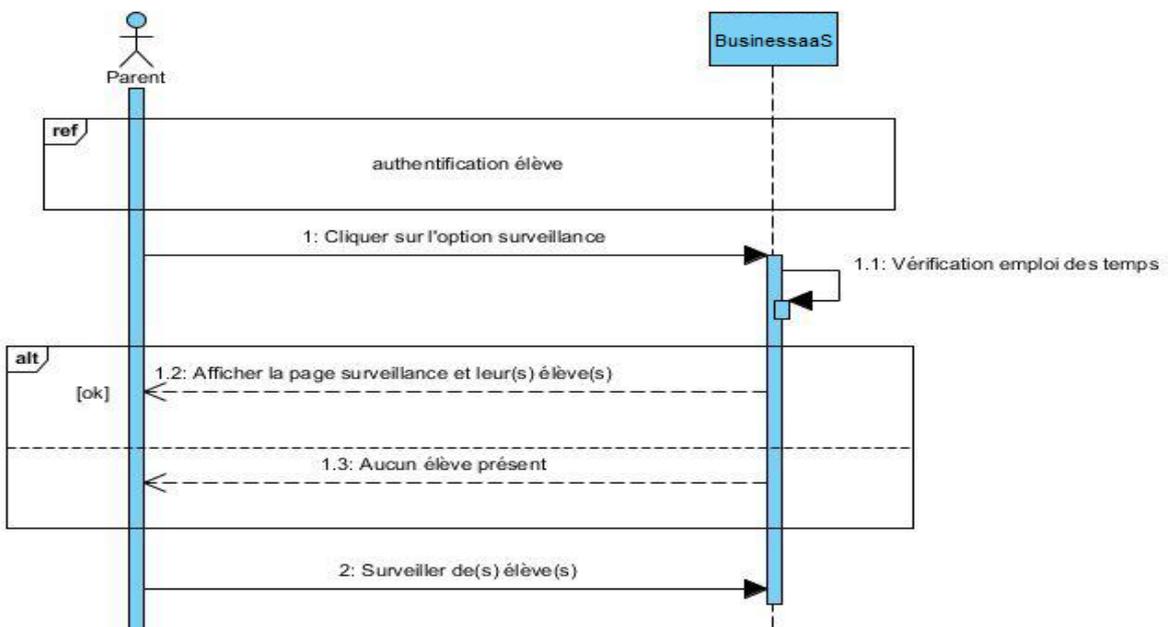
▪ Diagramme de séquence d'« abonnement » :



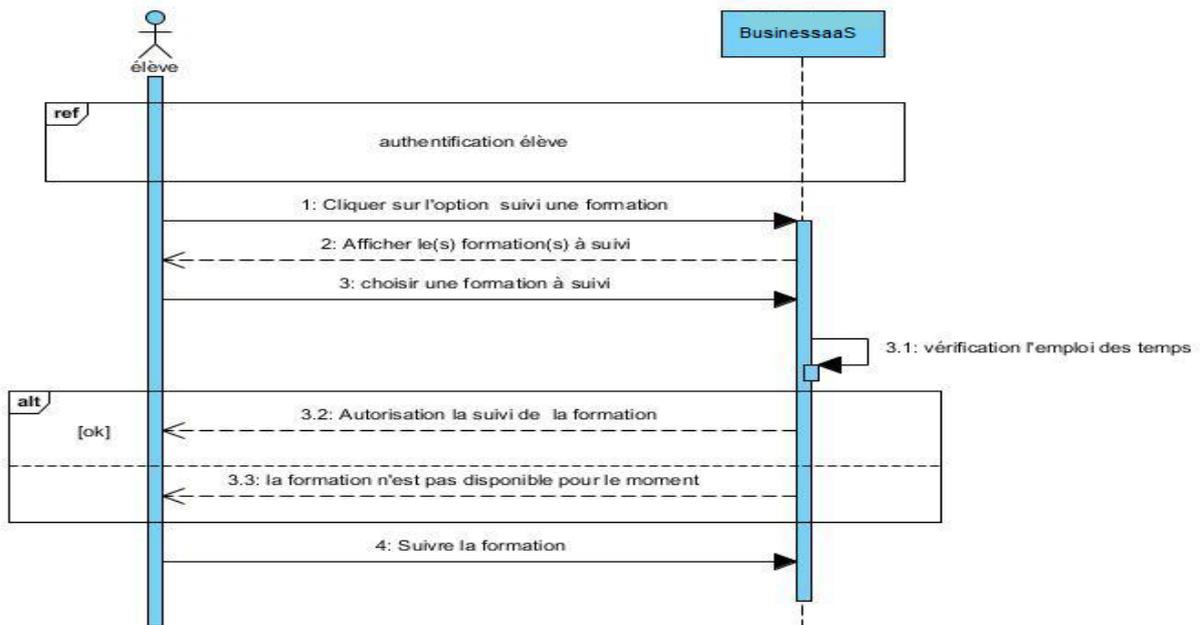
▪ Diagramme de séquence d' « inscription élève » :



▪ Diagramme de séquence de « surveillance » :



▪ Diagramme de séquence de « suivre une formation » :



6.2.2 Diagramme de classes d'analyse

Les diagrammes de classes jouent un rôle central dans l'analyse et le design orientés objet. Ils présentent un ensemble d'éléments de modèle statiques, leur contenu (structure interne) et leurs relations aux autres éléments. Les principaux éléments représentés dans un diagramme de classes sont les classes, les packages, les associations, les héritages et les dépendances.

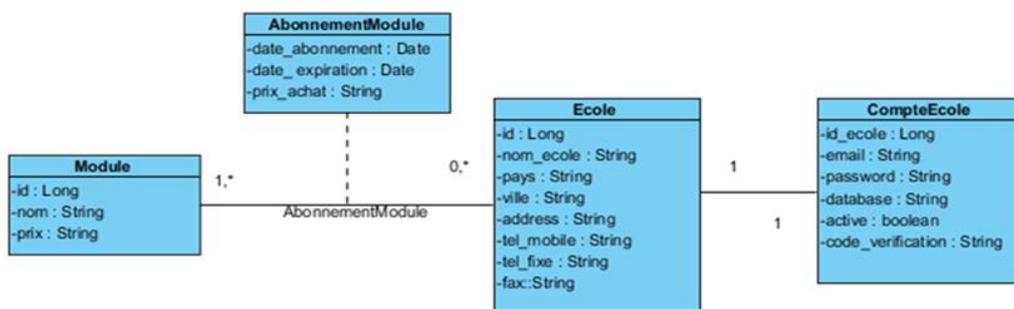


Figure 31 : Diagramme de classe d'analyse de BusinessaaS

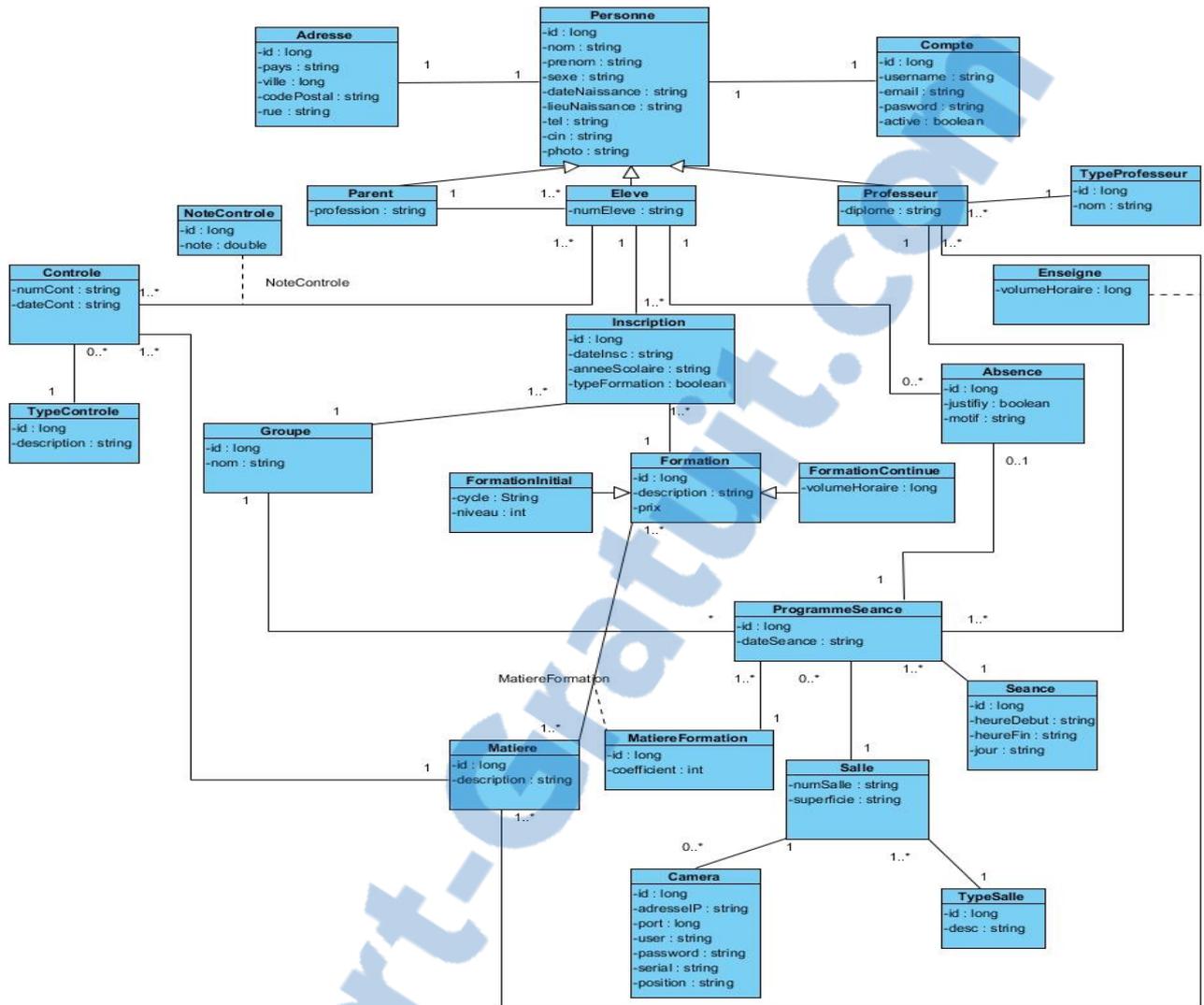
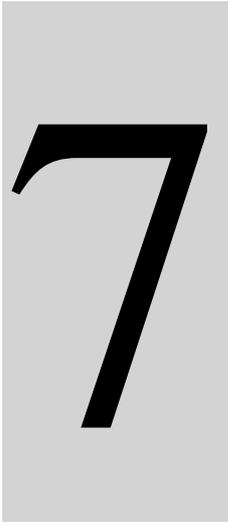


Figure 32 : Diagramme de classe d'analyse des écoles



Implémentation

Ce chapitre est consacré à la présentation de notre solution « Software as a service », qui comporte deux application web :

- **BusinessaaS** : qui présente nos services aux clients (écoles privé) et qui ouvre la possibilité de l'abonnement pour bénéficier de nos services.
- **Cloud Ecole** : application développée précisément dans les écoles privées afin de présenter à leurs clients, les services adoptés

Ainsi que le mécanisme de la sécurité utilisé afin d'assurer une bonne protection de données de nos clients.

7.1 Mécanismes de la sécurité

7.1.1 Java Simplified Encryption(Jasypt)

La librairie Jasypt (Java Simplified Encryption) permet de crypter/décrypter d'une manière très simple.

L'emploi de Jasypt permet au développeur d'accéder aux fonctionnalités de cryptage/décryptage avec un minimum d'efforts sans avoir une connaissance approfondie dans ce sujet. L'utilisation de Jasypt permet de bénéficier de :

- Haute-sécurité : des techniques de chiffrement standards, chiffrement unidirectionnel et bidirectionnel. Crypter les mots de passe, textes, chiffres, binaires ...
- Intégration transparente avec Hibernate.
- Intégration transparente avec Spring et Spring Security
- API Libre et ouverte pour l'usage avec n'importe quel fournisseur JCE

7.1.2 HyperText Transfer Protocol Secure(HTTPS)

Le protocole HTTPS permet l'échange de données entre client et serveur de manière sécurisée, en ayant recours au cryptage (technologie SSL/TLS). Il permet aussi au client d'authentifier le site serveur.

Le SSL (Secure Socket Layer) / TLS (Transport Layer Security) est le protocole de sécurité le plus répandu qui crée un canal sécurisé entre deux machines communiquant sur Internet ou un réseau interne.



Figure 33 : Transfert de données non sécurisé, pas de certificat SSL

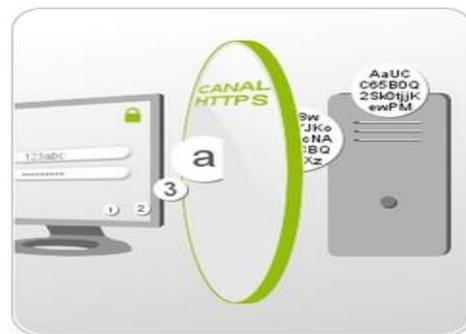


Figure 34 : Transfert de données sécurisé par certificat SSL :

Il fonctionne sur l'établissement de clés privées et publiques qui s'apparentent à l'utilisation d'une serrure et de sa clé :

- La clé privée est enregistrée sur le serveur.
- La clé publique, connue de tous, crypte les données à envoyer, qui, une fois réceptionnées par le serveur, sont décryptées au moyen de la clé privée.

7.2 Application web de BusinessaaS

7.2.1 Front office de BusinessaaS

- La page d'accueil de BusinessaaS :

Cet espace présente notre solution et ces différents modules (gestion, surveillance et formation à distance) et la société qui l'offre.



Figure 35 : Page d'accueil de BusinessaaS

▪ **La page services de BusinessaaS :**

Cette page présente les différents modules avec les services qu’offre chacun



BusinessaaS le secret du succès



la solution BusinessaaS est un modèle de déploiement dans lequel Cast-info loue en main à ses clients (les écoles privées) en tant que service à la demande au lieu de leur facturer la licence du logiciel. De cette façon, l'utilisateur final n'a plus besoin d'installer le logiciel. Elle permet de graduer le niveau d'externalisation, de l'hébergement du système d'information d'une école privée à l'externalisation complète ... BusinessaaS est composée actuellement de trois modules à savoir:

- MODULE DE GESTION
- MODULE DE SURVEILLANCE
- MODULE DE FORMATION À DISTANCE

Module de gestion

offre la gestion totale des écoles privées, tels que, la gestion des élèves, des enseignants, des formations, des emplois du temps, des notes des contrôles

Gestion des élèves

permet aux administrateurs des écoles privées d'inscrire des élèves dans les formations ...

Gestion des enseignants

permet aux administrateurs des écoles privées d'inscrire des enseignants ...

- MODULE DE GESTION
- MODULE DE SURVEILLANCE
- MODULE DE FORMATION À DISTANCE

Module de surveillance

permet aux parents des élèves de contrôler ses enfants au sein des écoles privées et aux administrateurs des écoles de contrôler les séances des cours. Pour bénéficier de ce module vous devez posséder des caméras ip et une adresse ip fixe.

surveillance parentale

Ce modèle permet aux parents des élèves de contrôler ses enfants au sein de l'école et aux administrateurs de contrôler les séances des cours.

Figure 36 : Page des modules de BusinessaaS

▪ **Le formulaire de création du compte d'école:**

Afin que les écoles bénéficient des modules de BusinessaaS, chacune doit avoir un compte. La figure ci-dessous présente le formulaire de création d'un compte pour une école donnée.

Figure 37 : Formulaire de création le compte d'école

Après la création du compte, l'utilisateur va recevoir à un E-mail, pour activer le compte créé.

Figure 38 : Page d'activation du compte

- **La page d'authentification des écoles :**

Afin de s'abonner aux services de BusinessaaS, les écoles doivent s'authentifier. La figure ci-dessous présente la page d'authentification.

Veuillez vous identifier pour continuer



Username:

Mot de passe: Mot de passe oublié?

Rester connecté Login

Créer une compte

Adresse

Country: Maroc
City: Nador
Telephone: +212 5635600
Email: Businnessaas@gmail.com

Businessaas



Figure 39 : Page d'authentification des écoles

- **La page de modifier la compte d'école**

Après la création du compte d'école et l'authentification, l'utilisateur de ce compte, peut afficher le profil de l'école, et peut même faire des modifications sur son compte, la figure ci-dessous présente la page d'un profil d'une école.



Figure 40 : Page de profil d'une école

▪ **La page d'abonnement**

Après l'authentification, l'école peut bénéficier des modules Businessaas. La figure ci-dessous illustre la page de choix de modules.



Bienvenue, cher Client

 CHOISISSEZ LE(S) MODULE(S) QUE VOUS VOULEZ ACHETER:

Adresse

Country: Maroc
 City: Nador
 Telephone: +212 5635600
 Email: Businessaas@gmail.com

GESTION

DATE DE DEBUT*: 2015-06-13

DATE FIN*: 2015-07-11

SURVEILLANCE

DATE DE DEBUT*: 2015-06-13

DATE FIN*: 2015-06-28

FORMATION À DISTANCE

DATE DE DEBUT*:

DATE FIN*:

Businessaas



Figure 41 : Page de choix des modules

Après le choix d'un ou plusieurs modules et la précision de la date de début et de la date de fin, nous cliquons ensuite sur « confirmer », la page suivante qui sera affichée, affichera le prix total à payer.



Figure 42 : Page de confirmation de l’abonnement

Après avoir appuyé sur le bouton « acheter », le client va être redirigé vers le site Paypal pour régler la somme due. La figure ci-dessous présente la page de paiement Paypal.

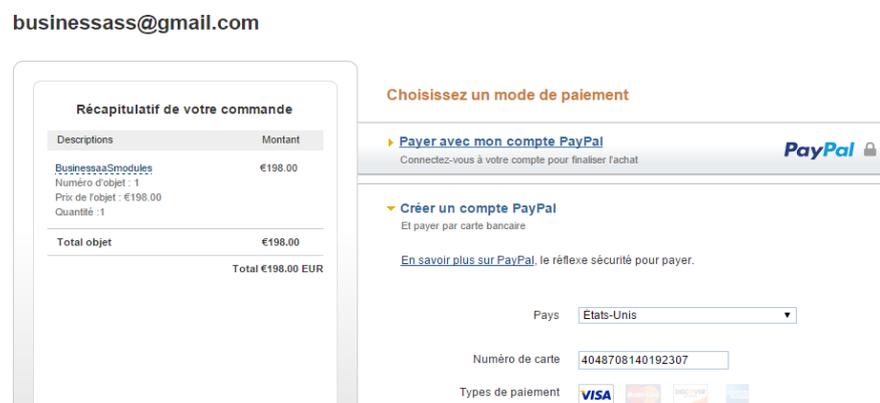


Figure 43 : Page de paiement PayPal

Le client va s’authentifier par son compte PayPal, pour régler les frais correspondant à sa demande.

L’application BusinessaaS va recevoir ensuite une requête de PayPal pour valider le choix de l’école. Si la requête retourne « SUCCESS », le paiement a été bien effectué. Dans le cas contraire elle retournera « CANCEL » si le paiement a été refusé.

7.2.2 Back office de BusinessaaS

▪ Espace de connexion d'administrateur BusinessaaS :

Pour gérer l'application BusinessaaS, l'administrateur doit s'authentifier. La figure ci-dessous présente la page d'authentification de l'administrateur.

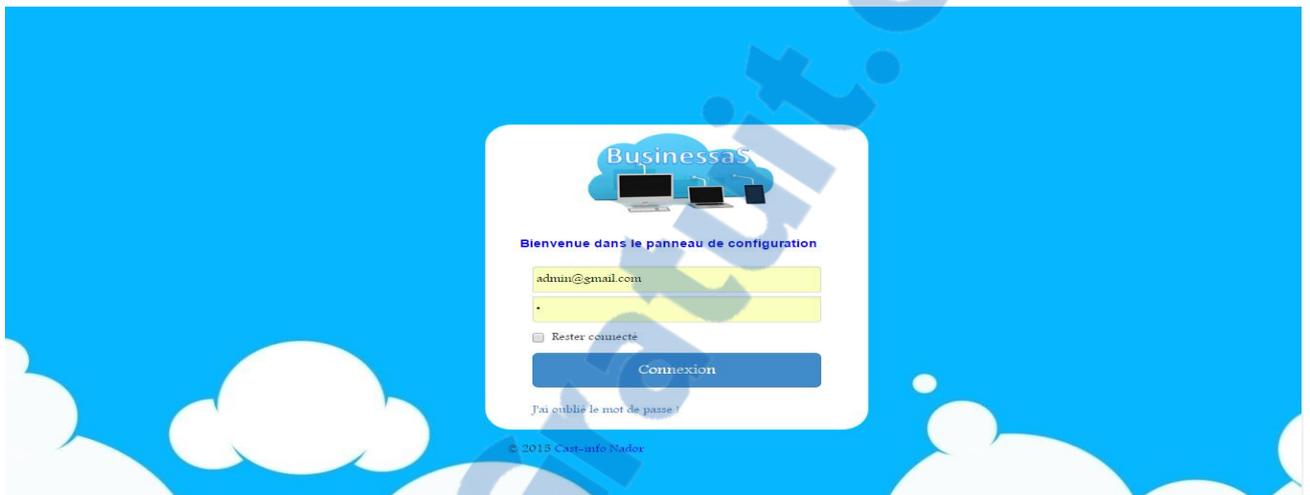


Figure 44 : Espace de connexion de l'administrateur de BusinessaaS

▪ Page d'accueil d'administrateur BusinessaaS :

Après que l'authentification ait été effectuée avec succès, la page d'accueil d'administrateur de BusinessaaS va afficher, comme indiqué dans la figure ci-dessous.



Figure 45 : Page d'accueil administrateur de BusinessaaS

▪ **Page de gestion de modules de BusinessaaS :**

L'administration de BusinessaaS permet aussi de modifier les prix des modules, comme illustré dans la figure ci-dessous.



Figure 46 : Page de gestions de modules de BusinessaaS

▪ **Page de gestion des clients de BusinessaaS :**

La figure ci-dessous, affiche la liste des écoles qui bénéficient des services de BusinessaaS et permet à l'administrateur de l'imprimer.



Figure 47 : Page de lister des clients de BusinessaaS

7.3 Application web des écoles privées (EcoleCloud)

Les clients de chaque école doivent sélectionner le nom de leur école. Comme indiqué dans la figure ci-dessous.

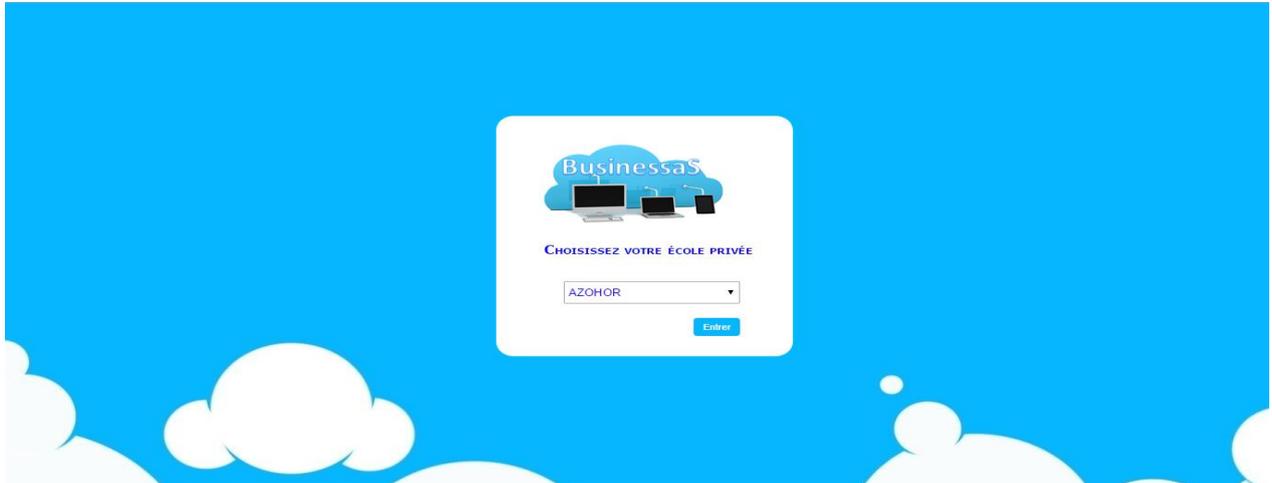


Figure 48 : La page de choix le nom d'école

Dans cette partie, nous allons présenter un exemple d'une école donnée qui bénéficie de tous les modules (module de gestion, de surveillance et de formation à distance) de BusinessaaS.

7.3.1 Front office de l'application EcoleCloud

Les utilisateurs de l'application EcoleCloud doivent s'authentifier afin de bénéficier de services proposés pour chaque type d'utilisateurs (élève, enseignant, parent). Sauf la page d'accueil sera affichée sans authentification

La figure ci-dessous présente la page d'authentification pour utilisateur élève par exemple.



Ecole ANAJAH : le secret du succès

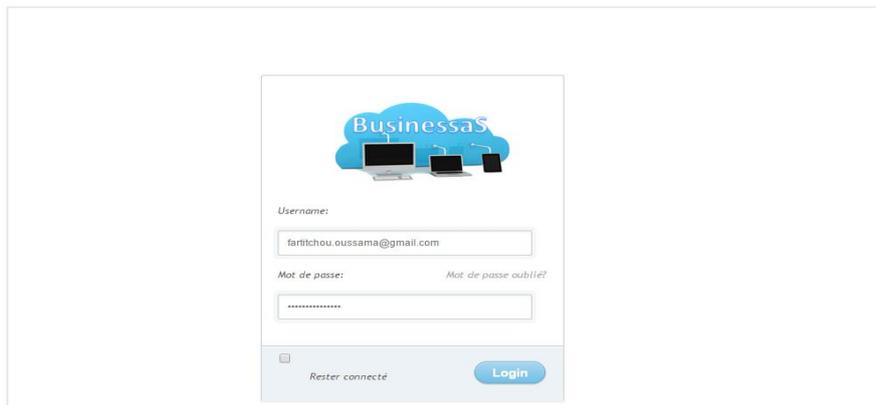


Figure 49 : Page d’authentification des utilisateurs de l’application des écoles

▪ La page d’accueil d’EcoleCloud :

La page d’accueil contient des informations sur l’école privée donnée. Comme indiqué dans la figure ci-dessous.



Ecole ANAJAH : le secret du succès



Ecole ANAJAH

L'école ANAJAH à été créée en 2002, agréé par le ministère de l'Education nationale sous le n ° 00256/02. Rue hassan 2 numero 121 nador. Tel : 05 89 62 35 37

Ecole ANAJAH : le secret du succès



Accompagner nos étudiants pour qu'ils gagnent en autonomie, en ouverture d'esprit, en adaptabilité... Autant de qualités indispensables aux managers commerciaux de demain. Notre ambition est de former des cadres, opérationnels, agiles, capables d'endosser très rapidement la responsabilité du développement commercial des futures organisations qui vont les accueillir. Pour cela, nous avons opté pour une stratégie pédagogique où l'étudiant doit rapidement se confronter à la réalité concrète de l'entreprise et devenir acteur de sa formation.

Figure 50 : La page d’accueil de l’application EcoleCloud

Module de gestion

Le module de gestion est composé de l'espace des élèves et de l'espace des enseignants

- **Espace des élèves :**

Les élèves de l'école après leur authentification peuvent consulter des actualités de l'école, d'afficher et télécharger leur emploi des temps, leurs cours en ligne et leur relevé des notes. La figure ci-dessous présente espace élèves.



Ecole ANAJAH : le secret du succès

Jour/Heure	Lundi	Mardi	Mercredi	Jeudi	Vendredi	Samedi
8:0->10:0	M:informatique Prof:zarwali.ah salle:1
8:00->10:00	M:Math Prof:zarwali.ah salle:1
10:15->12:0	M:physique Prof:Makhoufi.Im salle:1

Figure 51: L'espace élève de l'application des écoles

- **Espace enseignant :**

Les enseignant peuvent consulter des actualités de l'école, d'afficher et télécharger leur emploi des temps, uploader des cours etc. La figure ci-dessous présente l'espace d'enseignant.



Ecole ANAJAH : le secret du succès

Actualité | **Emploi des temps** | Upload cours | Message | Note Examen

Jour/Heure	Lundi	Mardi	Mercredi	Jeudi	Vendredi	Samedi
8:00->10:00	N:premiereG:A M:Mathsalle:1
8:0->10:0	N:premiereG:A M:informatiquesalle:1

Figure 52 : L'espace enseignant de l'application des écoles

Module de surveillance

Après que le parent d'un ou des élèves s'authentifie, il peut consulter des notifications sur la présence de leur enfants dans les séances de cours et aussi peut surveiller ses enfants via des caméras dans la salle de cours au sein de l'école. Comme indiquer dans la figure suivante.



Bienvenue Mr. Noor Chawki

Ecole ANAJAH : le secret du succès



Figure 53 : La page de surveillance de l'application des écoles

7.3.2 Back office de l'application EcoleCloud

- **Espace de connexion d'administrateur BusinessaaS :**

Pour gérer l'application des écoles, l'administrateur d'une école donnée doit s'authentifier. La figure ci-dessous présente la page d'authentification de l'administrateur

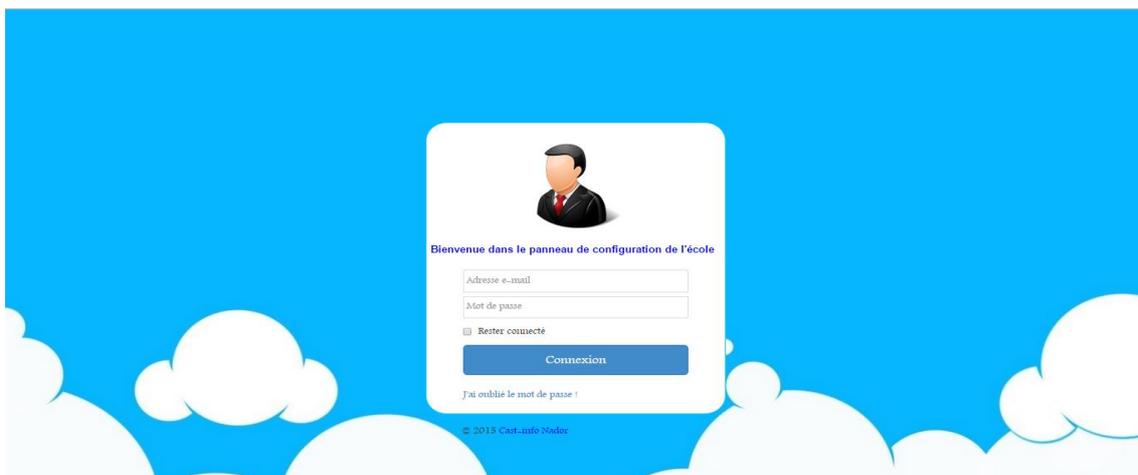


Figure 54 : Espace de connexion de l'administrateur de CloudEcole

- **Page de gestion d'accueil:**

Après que l'authentification ait été effectuée avec succès, la page de gestion d'accueil d'administrateur va afficher, elle permet à l'administrateur de gérer la page d'accueil de front office de l'école, comme indiqué dans la figure ci-dessous.



Panneaux D'administration d'ecole ANAJAH

Ajout profil | Modifie profil

Image : Aucun fichier choisi

Description :

Figure 55 : Page de gestion de la page d'accueil de l'application des écoles

- **La page de gestion du module de Gestion d'école**

L'espace de gestion du module de gestion est composé de l'espace de gestion des élèves et de l'espace de gestion des enseignants.

- **Espace de gestion des élèves :**

L'espace de gestion des élèves permet à l'administrateur d'inscrire des élèves, d'ajouter des formations, d'ajouter l'emploi des temps, de gérer les absences des élèves etc. comme indiqué ci-dessous.

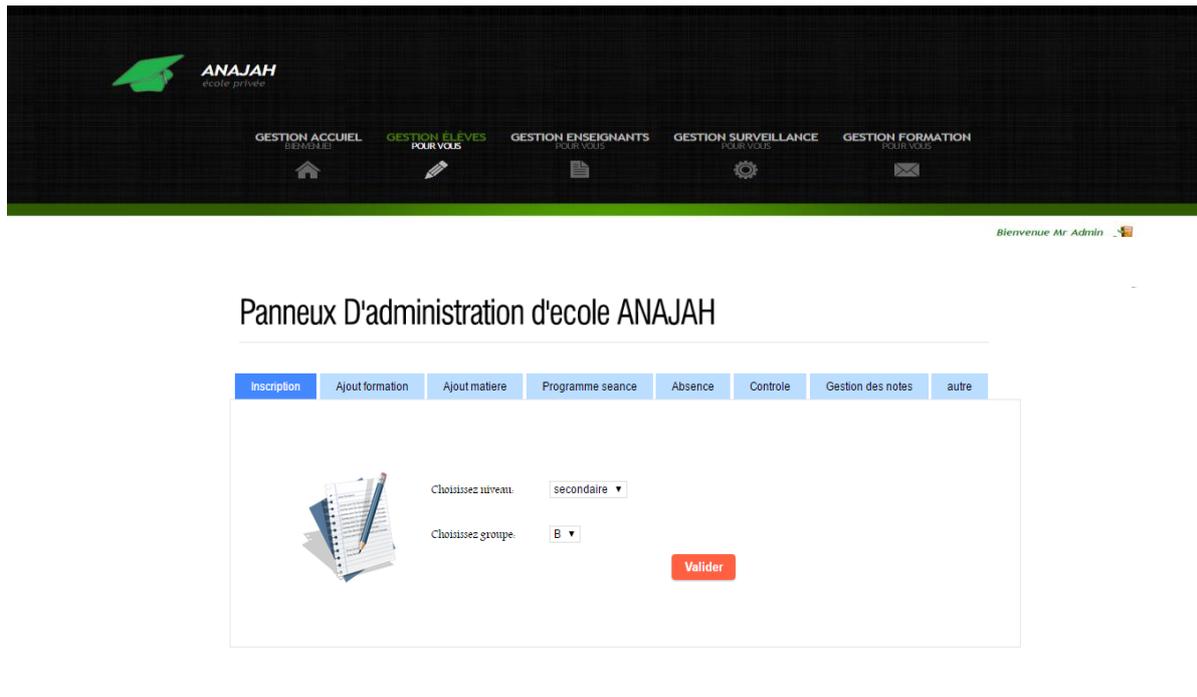


Figure 56 : Page de gestion du module de gestion de l’application EcoleCloud

▪ **Espace de gestion des enseignants :**

Les enseignant peuvent consulter des actualités de l’école, d’afficher et télécharger leur emploi des temps, uploader des cours etc. La figure ci-dessous présente l’espace d’enseignant.

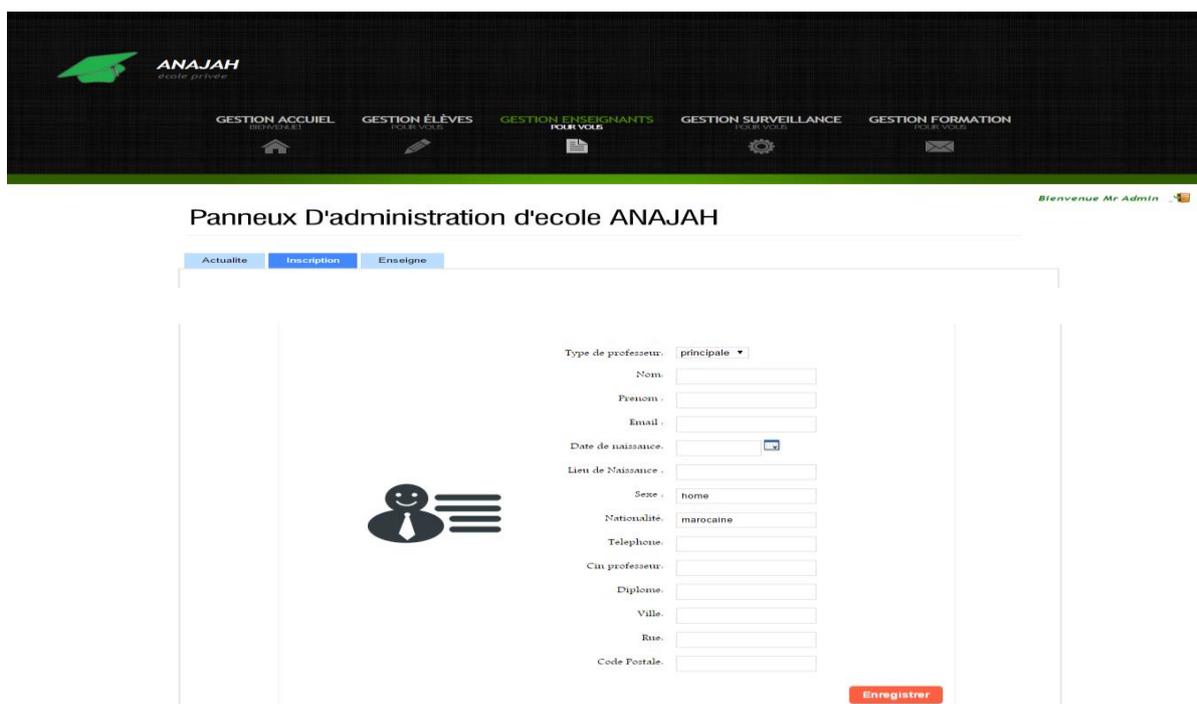


Figure 57 : Espace de gestion des enseignants d’application des écoles

Gestion de module de surveillance

Cette page permet à l'administrateur de gérer des camera IP des salles, comme indiqué dans la figure ci-dessous



Panneaux D'administration d'ecole ANAJAH

configuration camIP



Numero de Salle:

Adresse:

Port:

User:

Password:

Serial:

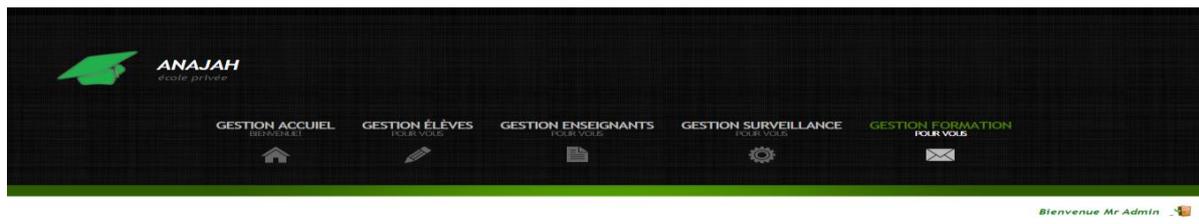
Position:

Ajouter

Figure 58 : Page de configuration des caméras IP des salles

Gestion de module de formation à distance

Cet espace permet à l'administrateur de gérer des formations à distance, comme illustré dans la figure suivante.



Panneaux D'administration d'ecole ANAJAH

Inscription Programme seance **Ajout formation** Emploi formation à distance Statistique formation Publication formation



Description:

Prix:

Ajouter

Figure 59 : Page de gestion du module de formation à distance d'EcoleCloud

Conclusion et perspectives

Pendant le déroulement de mon stage, j'ai eu l'occasion d'acquérir un maximum de connaissances sur le cloud computing, et de travailler avec les frameworks Struts2 et Hibernate, d'administrer des systèmes et réseaux, ce qui s'est avéré très enrichissant pour mon expérience professionnelle.

Le fait de travailler avec des responsables d'équipe expérimentés, nous a permis d'avoir une vision détaillée de la gestion, de la conception et plus généralement de la supervision des systèmes et l'élaboration des solutions.

Ce stage très diversifié du point de vue gestionnaire, technique et des traitements statistiques, nous a permis de découvrir des branches de métiers nouveaux dans lesquelles il nous sera possible d'évoluer.

Le problème que nous avons rencontré, est le manque des serveurs dédiés au cloud dans l'entreprise d'accueil, pour construire l'infrastructure demandée.

Nos perspectives principales et les plus importantes de notre projet sont de:

- Utiliser l'API de PayPal, au lieu de rediriger nos clients vers le site de PayPal pour payer les frais de leurs demandes
- Améliorer les applications : utiliser le format JSON pour charger le contenu de la page JSP, au lieu de charger toute la page
- Terminer le développement du module de formation à distance, d'ajouter un serveur de streaming pour permettre aux écoles de sauvegarder les séances des formations et d'ajouter un serveur chat pour permettre aux élèves des écoles d'interroger leurs formateurs pendant la séance de formation
- Intégrer le module de formation à distance aux réseaux sociaux, afin de permettre aux administrateurs des écoles de promouvoir leurs formations et d'avoir des statistiques sur la réussite de ces formations
- Améliorer le niveau de la sécurité de nos services

Annexe 1. Serveur Cloud

1. Installation et configuration Openstack Juno sous ubuntu 14.04 ^{[12] [13] [14]}

▪ Installation Openstack Juno

Il y a plusieurs méthodes d'installation OpenStack : soit via devstack (distribution All-In-One) ou depuis les packages. Lors de notre déploiement, nous avons choisi la première méthode.

- Télécharger Devstack: Nous allons récupérer la dernière version de Devstack via <https://github.com/openstack-dev/devstack.git>

```
git clone -b stable/juno https://github.com/openstack-dev/devstack.git
```

- Télécharger le fichier '**local.conf**' de configuration des services OpenStack :

```
cd devstack
wget https://github.com/smakam/openstack/raw/master/juno/local.conf.control
mv local.conf.control local.conf
```

- Exécuter DevStack

```
./stack.sh
```

- Redémarrer Openstack

```
./rejoin-stack.sh
```

- si l'installation est réussie, vous verrez le message suivant:

```
Horizon is now available at http://192.168.93.69/
Keystone is serving at http://192.168.93.69:5000/v2.0/
Examples on using novaclient command line is in exercise.sh
The default users are: admin and demo
The password: mohamed
This is your host ip: 192.168.93.69
2015-04-20 20:22:03.391 | stack.sh completed in 883 seconds.
fartitchou@mohamed:~/devstack$ _
```

2. Configuration Openstack Juno

Si tout s'est passé correctement, vous pouvez accéder au tableau de bord (Horizon) à partir d'autre ordinateur sur le réseau local en accédant à `http://server-ip-address` de votre navigateur et vous identifier par le login (admin ou demo) et le mot de passe que vous avez choisi lors de l'étape précédente.

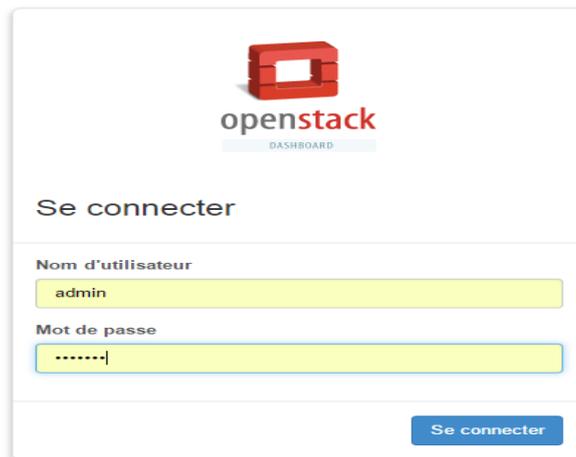


Figure 60 : Interface web d'authentification Openstack Juno

Maintenant, vous allez être redirigé vers la page du tableau de bord d'Openstack :

Usage

Nom de Projet	VCPUs	Disque	RAM	VCPU Heures	Go Heures Disque
admin	2	0	2Go	20,68	0,00

Affichage de 1 élément

Figure 61 : Tableau de bord d'Openstack Juno

- **Créer des réseaux:**

Une fois connecté au tableau de bord OpenStack, cliquez sur l'onglet "Admin" dans le menu de navigation de gauche, puis cliquez sur «Réseaux» sous la rubrique «Gestion Système» puis supprimez les réseaux par défaut et ajouter des réseaux selon vos besoins.

Sous la rubrique «Réseaux », cliquez sur le bouton "Créer un réseau", comme indiqué ci-dessous :

Réseaux

Réseaux								+ Créer un Réseau	Supprimer Réseaux
<input type="checkbox"/>	Projet	Nom du Réseau	Sous-Réseaux associés	Partagé	Statut	Admin State	Actions		
<input type="checkbox"/>	admin	private	private_subnet 10.0.0.0/8	non	ACTIVE	UP	Mettre à jour un Réseau Plus ▾		
<input type="checkbox"/>	admin	public	public_subnet 192.168.3.0/24	non	ACTIVE	UP	Mettre à jour un Réseau Plus ▾		

Affichage de 2 éléments

Figure 62 : Création des réseaux sous openstack

- **Créer des routeurs :**

Après la création de deux réseaux (public et private) maintenant, nous allons les relier par un routeur. Cliquez sur l'onglet "Projet" dans le menu de navigation de gauche, puis cliquez sur «Routeurs» sous la rubrique «Réseau». Enfin, cliquez sur le bouton "Créer un Routeur".

Routeurs

Routeurs					+ Créer un Routeur	Supprimer Routeurs
<input type="checkbox"/>	Nom	Statut	Réseau externe	Actions		
<input type="checkbox"/>	router1	Active	public	Effacer Passerelle Plus ▾		

Affichage de 1 élément

Figure 63 : Création des routeurs sous openstack

Après la création du routeur ajoutez les interfaces publique et privé comme indiqué ci-dessous :

Interfaces							+ Ajouter une Interface	Supprimer Interfaces
<input type="checkbox"/>	Nom	IP fixes	Statut	Type	Admin State	Actions		
<input type="checkbox"/>	(d886032b)	192.168.3.200	ACTIVE	Passerelle externe	UP			
<input type="checkbox"/>	(f1318790)	10.0.0.1	ACTIVE	Interface interne	UP	Supprimer Interface		

Affichage de 2 éléments

Figure 64 : Ajout des interfaces réseaux à un routeur sous openstack

- **Exécuter des instances :**

Etape1 : Gérer les règles de sécurité

Cliquez sur l'onglet "Projet" dans le menu de navigation de gauche, puis cliquez sur «Accès et Sécurité» sous la rubrique «Compute». Sous la rubrique «Groupes de sécurité», cliquez sur le bouton

"Modifier les règles" pour le groupe de sécurité "par défaut". Cliquez sur le bouton "Ajouter une règle", et dans la boîte de dialogue qui apparaît, ajouter les règles selon vos besoins.

Accès et Sécurité



Figure 65 : Gestion des règles de la sécurité sous openstack

Etape2 : Créer ou importer une paire de clés.

Dans le menu de navigation de gauche, cliquez sur «Accès et Sécurité» sous la rubrique «Compute». Dans la partie principale de l'écran, cliquez sur l'onglet "paires de clés," et choisissez "Créer paire de clés" ou "Importer paire de clés."



Figure 66 : Gestion les paires de clés sous openstack

Etape 3 : Ajouter les types les instances

Cliquez sur l'onglet "Admin" dans le menu de navigation de gauche, puis cliquez sur «Types d'instance» sous la rubrique «Gestion système».

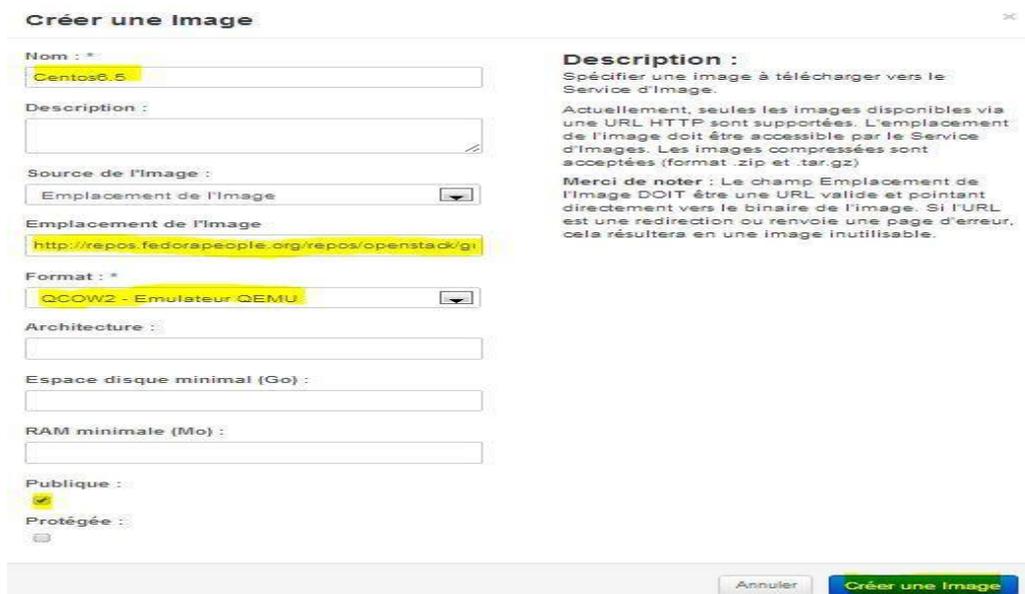
Sous la rubrique «Types d'instance », cliquez sur le bouton "Créer un type d'instance" et ajouter les types des instances selon vos besoins.

<input type="checkbox"/>	Nom du Type d'Instance	VCPUs	RAM	Disque racine	Disque éphémère	Disque de Swap	ID	Publique	Actions
<input type="checkbox"/>	m1.heat	1	1024Mo	10Go	0Go	2048Mo	15d168d8-5e95-47f0-a15d-423b8ac7cd96	Oui	Editer le type d'instance Plus ▾
<input type="checkbox"/>	m1.small	1	2048Mo	20Go	0Go	4096Mo	27434351-23d4-4d09-98fa-1108432dc76e	Oui	Editer le type d'instance Plus ▾

Figure 67 : Gestion les types d'instance sous openstack

Etape4 : Ajouter une image.

Dans le menu de navigation de gauche, cliquez sur "Images" sous la rubrique "Gérer Compute." Cliquez sur le bouton "Créer une image", situé dans la partie supérieure droite de l'écran. Dans la boîte de dialogue qui apparaît, saisissez "Centos6.5" dans le champ "Nom", "http://repos.fedorapeople.org/repos/openstack/guest-images/centos-6.5-20140117.0.x86_64.qcow2" dans le champ "Emplacement de l'image", dans le menu déroulant "Format" choisissez "qcow2", laissez le "disque Minimum" et les champs "Ram minimum" vierge, cochez la case "Public", et cliquez sur le bouton "Créer une image", comme indiqué ci-dessous



Créer une Image

Nom : *
Centos6.5

Description :

Source de l'image :
Emplacement de l'Image

Emplacement de l'image :
http://repos.fedorapeople.org/repos/openstack/gi

Format : *
QCOW2 - Emulateur QEMU

Architecture :

Espace disque minimal (Go) :

RAM minimale (Mo) :

Publique :
Protégée :

Description :
Spécifier une image à télécharger vers le Service d'Image.
Actuellement, seules les images disponibles via une URL HTTP sont supportées. L'emplacement de l'image doit être accessible par le Service d'Images. Les images compressées sont acceptées (format .zip et .tar.gz)
Merci de noter : Le champ Emplacement de l'Image DOIT être une URL valide et pointant directement vers le binaire de l'image. Si l'URL est une redirection ou renvoie une page d'erreur, cela résultera en une image inutilisable.

Annuler Créer une Image

Figure 68 : Création des images sous openstack

Etape5 : Lancez l'instance.

Dans la partie principale de l'écran, sous la rubrique «Images» rubrique, cliquez sur le bouton "Lancer" pour l'image "Centos6.5". Dans la boîte de dialogue résultante, fournir un nom dans le champ "Nom de l'instance", sélectionner un type d'instance, le pair de clé, le réseau de l'instance et cliquez sur le bouton "Lancer".

Lancer une Instance

Détails * **Accès et Sécurité *** Réseaux * Post-Création Options avancées

Zone de Disponibilité : nova

Nom de l'Instance : * SerWeb

Type d'instance : * m1.heat

Nombre d'Instances : * 1

Source de l'instance de démarrage. * Démarrage depuis une image

Nom de l'image : CentOS-6.5 (324,0 Mo)

Spécifier les détails de démarrage d'une instance.
Le tableau ci-dessous montre les ressources liées aux quotas et utilisées par ce projet.

Détails du Type d'Instance

Nom	m1.heat
VCPUs	1
Disque racine	10 Go
Disque éphémère	0 Go
Disque Total	10 Go
RAM	1,024 Mo

Limites du Projet

Nombre d'Instances 2 sur 10 utilisés

Nombre de VCPUs 2 sur 20 utilisés

RAM Totale 2 048 sur 51 200 Mo utilisés

Annuler Lancer

Figure 69 : Lancement une instance sous openstack

- **La topologie du réseau :**

Après la création des réseaux, routeur et exécution des instances. La figure ci-dessous présente la topologie du réseau de notre serveur cloud.

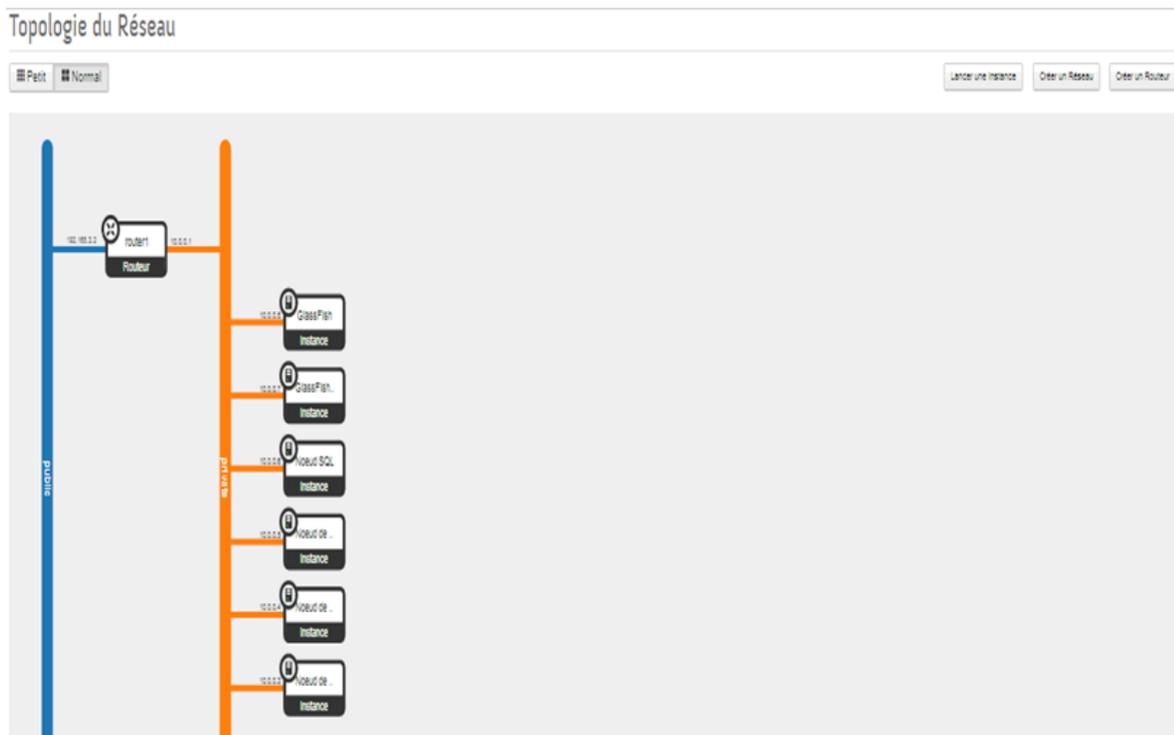


Figure 70 : Topologie réseau de serveur cloud

Annexe 2. Serveur GlassFish

Installation et configuration du serveur GlassFish 4.0 sur CentOS 6.5 : ^[9]

Pour installer et configurer le serveur GlassFish, nous allons suivre les étapes suivantes :

Etape 1: Installer JDK

- Téléchargez les paquetages d'une version stable JDK, à partir de : www.oracle.com
- Installez paquetage JDK:

```
# rpm -Uvh jdk-7u65-linux-i586.rpm
```

Etape 2 : Installer GlassFish

- Téléchargez le fichier d'installation de GlassFish:

```
#cd /opt  
  
#wget http://dlc.sun.com.edgesuite.net/glassfish/4.0/release/glassfish-4.0.zip
```

- Décompressez le fichier zip téléchargé:

```
#unzip glassfish-4.0.zip
```

Etape 3 : Démarrer le Serveur GlassFish

```
#unzip glassfish-4.0.zip #glassfish4/bin/asadmin start-domain
```

Etape 4 : Changez le mot de passe du compte d'administrateur.

```
cd /opt/glassfish4/glassfish/bin  
./asadmin --host 192.168.3.99 --port 4848 change-admin-password
```

Etape 5 : Activez le mode SSL pour sécuriser la connexion entre les instances du cluster et le DAS (Domain Application Server):

```
cd /opt/glassfish4/glassfish/bin  
./asadmin --host 192.168.3.99 --port 4848 enable-secure-admin
```

Etape 6 : Accès à la console d'administration GlassFish

Ouvrez votre navigateur web et accédez à <http://server-ip-address:4848>



Figure 71 : La page d'authentification de GlassFish

Après que l'authentification ait été effectuée avec succès, l'interface d'administration de GlassFish s'ouvre, comme indiqué ci-dessous.

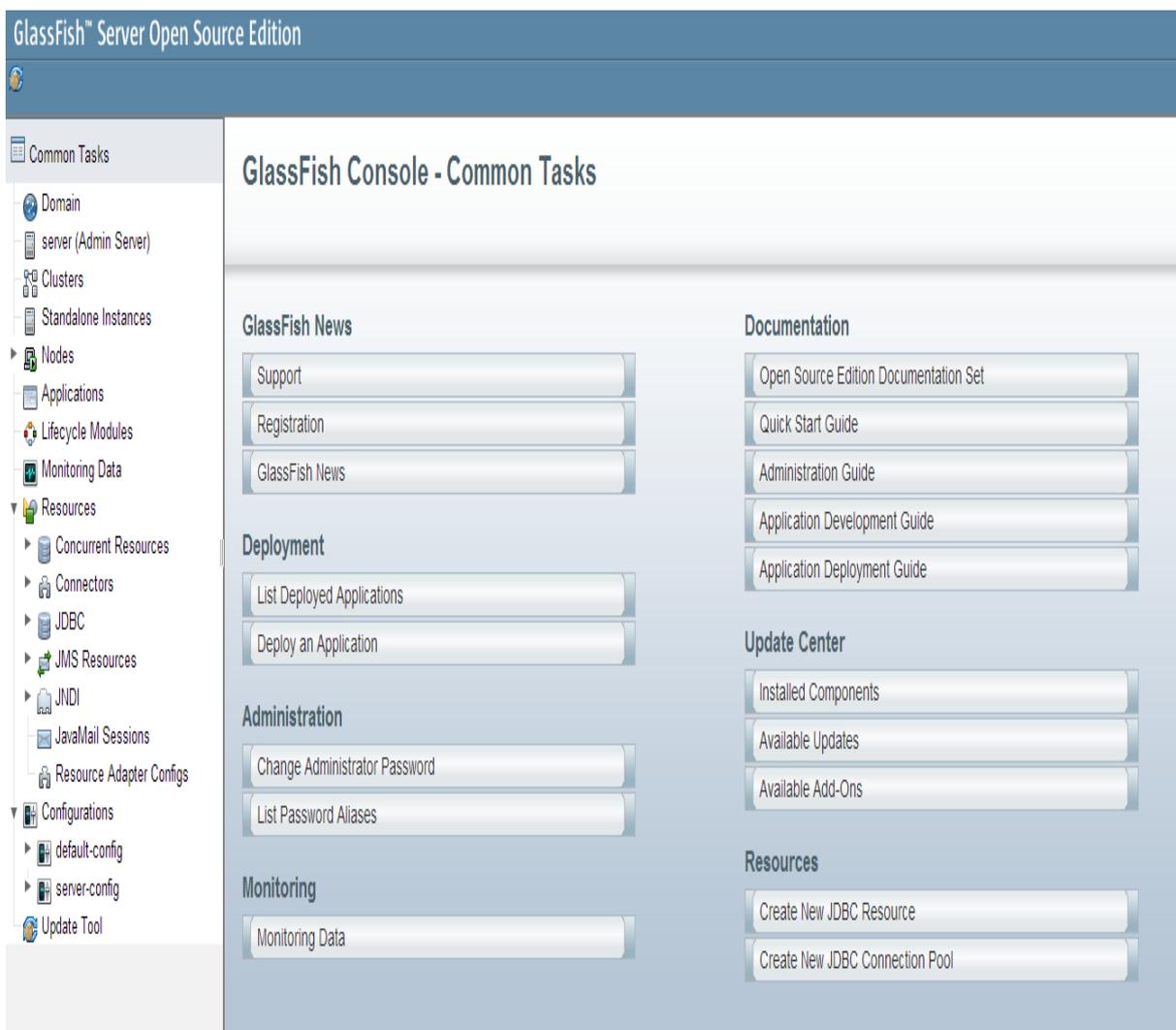


Figure 72 : L'interface d'administration de serveur GlassFish

Annexe 3. Cluster de Serveur GlassFish

Installation et configuration du Cluster de serveur GlassFish 4.0 sur CentOS 6.5: ^[15]

Après installation et configuration du serveur d'application GlassFish 4.0, maintenant, nous allons suivre les étapes suivantes pour installer et configurer le cluster de serveur GlassFish 4.0.

Etape 1 : Installation et configuration du cluster de serveur GlassFish

Nous allons suivre les mêmes étapes d'installation et de configuration du serveur GlassFish 4.0 que celles décrites précédemment « voir l'annexe 2 ».

Etape 2 : Création d'un nœud distant

Pour créer un nouveau nœud de cluster distant, nous pouvons soit utiliser l'outil **asadmin** dans un terminal ou il peut simplement être obtenu dans l'interface Web de la console d'administration. Pour ce faire nous allons utiliser la deuxième méthode. Dans l'arborescence des tâches courantes sur le côté gauche de la console, cliquez sur « Nodes », puis cliquez sur « New ». La forme de la figure ci-dessous doit être affichée.

The screenshot shows the 'New Node' configuration window. On the left is a tree view with 'Nodes' selected. The main area contains the following fields and options:

- Name:** A text input field with a red asterisk. Below it, a note states: 'Unique name for the node. The name must not contain any reserved words or characters.'
- Type:** A dropdown menu currently set to 'SSH'. A note below explains: 'If the type is CONFIG, the node is not enabled for remote communication and the DCOM or SSH information is removed from the page. To create instances on a remote node of type CONFIG, you must use the create-local-instance subcommand. You cannot use the Administration Console for this purpose.'
- Node Host:** A text input field. A note below states: 'Name of the host that the node represents. If the type is DCOM or SSH, the node host is required.'
- Node Directory:** A text input field. A note below states: 'Path to the directory that will contain files for instances created on this node. The default is "\${com.sun.aas.productRoot}/glassfish/nodes'.'
- Installation Directory:** A text input field containing the value '\$(com.sun.aas.productRoot)'. A note below states: 'The full path to the parent of the base installation directory of the GlassFish Server software on the host, for example, /export/glassfish4.'
- Install GlassFish Server:** A checkbox labeled 'Enabled'. A note below states: 'If selected, the GlassFish Server software on the DAS host is copied to the node host when the node is created.'
- SSH:** A section header.
- Force:** A radio button labeled 'Enabled'. A note below states: 'Specifies whether the node is created even if validation of the node's parameters fails.'
- SSH Port:** A text input field containing the value '22'. A note below states: 'The port to use for SSH connections to this node's host. The default is 22.'
- SSH User Name:** A text input field containing the value '\$(user.name)'. A note below states: 'The user that is to run the process for connecting to this node's host through SSH. The default is the user that is running the DAS process.'
- SSH User Authentication:** A dropdown menu set to 'Password'. A note below states: 'Select how the SSH user is authenticated when logging in to this node's host.'
- SSH User Password:** A text input field. A note below states: 'Type the password that the SSH user will use for logging in to the host that this node represents.'

Figure 73 : Création d'un nouveau nœud de cluster en utilisant la console d'administration

Nous devons remplir les champs du formulaire avec les valeurs qui ont été utilisés avant de créer le nœud distant:

- Name: glassfishCluster;
- Node Host: 192.168.3.100;
- SSH User Name: root
- SSH User Authentication: password;
- SSH Password: *****;

Etape 3 : Création d'un cluster et ses instances en utilisant la console d'administration

Après la création d'un nœud distant, sélectionnez « Clusters » dans l'arbre des tâches et cliquez sur le bouton « New ». Dans le formulaire qui sera affiché, tapez le nom du Cluster et, ci-dessous les instances étiquettes de serveurs à créer, cliquez sur le bouton « New » pour créer deux instances de chaque serveur GlassFish. Ensuite, remplissez les informations de chaque instance. Le formulaire rempli est présenté dans la figure ci-dessous.

New Cluster OK Cancel

To create a cluster that does not share its configuration, select the default-config configuration and the Make a Copy of the Selected Configuration option. To create a cluster that shares its configuration, select another configuration and the Reference the Selected Configuration option. If no nodes exist, create a node before adding instances to a cluster. To create a node, use the Nodes page.

Cluster Name:

Configuration:

The default-config configuration can only be copied, not referenced.

Make a Copy of the Selected Configuration
 Reference the Selected Configuration

Message Queue Cluster Config Type: Default: Embedded Conventional Cluster with Master Broker
 Custom

Server Instances to Be Created (4)

Select	Instance Name	Weight	Node
<input type="checkbox"/>	<input type="text" value="instance1"/>	<input type="text"/>	localhost-domain1
<input type="checkbox"/>	<input type="text" value="instance2"/>	<input type="text"/>	localhost-domain1
<input type="checkbox"/>	<input type="text" value="instance3"/>	<input type="text"/>	glassfishCluster
<input type="checkbox"/>	<input type="text" value="instance4"/>	<input type="text"/>	glassfishCluster

Figure 74 : Création d'un nouveau cluster en utilisant la console d'administration

Etape 4 : Gestion de cluster dans la console d'administration

Après que le cluster ait été créé, il est possible de voir ses instances, démarrer et arrêter à l'aide de la console d'administration. Pour ce faire, cliquez sur « Clusters » et utiliser

l'interface présentée dans figure ci-dessous. Cliquez sur le nom d'un Cluster ou sur l'une de ses instances. On aura ainsi accès à la configuration plus détaillée de chaque élément.

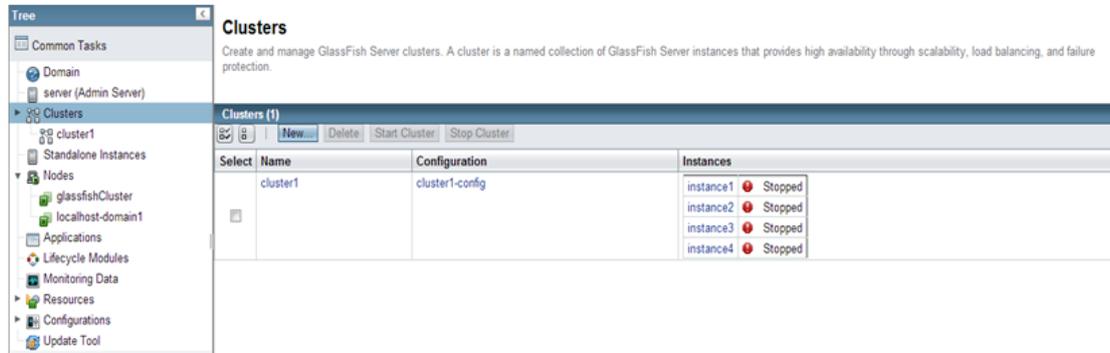


Figure 75 : Interface pour la gestion des clusters dans la console d'administration

Etape 5 : Tester la fonction de haute disponibilité de clusters GlassFish

Après que le cluster ait été créé et démarré, déployez une application à l'aide de la console d'administration. Cliquez sur l'onglet « Applications » dans le menu de navigation de gauche, puis cliquez sur « Deploy Applications or Modules ». Choisissez l'application à déployer et sélectionnez le cluster « cluster1 » que vous avez créé. Après cela, cliquez sur « OK » pour déployer l'application.

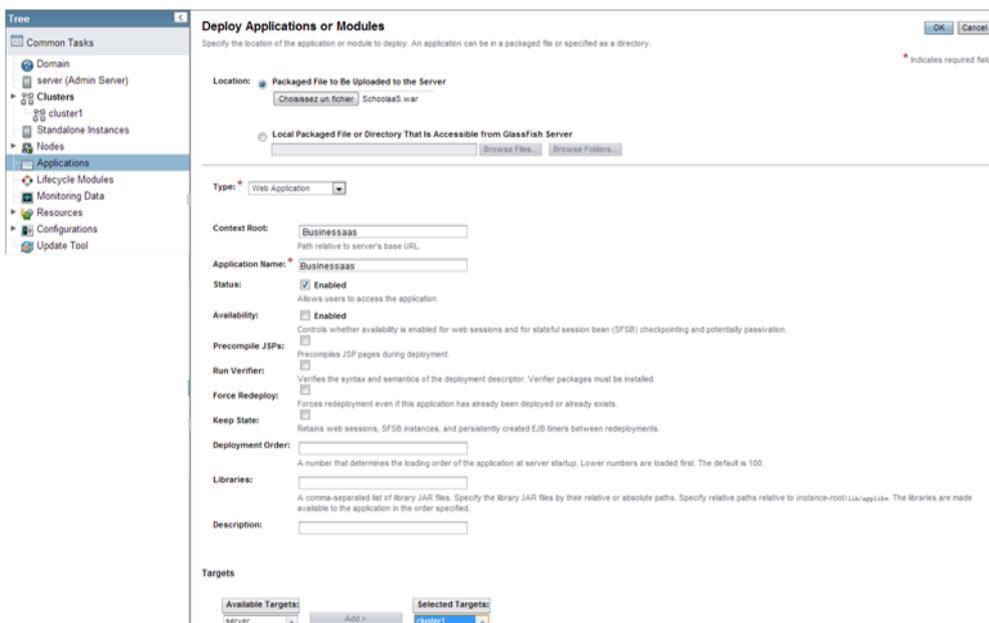


Figure 76 : Exemple de déploiement d'une application web

Après le déploiement, l'application sera disponible dans les quatre instances. Avant de l'ouvrir dans votre navigateur Web, vous devez connaître le port HTTP et HTTPS utilisé par chaque instance. Dans la console d'administration, cliquez sur « Applications » et lancez l'application que vous avez déployez. Une page avec des informations générales sur l'exemple choisi sera ouverte, et les éléments des Ports http et https montreront trois valeurs. L'une au milieu est le numéro de port à utiliser pour accéder à l'application dans le navigateur.

Lors de nos tests, les instances ont été de répondre sur les ports HTTP et HTTPS. Comme indiqué sur la figure ci-dessous.

Web Application Links

If the server or listener is not running, the link may not work. In this event, check the status of the server instance. After launching the web application, use the browser's Back button to return to this screen.

Application Name: Schoolaas

Links:

```
[instance1] http://glassfish:28080/Businessaas
[instance1] https://glassfish:28181/Businessaas
[instance2] http://glassfish:28081/Businessaas
[instance2] https://glassfish:28182/Businessaas
[instance3] http://192.168.3.100:28080/Businessaas
[instance3] https://192.168.3.100:28181/Businessaas
[instance4] http://192.168.3.100:28081/Businessaas
[instance4] https://192.168.3.100:28182/Businessaas
```

Close

Figure 77 : les adresses d'une application déployée

Donc n'importe laquelle de ces adresses, peut ouvrir la page de l'application« Businessaas ».

Annexe 4. Serveur MySQL cluster

Installation et configuration du serveur MySQL cluster sous CentOS 6.5 :^[16]

Notre cluster MySQL est composé de quatre nœuds :

- Nœud SQL (sqlNode : 192.168.3.143)
- Nœud de gestion (managementNode : 192.168.3.140).
- Nœud de données 1 (dataNode1 : 192.168.3.138).
- Nœud de données 2 (dataNode2 : 192.168.3.139).

Nous allons suivre les étapes suivantes pour installer et configurer le serveur MySQL cluster.

Étape 1 : Préparation des serveurs

- Téléchargez le logiciel MySQL Cluster à partir de: <http://www.mysql.com/downloads/cluster/>
- Sur chaque nœud, unarchive le fichier tar.gz et déplacez les fichiers vers /usr/local/mysql

```
#tar xzf mysql-cluster-gpl-7.3.6-linux-glibc2.5-i686.tar.gz  
#mv mysql-cluster-gpl-7.3.6-linux-glibc2.5-i686 /usr/local/mysql
```

Étape 2 : Installation et configuration de nœud de gestion

- Créez le répertoire pour stocker les données de nœud de gestion

```
#mkdir /usr/local/mysql/mysql-cluster
```

- Copiez le nécessaire des fichiers binaires dans /usr/sbin

```
#cp /usr/local/mysql/bin/ndb_mgm* /usr/sbin
```

- Rendez-le exécutable

```
# chmod +x /usr/sbin/ndb_mgm*
```

- Configurez le nœud de gestion, Dans le fichier de configuration (`vi/var/lib/mysql-cluster/config.ini`), ajoutez les lignes suivantes:

```
[NDBD DEFAULT]

NoOfReplicas: 2 #Number of replicas, default:2

DataMemory: 100M

IndexMemory: 20M

[NDB_MGMD]

HostName          =          192.168.3.140
DataDir = /usr/local/mysql/mysql-cluster

[NDBD]

HostName = 192.168.3.138

DataDir = /usr/local/mysql/data

[NDBD]

HostName = 192.168.3.139

DataDir = /usr/local/mysql/data

[MYSQLD]

HostName = 192.168.3.143
```

Etape 3 : Installer et configurer le nœud de données

- Copiez le fichier binaire `ndbd` dans `/usr/sbin`

```
# cp /usr/local/mysql/bin/ndbd /usr/sbin
```

- Rendez-le exécutable

```
# chmod +x /usr/sbin/ndbd
```

- Créez le répertoire de données

```
# mkdir -p /usr/local/mysql /data
```

- Configurez le nœud de données (même pour chaque nœud ndbd)

Dans le fichier de configuration (*/etc/my.cnf*), ajoutez les lignes suivantes:

```
[mysqld]

ndbcluster

[mysql_cluster]

ndb-connectstring=192.168.3.140
```

Etape 4 : Installer et configurer le nœud MySQL

- Créer un compte utilisateur mysql

```
#groupadd mysql
#useradd -g mysql mysql
```

- Créez et remplissez la base de données du système

```
#cd /usr/local/mysql

#scripts/mysql_install_db --user=mysql
```

- Définissez les droits d'accès

```
# cd /usr/local/mysql
# chown -R root .
# chown -R mysql data
# chgrp -R mysql .
```

- Configurez le service de démarrage et activez-le de sorte que le processus de nœud SQL se met en marche au démarrage du système.

```
# cp /usr/local/mysql/support-files/mysql.server /etc/init.d/
# chmod +x /etc/init.d/mysql.server
# chkconfig mysql.server -add
# chkconfig mysql.server on
```

- Configurez le serveur MySQL

Dans le fichier de configuration (*/etc/my.cnf*), ajoutez les lignes suivantes:

```
[mysqld]
ndbcluster

[mysql_cluster]
ndb-connectstring=192.168.3.140
```

Etape 5 : Démarrez le cluster

Nœud de gestion devrait être lancé en premier, suivi par les nœuds de données et enfin nœud SQL.

- Lancez le nœud de gestion

```
# ndb_mgmd -f /usr/local/mysql-cluster/config.ini
```

- Lancez le nœud de données

```
# ndbd
```

- Lancez le nœud SQL

```
# service mysql.server start
```

Etape 6 : Vérifiez les services de cluster

Sur le nœud de gestion, exécutez la commande suivante et vérifiez si tous les nœuds sont démarrés

```
# ndb_mgm -e show
```

Etape 7 : Arrêt le Cluster

- Pour arrêter le cluster, il faut suivre cet ordre: Serveur MySQL puis Nœud de gestion.
- Connectez-vous au nœud MySQL et exécutez la commande suivante:

```
# service mysql.server stop
```

- Connectez-vous au nœud de gestion et exécutez la commande suivante:

```
# ndb_mgm -e shutdown
```

Annexe 5. Serveur Nagios

I. Installation et configuration de Nagios sous CentOS 6.5 : ^[17] ^[18]

1. Installer les composants requis pour Nagios Server (192.168.1.34):

```
#yum install -y gd gd-devel httpd php gcc glibc glibc-common
```

2. Par défaut Nagios ne se trouve pas dans référentiel officiel de centos. Il faut donc ajouter le dépôt EPEL afin d'installer Nagios:

```
#wget http://dl.fedoraproject.org/pub/epel/6/i386/epel-release-6-8.noarch.rpm  
#rpm -ivh epel-release-6-8.noarch.rpm
```

3. Installer Nagios en serveur 192.168.1.34:

```
#yum install -y nagios*
```

4. Configurer Nagios:

- 4.1. Modifier les lignes suivantes dans le fichier de configuration Nagios (/etc/httpd/conf.d/nagios.conf):

```
## Comment Lines 15 & 16 ##  
# Order allow,deny  
# Allow from all  
## Uncomment and Change lines 17,18 & 19 as shown below ##  
Order deny,allow  
Deny from all  
Allow from 127.0.0.1 192.168.1.0/24
```

- 4.2. Définir mot de passe Nagiosadmin:

```
#htpasswd /etc/nagios/passwd nagiosadmin
```

- 4.4. Permettre au service de http par iptables:

```
#vim /etc/sysconfig/iptables
```

Et ajouter l'entrée suivante:

```
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
```

5. Lancer Nagios et les services httpd. Ils se lancent automatiquement à chaque démarrage:

```
#!/etc/init.d/nagios start
#!/etc/init.d/httpd start
#chkconfig nagios on
#chkconfig httpd on
```

6. Dans un navigateur tapez `http://192.168.1.34/nagios/`, puis entrez le mot de passe que nagiosadmin a créé auparavant:

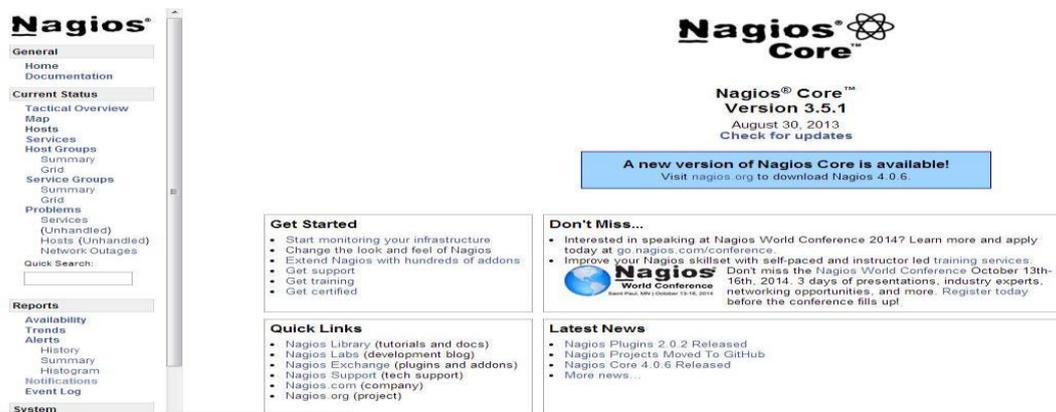


Figure 78 : Interface web de Nagios

II. NRPE Installer et configurer:

Nous pouvons surveiller grâce à ping, tous les ports ouverts comme serveur web, serveur de messagerie, etc. Mais pour les services internes qui sont à l'écoute sur localhost, comme MySQL, et les services système, nous aurons besoin d'utiliser NRPE.

NRPE (Nagios Remote Plugin Executor) est un "Addons" pour Nagios qui permet d'exécuter des plugins sur des machines (Linux/Unix) distantes. La principale raison pour cela est de permettre à Nagios de superviser les ressources "locales" (comme la charge CPU, utilisation de la mémoire, etc) sur machines distantes. NRPE doit être installé sur les machines Linux / Unix à distance.

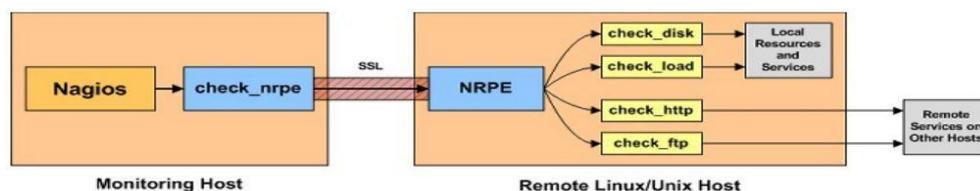


Figure 79 : Le fonctionnement de NRPE

1. Installer NRPE on Clients linux:

```
rpm -Uvh http://dl.fedoraproject.org/pub/epel/6/x86_64/epel-release-6-8.noarch.rpm
rpm -Uvh http://rpms.famillecollet.com/enterprise/remi-release-6.rpm
yum -y install nagios-plugins-all nrpe openssl
chkconfig nrpe on
```

2. Modifier le fichier /etc/nagios/nrpe.cfg:

```
log_facility=daemon
pid_file=/var/run/nrpe/nrpe.pid
server_port=5666
nrpe_user=nrpe
nrpe_group=nrpe
allowed_hosts=192.168.1.34 # Adresse IP de serveur nagios
dont_blame_nrpe=1
debug=0
command_timeout=60
connection_timeout=300
include_dir=/etc/nrpe.d/
command[check_users]=/usr/lib/nagios/plugins/check_users -w 5 -c 10
command[check_load]=/usr/lib/nagios/plugins/check_load -w 15,10,5 -c 30,25,20
command[check_disk]=/usr/lib/nagios/plugins/check_disk -w 20% -c 10% -p
/dev/sda1
command[check_zombie_procs]=/usr/lib/nagios/plugins/check_procs -w 5 -c 10 -s Z
command[check_total_procs]=/usr/lib/nagios/plugins/check_procs -w 150 -c 200
command[check_procs]=/usr/lib/nagios/plugins/check_procs -w $ARG1$ -c $ARG2$ -s $ARG3$
```

Démarrer NRPE:

```
service nrpe start
```

III. Ajouter des machines Linux, des routeurs et des switches au serveur Nagios:

Nous devons définir la commande “check_nrpe” dans le fichier /etc/nagios/objects/commands.cfg de votre serveur Nagios comme suite:

```
define command{
    command_name check_nrpe
    command_line $USER1$/check_nrpe -H $HOSTADDRESS$ -c $ARG1$}
```

1. Ajouter une machine Linux:

Nous allons définir la machine, son groupe, les partitions et ses services à superviser dans le fichier `/usr/local/nagios/etc/objects/Linux.cfg` de serveur Nagios comme illustré ci-dessous:

- Définir la machine linux

```
define host{
    use                linux-server
    hostg_name        serBD
    alias             server data base
    address           192.168.1.35
    max_check_attempts 5
    check_period      24*7
    notification_interval 30
    notification_period 24*7 }
```

- Définir le groupe de la machine

```
define hostgroup{
    hostgroup_name    linuxServers
    alias             Linux Servers
    members           SerBD , SerWeb, SerBp }
```

- Définir le service PING de la machine

```
define service{
    use                generic-service
    host_name          serBD
    service_description PING
    check_command      check_ping!100.0, 20%!500.0, 60% }
```

- Définir le service SSH de la machine

```
define service{
    use                generic-service
    host_name          serBD
    service_description SSH
    check_command      check_ssh
    notifications_enable 0 }
```

- Définir le service CPU load de la machine

```
define service{
    use                generic-service
    host_name          serBD
    service_description CPU Load
    check_command      check_nrpe!check_load }
```

- Définir le service login users de la machine

```
define service{
    use                generic-service
    host_name          serBD
    service_description login users
    check_command      check_nrpe!check_users }
```

- Définir le service de la partition var de la machine

```
define service{
    use                generic-service
    host_name          serBD
    service_description disk var
    check_command      check_nrpe!check_var }
```

- Définir le service de la partition boot de la machine

```
define service{
    use                generic-service
    host_name          serBD
    service_description disk boot
    check_command      check_nrpe!check_boot
}
```

- Définir le service de la partition racine de la machine

```
define service{
    use                generic-service
    host_name          serBD
    service_description disk racine
    check_command      check_nrpe!check_racine }
```

- Définir le service mysqld de la machine

```
define service{
    use                generic-service
    host_name          serBD
    service_description check mysqld
    check_command      check_nrpe!check_procs_mysqld }
```

Une fois la configuration terminée, redémarré le service Nagios. Après quelques instants nous pourrons connaître l'état des services et des partitions de notre machine comme illustré ci-dessous:

Host	Service	Status	Last Check	Duration	Attempt	Status Information
serBD	CPU Load	OK	05-25-2015 10:51:33	0d 1h 48m 29s	1/3	OK - Charge moyenne: 0.00, 0.00, 0.00
	PING	OK	05-25-2015 10:52:48	0d 1h 47m 14s	1/3	PING OK - Paquets perdus = 0%, RTA = 0.66 ms
	SSH	OK	05-25-2015 10:54:03	2d 20h 39m 29s	1/3	SSH OK - OpenSSH_5.3 (protocol 2.0)
	check mysqld	OK	05-25-2015 10:59:28	0d 1h 50m 34s	1/3	PROCS OK: 1 processus avec nom de la commande 'mysqld'
	disk boot	OK	05-25-2015 10:50:43	0d 1h 49m 19s	1/3	DISK OK - free space: /boot 858 MB (91% inode=99%):
	disk racine	OK	05-25-2015 10:51:58	0d 1h 48m 4s	1/3	DISK OK - free space: / 2825 MB (72% inode=87%):
	disk var	OK	05-25-2015 10:53:13	2d 20h 9m 17s	1/3	DISK OK - free space: /var 3544 MB (94% inode=98%):
	login users	OK	05-25-2015 10:54:28	2d 20h 33m 14s	1/3	UTILISATEURS OK - 1 utilisateurs actuellement connectés sur

Figure 80 : La fenêtre de l'état des services de la machine linux

2. Ajouter un router:

Nous allons définir le router, son groupe et ses services à superviser dans le fichier `/usr/local/nagios/etc/objects/router.cfg` du serveur Nagios comme illustré ci-dessous:

- Définir le groupe des routeurs

```
define hostgroup{
    hostgroup_name    routers
    alias             Networking Routers}
```

- Définir le groupe le routeur

```
define host{
    use                generic-switch
    host_name          router-ads120mb
    alias              router-ads120mb
    address            41.248.243.114
    hostgroups         routers}
```

- Définir le service PING du routeur

```
define service{
    use                generic-service
    host_name          router-ads120mb
    service_description PING
    check_command      check_ping!200.0, 20%!600.0, 60%
    normal_check_interval5
    retry_check_interval    1 }
```

Une fois la configuration terminée nous allons redémarrer le service Nagios et après quelques instants nous pourrons connaître l'état de notre router comme illustré ci-dessous:

Service Status Details For Host 'router-adsl20mb'

Limit Results: 100

Host	Service	Status	Last Check	Duration	Attempt	Status Information
router-adsl20mb	PING	OK	05-24-2015 09:37:17	1d 19h 38m 15s	1/3	PING OK - Paquets perdus = 0%, RTA = 2.81 ms

Figure 81 : La fenêtre de l'état de service PING de routeur

3. Ajouter un switch:

Nous allons définir le switch, son groupe et ses services à superviser dans le fichier `/usr/local/nagios/etc/objects/switch.cfg` de serveur Nagios comme illustré ci-dessous:

- Définir le groupe des switches

```
define hostgroup{
    hostgroup_name    switches
    alias             Network Switches}
```

- Définir le switch

```
define host{
    use                generic-switch
    host_name          Swirch_Cisco_1
    alias              Swirch Cisco
    address            192.168.1.68
    hostgroups         switches }
```

- Définir le service PING du switch

```
define service{
    use                generic-service
    host_name          Swirch_Cisco_1
    service_description PING
    check_command      check_ping!200.0, 20%!600.0, 60%
    normal_check_interval5
    retry_check_interval    1 }
```

Une fois la configuration finie, nous redémarrons le service Nagios. Après quelques instants nous pourrons connaître l'état de notre switch comme illustré ci-dessous:

Service Status Details For Host 'Switch_Cisco_1'

Limit Results: 100

Host	Service	Status	Last Check	Duration	Attempt	Status Information
Switch_Cisco_1	PING	OK	05-24-2015 09:19:16	1d 19h 36m 15s	1/3	PING OK - Paquets perdus = 0%, RTA = 2.81 ms

Figure 82 : La fenêtre de l'état de service PING de switch

Annexe 6. Serveur Backup(Bacula)

Installation et configuration: Bacula server et Bacula client sur Centos 6.5 : ^[19]^[20]

1. Installer et configuration Bacula server:

Nous allons utiliser MySQL pour la base de données, vous pouvez utiliser PostgreSQL ou MySQL. L'adresse IP du serveur de sauvegarde est "192.168.2.2/24".

- Installer Bacula server et le serveur mysql en utilisant la commande:

```
# yum install bacula-director-mysql bacula-console bacula-client bacula-storage-mysql mysql-server mysql-devel -y
```

- Démarrez le service MySQL et créer mot de passe root pour mysql:

```
# service mysqld start
# chkconfig mysqld on
# mysqladmin -u root password *****
```

- Ensuite, lancez les commandes suivantes une par une pour créer la base de données et les tables nécessaires pour Bacula.

```
# /usr/libexec/bacula/grant_mysql_privileges -u root -p
# /usr/libexec/bacula/create_mysql_database -u root -p
# /usr/libexec/bacula/make_mysql_tables -u root -p
# /usr/libexec/bacula/grant_bacula_privileges -u root -p
```

Maintenant mettre à jour tous les fichiers de configuration de Bacula avec nouveau mot de passe et adresses, comme indiqué ci-dessous.

- **Mettre à jour Bacula Director:**

Dans le fichier `/etc/bacula/bacula-dir.conf`, Soyez conscient que vous devez utiliser un nom de domaine complet pour ajouter des clients ou tout simplement utiliser l'adresse IP à la place.

```
[...]
Director {
  Name = bacula-dir
  DIRport = 9101          # where we listen for UA connections
  QueryFile = "/usr/libexec/bacula/query.sql"
  WorkingDirectory = "/var/spool/bacula"
  PidDirectory = "/var/run"
```

```

Maximum Concurrent Jobs = 1
Password = "*****"      # Console password
Messages = Daemon
    [...]
Client {
    Name = bacula-fd
    Address =192.168.2.2
    FDPort = 9102
    Catalog = MyCatalog
    Password = "*****"      # password for FileDaemon
    File Retention = 30 days      # 30 days
    Job Retention = 6 months      # six months
    AutoPrune = yes              # Prune expired Jobs/Files
}
[...]
Storage {
    Name = File
    Address =192.168.2.2
    SDPort = 9103
    Password = "*****"
    Device = FileStorage
    Media Type = File
}
[...]
# Generic catalog service
Catalog {
    Name = MyCatalog
    dbname = "bacula"; dbuser = "bacula"; dbpassword = "*****"
}
[...]
Console {
    Name = bacula-mon
    Password = "*****"
    CommandACL = status, .status
}

```

- **Mettre à jour Bacula Console**

Dans le fichier `/etc/bacula/bconsole.conf`, changer le mot de passe de la console:

```

Director {
    Name = bacula-dir
    DIRport = 9101
    address = localhost
    Password = "*****"}

```

- **Mettre à jour Storage Daemon**

Dans le fichier `/etc/bacula/bacula-sd.conf`, mettre à jour le mot de passe et également définir le chemin de votre périphérique Archive.

```
[...]
Director {
  Name = bacula-dir
  Password = "*****"
}
Director {
  Name = bacula-mon
  Password = "*****"
  Monitor = yes
}
[...]
Device {
  Name = FileStorage
  Media Type = File
  Archive Device = /mybackup
  LabelMedia = yes;           # lets Bacula label unlabeled media
  Random Access = Yes;
  AutomaticMount = yes;      # when device opened, read it
  RemovableMedia = no;
  AlwaysOpen = no;
}
[...]
```

- **Mettre à jour file daemon**

Dans le fichier `/etc/bacula/bacula-fd.conf`, mettre à jour le mot de passe.

```
Director {
  Name = bacula-dir
  Password = "*****"
}
Director {
  Name = bacula-mon
  Password = "*****"
  Monitor = yes
}
```

- **Créer le répertoire d'archivage "mybackup"**

```
# mkdir /mybackup
# chown bacula /mybackup
```

- **Redémarrer les démons Bacula**

Maintenant nous avons terminé tous les mots de passe et les modifications d'adresse. Redémarrer tous les démons Bacula. Il faut le faire pour démarrer automatiquement à chaque redémarrage.

```
# service bacula-dir start
# service bacula-fd start
# service bacula-sd start
# chkconfig bacula-dir on
# chkconfig bacula-fd on
# chkconfig bacula-sd on
```

2. Gérer Bacula server avec Webmin:

Webmin est une interface Web pour l'administration de système Linux.

- **Téléchargez et installez une version de Webmin:**

```
#wget http://prdownloads.sourceforge.net/webadmin/webmin-1.670-1.noarch.rpm
#rpm -U webmin-1.670-1.noarch.rpm
```

- **Réglez Firewall / routeur**

Après l'installation de Webmin, si vous voulez accéder au serveur Bacula au travers d'un système distant, permettre au port de webmin "10000" et aux ports "9101", "9102" bacula, "9103" à travers votre pare-feu ou travers un routeur. Ajoutez ces lignes suivantes dans votre fichier de configuration iptables, puis redémarrer iptables.

```
[...]
-A INPUT -m state --state NEW -m tcp -p tcp --dport 10000 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 9101 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 9102 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 9103 -j ACCEPT
[...]
```

- **Accès au Bacula via Webmin:**

Vous trouverez le système de sauvegarde Bacula dans le volet gauche de la console de Webmin:



Cliquez sur le lien "**Bacula Backup System**". Initialement, le serveur Bacula ne démarre pas automatiquement. Pour lancer le serveur Bacula cliquez sur le lien "**Module Configuration**" sur à droite de la page "**Bacula Backup System**".

Help.
Module Config

Bacula Backup System

Failed to connect to the Bacula database : Failed to load the database DBI driver Pg at ./bacula-backup-lib.pl line 44. Maybe it is not set up, or the [module configuration](#)

Sélectionnez la base de données à savoir "MySQL" et entrez le mot de passe de l'utilisateur de base de données Bacula. Puis cliquez sur Enregistrer.

Configuration
For module Bacula Backup System

Configurable options for Bacula Backup System

Configurable options

Default backup wait mode Wait for completion Run in background

Automatically apply director configuration? Yes No

Get node group information from Webmin Servers Index module
 OCM Manager database
 Nowhere

Always show remote directors? Yes No

Bacula database settings

Database type PostgreSQL MySQL SQLite

User to login to database as

Password to login with

Bacula database server This system

Database or file containing Bacula information

File settings

Bacula configuration directory

Full path to bextract command

Full path to bls command

Full path to btape command

Start and stop Bacula using Init scripts bacula command

[Save](#)

Figure 83 : Configuration module de Bacula

Maintenant, vous obtiendrez la fenêtre comme indiqué ci-dessous.

Login: root

Help.
Module Config

Bacula Backup System
Bacula 5.0.0
Contributed by Linmin

Search Docs...

Director Configuration

Director Configuration Backup Clients File Sets Backup Schedules
Backup Jobs Volume Pools Storage Daemons

Storage Daemon Configuration

Storage Daemon Configuration Storage Devices

File Daemon Configuration

File Daemon Configuration

Backup and Restore Actions

Run Backup Job Director Status Client Status Storage Daemon Status
Label Volume Volumes In Pool Mount or Unmount Restore Backup

Process statuses: Bacula Director daemon - Up | Storage daemon - Up | File daemon - Up

[Restart Bacula](#) Click this button to stop and re-start the Bacula daemon processes listed above. This may be needed to activate storage device configurations.

[Stop Bacula](#) Click this button to shut down the Bacula daemon processes listed above.

[Start At Boot](#) Yes No Change this option to control whether or not Bacula is started at system boot time.

Figure 84 : Tableau de bord de Bacula

3. Installer et configuration de Bacula client sous Linux:

- Installez le composant du fichier sur Bacula client:

```
yum -y install bacula-client bacula-console
```

- Configurer le fichier Bacula (**/etc/bacula/bacula-fd.conf**)

```
Director {
    Name = bacula-dir
    Password = "*****"
}
Director {
    Name = bacula-mon
    Password = "*****"
    Monitor = no
}
```

- Puis démarrer le service Bacula.

```
# service bacula-fd start
# chkconfig bacula-fd on
```

- Configurer Bacula bconsole(**/etc/bacula/bconsole.conf**)

```
Director {
    Name = bacula-dir
    DIRport = 9101
    # Director Daemon's hostname or IP address
    address = 192.168.2.2
    # specify password to connect to Director Daemon
    Password = "*****"
}
```

4. Exemple de sauvegarde:

- **Backup clients:**

Nous allons préciser le nom, le mot de passe et adresse IP du client à sauvegarder comme indiqué ci-dessous.

Module Index Create Backup Client

Details of client to be backed up

Client FD name	<input type="text" value="SerWeb"/>	Bacula FD port	<input type="text" value="9102"/>
Bacula FD password	<input type="text" value="1234567"/>	Prune expired jobs and files?	<input type="radio"/> Yes <input type="radio"/> No <input checked="" type="radio"/> Default
Hostname or IP address	<input type="text" value="192.168.3.5"/>	Keep backup jobs for	<input type="text" value="6"/> months
Catalog to use	<input type="text" value="MyCatalog"/>	Enable TLS encryption?	<input type="radio"/> Yes <input type="radio"/> No <input checked="" type="radio"/> Default
Keep backup files for	<input type="text" value="30"/> days	Verify TLS clients?	<input type="radio"/> Yes <input type="radio"/> No <input checked="" type="radio"/> Default
Only accept TLS connections?	<input type="radio"/> Yes <input type="radio"/> No <input checked="" type="radio"/> Default	TLS PEM certificate file	<input type="text" value="None"/>
TLS PEM key file	<input type="text" value="None"/>	TLS PEM key file	<input type="text" value="None"/>
TLS PEM certificate authority file	<input type="text" value="None"/>	TLS PEM certificate authority file	<input type="text" value="None"/>

Figure 85 : création Backup client

- **File Sets:**

Nous allons préciser le fichier ou la partie à sauvegarder, comme indiqué ci-dessous.

Module Index Create File Set

Backup file set details

File set name:

Files and directories to backup:

File signature type:

Files and directories to skip:

Compression type:

Limit backup to one filesystem? Yes No Default

Figure 86:Création la partie à sauvegarder

- **Backup Schedules:**

Nous allons définir un calendrier de sauvegarde: préciser le nom, type et le temps de sauvegarde, comme indiqué ci-dessous:

Module Index Create Backup Schedule

Backup schedule details

Backup schedule name:

Run levels and times	Backup level	Volume	Run at times
<input type="button" value="..."/>	<input type="text" value="Full"/>	<input type="text" value="<Default>"/>	<input type="text" value="at 00:00"/>
<input type="button" value="..."/>	<input type="text" value="<Default>"/>	<input type="text" value="<Default>"/>	<input type="text"/>
<input type="button" value="..."/>	<input type="text" value="<Default>"/>	<input type="text" value="<Default>"/>	<input type="text"/>

Figure 87 : Définir le calendrier de sauvegarde

- **Backup Jobs:**

Nous allons créer un travail de sauvegarde et nous allons préciser: le nom, le type de travail, le client à sauvegarder, le calendrier et le type de sauvegarde souhaité. Comme indiqué ci-dessous:

Module Index Create Backup Job

Backup job details

Backup job name:

Backup job enabled? Yes No

Default type: Default definition Stand-alone job Inherit defaults from

Job type:

Client to backup:

Backup on schedule:

Volume pool:

Backup priority: Default

Backup level:

File set to backup:

Destination storage device:

Destination for messages:

Command before job: Default

Command after job: Default

Command before job (on client): Default

Command after job (on client): Default

Figure 88 : Création un travail de sauvegarde

- **Run Backup Job:**

Pour démarrer un travail de sauvegarde il suffit de préciser le travail à démarrer, comme indiqué ci-dessous:

Module Index
Help..

Run Backup Job

Backup job details

Job to run: backup_web (File set Full on SerWeb)

Wait for results? Yes No

Backup Now

[Return to module index](#)

Figure 89 : Démarrage le travail de sauvegarde

- **Restore Backup:**

Pour restaurer des données il suffit de préciser le travail à restaurer, le fichier et le client ou bien de mettre les données à restaurer, comme indiqué ci-dessous:

Module Index
Help..

Restore Backup

Options for restore of previous backup job

Job to restore: 10 - backup_web (2014-05-27 14:35:16) - Full

Files to restore: /home/backup

Restore from storage device: File

Restore to client or group: SerWeb (on 192.168.3.5)

Restore to directory: Default (/tmp/bacula-restores) Other root directory

Wait for results? Yes No

Restore Now

Figure 90 : Restauration

Annexe 7. Firewall (PfSense)

Installation et configuration PFSense : ^[21]

1. Configuration minimale :

CPU : 133 Mhz mais 400 Mhz est recommandé.

Mémoire : 128 Mb.

Disque Dur : 1 Gb.

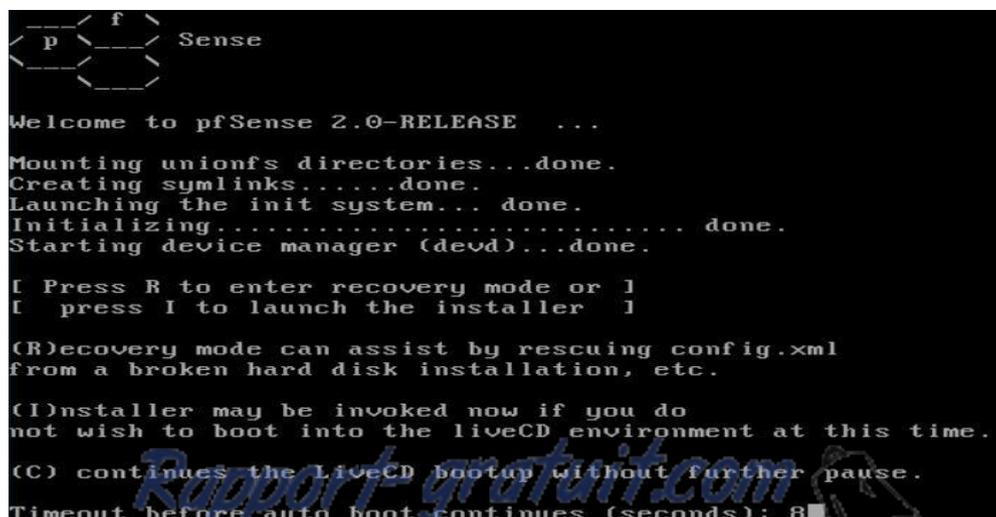
Cartes réseaux : 2 ou plus suivant le réseau voulu.

2. Installation de Pfsense :

Téléchargez l'image de pfSense dans la section « Download » de pfSense (<http://www.pfsense.com>). Démarrez votre ordinateur à partir du CD de l'image de pfSense. L'installation va alors commencer. Laissez alors le compte à rebours se terminer (10 secondes) ou appuyez directement sur « Entrée ». Dans ce dernier cas, le démarrage par défaut est alors choisi.



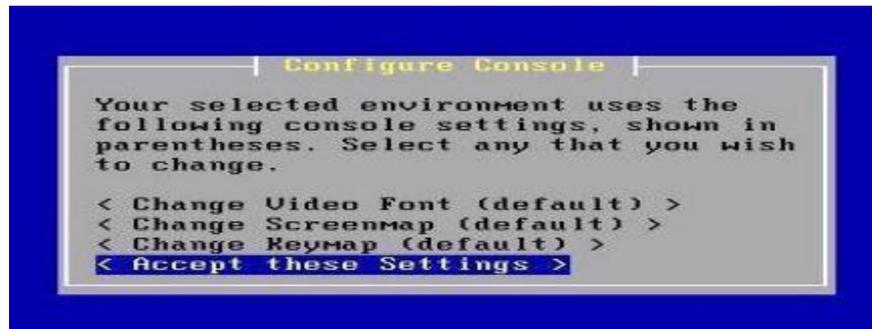
L'installation va se poursuivre un moment, avec un défilement de commandes, jusqu'à s'arrêter sur l'écran suivant :



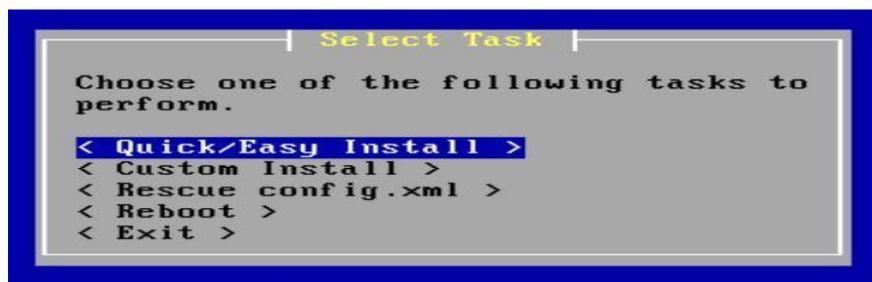
Tapez la lettre **I** pour lancer l'installation (sinon on boot sur le live-cd Pfsense, dans ce cas mais on ne l'installe pas).

L'installation qui va suivre se fait en acceptant toutes les options par défaut. Il suffit d'accepter toutes les demandes (formatage si nécessaire et création de la partition).

Placez-vous sur « Accept these Settings » et tapez « Entrée »



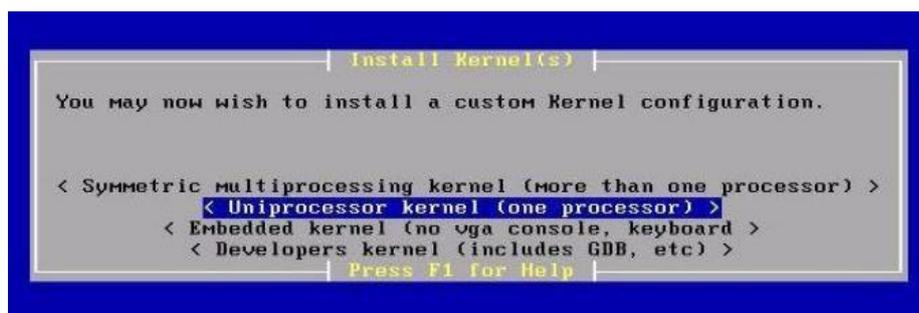
Placez-vous sur « Quick/Easy Install » et tapez « Entrée ».



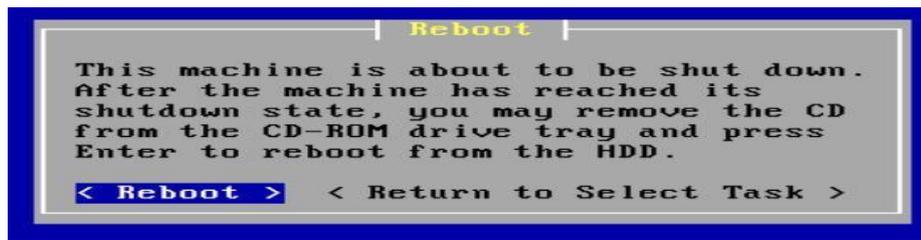
Confirmez le processus d'installation avec <OK>. La fenêtre ci-dessous va apparaître.



Sélectionnez le type du kernel (noyau) à installer.



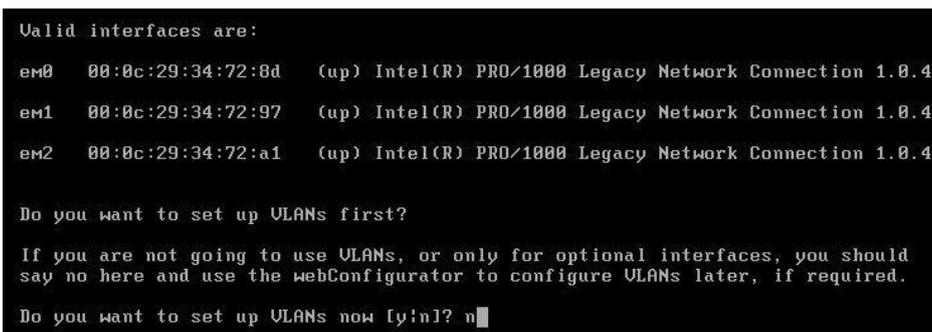
L'installation est terminée. Tapez sur « Entrée » pour redémarrer la machine.



Si l'installation s'est bien déroulée, la machine démarre sur le nouveau système, et vous allez obtenir l'écran ci-dessous :

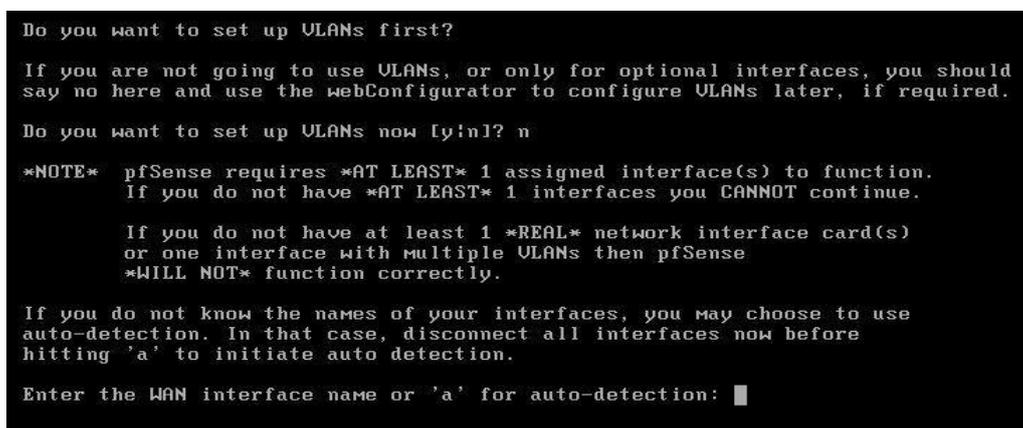


Le temps de chargement des divers paramètres du système d'exploitation peut être long, mais vous allez ensuite aboutir à l'écran ci-dessous :



3. Configuration de serveur PfSense:

Maintenant, il va falloir paramétrer les cartes réseaux afin de correctement les attribuer. Le nommage des différentes cartes étant parfois peu explicite, tapez « a » pour déclencher la détection automatique ou déterminer le nom de l'interface réseau, comme indiqué ci-dessous.



Une fois la configuration des cartes effectuée, nous arrivons à l'écran ci-dessous qui récapitule les différentes cartes réseau et leur association, tapez « y » et validez par « Entrée »:

```
The interfaces will be assigned as follows:
WAN   -> em0
LAN   -> em1
OPT1  -> em2

Do you want to proceed [y!n]?y
```

L'adresse par défaut du LAN est 192.168.1.1, nous allons la modifier en 10.0.0.1. Saisir l'option « 2 », puis taper la nouvelle adresse IP et son masque comme indiqué ci-dessous.

```
Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 10.0.0.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0  = 16
     255.0.0.0   = 8

Enter the new LAN IPv4 subnet bit count:
> 8
```

A ce stade là, vous pouvez mettre de côté pfsense. La configuration se fera depuis un PC du réseau via un navigateur web. Lancez un navigateur web, et dans la barre d'adresse, saisissez <http://adresse-ip-pfsense/> puis validez par « Entrée ». On arrive sur la page d'identification ci-dessous. Le login et le mot de passe par défaut sont (admin, pfsense):



Figure 91 : La fenêtre d'authentification PfSense

La première chose à faire est de modifier le mot de passe par défaut. Pour cela, il faut se rendre dans l'onglet System/User Manager, puis de cliquer sur le « e » pour éditer le profil de l'administrateur comme indiqué ci-dessous:

System: User Manager ?

Users Groups Settings Servers

Defined by: SYSTEM

Disabled:

Username:

Password:
 (confirmation)

Full name:
User's full name, for your own information only

Expiration date:
Leave blank if the account shouldn't expire, otherwise enter the expiration date in the following format: mm/dd/yyyy

Figure 92 : La fenêtre de user manager PfSense

Puis, il faut configurer l'adresse IP du WAN et du DMZ. Pour cela, se rendre dans l'onglet Interfaces/DMZ, puis taper la nouvelle adresse IP et son masque comme indiqué ci-dessous:

Interfaces: DMZ + ? ?

General configuration

Enable: Enable Interface

Description:
Enter a description (name) for the interface here.

IPv4 Configuration Type:

IPv6 Configuration Type:

MAC address:
This field can be used to modify ("spoof") the MAC address of this interface (may be required with some cable connections)
 Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank

MTU:
If you leave this field blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS:
If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.

Speed and duplex: - Show advanced option

Static IPv4 configuration

IPv4 address: /

Gateway: - or add a new one.
If this interface is an Internet connection, select an existing Gateway from the list or add one using the link above

Private networks

Block private networks
When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). You should generally leave this option turned on, unless your WAN network lies in such a private address space, too.

Block bogon networks
When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets you receive.

Note: The update frequency can be changed under System->Advanced Firewall/NAT settings.

Figure 93 : La fenêtre de configuration des interfaces de PfSense

Annexe 8. SNORT

Nous allons suivre les phases ci-dessous pour installer et configurer SNORT sous PfSense.

Etape 1 : Installation du package de SNORT.

Sous PfSense nous allons cliquer sur (System puis packages), et nous allons choisir SNORT dans la liste, comme indiqué ci-dessous.

snort	Security	No info, check the forum	2.8.2.1_1	Snort is a libpcap-based packet sniffer/logger which can be used as a lightweight network intrusion detection system. It features rules based logging and can perform content searching/matching in addition to being used to detect a variety of other attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, and much more.
-------	----------	--------------------------	-----------	---

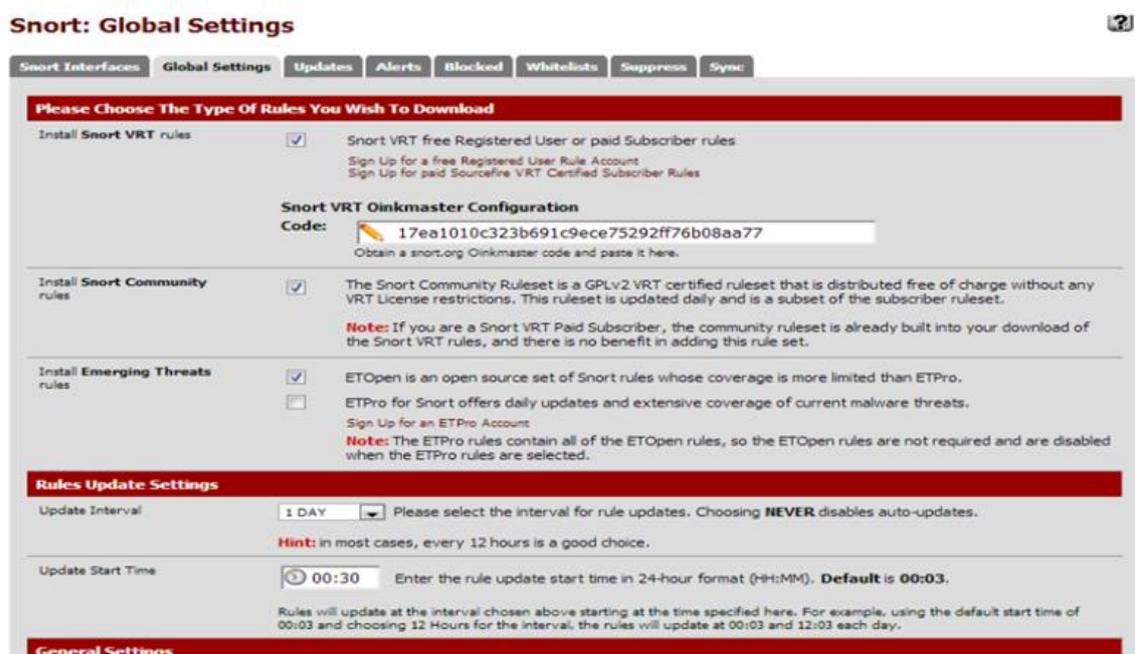
Etape 2 : Récupération du code de configuration

D'abord nous devons créer un compte sur www.snort.org, pour avoir Oinkcode, c'est un code qui nous sera demandé lors de la configuration de SNORT et qui nous permettra de récupérer les règles prédéfinies des attaques les plus connues.



Etape 3 : Configuration de SNORT

Après que l'installation ait été effectuée, nous allons cliquer sur l'onglet **Global settings** et permettre le téléchargement des règles que nous souhaitons utiliser.



Etape4 : Mettre à jour les règles

L'onglet est utilisé pour vérifier l'état des paquets de règles téléchargés et à télécharger nouvelles mises à jour.

Etape 5 : Sélectionnez les types de règles que vous voulez protéger votre réseau.

Cliquez sur l'onglet **Catégories**, puis cochez les cases de catégories de règles que vous souhaitez utiliser.

Enabled	Ruleset: ET Open Rules	Enabled	Ruleset: Snort Text Rules	Enabled	Ruleset: Snort SO Rules
<input type="checkbox"/>	emerging-activex.rules	<input type="checkbox"/>	snort_app-detect.rules	<input type="checkbox"/>	snort_bad-traffic.so.rules
<input type="checkbox"/>	emerging-attack_response.rules	<input type="checkbox"/>	snort_attack-responses.rules	<input type="checkbox"/>	snort_chat.so.rules
<input type="checkbox"/>	emerging-botcc.portgrouped.rules	<input type="checkbox"/>	snort_backdoor.rules	<input type="checkbox"/>	snort_dos.so.rules
<input type="checkbox"/>	emerging-botcc.rules	<input type="checkbox"/>	snort_bad-traffic.rules	<input type="checkbox"/>	snort_exploit.so.rules
<input type="checkbox"/>	emerging-chat.rules	<input type="checkbox"/>	snort_blacklist.rules	<input type="checkbox"/>	snort_icmp.so.rules
<input type="checkbox"/>	emerging-ciarmy.rules	<input type="checkbox"/>	snort_botnet-cnc.rules	<input type="checkbox"/>	snort_imap.so.rules
<input type="checkbox"/>	emerging-compromised.rules	<input type="checkbox"/>	snort_browser-chrome.rules	<input type="checkbox"/>	snort_misc.so.rules
<input type="checkbox"/>	emerging-current_events.rules	<input type="checkbox"/>	snort_browser-firefox.rules	<input type="checkbox"/>	snort_multimedia.so.rules
<input type="checkbox"/>	emerging-deleted.rules	<input type="checkbox"/>	snort_browser-ie.rules	<input type="checkbox"/>	snort_netbios.so.rules
<input type="checkbox"/>	emerging-dns.rules	<input type="checkbox"/>	snort_browser-other.rules	<input type="checkbox"/>	snort_nntp.so.rules
<input type="checkbox"/>	emerging-dos.rules	<input type="checkbox"/>	snort_browser-plugins.rules	<input type="checkbox"/>	snort_p2p.so.rules
<input type="checkbox"/>	emerging-drop.rules	<input type="checkbox"/>	snort_browser-webkit.rules	<input type="checkbox"/>	snort_smtp.so.rules
<input type="checkbox"/>	emerging-dshield.rules	<input type="checkbox"/>	snort_chat.rules	<input type="checkbox"/>	snort_snmp.so.rules
<input type="checkbox"/>	emerging-exploit.rules	<input type="checkbox"/>	snort_content-replace.rules	<input type="checkbox"/>	snort_specific-threats.so.rules
<input type="checkbox"/>	emerging-ftp.rules	<input type="checkbox"/>	snort_ddos.rules	<input type="checkbox"/>	snort_web-activex.so.rules
<input type="checkbox"/>	emerging-games.rules	<input type="checkbox"/>	snort_deleted.rules	<input type="checkbox"/>	snort_web-client.so.rules
<input type="checkbox"/>	emerging-icmp.rules	<input type="checkbox"/>	snort_dns.rules	<input type="checkbox"/>	snort_web-iis.so.rules
<input type="checkbox"/>	emerging-icmp_info.rules	<input type="checkbox"/>	snort_dos.rules	<input type="checkbox"/>	snort_web-misc.so.rules
<input type="checkbox"/>	emerging-imap.rules	<input type="checkbox"/>	snort_experimental.rules		
<input type="checkbox"/>	emerging-inappropriate.rules	<input type="checkbox"/>	snort_exploit-kit.rules		
<input type="checkbox"/>	emerging-info.rules	<input type="checkbox"/>	snort_exploit.rules		
<input type="checkbox"/>	emerging-malware.rules	<input type="checkbox"/>	snort_file-executable.rules		

Bibliographie

- [1] : Laurie Sullivan 2006.
- [2] : Nicols Grevet , Le Cloud Computing évolution ou révolution,Mémoire de recherche,M2IRT 2009.
- [3]: M. Armbrust, A. Fox, R. Gri_th, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, et al. Above the clouds: A berkeley view of cloud computing. EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2009-28, 2009.
- [4]: Brian J.S. Chee, Curtis Franklin Jr., Cloud Computing: Technologies and Strategies of the Ubiquitous Data Center, CRC Press, 2010
- [5] : Cloud Computing - Informatique en nuage Jean-Paul FIGER
- [6]: Eucalyptus. <http://www.eucalyptus.com/>.
- [7]: Opennebula. <http://www.opennebula.org/>.
- [8]: M. Tranchant, Veille technologique : UE NFE107 Architecture et Urbanisation de Systèmes d'Informations, Rapport technique, décembre 2008.
- [9] :<http://glassfish.java.net/fr>
- [10] : <http://www.jboss.org/>
- [11] : <http://db-engines.com/en/ranking>
- [12]: <https://sreeninet.wordpress.com/2015/02/21/openstack-juno-install-using-devstack/>
- [13]: <http://openstack-cloud-mylearning.blogspot.com.es/2015/02/openstack-juno-devstack-installation.html>
- [14]: <http://chianingwang.blogspot.com.es/2014/11/how-to-install-openstack-juno-on.html>
- [15]: <http://mrbool.com/clustering-whats-new-in-glassfish-3-1-part-2/22712>
- [16]: <http://www.clusterdb.com/mysql-cluster/deploying-mysql-cluster-over-multiple-hosts>
- [17]: <http://www.thelinuxwiki.in/2013/11/how-to-configure-nagios-nrpe-in-centos.html>
- [18]: <http://rowell.dionicio.net/installing-nagios-3-5-on-centos-6-5-minimal/>
- [19]: <http://www.unixmen.com/install-and-configure-bacula-server-in-centos-6-4-rhel-6-4/>
- [20]: <http://www.server-world.info/en>
- [21]: <https://www.pfsense.org>