

# Migration dans le cloud de l'infrastructure de Medicarche

## Rapport de synthèse

Présenté le 16/12/2022

par

Beni MULUMBA et Medhi Abbas

*Encadrant entreprise :* Christophe CERIN

---

Rocket by Accenture



# Table des matières

<b>Introduction</b>	<b>1</b>
<b>Bloc 1 : Migration de l'entreprise Medicarche dans le cloud</b>	<b>2</b>
<b>Chapitre 1 Présentation de la société Rocket Cloud</b>	<b>3</b>
1.1 Date Importantes . . . . .	3
1.2 Nos Partenaires . . . . .	4
1.3 Nos Clients . . . . .	4
1.4 Profils Équipe . . . . .	4
<b>Chapitre 2 Situation actuelle de l'entreprise MedicArche</b>	<b>6</b>
2.1 Compréhension des besoins . . . . .	7
2.2 Analyse de l'infrastructure existante . . . . .	7
2.3 Dysfonctionnements . . . . .	8
2.4 Matrice d'exigences . . . . .	9
2.4.1 Fonction principales . . . . .	9
2.4.2 Fonctions contraintes . . . . .	10
<b>Chapitre 3 Proposition des solutions Cloud</b>	<b>11</b>
3.1 Définition du périmètre . . . . .	12
3.2 Analyse swot du cloud . . . . .	13
3.2.1 Contrainte organisationnelle . . . . .	13
3.2.2 Contrainte technique . . . . .	13
3.2.3 Contrainte Budgétaire . . . . .	13
3.2.4 Déroulement du projet . . . . .	14
3.2.5 Méthodologie . . . . .	15
3.2.6 Planification du projet . . . . .	15

3.3	Politique de sécurité . . . . .	17
3.3.1	Gestion d'authentification et accès aux ressources . . . . .	17
3.3.2	Sauvegarde des données et restauration . . . . .	17
3.3.3	Gestion de la montée en charge et de la disponibilité . . . . .	18
3.3.4	Téléphonie en ToIP sur le Cloud. . . . .	18
3.3.5	Coût de la téléphonie ToIP . . . . .	19
3.3.6	Architecture Amazon AWS . . . . .	20
3.3.7	Coût de l'infrastructure AWS . . . . .	20
3.3.8	Architecture OpenStack . . . . .	21
3.3.9	Coût de l'infrastructure Openstack . . . . .	22
3.3.10	Lien entre l'architecture on-premise et l'architecture AWS . . . . .	22
3.3.11	Lien entre l'architecture on-premise et l'architecture Openstack . . . . .	23
3.4	Opex vs Capex . . . . .	25
<b>Chapitre 4</b>	<b>Gouvernance, gestion de risque et conformité</b>	<b>27</b>
4.1	Aspect Juridique . . . . .	27
4.2	Politique RGPD . . . . .	28
4.3	Sécurité des données . . . . .	28
4.4	Norme de sécurité dans le cloud . . . . .	29
4.5	Gestion de risques . . . . .	30
<b>Bloc 2</b>	<b>Intégration de l'infrastructure Medicarche dans le cloud</b>	<b>31</b>
<b>Chapitre 5</b>	<b>Environnement de travail</b>	<b>32</b>
<b>Chapitre 6</b>	<b>Procédure d'intégration de l'infrastructure Medicarche</b>	<b>35</b>
6.1	Installation de Openstack . . . . .	37
6.1.1	Tableau de bord Openstack . . . . .	38
6.1.2	Topologie réseau dans Openstack . . . . .	39
6.1.3	Les gabarits . . . . .	39
6.1.4	Les images . . . . .	40
6.1.5	Les instances . . . . .	41
6.1.6	Les groupes de sécurité . . . . .	42
6.1.7	Les paires de clé . . . . .	43
6.1.8	Gestions des utilisateurs . . . . .	43
6.2	Déploiement des applications de l'entreprise Medicarche . . . . .	43

6.2.1	Installation d'Odoo . . . . .	44
6.2.2	Installation de Nextcloud . . . . .	44
6.2.3	Installation de Syncthing . . . . .	44
6.2.4	Site web Medicarche . . . . .	45
6.3	Description du plan des tests . . . . .	45
6.3.1	Test de montée en charge . . . . .	45
6.3.2	Test de stress du système . . . . .	46
6.3.3	Test de performance . . . . .	47
<b>Bloc 3 : Administration de l'infrastructure Medicarche</b>		<b>48</b>
<b>Chapitre 7 Solution de supervision des VMs</b>		<b>49</b>
7.1	Introduction . . . . .	49
7.1.1	Grafana . . . . .	49
7.1.2	Prometheus . . . . .	50
7.1.3	ELK Stack . . . . .	50
7.1.4	Solutions de supervision de l'infrastructure Openstack . . . . .	51
7.1.5	GLPI . . . . .	51
<b>Bloc 4 : Veille et Evolution d'une infrastructure</b>		<b>53</b>
<b>Chapitre 8 Méthodologie adoptée pour la veille technologique</b>		<b>54</b>
8.1	Type d'information recherché et le mode d'accès . . . . .	54
8.2	Sources d'informations . . . . .	55
8.3	Organisation, trie et analyse de l'information . . . . .	56
<b>Conclusion</b>		<b>57</b>
<b>Bibliographie</b>		<b>58</b>
<b>Annexe A Services cloud utilisés</b>		<b>59</b>
<b>Annexe B Services Openstack utilisés</b>		<b>61</b>
<b>Annexe C CONTRAT DE SERVICES INFORMATIQUES</b>		<b>63</b>

# Introduction

Les organisations se tournent de plus en plus vers la migration des données et des applications vers le Cloud d’après le dernier rapport intitulé ”Flexera 2022 State of the Cloud Report” [1]. Bien gérées, les migrations vers le Cloud amènent de nombreux avantages, tels que la maîtrise et la réduction des coûts, une plus grande flexibilité et une meilleure protection des données qu’une solution hébergée dans l’entreprise. Mal gérées, ces migrations peuvent dégrader les performances et la sécurité des données. Le passage depuis des serveurs on-premise i.e. ; hébergés dans l’entreprise, vers le Cloud permet de réaliser des économies en infrastructure et en personnel. Le Cloud s’avère plus flexible [1] dans la mesure où les clients peuvent facilement ajouter des CPU et augmenter la quantité de RAM ainsi que le nombre de serveurs quand ils le souhaitent. Les fournisseurs Cloud offrent des services de sauvegarde (backup) élaborés évitant toute perte de données.

La mission qui a été confiée à notre entreprise, dénommée ROCKET CLOUD, consiste à analyser les alternatives permettant de résoudre la problématique de migration dans le cloud de la société MedicArche. MedicArche pourra donc effectuer un choix éclairé de la solution qui lui semble la plus appropriée car nous proposons deux orientations, l’une via un cloud public, l’autre via un cloud privé.

Dans ce document, nous décrivons les différentes étapes de conception, d’implémentation, et de mise en service de l’infrastructure dans le cloud. La mise en place d’une infrastructure débute lorsqu’un besoin est exprimé qui justifie sa création et se termine quand elle est opérationnelle, tout en respectant les besoins du client.

# **Bloc 1 : Migration de l'entreprise Medicarche dans le cloud**

# Chapitre 1

## Présentation de la société Rocket Cloud

L'entreprise Rocket Cloud est une entreprise informatique spécialisé dans le domaine du cloud. Nos activité principale sont :

- le développement des applications
- la migration dans le cloud des infrastructures
- la sécurité des infrastructures

### 1.1 Date Importantes

Voici quelques dates importantes de la création de la société Rocket Cloud.

- 2005 : Création de la société Rocket Cloud
- 2006 : Projet de conception et de la mise en place d'un SI dans le cloud.
- 2008 : Recrutement des ingénieurs Devops Cloud



FIGURE 1.1 – Nos principaux partenaires

## 1.2 Nos Partenaires

## 1.3 Nos Clients

Parmi les clients qui nous ont fait confiance, nous avons les clients ci-dessous.



FIGURE 1.2 – nos clients

## 1.4 Profils Équipe

Nous disposons d'une équipe hétérogène de 5 ingénieurs dont la composition est la suivant :

- Un consultant Devops Cloud (Chef de projet niveau 5)



- deux architectes Devops Cloud (niveau 9)
- un ingénieur systèmes et réseaux (niveau 11)
- un administrateur de base de données (niveau 10)
- un consultant Cloud (niveau 13)

Nous avons une équipe des experts qualifiés dans tout ce qui est formation. Ils ont eu à démontrer leurs compétences pour la formation nos clients dans le cadre de la mise en production des nouvelles installations.

L'équipe que nous mettons en place répondre à l'appel d'offre ainsi que pour la formation de la DSI est composée des ingénieurs qualifiés.

Nous nous engageons à appliquer la veille technologie dans le cadre de la formation de la DSI afin que ce dernier puisse utiliser les outils qui sont à la pointe de la technologie actuellement.

Nous avons également une équipe dédié au Help-desk téléphonique composée de 7 personnes :

- 4 techniciens à temps complet (Support Niveau 1 et 2)
- 6 ingénieurs pour les incidents de type urgent (Niveau 4 et 5)

# Chapitre 2

## Situation actuelle de l'entreprise MedicArche

La société MedicArche, spécialisée dans la recherche sur les virus, est située sur 2 sites, à la Defense dans la Grande Arche (site dénommé ARCHE), et à PARIS rue de l'Arcade, dans le 8ème arrondissement (site dénommé ARCADE). Sa croissance est actuellement importante, en raison des demandes liées à la crise sanitaire. Aussi envisage-t-elle d'ouvrir de nouveaux sites, pour répondre aux besoins du marché. Ses effectifs sont d'environ 50 personnes. A échéance d'un an, elle pense les doubler.

Nous avons effectuée une analyse SWOT dans le contexte de du projet qui est la suivante :

Forces	Faiblesses
<ul style="list-style-type: none"><li>★ Évolutive</li><li>★ Capacité de gérer la montée en charge</li><li>★ Intégration avec les applications existant</li><li>★ Politique de sécurité conforme à l'ISO/IEC 27001</li></ul>	<ul style="list-style-type: none"><li>★ Difficulté de répondre aux besoin du marché</li><li>★ Difficulté de suivre la croissance</li><li>★ Architecture vieillissante et obsolète</li><li>★ Dépense lié à l'entretien de l'infrastructure</li><li>★ Liaison entre les deux sites inadaptés</li></ul>
Opportunités	Menaces
<ul style="list-style-type: none"><li>★ Secteur d'activité prometteur</li><li>★ Réduction des coûts</li></ul>	<ul style="list-style-type: none"><li>★ Risque lié à la sécurité</li><li>★ Coupure lié aux sinistres</li></ul>

FIGURE 2.1 – Analyse swot du projet



Après avoir mené une étude basée sur l'infrastructure matérielle, nous avons estimé le coût de l'infrastructure ainsi que des personnels qui intervient dans le tableau suivant :

Tableau d'immobilisation			
Rubriques	Nature	Description	Coût
Matériel informatique	Achat matériel	Matériel de bureau et matériel informatique	335 000 €
Prestations externes	Entretien et réparation	audit sur la sécurité maintenance de l'infra	150 000 €
Logiciels	Achat logiciel	Matériel de bureau et matériel informatique	50 000 €
Frais Installation	Installation	Installations générales, agencements, aménagements divers	35 000 €
Electricité	Achat service	Fournitures non stockables (eau, énergie...)	8500 €
Télécommunications	Achat matériel	Frais postaux et de télécommunications	12 000 €
Prestations externes	Achat service	gardiennage	5000 €
<b>TOTAL</b>			<b>595 000 €</b>

FIGURE 2.3 – Estimation coût infrastructure on-premise

## 2.3 Dysfonctionnements

L'équipe informatique de la société MedicArche a été chargée de faire l'analyse de leur système informatique pour trouver l'origine des problèmes et la limite de l'infrastructure on premise. Après étude vous avez référencé différents problèmes, qui sont :

- Aucun plan de maintenance matériel et logiciel : perte estimé par an 15 000 €
- Pas de plan de continuité d'activité en cas de sinistre : 10 000€
- Pas de gestion des incidents, ni de bases de connaissances : montant global à l'année s'élève à 6500 €.
- Infraction de la norme DEEE : pas de gestion de fin de vie des équipements.

L'ensemble de ces problèmes engendre une perte estimée à 31 500€ par an.

## 2.4 Matrice d'exigences

### 2.4.1 Fonction principales

Fonctions	Exigences	Reformulation des besoins	Objectifs	Critère échanges
<b>FP1:</b> L'infrastructure est évolutive et est capable d'absorber les multiplications des sites	Etre évolutive, être en capacité d'absorber la multiplication des sites	service réseau virtuel ayant la capacité de communiquer entre eux	Communication entre les sites existants et les probables sites qui devront être mis en place.	Recommandé (2/4)
<b>FP2:</b> L'infrastructure est en capacité de gérer la montée en charge	la montée en charge pourra être importante sur le site Web de consultation de la société, plus de 10000 connexions par jour sont envisagées	Mise en place d'un répartiteur de charge et d'un équilibreur de charge	Plus de 10000 connexions par jour sont envisagées sur le site web de l'entreprise	Recommandé (2/4)
<b>FP3:</b> L'infrastructure est capable de gérer la mise en place de l'authentification	Mise en place de la politique de sécurité	Service authentification à double facteur (MFA)	Sécuriser l'accès à la plate-forme en s'identifiant de manière sécurisée	Recommandé (2/4)
<b>FP4:</b> L'infrastructure gère le sauvegarde des données	Mise en place de la politique de sécurité	Service de sécurisation des données	Sécuriser les données en le cryptant	Recommandé (2/4)

FIGURE 2.4 – Matrice des exigences FP

## 2.4.2 Fonctions contraintes

Fonctions	Exigences	Reformulation des besoins	Objectifs	Critère échanges
<b>FC1:</b> L'infrastructure doit préserver l'environnement de l'entreprise	Aucune dégradation de l'environnement  Ne modifie pas les aménagements des locaux, du mobilier, du matériel médical, visuelle et acoustique	Influence minime pour l'entreprise	Ne pas modifier l'activité	Bloquant (4/4)
<b>FC2:</b> L'infrastructure doit être compatible avec la compétence du service informatique	Un administrateur système et réseaux cloud	Adéquation entre les compétences de l'équipe informatique et la solution proposée	Utilisation et gestion de l'infrastructure de manière optimale	Indispensable (3/4)
<b>FC3:</b> L'infrastructure ne doit pas perturber les habitudes de travail du personnel.	Aucun dérangement du personnel  Aucun changement de leurs fonctionnements de travail	Garder la même organisation de travail du personnel	Maintenir la productivité actuelle	Indispensable (3/4)
<b>FC4:</b> L'infrastructure doit être facile d'accès	Disponible à toutes personnes autorisées  Disponible à tout moment	Facilité pour accéder au système	Accès rapide, efficace et simple au système	Indispensable (3/4)

FIGURE 2.5 – Matrice des exigences FC

# Chapitre 3

## Proposition des solutions Cloud

Après avoir effectué une étude comparative des différents fournisseurs Cloud, entre les solutions de type Cloud public et des solutions de type Cloud privé, nous avons pu définir vos besoins ainsi que les objectifs motivant votre changement. Nous avons donc étudié trois solutions qui répondraient potentiellement à vos attentes. La solution apparaissant comme étant optimale à la fin de cette partie sera celle présentée dans cette réponse à appel d'offres.

Voici le tableau comparatif des solutions envisagées :

Critère de choix	AWS	Open Stack	Microsoft Azure
Hautement disponible	+++	+++	+++
Journalisation des activités des flux	+++	+++	+++
Déploiement intuitif et en accord avec votre planning	+++	+	+++
Correspondance avec la taille de l'entreprise	+++	++	+++
Ressources et fonctionnalités nécessaires à l'environnement	+++	+	+++
En accord avec le budget	+++	++	++
Sécurité	+++	++	+++
Evolutivité	+++	+++	+++
Facilité d'intégration	+++	++	+++
Multi-langues	+++	+++	+++
Outils de messagerie	+++	+	+++
Logiciel de gestion intégré ERP	+++		+++

FIGURE 3.1 – comparatif des solutions cloud

Après consultation effectués avec nos collaborateurs, nous avons pu écarter les solutions Microsoft Azure malgré les avantages que la solution pourrait apporter à la migration de l'infrastructure on premise de MedicArche. Nous avons listés les raisons dans le tableau suivant :

Solutions	Arguments
Microsoft Azure	<ul style="list-style-type: none"><li>• Une forte dépendance au prestataire de services</li><li>• De nouvelles fonctions sont ajoutées régulièrement et certaines fonctions peuvent être supprimées</li></ul>

FIGURE 3.2 – Tableau des arguments

### 3.1 Définition du périmètre

A l'issue d'une étude approfondie sur l'infrastructure existant, qui a donné lieu à une cartographie de l'infrastructure on-premise, nous sommes en présence de plusieurs perspectives concernant la migration dans le cloud. Différents contraintes ont été relevées lors de la définition du périmètre du projet qui sont de type organisationnelle, technique et budgétaire.



## 3.2 Analyse swot du cloud

Forces	Faiblesses
<ul style="list-style-type: none"> <li>★ Dimension à la demande</li> <li>★ Vitesse de la mise en oeuvre</li> <li>★ Investissement plus faible</li> </ul>	<ul style="list-style-type: none"> <li>★ Contrôle de la sécurité basé sur la confiance</li> <li>★ Solutions hétérogène</li> <li>★ La disponibilité sur service dépend de celle d'internet</li> </ul>
Opportunités	Menaces
<ul style="list-style-type: none"> <li>★ Secteur d'activité prometteur</li> <li>★ Recentrer les investissements sur le cœur du métier</li> <li>★ Profiter de l'innovation réservées aux grandes entreprises</li> </ul>	<ul style="list-style-type: none"> <li>★ Coût maîtrisé si l'usage est maîtrisé</li> <li>★ Dépendance au fournisseur</li> <li>★ Débordement de la DSI par les métiers</li> </ul>

FIGURE 3.3 – Analyse swot

### 3.2.1 Contrainte organisationnelle

Les contraintes organisationnelles sont les suivantes :

- Le laboratoire souhaite une réponse à l'appel d'offre pour le 28/04/2022
- La solution doit être mise en place et être opérationnelle pour le 27/07/2022

### 3.2.2 Contrainte technique

L'infrastructure doit :

- doit préserver l'environnement de l'entreprise
- doit être compatible avec la compétence du service informatique
- ne doit pas perturber les habitudes de travail du personnel.
- doit être facile d'accès

### 3.2.3 Contrainte Budgétaire

Une étude sur l'estimation budgétaire du projet a été réaliser par nos services et cela s'élève à 477 177,52 € TTC au cas où vous optiez pour la solution AWS et 3 494 000 € pour la solution Openstack.

### 3.2.4 Déroulement du projet

La migration de l'infrastructure de l'entreprise MedicArche se déroulera en plusieurs phases qui sont décrit dans le tableau suivant :



FIGURE 3.4 – Phase de migration de l'infrastructure

et dans le cadre du management du projet elle sera repartie comme suite :

Nom de la tâche	Durée	Nom des ressources	Coût Salarial
<b>Phase préliminaire</b>	<b>20 jours</b>		<b>15000 €</b>
Etude préalable	7 jours	Chef de projet	6000 €
Recueil des besoins du client	7 jours	Ingénieur Cloud	4500 €
Etude comparative	6 jours	Ingénieur Cloud	4500 €
<b>Phase d'étude détaillée</b>	<b>30 jours</b>		<b>16000 €</b>
Etude de l'infrastructure existante	10 jours	Ingénieur Cloud	5000 €
Conception de l'infrastructure cloud	15 jours	Architecte Cloud	7000 €
Etude sur les technologies ToIP	5 jours	Ingénieur Cloud	4000 €
<b>Phase de réalisation</b>	<b>60 jours</b>		<b>21000 €</b>
Implémentation de l'infrastructure	30 jours	Ingénieur Cloud	5000 €
Mise en production de l'infrastructure	10 jours	Ingénieur Cloud	5000 €
Homologation	5 jours	Chef de projet	6000 €
Test de l'infrastructure	15 jours	Ingénieur Cloud	5000 €
<b>Phase de réception</b>	<b>20 jours</b>		<b>21000 €</b>
Effectuer les modifications demandées par la Commission de validation	5 jours	Chef de projet	6000 €
Formation de la DSI	15 jours	Ingénieur Cloud	15000 €

FIGURE 3.5 – Phase de migration de l'infrastructure

Le coût final est la somme de coûts salariaux additionnées à d'autre coûts que nous avons pas le droit de détailler. La somme de tous les phases nous donne 73000 € TTC.

### 3.2.5 Méthodologie

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

L'intérêt de ces différentes activités est de réaliser une infrastructure de qualité afin d'être en phase avec les exigences du client.

### 3.2.6 Planification du projet

La planification du projet consiste en une phase d'étude préalable, de recueil des besoins utilisateurs, de l'étude de l'infrastructure existante, de l'étude et conception du

projet, de l'implémentation, de l'homologation, de la mise en production et de la formation de la DSI. Nous avons détaillé le déroulement du projet dans le diagramme suivant :

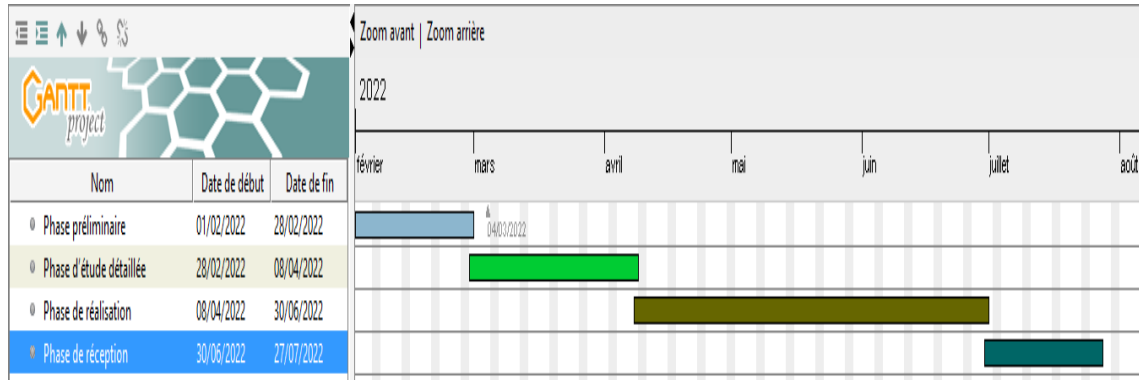


FIGURE 3.6 – Diagramme de Gantt

Afin d'identifier les rôles et les responsabilités des intervenants au sein de chaque processus et activités une matrice de responsabilité a été mise en place.

Phases	Chef de projet	Consultant cloud	Architecte cloud	Collaborateur (client)	Sponsor
préliminaire (Définition des besoins)	I	C	C	R	A
étude détaillée	A	R	C	I	I
réalisation	A	C	I	I	I
migration	A	C	I	I	I
réception	A	I	I	I	I

	Responsable (R)
	Rendre compte (A)
	Consulté (C)
	informé (I)

FIGURE 3.7 – Matrice RACI

## 3.3 Politique de sécurité

Les données hébergées dans un data center bénéficient d'un niveau de protection plus fort qu'en local. Contrôles stricts des accès utilisateurs et administrateurs, redondance des sauvegardes, vidéo surveillance (en plus des badges) des accès physiques.

### 3.3.1 Gestion d'authentification et accès aux ressources

La gestion d'authentification consistera à renforcer la stratégie de mot de passe en obligeant l'utilisateur à construire un mot de passe complexe qui respecte la stratégie de compte MedicArche. En plus du mot de passe, une authentification à deux facteur (MFA) sera mise en place et le SSO. Comme il est précisé dans le cahier de charger nous avons mis en place un annuaire qui permettra de gérer les accès aux ressources et la complexité de mot de passe.

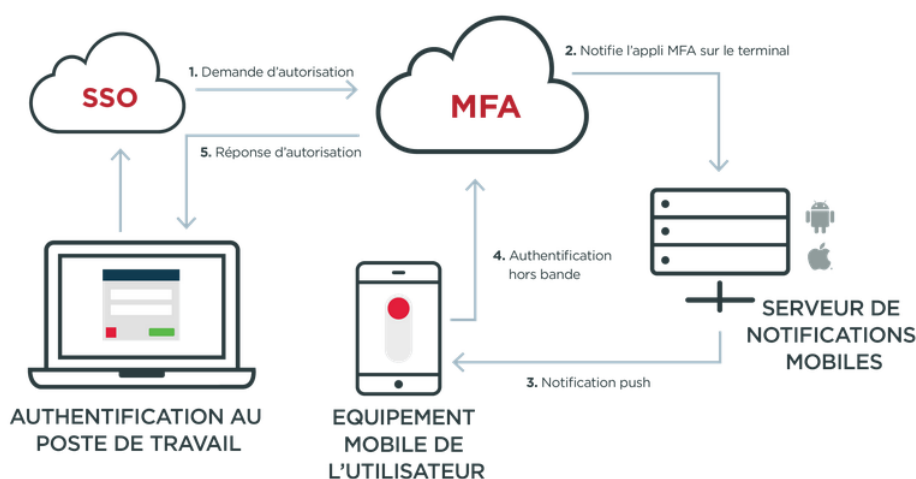


FIGURE 3.8 – Gestion d'authentification

Les employés de medicArche pourront se connecter l'infrastructure de MedicArche via un canal sécurisé avec un VPN (Virtual Private Network).

### 3.3.2 Sauvegarde des données et restauration

La sauvegarde des données s'effectuera de manière incrémentale. en cas de perte des données une politique de restauration sera mise en place pour restaurer les données. Les données sauvegarder seront cryptés et pourra avoir accès que les personnes qui on le droit.

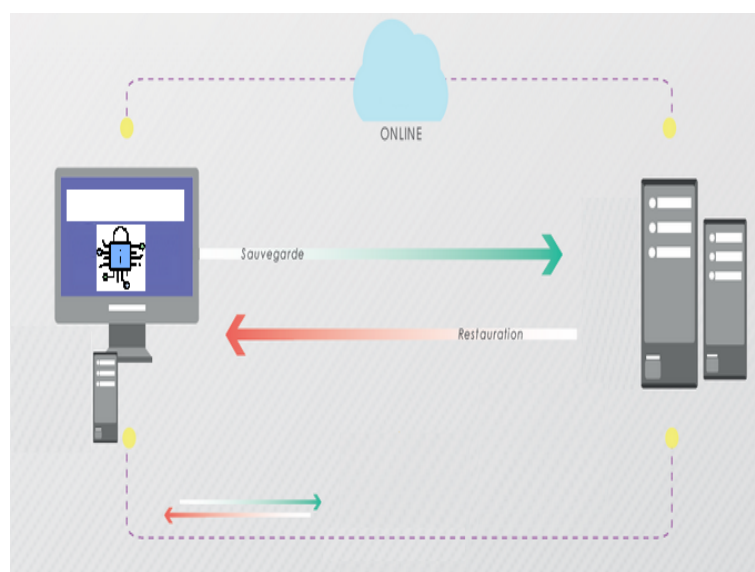


FIGURE 3.9 – Sauvegarde et restauration

### 3.3.3 Gestion de la montée en charge et de la disponibilité

La gestion de la montée en charge et de la disponibilité sera assurée par la mise en place de l'autoscaler et du load balancer qui sont fournis par les providers cloud. Dans le cas de Amazon AWS les services comme AWS Elastic Load Balancing (gère la montée en charge) et AWS Auto Scaling (assure la haute disponibilité) sont préconisés.

Ces mêmes services sont assurés sont aussi présents dans Openstack sous le nom d'Octavia (load balancer) et Heat/Telemetry (auto scaling).

### 3.3.4 Téléphonie en ToIP sur le Cloud.

La technologie de la téléphonie cloud repose sur un système utilisant la VoIP (Voice Over Internet Protocol). Nous vous proposons trois solutions skype, Microsoft teams et Asterisk. Les deux premières sont les plus utilisées sur le marché.



FIGURE 3.10 – Solution ToIp

### 3.3.5 Coût de la téléphonie ToIP

Parmi les 3 technologies nous vous présentons le tarif de Teams qui est une application complète de ToIP la plus complète et le plus utilisé.

	prix unitaire	utilisateur	par mois	par an
Teams	10,50 €	50	525 € / mois	6300 €

FIGURE 3.11 – tarif Teams

3.3.6 Architecture Amazon AWS

L'architecture qui ci-dessous donne un aperçu de l'infrastructure qui sera déployée sur Amazon web service. Pour réduire les coûts l'infrastructure a été simplifiée tout en gardant le coeur des services de l'infrastructure on-premise.

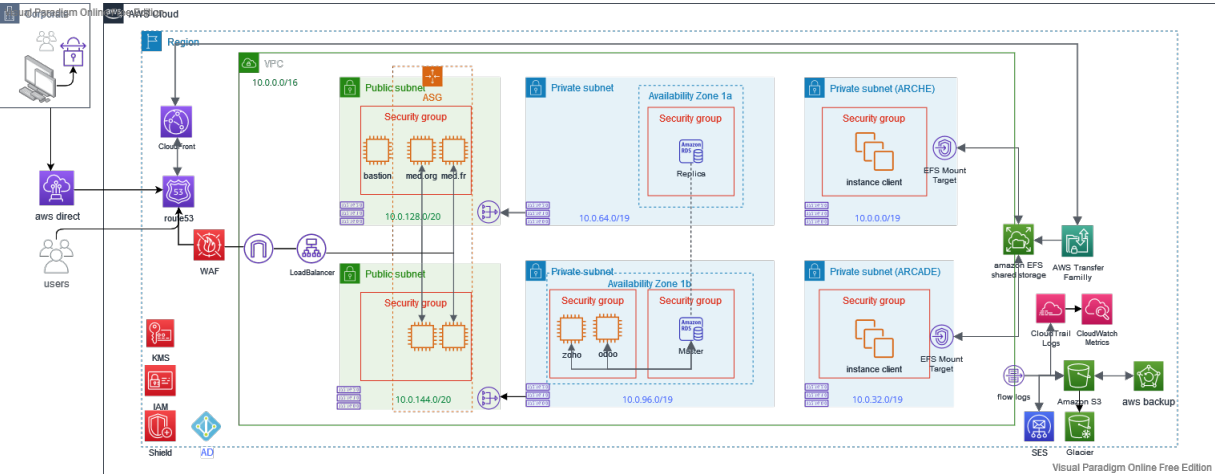


FIGURE 3.12 – Architecture AWS

Plusieurs service AWS décrits en annexe seront utilisés dans notre architecture pour avoir un système qui répond à votre cahier de charge.

3.3.7 Coût de l'infrastructure AWS

Le coût total des services de l'infrastructure avec AWS est de 404.177,52 €. Le tableau ci-dessous donne plus de détail par mois et par an de coût d'utilisation de chaque service.

Région	Service	Frais initiaux	Frais mensuels	Total par an	Devise
UE (Paris)	Amazon EC2	0	58.9	706.80	EU
UE (Paris)	AWS Web Application Firewall (WAF)	0	250	3000.00	EU
UE (Paris)	Amazon CloudFront	0	425.01	5100.12	EU
UE (Paris)	AWS Transfer Family	0	339	4068.00	EU
UE (Paris)	Application Load Balancer	0	1858.92	22307.04	EU
UE (Paris)	Amazon RDS for SQL server	0	20847.8	250173.60	EU
UE (Paris)	S3 Standard	0	2351.77	28221.24	EU
UE (Paris)	S3 Glacier Flexible Retrieval	0	2044.1	24529.20	EU
UE (Paris)	Data Transfer	0	0	0.00	EU
UE (Paris)	Amazon Elastic File System (EFS)	0	434.4	5212.80	EU
UE (Paris)	AWS CloudTrail	0	0	0.00	EU
UE (Paris)	AWS Directory Service	0	950.46	11405.52	EU
UE (Paris)	Standard topics	0	2099.5	25194.00	EU
UE (Paris)	Amazon WorkMail	0	240	2880.00	EU
UE (Paris)	Amazon Route 53	0	1276	15312.00	EU
UE (Paris)	AWS Key Management Service	0	106	1272.00	EU
UE (Paris)	AWS Direct Connect	0	0	0.00	EU

FIGURE 3.13 – Tarif services AWS



### 3.3.8 Architecture OpenStack

L'architecture du cloud privé avec Openstack a été conçue de manière à faire apparaître les éléments de l'infrastructure d'une manière générique. Certains services, comme l'Active Directory peuvent être implémentés dans des machines locales du site de l'entreprise MedicArche puis interconnectés avec OpenStack.

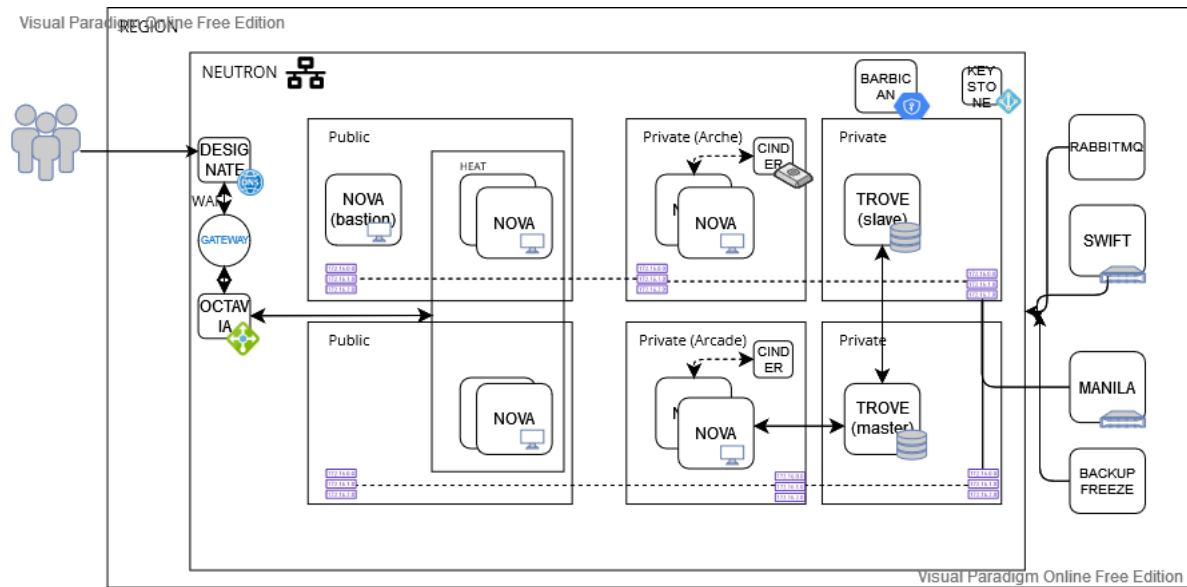


FIGURE 3.14 – Infrastructure OpenStack

Openstack propose différents services qui seront utilisés pour implémenter l'architecture.

### 3.3.9 Coût de l'infrastructure Openstack

Dans le cadre de OpenStack qui est un ensemble de logiciels open source permettant de déployer des infrastructures de cloud computing, son utilisation est gratuite mais pas le coût de l'hébergement. Le tableau ci-dessous montre le coût de l'utilisation des services hébergés par mois et pour une année.

Services	Frais initiaux	Frais mensuels	Total par an
Nova	0	450 €	5400 €
Designate	0	300 €	3600 €
Licence	0	50 €	600 €
Octavia	0	200 €	2400 €
Trove	0	800 €	9600 €
Barbican	0	200 €	2400 €
Keystone	0	100 €	1200 €
RabbitMQ	0	600 €	7200 €
Swift	0	700 €	8400 €
Manila	0	400 €	4800 €
Backup Freeze	0	800 €	9600 €
Glance	0	600 €	7200 €
Cinder	0	500 €	6000 €
Sécurité	0	2000 €	24000 €
<b>Total</b>			<b>92400 €</b>

FIGURE 3.15 – coût hébergement OpenStack

Après calcul de l'hébergement chez OVH pour toute l'infrastructure en multipliant 68400 par le nombre des utilisateurs qui est de 50 cela nous donne 3 421 000 €

### 3.3.10 Lien entre l'architecture on-premise et l'architecture AWS

En partant de l'architecture on-premise, nous avons pu élaborer une architecture dans AWS qui correspondra aux éléments évoqués dans le cahier de charge. Dans les lignes qui nous allons faire le lien entre l'architecture on-premise et l'architecture AWS.

L'architecture on-premise est répartie en 3 parties qui sont le DMZ, le site ARCADE et le site Arche.

Dans le DMZ on retrouve un serveur ftp, un serveur dns public et les deux sites web de l'entreprise qui sont respectivement medicarche.org et medicarche.com les tous derrières

un routeur qui fait office de pare-feu.

Dans le site Arche on retrouve 2 étages. Le premier étage ne contient que les postes des collaborateurs et dans le deuxième étages on trouve le serveur des fichiers, le serveur de log, le serveur de backup, le serveur dns local. Les serveurs des fichiers sont relié à un san et le san à un swith. Les deux étages sont relié à travers d'un routeur et le routeur du site Arche à son tour se connect à la DMZ.

Dans le site Arcade on retrouve les ordinateurs des collaborateurs, un serveur dns medicarche pour assurer la réplication, un serveur odoo et zoho desk, et trois serveur de fichier relié à un nas.

Dans l'architecture AWS le réseau medicArche est représenté par un VPC (virtual private cloud). On faissant un zoom dans le vpc, on retrouve le DMZ qui est remplacé par un sous-réseau public dans AWS. Dans le sous-réseau public on a deux instances EC2 qui héberge les sites web de l'entreprise respectivement celui de medicarche.com et medicarche.fr.

Les site arcade et arche sont représenté par quatre sous-réseaux privés repartie dans 2 zones d'availabilités. Les deux premiers sous-réseaux privés, recevront les machines des collaborateurs et les deux derniers sous-réseaux seront réservé pour les base de données tout en assurant la réplication entre les deux serveurs.

Les services AWS Transfert File nous permettra de mettre en place le transfert de fichier, le service S3 jouera le rôle du serveur san comme dans l'architecture on-premise.

L'annuaire active directory sera assuré par le service IAM d'amazon ou AWS Directory Service. Après concertation entre les membres de l'équipe Rocket Cloud, nous avons opté pour l'utilisation du service IAM parce que le servier est gratuit contrairement au service AWS Directory Service. D'autre service qui n'apparaissent pas dans l'architecture on-premise sont utilisés pour répondre au besoin de client.

### 3.3.11 Lien entre l'architecture on-premise et l'architecture Openstack

Dans l'architecure openstack, on retrouve le réseau de l'entreprise MedicArche qui est représenté par le service neutron qui fait office de réseau dans l'environnement cloud openstack.

Dans le neutron on a deux sous-réseaux public et quatre sous-réseaux privées. Dans la partie public on retrouve les sites medicarche.org et medicarche.fr qui sont hébergés dans nova (un service qui fourni des machines virtuelles dans openstack). Dans les deux pre-

---

mier sous-réseaux privés, on retrouve les deux sites arche et arcade qui contiennent les machines des collaborateurs et les deux derniers sous-réseaux sont réservés pour accueillir les serveurs des données et les serveurs des fichiers. Le service Keystone jouera le rôle de serveur active directory et le service barbican pour la gestion des clé. Le service designate fait office de service dns. Dans l'architecture on-premise on avait besoin d'un serveur dns pour effectuer la résolution de nom. Étant soumis au problème de lisibilité dans l'architecture nous avons privilégié de mettre en avant les éléments important qui apparaissent dans l'architecture on-premise.

### 3.4 Opex vs Capex

Nous avons établi un comparatif[2] entre les dépenses lié l'infrastructure on premise et les dépenses de l'infrastructure dans le cloud avec le graphe et dans le tableau ci-dessous :

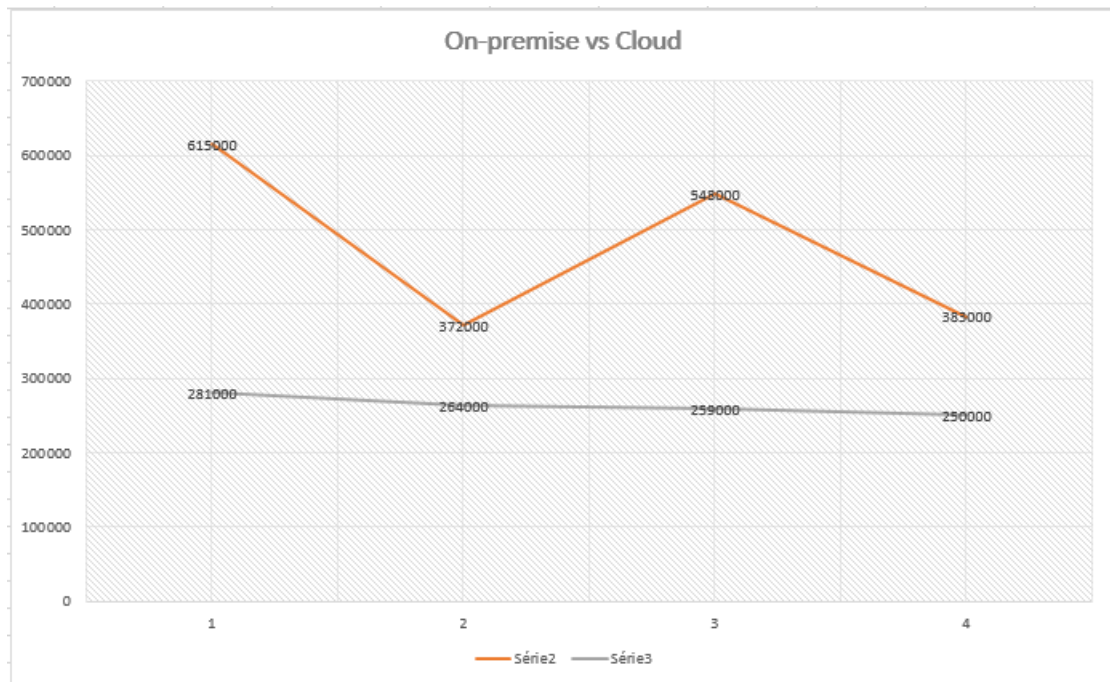


FIGURE 3.16 – Graphe on-premise vs cloud pour 50 utilisateurs

En étudiant le graphe nous remarquons au bout de la 4 ème année les dépenses d'exploitation lié à l'infrastructure on-premise varie énormément par rapport à celui du cloud.

50 utilisateurs	on-premise				
	Année 1	Année 2	Année 3	Année 4	Total 4 années
Total évaluation et selection	15000	0	0	0	15 000,00
Total IT Infrastructure	335000	150000	300000	160000	945 000,00
Total application software/support	50000	25000	50000	26000	151 000,00
Total application implémentation/support	35000	32000	33000	32000	132 000,00
Total prestation externe	150000	150000	150000	150000	600 000,00
Total formation	30000	15000	15000	15000	75 000,00
<b>Coût total</b>	<b>615000</b>	<b>372000</b>	<b>548000</b>	<b>383000</b>	<b>1 918 000,00</b>
<b>Total coût VAN (7%)</b>	<b>574 766,35</b>	<b>347 663,55</b>	<b>512 149,53</b>	<b>357 943,92</b>	<b>1 792 523,36</b>
Cumulative TCO VAN	574 766,35	922 429,90	1 434 579,43	1 792 523,35	-

50 utilisateurs	cloud				
	Année 1	Année 2	Année 3	Année 4	Total 4 années
Total évaluation et selection	10000	0	0	0	10 000,00
Total IT Infrastructure	0	0	0	0	0,00
Total application software/support	27000	24000	21000	15000	87 000,00
Total application implémentation/support	29000	25000	23000	20000	97 000,00
Total prestation externe	200000	200000	200000	200000	800 000,00
Total formation	15000	15000	15000	15000	60 000,00
<b>Coût total</b>	<b>281000</b>	<b>264000</b>	<b>259000</b>	<b>250000</b>	<b>1 054 000,00</b>
<b>Total coût VAN (7%)</b>	<b>262 616,82</b>	<b>246 728,97</b>	<b>242 056,07</b>	<b>233 644,85</b>	<b>985 046,72</b>
Cumulative TCO VAN	262 616,82	509 345,79	751 401,86	985 046,71	-

FIGURE 3.17 – Tableau opex capex pour 50 utilisateurs

100 utilisateurs	on-premise				
	Année 1	Année 2	Année 3	Année 4	Total 4 années
Total évaluation et selection	15000	0	0	0	15 000,00
Total IT Infrastructure	670000	300000	600000	320000	1 890 000,00
Total application software/support	100000	50000	100000	52000	302 000,00
Total application implémentation/support	70000	64000	66000	64000	264 000,00
Total prestation externe	250000	250000	250000	250000	1 000 000,00
Total formation	60000	30000	30000	30000	150 000,00
<b>Coût total</b>	<b>1165000</b>	<b>694000</b>	<b>1046000</b>	<b>716000</b>	<b>3 621 000,00</b>
<b>Total coût VAN (7%)</b>	<b>1 088 785,04</b>	<b>648 598,13</b>	<b>977 570,09</b>	<b>669 158,87</b>	<b>3 384 112,14</b>
Cumulative TCO VAN	1 088 785,04	1 737 383,17	2 714 953,26	3 384 112,13	-

100 utilisateurs	cloud				
	Année 1	Année 2	Année 3	Année 4	Total 4 années
Total évaluation et selection	20000	0	0	0	20 000,00
Total IT Infrastructure	0	0	0	0	0,00
Total application software/support	54000	48000	42000	30000	174 000,00
Total application implémentation/support	58000	50000	46000	40000	194 000,00
Total prestation externe	400000	400000	400000	400000	1 600 000,00
Total formation	30000	30000	30000	30000	120 000,00
<b>Coût total</b>	<b>562000</b>	<b>528000</b>	<b>518000</b>	<b>500000</b>	<b>2 108 000,00</b>
<b>Total coût VAN (7%)</b>	<b>525 233,64</b>	<b>493 457,94</b>	<b>484 112,14</b>	<b>467 289,71</b>	<b>1 970 093,45</b>
Cumulative TCO VAN	525 233,64	1 018 691,58	1 502 803,72	1 970 093,43	-

FIGURE 3.18 – Tableau opex capex pour 100 utilisateurs

# Chapitre 4

## Gouvernance, gestion de risque et conformité

### 4.1 Aspect Juridique

Constituant une des propriétés du Cloud Computing, l'abstraction sur la localisation des données peut limiter les possibilités de recours au Cloud, si l'on n'y prend pas garde, dans la mesure où en cas de litiges il serait difficile de déterminer le droit applicable : celui du fournisseur, du client, ou du pays d'hébergement des données. En fonction des opérateurs, vous avez la possibilité de choisir l'emplacement de votre hébergeur de données (Europe, Suisse, etc. . .), mais il serait toujours préférable d'étudier avec le service juridique [3] de l'entreprise ses spécifications avant la signature définitive de tout contrat.

Le Service Level Agreement (SLA) est un paramètre qui aide également au passage dans le Cloud car il s'agit du document qui définit la qualité de service requise entre un prestataire et un client.

Ainsi, l'entreprise peut s'appuyer sur ce document afin de spécifier les responsabilités du fournisseur de service à savoir les niveaux de disponibilité (99,99999%), de performance et d'accessibilité, les garanties sur l'intégrité des données ainsi que les conditions de restitution des données en cas de changement d'opérateur et les pénalités (financières ou autres) concernant la facturation en cas de manquement au SLA. Grâce à ce document, il est également possible de définir la garantie sur le temps de rétablissement d'un Datacenter dans le cas où un désastre (inondation, incendie) se produit, et des sauvegardes en tenant compte d'un engagement de l'opérateur à mener des sauvegardes régulières des données et à conserver une copie dans un site distant.

## 4.2 Politique RGPD

Le Règlement Général sur la Protection des Données [4] est un texte adopté par l'ensemble des 28 pays membres de l'Union Européenne. Ce texte apparaît comme une véritable référence dans la lutte pour la protection des données du fait qu'il harmonise cette protection à l'ensemble des entreprises, structures publiques et citoyens européens. Rocket Cloud s'engage à garantir un niveau de protection élevé des Données personnelles des Personnes concernées qui utilisent le Site et autres Produits ou Services et de toute autre personne dont elle traite les Données à caractère personnel.

Rocket Cloud s'engage à respecter la réglementation applicable (notamment les articles 5 et 6 du RGPD) à l'ensemble des Traitements de Données à caractère personnel qu'elle met en œuvre. Plus particulièrement, Rocket Cloud s'engage notamment à respecter les principes suivants :

- Les Données à caractère personnel sont traitées de manière licite, loyale et transparente (licéité, loyauté, transparence) ;
- Les Données à caractère personnel sont collectées pour des finalités déterminées, explicites et légitimes, et ne sont pas traitées ultérieurement d'une manière incompatible avec ces finalités (limitation des finalités) ;
- Les Données à caractère personnel sont conservées de manière adéquate, pertinente et sont limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ;
- Les Données à caractère personnel sont exactes, tenues à jour et toutes les mesures raisonnables sont prises pour que les données inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude).

## 4.3 Sécurité des données

La gestion des risques [4] permet de déterminer les précautions à prendre « au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données » .

Rocket Cloud met en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque inhérent à ses opérations de Traitement, répondre aux exigences réglementaires et protéger les droits et les Données à caractère personnel des Personnes concernées dès la conception des opérations de Traitement.



La sécurité est un point important pour la protection des données de ce fait les services AWS qui assurerons la sécurité sont :

- la création de rôle IAM en partant du moindre privilège
- l'utilisation de Trusted Advisor aident à identifier des moyens d'optimiser l'infrastructure AWS, d'améliorer la sécurité et les performances, de réduire les coûts totaux et de surveiller les limites de service.
- la mise en place du multi factor authentication (MFA)
- Le cryptage des buckets S3 et de glacier lors de la création pour mettre un accent sur la sécurité des données.
- Mise en place du service AWS WAF (Web application firewall) qui joue le rôle du pare-feu pour les applications web.
- Configuration des groupes de sécurités et de Network access control list (NACL) pour limiter les trafic entrant et sortant.

Par ailleurs, Rocket Cloud impose contractuellement le même niveau de protection des Données à caractère personnel à ses sous-traitants (prestataires, fournisseurs, etc.).

Enfin, Rocket Cloud s'engage à respecter tout autre principe s'imposant au regard de la réglementation applicable en matière de protection des Données personnelles, et plus précisément concernant les droits conférés aux Personnes concernées, les durées de conservation des Données à caractère personnel ainsi que les obligations relatives aux transferts trans-frontaliers de Données à caractère personnel.

Rocket Cloud s'engage à conserver les Données à caractère personnel des Personnes concernées pour une durée n'excédant pas celle nécessaire à l'accomplissement des finalités pour lesquelles elles sont traitées, augmentée du délai de prescription légale. De plus, Rocket Cloud conserve les Données à caractère personnel des Personnes concernées conformément aux durées de conservation imposées par les lois applicables en vigueur, le cas échéant.

## 4.4 Norme de sécurité dans le cloud

Avec la révolution numérique, le monde digital a vu la quantité de données traitées augmenter de manière exponentielle. Ces données sont aujourd'hui devenues l'une des principales richesses des entreprises.

Bien souvent, la question n'est plus de savoir « si » le virage vers le cloud doit être amorcé, mais plutôt « comment » : il s'agit là d'une décision stratégique et cruciale pour

la gestion effective des données [5]. Néanmoins, cette dernière doit s'accompagner d'un maximum de garanties quant à la protection des données.

## 4.5 Gestion de risques

La matrice de gestion de risque [6] permet d'identifier, évaluer et hiérarchiser les risques lié aux activités d'une organisation. Conformément à notre politique d'anticipation nous traitons de risques spécifiques dans la matrice des risques lié au projet et leurs traitements.

Risque	Probabilité de 1 = Très important 4 = Très probable	Gravité 1 = Faible 4 = Très grave	Indice de risque (IRI)	IRI
L'organisation de l'équipe n'est pas apte à faire face à une situation de stress (1)	2	4	4	Secondaire
Un de membre de l'équipe se démotive ou se désintègre du projet (2)	3	3	9	Important
Difficulté lié à la gestion du budget (3)	3	4	12	Très important
L'infrastructure ne correspond pas aux attentes du client (4)	3	4	12	Très important
Perte de donnée lors de la migration (5)	2	4	8	Important
Manque d'implication des utilisateurs (6)	1	3	3	Mineur
Manque des collaborateurs compétents (7)	1	4	4	Secondaire

FIGURE 4.1 – Matrice des risques

Les remédiations sont les suivantes :

- priorité (1) : mise en place d'une cellule de suivi psychologique
- priorité (2) : remplacement par un collaborateur ayant le même profil
- priorité (3) : calcul des coûts prévisionnelles avec les outils dédiés
- priorité (4) : informer le client à chaque processus
- priorité (5) : mise en place d'un serveur de sauvegarde avant toute manipulation
- priorité (6) : équipe des formateurs spécialisés dans la pédagogie en entreprise
- priorité (7) : faire appel à des consultants de niveau supérieur

## **Bloc 2 : Intégration de l'infrastructure Medicarche dans le cloud**

# Chapitre 5

## Environnement de travail

L'environnement de travail qui a permis de mettre en place le déploiement de l'infrastructure de l'entreprise Medicarche est composé d'une machine hôte dont le système d'exploitation est Microsoft Windows 10. La machine hôte est une machine dont le type de processeur est un i5 composé de 8 cœurs physique et 4 cœurs logique, d'une mémoire RAM de 16 gigabyte et d'un disque dur de 300 gigabyte.

Comme hyperviseur nous avons utilisé VirtualBox qui est un hyperviseur open source. Pour faciliter la communication au niveau réseau nous utilisons deux cartes réseaux. La première carte réseau est configuré en utilisant l'option NAT qui permettra la communication de la machine virtuel hôte vers internet et la deuxième carte réseau est configuré avec l'option hôte privée pour faciliter la communication entre la machine virtuelle et la machine physique.

Le déploiement a été réalisé grâce à Vagrant qui est un outil de création et de configuration des environnements de développement virtuels qui facilite aussi l'automatisation. Avec Vagrant on peut déployer des systèmes d'exploitation légère, moins gourmande en ressource en quelques minutes. A l'aide de Vagrant nous avons déployé la machine virtuelle avec les caractéristiques suivantes :

- Système d'exploitation Linux Ubuntu Focal 20.04
- Disque dur de 100 gigabytes
- Mémoire RAM de 10 gigabytes
- 12 vCPUs
- Adresse IP 192.168.33.16

Visual Code est un environnement de développement intégré puissant qui facilite la création de scripts. Pour administrer la machine hôte qui héberge le cloud privé de l'en-

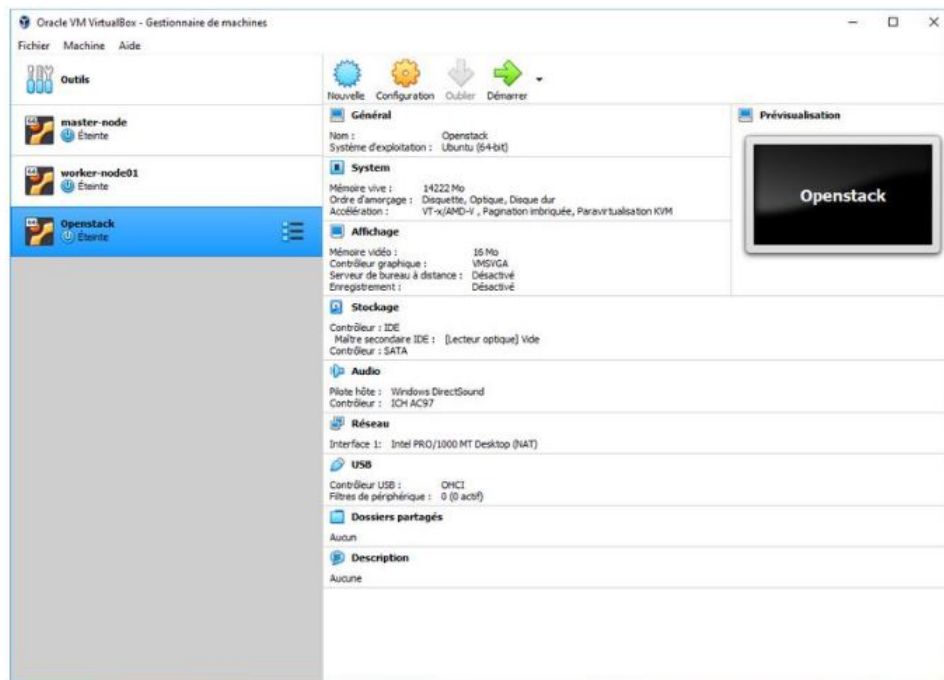


FIGURE 5.1 – caractéristique machine virtuelle

treprise Medicarche nous avons installé des plugins. Parmi les extensions que nous avons installées nous avons RemoteSSH une extension qui permet de se connecter en mode SSH dans les machines virtuelles se trouvant dans le cloud privé de l'entreprise Medicarche pour pouvoir effectuer des actions d'administration si cela s'avère nécessaire. Packer est une solution open source permettant de construire des images machine pour de multiples plateforme cloud. Pour construire les images que nous allons utiliser dans Openstack premièrement nous avons récupérer une image Linux Ubuntu Bionic 18.04 sur le site officiel de Openstack avec le format QCOW2. Pour personnaliser l'image nous avons utiliser Packer en définissant un utilisateur par défaut et le mot de passe, la capacité maximale de mémoire RAM, de disque dur, le format, le format du clavier, la langue du système d'exploitation et le nombre de processeur pouvant être utilisé. Git est un logiciel de gestion de versions décentralisé. C'est un logiciel libre et gratuit. Elle nous a été utile pour faire du versioning des scripts utilisé tout au long du déploiement de l'infrastructure. Nous mettrons à votre disposition tous les scripts utilisés pour déployer le cloud privé de Medicarche.



FIGURE 5.2 – Environnement

# Chapitre 6

## Procédure d'intégration de l'infrastructure Medicarche

L'intégration de l'infrastructure se fait en utilisant le concept de l'infrastructure as a code. De la mise en place de l'infrastructure Openstack au déploiement des applications nous avons utilisé des scripts bash pour automatiser l'installation.

Le script est écrit de sorte à automatiser :

- Le déploiement de l'infrastructure Openstack
- La création des instances
- La création des paires de clé RSA pour les instances
- La création des règles de sécurité
- Le clonage et le téléversement de l'image Linux Ubuntu et son déploiement
- La configuration de la connexion SSH de chaque instance pour assurer le déploiement des applications qui sont Syncthing, Nextcloud, Odoo et le site de l'entreprise Medicarche.

Nous avons pensé à la mise en place d'un serveur mandataire pour permettre aux employés de Medicarche d'avoir accès aux applications de manière sécurisée. Avant d'entrer dans le vif du sujet nous aimerons faire une pique de rappel concernant l'architecture de base présenté lors de la conception de l'infrastructure Medicarche. Cette Figure 2 - environnement 6 architecture représente les besoins réels effectué lors de la rédaction du cahier de charge. Lors de la conception de la plateforme de Medicarche, nous avons proposé deux types de solution cloud qui sont AWS un fournisseur public et Openstack un Cloud de type privée. L'entreprise Medicarche avait opté pour Openstack lors de l'appel d'offre.

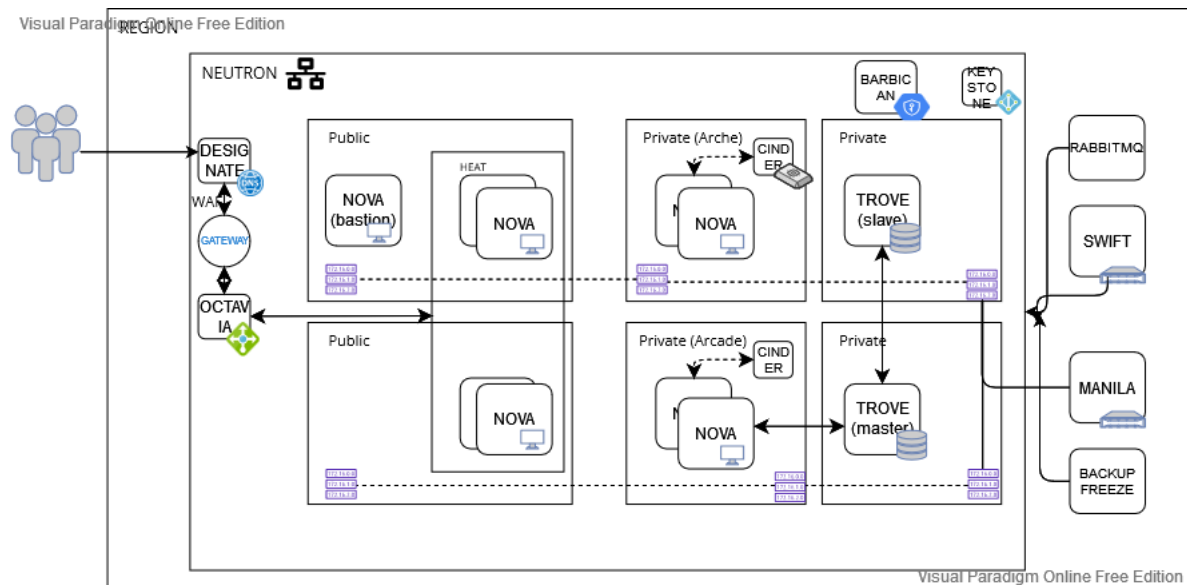


FIGURE 6.1 – Infrastructure OpenStack

À la suite des difficultés rencontrées en rapport avec les performances de la machine virtuelle hôte où s'exécute Openstack nous sommes obligé d'utiliser que des services qui nous permettront d'avoir une maquette qui fonctionne correctement à l'aide du script de déploiement et par après une fois que le problème résolu nous pourrions revenir sur la maquette de base.

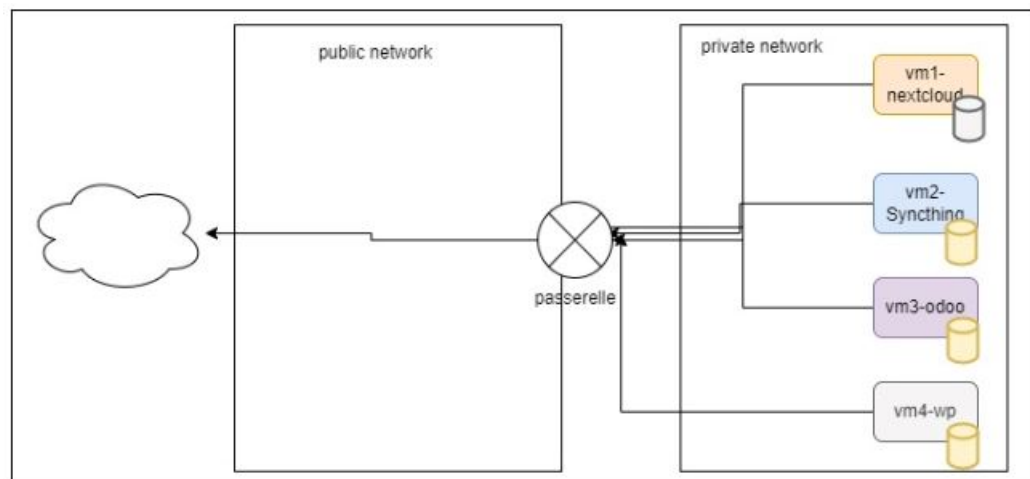


FIGURE 6.2 – Maquette déployée

Le déploiement de l'infrastructure Medicarche a été scripté de bout en bout. Pour commencer le déploiement on a juste exécuté la commande `vagrant up` une commande de l'outil `vagrant` qui permet de créer une machine virtuelle. Nous avons provisionné le script



de déploiement dans le fichier `vagrantfile` afin d'automatiser l'installation de Openstack ainsi que le déploiement des applications et du site web.

```
1  Vagrant.configure("2") do |config|
2    # installer le plugin vagrant plugin install vagrant-disksize
3    config.disksize.size = '100GB'
4    config.vm.define "openstack" do |os|
5      os.vm.box = "bento/ubuntu-20.04"
6      os.vm.hostname = "openstack"
7      #os.vm.provision "docker"
8      os.vm.box_url = "bento/ubuntu-20.04"
9      os.vm.network :private_network, ip: "192.168.33.16"
10     os.vm.provider :virtualbox do |v|
11       v.customize ["modifyvm", :id, "--natdnshostresolver1", "on"]
12       v.customize ["modifyvm", :id, "--natdnsproxy1", "on"]
13       v.customize ["modifyvm", :id, "--memory", 10000]
14       v.customize ["modifyvm", :id, "--name", "openstack"]
15       v.customize ["modifyvm", :id, "--cpus", "12"]
16     end
17     os.vm.provision "shell", path: "scripts/openstack.sh"
18   end
19 end
```

FIGURE 6.3 – Provision de la machine virtuelle

## 6.1 Installation de Openstack

OpenStack est un ensemble de logiciels open source permettant de déployer une infrastructure de type cloud privé en suivant le model infrastructure en tant que service (IaaS). Une fois l'environnement Openstack installé, les credantials nous sont fournis afin d'accéder à la console en tant qu'administrateur. Par défaut Openstack configure la partie réseau en créant un sous réseau privé, un sous réseau public, la table de routage et d'autres services pour ne citer que ceux-là. La commande `iptables` nous permet d'autoriser le trafic venant de Openstack vers internet.

```

1  #!/bin/bash
2
3  echo "Bienvenue dans l'installation automatisée de l'infra medicarche"
4  echo 'debconf debconf/frontend select Noninteractive' | debconf-set-selections
5  sudo apt-get install -y -q
6  sudo apt-get install dialog apt-utils -y
7  sudo snap install microstack --edge --devmode
8  sudo microstack init --auto --control
9  sudo apt-get install git sshpass -y
10
11 sudo iptables -t nat -A POSTROUTING -s 10.20.20.1/24 ! -d 10.20.20.1/24 -j MASQUERADE
12 sudo sysctl net.ipv4.ip_forward=1
13
14 #Recuperation des access pour se connecter à la console
15 sudo snap get microstack config.credentials.keystone-password
16
17 #Recuperation des scripts d'installation des vms et l'installation des applications
18 git clone https://gitlab.com/Genuiz/medicopen.git
19 cd medicopen
20 source auto.sh

```

FIGURE 6.4 – Script d'installation Openstack

### 6.1.1 Tableau de bord Openstack

Le tableau de bord permet de visualiser l'ensemble de ressources de l'infrastructure. Cela nous permet aussi de garder un œil sur l'évolution de l'infrastructure. Nous pouvons avoir facilement une vue sur les instances en cours d'utilisation, la quantité des vCPUs, la quantité de la RAM alloué aux instances en cours d'utilisation, les volumes, les groupes de sécurités, les sous réseaux, les ports, les routeurs ainsi les adresses IP publique.

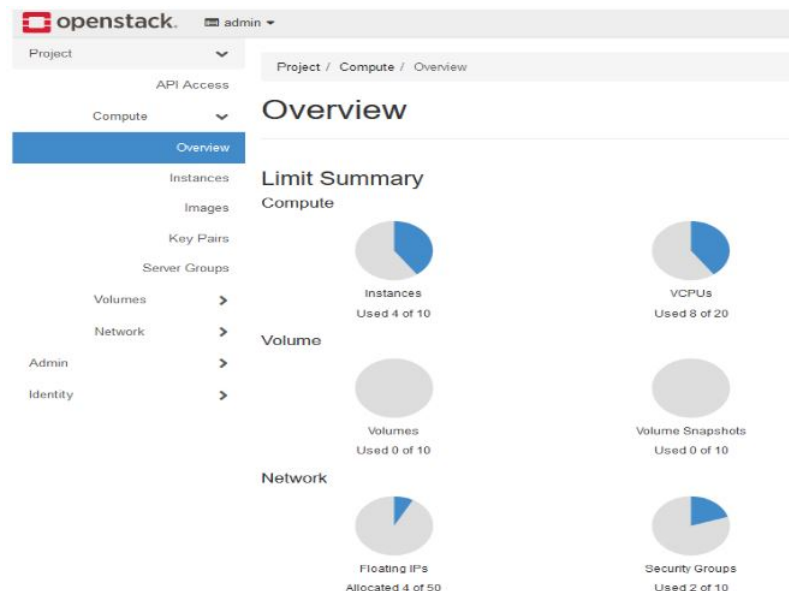


FIGURE 6.5 – Tableau de bord Openstack

### 6.1.2 Topologie réseau dans Openstack

Lors de l'installation de Openstack plusieurs fonctionnalités sont installées par défaut. Une topologie réseau représentant l'architecture du réseau. Nous avons utilisé un sous réseau privé et un sous réseau public. Pour de raison de sécurité, nous avons déployer les machines virtuelles contenant les applications web dans le réseau privé et nous avons pensé à les attribuer une adresse IP privé dont la passerelle est 192.168.222.1. Pour permettre la communication avec internet, un routeur virtuel fait office de passerelle entre le réseau privé et le sous réseau public. L'adresse IP de la passerelle est 10.20.20.224.

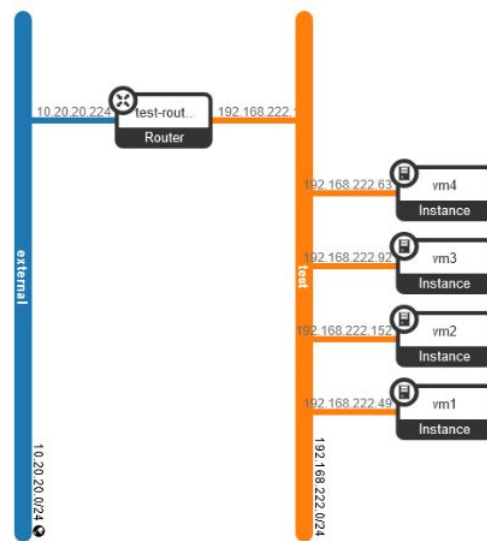


FIGURE 6.6 – Topologie Réseau Openstack

### 6.1.3 Les gabarits

Openstack permet de personnaliser des gabarits qui sont utilisés pour déployer les instances. Le plus petit gabarit par défaut consomme 512 Mo de mémoire par instance. Dans le contexte du déploiement de la plateforme Mediacarhe nous avons créé différent type de gabarit qui permettrons d'accueillir les applications. Lors de la création du gabarit on définit les paramètres suivants :

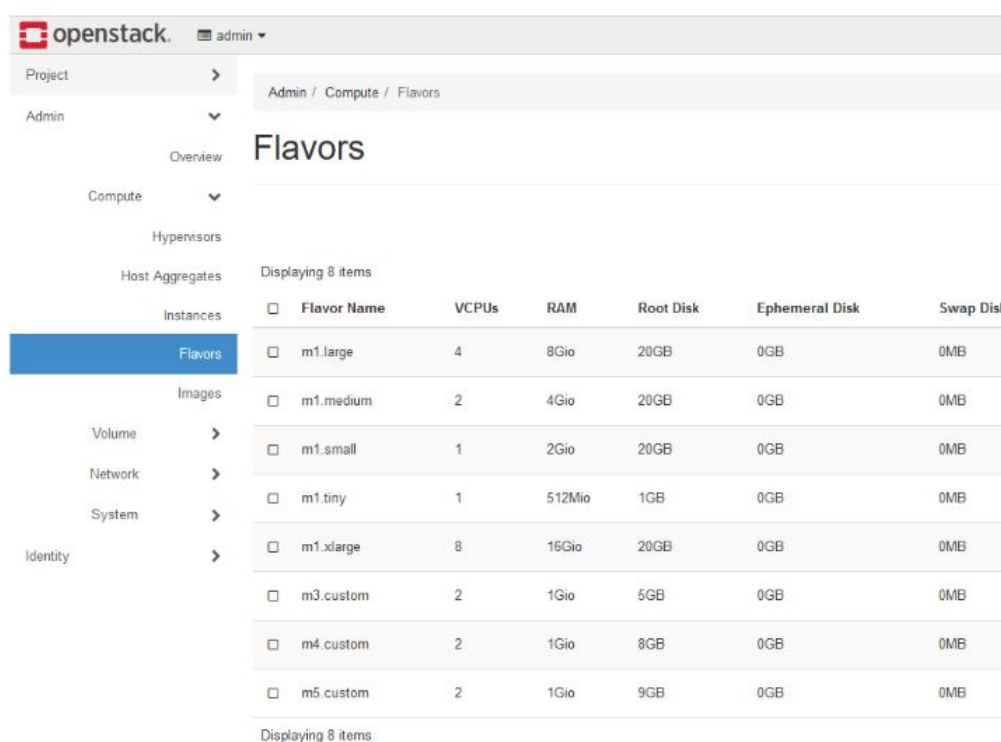
- le nom
- le vCPU
- la RAM

- le Disque dur principal
- possibilité d'ajouter un disque dur éphémère
- la portée public ou privée
- le swap

On a aussi la possibilité d'ajouter des metadatas pour mieux identifier le gabarit.

```
1 #Creation des gabarits qui accueilleront les vms contenant des applications
2 microstack.openstack flavor create m3.custom --id auto --ram 1024 --disk 5 --vcpus 2
3 microstack.openstack flavor create m4.custom --id auto --ram 1024 --disk 8 --vcpus 2
4 microstack.openstack flavor create m5.custom --id auto --ram 1024 --disk 9 --vcpus 2
```

FIGURE 6.7 – script création gabarit



Flavor Name	VCPUs	RAM	Root Disk	Ephemeral Disk	Swap Disk
m1.large	4	8Gio	20GB	0GB	0MB
m1.medium	2	4Gio	20GB	0GB	0MB
m1.small	1	2Gio	20GB	0GB	0MB
m1.tiny	1	512Mio	1GB	0GB	0MB
m1.xlarge	8	16Gio	20GB	0GB	0MB
m3.custom	2	1Gio	5GB	0GB	0MB
m4.custom	2	1Gio	8GB	0GB	0MB
m5.custom	2	1Gio	9GB	0GB	0MB

FIGURE 6.8 – gabarits openstack

### 6.1.4 Les images

Par défaut Openstack offre une image par défaut Cirros qui permet d'effectuer des tests au niveau de la couche réseau. Nous avons automatisé la création et le téléversement de l'image dans Openstack. Une image Linux Ubuntu Bionic sera utilisée par tous les

instances. Lors du téléversement de l'image on définit le nom du système d'exploitation, la visibilité et le format du disque (QCOW2).

```
1 #Clonage du systeme d'exploitation Ubuntu dans un repos d'istant afin de televerser l'OS dans Microstack
2 git clone https://gitlab.com/Genuiz/os-ubuntu-openstack.git
3 microstack.openstack image create --container-format bare --disk-format qcow2 --file \
4 ./os-ubuntu-openstack/focal-server-cloudimg-amd64.img ubuntu
```

FIGURE 6.9 – script déploiement images

Pour pouvoir mettre en place cette solution nous avons créé un dépôt git pour stocker les images que nous allons utiliser lors de l'automatisation. On commence par cloner le dépôt à la racine puis on exécute la commande qui microstack.openstack pour crée l'image ubuntu depuis le dossier os- ubuntu-openstack.

### 6.1.5 Les instances

Les instances dans Openstack sont des machines virtuelles qui s'exécutent dans un sous réseau. Nous avons déployé les applications "web" Odoo, Nextcloud, Syncthing et un serveur Apache pour le site web de l'entreprise Medicarche. Pour chaque application nous avons utilisé un gabarit spécifique afin de respecter le minimum requis de ressources (CPU, RAM, Disque) tel qu'il est spécifié dans la documentation des applications.

Nous avons pensé à mettre les machines virtuelles dans un même sous réseau privé et avons utilisé un groupe de sécurité pour apporter cette dimension à notre architecture. Le groupe de sécurité a pour objectif de mettre en place le principe de moindre privilège c'est-à-dire de n'autoriser que les ports nécessaires en entrée. Parmi les ports autorisés pour atteindre les machines virtuelles nous avons :

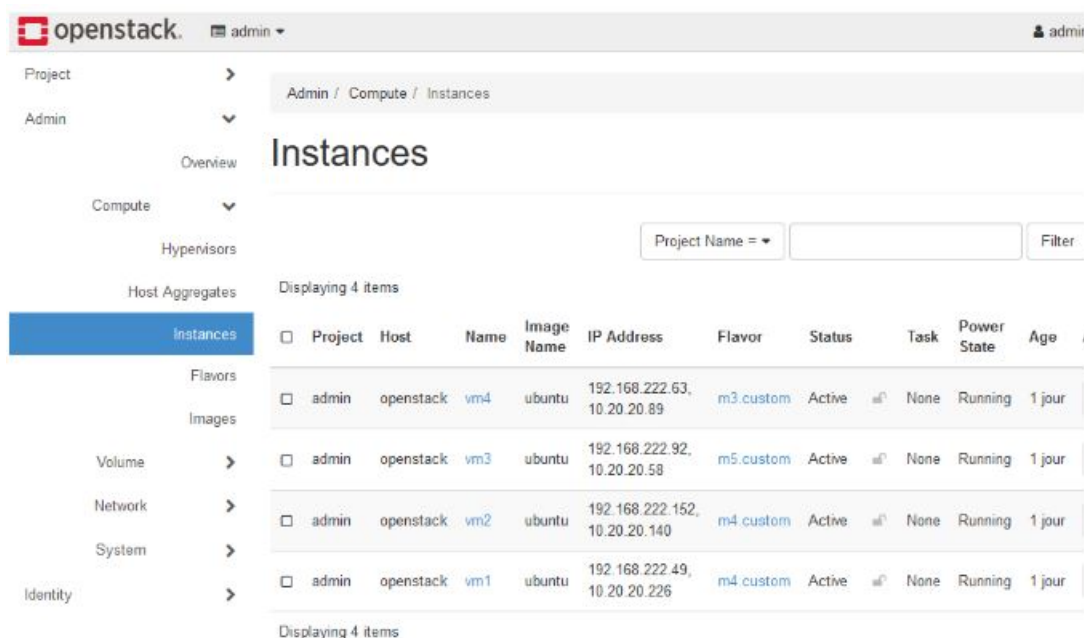
- Le port 8088 qui permet d'atteindre le site web de l'entreprise ;
- Le port 8087 qui permet d'atteindre l'application Odoo ;
- Le port 8806 qui permet de communiquer avec l'application Nextcloud ;
- Le port 8885 qui permet de communiquer avec l'application Syncthing ;
- Le port 22 pour assurer une connexion sécurisée en SSH ;
- Le Port 80 pour autoriser la communication en http.

Les machines virtuelles ont toutes une adresse IP privée et une adresse IP publique afin de communiquer sur le réseau privé (communication entre les machines virtuelles) et

sur le réseau externe pour la communication avec l'extérieur. Openstack propose un outil pour le log de toutes les actions effectuées sur la machine virtuelle. Elles peuvent être auditées grâce à cette fonctionnalité. Les machines virtuelles utilisent une clé privée créée lors du déploiement cela permet de mettre un accent sur la sécurité. Le script de la Figure 8 donne un aperçu de la création de la machine virtuelle et l'association d'une adresse ip virtuelle.

```
2 microstack.openstack server create --network test --security-group private-sg \
3 --key-name sto4_key --flavor m4.custom --image ubuntu $machine
4 microstack.openstack floating ip create external
```

FIGURE 6.10 – script de création de la machine virtuelle



Project	Host	Name	Image Name	IP Address	Flavor	Status	Task	Power State	Age
admin	openstack	vm4	ubuntu	192.168.222.63, 10.20.20.89	m3.custom	Active	None	Running	1 jour
admin	openstack	vm3	ubuntu	192.168.222.92, 10.20.20.58	m5.custom	Active	None	Running	1 jour
admin	openstack	vm2	ubuntu	192.168.222.152, 10.20.20.140	m4.custom	Active	None	Running	1 jour
admin	openstack	vm1	ubuntu	192.168.222.49, 10.20.20.226	m4.custom	Active	None	Running	1 jour

FIGURE 6.11 – les instances dans openstack

### 6.1.6 Les groupes de sécurité

Un groupe de sécurité agit en tant que pare-feu virtuel pour les instances afin de contrôler le trafic entrant et sortant. Nous avons mis en place un groupe de sécurité nommé private-sg afin d'autoriser que les ports et les adresses IP nécessaires à la communication des instances (voir plus haut). Afin de resserrer le trafic entrant nous avons appliqué la stratégie de moindre privilège en autorisant que le strict nécessaire.

Openstack offre une interface d'administration des groupes de sécurité, on peut ajouter, modifier ou supprimer le trafic entrant ou le trafic sortant. En cas de dépannage rapide cela permettra à la DSI de Medicarche de pouvoir intervenir pour pouvoir régler des problèmes.

### 6.1.7 Les paires de clé

Pour avoir accès à la machine virtuelle et pouvoir faire les opérations d'administration, nous avons, lors de la création des instances, mis en place un script qui permet de créer une paire de clés RSA et de les associer à l'instance. Ce type de connexion permet de renforcer la sécurité; ainsi seuls les administrateurs de Medicarche pourrons avoir accès aux instances pour effectuer les taches de maintenances. Le script de la Figure 9 permet d'automatiser la création d'une clé pour se connecter en SSH dans la machine virtuelle. On crée la paire de clé en attribuant le droit au propriétaire de la clé et en modifiant le fichier en lecture seule.

```
1
2 #Creation de la pair de cle rsa pour securiser la connexion vms tournant sur Microstack de puis l'hote.
3 ssh-keygen -q -C "" -N "" -f open_key
4 sudo chown vagrant open_key
5 sudo chmod 400 open_key
6 microstack.openstack keypair create --public-key open_key.pub sto4_key
7 microstack.openstack keypair list
```

FIGURE 6.12 – script création de pair de clé

### 6.1.8 Gestions des utilisateurs

TODO

## 6.2 Déploiement des applications de l'entreprise Medicarche

Pour assurer le partage des documents, la synchronisation des données entre les services, les gestions des activités de l'entreprise nous avons mise en place un script qui permet de procéder à l'installation, la configuration ainsi que le déploiement des applications dans les machines virtuelles. Pour répondre à la demande de l'entreprise nous avons proposé les applications suivantes :

- Odoo;
- NextCloud;



- Syncthing ;
- Wordpress.

Nous donnons un aperçu des différentes fonctionnalités de chacune de ces applications un peu plus loin dans le texte et au moment des explications sur leurs déploiements. L'architecture de déploiement reste la même pour toutes les applications. Elle est donc générique. Le déploiement de la base de données et du serveur web se fait dans l'instance. Cela n'est pas une solution qui permet de rendre l'architecture hautement disponible et tolérante aux pannes mais à la suite des contraintes rencontrées en termes de performance de la machine hôte et du nombre réduit de machines virtuelles pouvant être utilisées nous avons préféré déployer les applications en favorisant une architecture monolithe.

### 6.2.1 Installation d'Odoo

Odoo est initialement un progiciel open-source de gestion intégré comprenant de très nombreux modules permettant de répondre à de nombreux besoins de gestion des entreprises, ou de gestion de la relation client. Dans le contexte Medicarche, l'application Odoo utilise une base de données PostgreSQL installée en local dans la machine virtuelle. Pour exposer l'application web et permettre l'accès aux collaborateurs, l'utilisation du reverse proxy ou serveur mandataire a été mis en place afin d'exposer l'application web de manière sécurisée.

### 6.2.2 Installation de Nextcloud

Nextcloud est un logiciel libre de site d'hébergement de fichiers et une plateforme de collaboration. La solution NextCloud apporte un haut niveau de protection et de contrôle des informations et communications dans l'entreprise. Les utilisateurs peuvent conserver toutes leurs données sur leurs serveurs internes, y compris les métadonnées. Dans le contexte Medicarche, NextCloud utilise en local un serveur Apache avec une base de données MySQL. Ces services sont tous installés dans une seule machine virtuelle. De même, nous avons mis en place un serveur mandataire pour exposer l'application web afin de la rendre accessible sur internet de manière sécurisée.

### 6.2.3 Installation de Syncthing

Syncthing est une application de synchronisation de fichiers pair à pair open source disponible pour Windows, Mac, Linux, Android, Solaris, Darwin et BSD. Aucun compte



ni enregistrement préalable à l'utilisation auprès d'un tiers n'est nécessaire, ni même optionnelle. L'application tourne localement dans la machine virtuelle en utilisant l'adresse IP 127.0.0.1. Pour avoir accès depuis l'extérieur de la machine virtuelle, on doit utiliser le reverse proxy pour pouvoir exposer l'application à tous les collaborateurs de l'entreprise Medicarche.

#### 6.2.4 Site web Medicarche

Wordpress est un système de gestion de contenu (CMS) libre et open-source. Ce logiciel écrit en PHP repose sur une base de données MySQL. Le site de l'entreprise est exposé sur internet permettant à toute personne le désirant d'y avoir accès. Comme pour les autres applications web, le site web de l'entreprise est déployé sur un serveur Apache et utilise une base de données MySQL. Nous avons veillé à appliquer aussi le reverse proxy afin d'exposer le site sur internet.

### 6.3 Description du plan des tests

Dans le cadre du projet de déploiement il est important de passer des tests. Plus précisément, nous avons effectué un plan de test de capacité du système, un test de montée en charge des applications ou du site web de l'entreprise Medicarche et un test de stress du système. Nous documentons cela dans les lignes qui suivent.

#### 6.3.1 Test de montée en charge

Le test de montée en charge que nous prévoyons d'effectuer est un test au cours duquel nous aurons simulé un nombre d'utilisateurs sans cesse croissant de manière à déterminer quelle charge limite le système est capable de supporter sans tomber. Nous effectuerons un test sur l'application Odoo, Nextcloud, Syncthing et le site web de l'entreprise Medicarche. Nous avons prévu de mettre en place un script en utilisant l'outil h2load. Une fois l'utilitaire installé, on a à exécuter la commande décrite à la Figure 10, que l'on prévoit de scripter, pour toutes les autres applications de la plateforme Medicarche. Dans ce script nous simulons 100 clients qui produiront au total 10000 requêtes HTTP. En résumé, le script de la Figure 10 permet de faire le test de montée en charge d'une machine virtuelle en passant en paramètre le nombre de clients et le nombre de requêtes.

```

vagrant@openstack:~/medicopen$ h2load -n10000 -c100 -t2 http://192.168.33.16:8088/
starting benchmark...
spawning thread #0: 50 total client(s). 5000 total requests
spawning thread #1: 50 total client(s). 5000 total requests
Application protocol: h2c

finished in 12.96ms, 0.00 req/s, 3.56MB/s
requests: 10000 total, 100 started, 0 done, 0 succeeded, 10000 failed, 10000 errored, 0 timeout
status codes: 0 2xx, 0 3xx, 0 4xx, 0 5xx
traffic: 47.17KB (48300) total, 0B (0) headers (space savings 0.00%), 0B (0) data

time for request:      min      max      mean      sd      +/- sd
time for connect:    281us    2.92ms    1.53ms    780us    57.00%
time to 1st byte:      0us      0us      0us      0us      0.00%
req/s                : 0.00      0.00      0.00      0.00    100.00%
vagrant@openstack:~/medicopen$

```

FIGURE 6.13 – test de montée en charge

### 6.3.2 Test de stress du système

Pour s'assurer que les gabarits choisis pour accueillir les applications web de l'entreprise Medicarche répondent bien au minimum des capacités requises, nous mettons en place ce type de test qui a pour objectif de stresser le CPU, la mémoire RAM, le I/O et le disque. Pour cela nous utilisons l'outil stress and stress-ng. L'installation s'effectue en ligne de commande et on pourra voir le résultat sur l'interface CLI. Sur la Figure 11 nous pouvons voir sur le tableau de bord les points importants comme le trafic du réseau, les nombres des requêtes, le nombre des nouveaux utilisateurs, des tentatives de connexion.

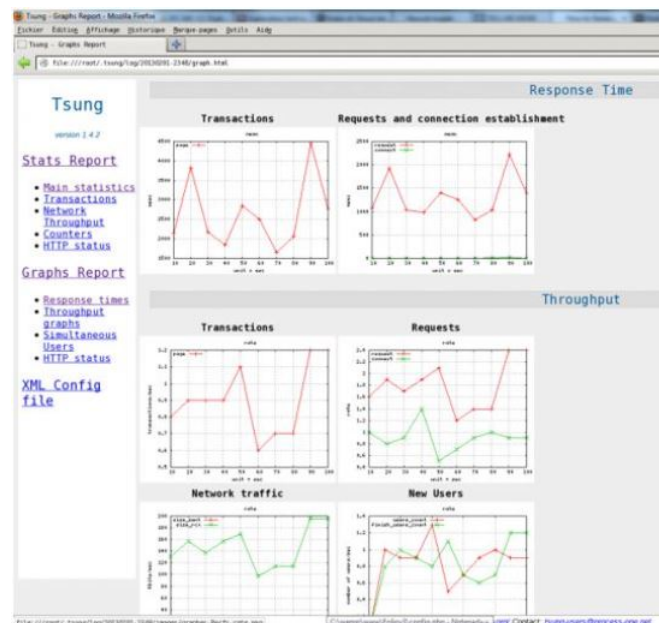


FIGURE 6.14 – résultat du test

---

### 6.3.3 Test de performance

Après avoir installé les applications web de l'entreprise Medicarche, on doit vérifier que le système répond normalement aux attentes du client. Pour s'assurer que c'est réellement le cas, nous avons choisi d'utiliser l'outil Tsung qui est approprié pour ce type de test. Tsung est un outil de test de performances permettant de réaliser des benchmarks massifs. De manière résumée, Tsung est un outil qui nous permettra de faire un rapport sur les statistiques du système, des transactions, du réseau, du débit et même des statuts liés aux requêtes HTTP.

## **Bloc 3 : Administration de l'infrastructure Medicarche**

# Chapitre 7

## Solution de supervision des VMs

Parmi les solutions les plus utilisées, d'après l'outil Google Trend, pour faire de la supervision, sont Prometheus, Nagios, InfluxDB, Grafana. Dans cette section, nous allons décrire les fonctionnalités de haut niveau de ces outils.

### 7.1 Introduction

la surveillance du cloud est une méthode d'examen, d'observation et de gestion du flux opérationnel dans une infrastructure informatique basée sur le cloud. Des techniques de gestion manuelles ou automatisées permettent de confirmer la disponibilité et les performances des sites Web, des serveurs, des applications et d'autres infrastructures en nuage. Cette évaluation continue des niveaux de ressources, des temps de réponse des serveurs et de la vitesse a pour objectif de prévoir un état problématique éventuel d'un service cloud avant que des problèmes plus graves surviennent, par exemple la défaillance totale de tous les services cloud.

Dans ce qui suit nous utilisons des outils bien connus dans la communauté pour réaliser de la supervision cloud, outils déployés soit manuellement soit automatiquement, pour surveiller soit les VM, donc le système d'exploitation de la VM (sous section 6.2), soit de manière automatique (sous section 6.3), pour surveiller le cloud i.e. les services disponibles pour OpenStack / MicroStack.

#### 7.1.1 Grafana

Grafana est un outil qui permet de visualiser les données à travers un tableau de bord. Il permet de réaliser des tableaux de bord et des graphiques depuis plusieurs sources dont des

bases de données temporelles comme Graphite, InfluxDB, Prometheus et Elasticsearch. Grafana est multiplateforme. Il s'appuie sur un stockage dans une base de données. Il peut être déployé avec Docker. Il est écrit en Go, langage de programmation promulgué par Google, et dispose d'une API HTTP complète.

### 7.1.2 Prometheus

Prometheus est un logiciel libre de surveillance informatique et générateur d'alertes. Il enregistre des métriques en temps réel dans une base de données de séries temporelles (avec une capacité d'acquisition élevée) en se basant sur le contenu de points d'entrée exposés à l'aide du protocole HTTP. Prometheus fonctionne de la manière suivante :

- Plusieurs agents (exporteurs), qui s'exécutent généralement sur les machines à surveiller,
- exposent les métriques de suivi ;
- Prometheus sert alors pour la centralisation et le stockage des métriques ;
- Alertmanager déclenche l'émission d'alertes en fonction de règles métiers.

Pour visualiser les métriques, Grafana ou Zabbix peuvent être utilisés pour la restitution des métriques sous la forme de tableaux de bord. Prometheus a son propre langage de requête, PromQL, utilisé pour créer des tableaux de bord et les alertes.

### 7.1.3 ELK Stack

ELK Stack est l'une des principales solutions open-source de monitoring et de gestion des logs pour les entreprises qui souhaitent bénéficier des avantages de la centralisation des logs. C'est un outil d'analyse de logs composé de 3 logiciels : Elasticsearch, Logstash et Kibana.

- Elasticsearch permet d'extraire les données ;
- Logstash est un outil pour la saisie, le traitement et la remontée des données logs.
- Sa fonction est d'analyser, filtrer et de découper les logs pour les transformer en documents formatés à destination d'Elasticsearch ;
- Kibana est un outil de visualisation.

Nous avons pu déployer la stack ELK afin de centraliser les logs et de les traiter. Cela permet à l'entreprise MediArche d'avoir une trace de chaque action effectuée dans l'infrastructure.

Nous avons pensé également à rajouter l'agent packetbeat qui est un analyseur de paquets réseau en temps réel qu'on peut utiliser avec Elasticsearch pour fournir un système de surveillance des applications et d'analyse des performances.

#### 7.1.4 Solutions de supervision de l'infrastructure Openstack

Il existe plusieurs solutions, payantes et celles dite open source, pour effectuer la supervision d'une infrastructure OpenStack. En creusant un peu plus le sujet par de la veille technologique, nous avons trouvé que les solutions les plus utilisées par les entreprises concernent Prometheus/Grafana, Zabbix, InfluxBD et la stack ELK, pour ne citer que celle-là. L'infrastructure Openstack peut alors être monitorée des plusieurs manières. La

première solution est d'installer les binaires de prometheus dans une machine virtuelle dédiée et d'installer les agents (Node exporter) dans chaque VM de l'infra. Cette solution permet simplement de récupérer les métriques venant de chaque machine virtuelle à travers les agents déployés au préalable. La deuxième solution permet de superviser toute

l'infrastructure (l'hyperviseur) Openstack en créant, selon la terminologie consacrée, un job qui permet de rendre le service de découverte (discovery). Cela permet de récupérer toutes les métriques de l'infrastructure Openstack, comme par exemple les instances, network,... Cette solution a pour avantage de faire la supervision de toute l'infrastructure, depuis les VMs jusqu'à l'hyperviseur OpenStack, dans un seul et même tableau de supervision.

#### 7.1.5 GLPI

GLPI (sigle de Gestionnaire Libre de Parc Informatique) est un logiciel libre de gestion des services informatiques (ITSM) et de gestion des services d'assistance (issue tracking system et ServiceDesk). Cette solution libre est éditée en PHP et distribuée sous licence GPL. Elle permet de visualiser l'évolution du parc informatique grâce à des plugins.

Le plugin FusionInventory utilisé dans le cas de notre projet permet de faire l'inventaire et la maintenance d'un parc informatique. Il recupere les informations des composants du parc informatique à travers l'agent FusionInventory installé dans chaque ordinateur, machine virtuelle ou tout autre composant du parc. Concernant le ServiceDesk, Glpi

---

permet de mettre en place gestion des incidents, de problèmes et des demandes. Nous avons la possibilité de créer des tickets et d'en faire le suivi. Dans le contexte du projet Médicarche, nous avons mis en place la gestion de parc informatique c'est à dire le recensement des ordinateurs ou des outils informatiques qui composent le parc et le ServiceDesk pour la gestion des tickets en interne. Le contact de la DSI pour les incidents, les problèmes ou les demandes passera par le biais de Glpi car les collaborateurs de l'entreprise Médicarche auront le droit de soumettre un ticket à l'équipe de la DSI.



## **Bloc 4 : Veille et Evolution d'une infrastructure**

# Chapitre 8

## Méthodologie adoptée pour la veille technologique

L'organisation de la veille technologique suit un processus qui s'articule autour de trois grandes étapes qui sont la collecte l'information, l'analyse et la synthétisation et la diffusion de l'information. Dans cette section, nous présenterons les méthodes adoptées, en décrivant ses méthodes de travail et les outils qui interviennent dans les différentes phases de collecte d'information, et bien sûr leurs finalités.

### 8.1 Type d'information recherché et le mode d'accès

Au lieu de visiter de nombreux sites web au risque de manquer de régularité, nous avons jugé de faire venir les media à l'aide d'outils disponibles en ligne pour les utilisateurs, sous forme d'alertes ou de page centralisé (méthode pull). Avec la méthode pull on peut avoir accès à l'information recherché par :

- Des alertes courriel en s'abonnant aux news lettre
- Des listes de diffusion parlant du sujet Agiles, DevOps ou DevSecOps
- Des logiciels de surveillance des pages web comme Google Alerts
- Des flux d'actualité avec l'outil Netvibes qui regroupe les flux d'actualité des différents sites
- Les abonnements aux forums dédiés à la veille technologique

Centraliser l'information sur un seul outil est un gain de temps considérable qui permet de

gagner du temps lors d'une veille technologique. Dans le contexte de l'entreprise Medicarche après avoir les types d'information recherché sera plus accès sur les démarches Agiles et sur l'organisation DevOps ou DevSecOps.

## 8.2 Sources d'informations

Du fait que le temps est précieux en entreprise, il serait judicieux de ne pas se perdre en recherchant l'information sur internet. Pour bien mener les recherches il faut bien cibler les sources. Plusieurs critères permettent de définir la pertinence de l'information. Les critères les plus utilisés selon le site [coursbtsam](#) sont :

- L'identification de la source : l'information dont on a identifié l'auteur ainsi que le support d'origine.
- L'accessibilité de l'information : Une information identifiée doit rester accessible, c'est-à-dire facilement localisée et retrouvée.
- La fiabilité de l'information : Avant toute utilisation, le contenu d'une information doit avoir été vérifié et éventuellement recoupé par redondance.
- Les nouveautés sur le sujet recherché : L'information doit apporter quelque chose de nouveau, d'original, qui augmente les connaissances de l'entreprise.
- Une information précise, exacte et exhaustive : Le collaborateur doit s'assurer de l'exactitude et de la complétude des informations qu'il transmet à son manager.
- Une information actualisée : Une information obsolète diminue son utilité. Sa mise à jour, son actualisation sont des critères importants de pertinence.
- L'utilité de l'information : L'information « utile » au manager est celle qui, face à une situation donnée, va lui permettre de prendre la bonne décision.

Dans le cas d'utilisation d'un outil de veille il est préconisé de faire le choix sur les sources d'informations. Nos sources d'informations utilisées sont :

- Les médias sociaux : fournissent des informations précieuses sur ce que les gens disent du sujet, des services ou des solutions. Ils sont particulièrement utiles car ils donnent un accès direct à la fois aux concurrents de l'entreprise.
- La presse informatique : Leurs contenus indiquent ce que sont les grandes nouveautés. Bien que possiblement orientés selon les sponsors, ils diffusent des informations intéressantes.
- Les études et publications scientifiques sont aussi une très bonne méthode pour avoir accès aux informations à jour.

- Les données issues de centres de recherche et des universités
- Les conférences des Scrum Master et de DevSecOps expérimenté

## 8.3 Organisation, trie et analyse de l'information

La valeur ajoutée de la veille technologique apparaît dans cette phase, une fois les données collectées. Il s'agit de faire en sorte de les structurer de manière cohérente pour qu'elles soient exploitables. En regroupant les informations venant de différentes sources

citées plus haut, nous nous sommes constitué une base des connaissances qui me permet de dresser les points importants concernant le sujet recherché. Le tri et l'analyse de

l'information s'effectue selon la pertinence des sources d'informations. Est-elle une information qui est d'actualité ? La source qui diffuse l'information est-elle une source fiable ? L'information recherchée pourra-t-elle apporter une valeur ajoutée dans la démarche de l'entreprise ?

Pour répondre à cette problématique nous avons utilisé les outils suivants :

- Avec l'outil Netvibes nous avons suivi en temps réel l'actualité de différents sites internet en le regroupant dans l'outil pour avoir un ensemble de contenu concernant un sujet donnée dans le même namespace.
- Nous avons pris le soin de trié les sources afin de l'incorporer dans l'outil Netvibes

Les sites que nous avons utilisés sont :

- <https://www.lemondeinformatique.fr>
- <https://www.contrepoints.org>
- <https://www.tandfonline.com>
- <https://www.atlassian.com>
- <https://thenewstack.io>

## Conclusion

En tant qu'entreprise Rocket Cloud, nous avons analyser, conceptualiser et mise en oeuvre la migration dans le Cloud de l'infrastructure on-premise de MedicArche en proposant deux architectures celui d'AWS et d'Openstack. Dans ces architectures cloud nous avons d écrit différent services qui nous permettra d'avoir un système sécurisé, tolérant aux pannes, évolutive, et ayant la capacité d'absorber la multiplication des sites ainsi que la montée en charge. La migration dans le cloud sera bénéfique pour l'entreprise MedicArche par le fait que le passage dans le cloud de leur infrastructure on-premise permettra 'a l'entreprise de faire des économies, de réduire les coûts d'exploitation des logiciels par leurs utilisations directement en ligne. L'entreprise n'aura pas besoin d'investir dans les équipements (serveur, équipements réseaux, . . .). Une partie de la sécurité et de la maintenance sera assuré par le fournisseur et l'autre partie par l'entreprise elle même. Nous avons mener cette exercice pour proposer un système qui répondant aux besoins de l'entreprise MedicArche qui est celui d'avoir un système évolutif.

# Bibliographie

- [1] Rapport sur l'état du cloud Le monde post pandémie, <https://info.flexera.com/CM-REPORT-State-of-the-Cloud>.
- [2] Calculateur du coût total de possession, <https://www.softwareadvice.com/tco/>.
- [3] Aspects juridiques du cloud computing, [https://www.leclerelouvier-avocats.com/media/filer\\_public/f7/fe/f7fed023-c72c-46e9-92f1-7d3f0659e57ea/cloud\\_computing.pdf](https://www.leclerelouvier-avocats.com/media/filer_public/f7/fe/f7fed023-c72c-46e9-92f1-7d3f0659e57ea/cloud_computing.pdf).
- [4] Politique de protection des données, <https://expertises.ademe.fr/lademe/infos-pratiques/politique-protection-donnees-a-caractere-personnel>.
- [5] Norme de sécurité dans le cloud, <https://www.prosica.fr/blog/131-bonnes-pratiques-pour-la-securite-dans-le-cloud-la-norme-iso-27017.html>.
- [6] La gestion de risque, [https://webcache.googleusercontent.com/search?q=cache:PXDEpNTToTUKJ:htGuide\\_Securite\\_avance\\_Methode.pdf+&cd=16&hl=fr&ct=clnk&gl=fr](https://webcache.googleusercontent.com/search?q=cache:PXDEpNTToTUKJ:htGuide_Securite_avance_Methode.pdf+&cd=16&hl=fr&ct=clnk&gl=fr).

# Annexe A

## Services cloud utilisés

- Route 53 est un service de système de noms de domaine évolutif et hautement disponible.
- Amazon S3 est un site d'hébergement de fichiers proposé par Amazon Web Services. Amazon S3 propose des services de stockage à travers des services Web.
- Amazon Glacier est un site d'hébergement de fichiers proposé par Amazon Web Services. Peu onéreux, Amazon Glacier est conçu pour l'archivage à long terme et les sauvegardes
- EC2 est un service proposé par Amazon permettant à des tiers de louer des serveurs sur lesquels exécuter leurs propres applications web.
- VPC est un groupe de ressources informatiques configurables à la demande dans un environnement de cloud public, qui fournit un certain niveau d'isolement entre les différentes organisations (appelées utilisateurs) qui utilisent ces ressources
- RDS est un service de base de données relationnelle distribué par Amazon Web Services.
- Cloud Watch est un service de surveillance et d'observabilité conçu pour les ingénieurs DevOps, les développeurs, les ingénieurs en fiabilité des sites (SRE), les directeurs techniques et les propriétaires de produits.
- Cloud Trail permet l'administration, la conformité, ainsi que l'audit opérationnel et des risques de votre compte AWS.
- AWS Backup permet de centraliser et d'automatiser la protection des données sur les services AWS et les charges de travail hybrides.
- Amazon EFS offre un stockage de fichiers scalable, destiné à être utilisé avec Amazon EC2.
- AWS Directory permettent de stocker des informations sur les utilisateurs, groupes et périphériques. Les administrateurs les utilisent pour gérer l'accès à des informations et ressources.
- AWS Autoscaling ont la capacité d'ajouter ou de soustraire des ressources d'un groupe. Chez AWS, par exemple, les utilisateurs peuvent créer un groupe Auto-scaling et utiliser

cette fonction pour y ajouter des ressources

- AWS Load Balancer répartit automatiquement le trafic entrant d'applications sur plusieurs cibles et appliances virtuelles dans une, ou plus d'une, zones de disponibilité (AZ).
- AWS Cloud Front est un réseau de diffusion de contenu (CDN) conçu pour des performances élevées, pour la sécurité et pour la simplicité de développement.
- AWS IAM fournit un filtre de contrôle d'accès dans tous les services AWS. Avec IAM, vous pouvez contrôler l'accès aux services et ressources AWS et sous conditions. Avec les politiques IAM, vous pouvez gérer les autorisations de votre main-d'œuvre et de vos systèmes afin de garantir des autorisations limitées.



# Annexe B

## Services Openstack utilisés

- Neutron est un projet OpenStack pour fournir un "réseau en tant que service" entre les périphériques d'interface (par exemple, les vNIC) gérés par d'autres services Openstack (par exemple, nova). Dans AWS, elle correspond au service Amazon VPC (virtual private network).
- Designate est une implémentation Open Source DNS-as-a-Service et fait partie de l'écosystème de services OpenStack pour l'exécution de clouds. Dans AWS elle correspond au service Route 53.
- Octavia est une solution d'équilibrage de charge open source à l'échelle de l'opérateur conçue pour fonctionner avec OpenStack. Dans AWS elle correspond au load balancer.
- Nova est un composant spécifique du logiciel open source OpenStack utilisé pour créer des machines virtuelles. Dans AWS elle correspond à EC2 (elastic cloud computer)
- Trove est une base de données en tant que service pour OpenStack. Il est conçu pour fonctionner entièrement sur OpenStack, dans le but de permettre aux utilisateurs d'utiliser rapidement et facilement les fonctionnalités d'une base de données relationnelle ou non relationnelle sans avoir à gérer des tâches administratives complexes. Dans AWS elle correspond au service RDS (relational database Services).
- Manila est le service OpenStack Shared Filesystems pour fournir des systèmes de fichiers partagés en tant que service. Dans AWS elle correspond au service EFS (Elastic file system).
- Swift est le stockage objet. Il peut connecter les stockages dans différents endroits afin de pouvoir utiliser des objets de données répartis aléatoirement sur des stockages adjacents.
- Le service d'identité d'OpenStack, Keystone, vérifie l'identité de l'utilisateur et fournit des informations sur les ressources auxquelles l'utilisateur a accès. Dans AWS elle correspond à l'IAM (identity and access management).
- Barbican est le service OpenStack Key Manager. Il fournit un stockage, un appropi-

sionnement et une gestion sécurisés des données secrètes. Dans AWS elle correspond au service KMS (key management service).

# Annexe C

## CONTRAT DE SERVICES INFORMATIQUES

ENTRE -----  
-----  
----- (Ci-après appelé(e)  
le client) d'une part

ET : l'entreprise Rocket Cloud ayant son siège sociale au 1 rue Massena Paris 75013. (Ci-après appelé le prestataire de services) d'autre part  
(le client et le prestataire de services ci-après collectivement appelés "les parties")

Il a été convenu ce qui suit :

PRÉAMBULE :

CONSIDÉRANT QUE le client désire obtenir divers services informatiques de la part du prestataire de services

CONSIDÉRANT QUE le prestataire de services accepte de fournir au client les services informatiques ci-après décrits, moyennant bonne et valable considération

CONSIDÉRANT QUE les parties désirent confirmer leur entente par écrit ;

**EN CONSÉQUENCE DE CE QUI PRÉCÈDE, LES PARTIES CONVIENNENT DE CE QUI SUIT :**

## **1.00 PRÉAMBULE**

Le préambule fait partie intégrante du présent contrat.

## **2.00 OBJET**

### **2.01 Services**

Le prestataire de services s'engage envers le client à fournir les services informatiques (ci-après appelés "les services") décrits dans les spécifications qui figurent en annexe "BON DE COMMANDE" du présent contrat (ci-après appelées "les spécifications").

### **2.02 Localisation des données**

La localisation de données est l'acte de stocker des données sur tout appareil physiquement présent à l'intérieur des frontières d'un pays spécifique où les données ont été générées. En ce basant sur l'activité de l'entreprise, les données seront héberger et traiter dans un data center qui se trouver dans le territoire national en conformité avec les recommandation de la CNIL.

Le stockage des données consiste à recueillir et conserver des informations numériques, c'est-à-dire les octets et bits des applications, protocoles réseau, documents, fichiers multimédias, carnets d'adresses, préférences utilisateur... Le Traitement et le stockage de données de l'entreprise se fera dans le cloud. Les données stockées dans un emplacement accessible depuis Internet par toute personne qui dispose d'une autorisation. Concernant l'accès aux données l'entreprise MedicArche à le plein droit sur l'ensemble des données qui seront stockées dans le cloud et à le pouvoir d'accéder à n'importe quel instant et c'est de même pour les accès aux logs.

### **2.03 La réversibilité et confidentialité des données**

La récupération et la jouissance de données, généralement après les avoir confiées à un tiers se sera lorsque le client souhaite mettre fin à la prestation, souhaite changer de fournisseur prestataire ou les héberger en local. La réversibilité est fait en restituant les données dans leur intégralité et dans leur intégrité. Ces données doivent être à nouveau exploitable. Le délai de mise à disposition des données sera fait dans un délai raisonnable auquel l'entreprise souscripteur sera libre d'apprécier.

Elle est mise en place par ce qui suit :

- une documentation régulière du projet
- l'utilisation de matériel et de technologies standards et régulièrement mises à jour
- la planification des différentes étapes de transfert des données au client

Tout est mise en place en respectant les recommandations de la CNIL. Les données de l'entreprise MedicArche, sont strictement confidentiel et ne peut être divulgué en aucun cas.

#### **2.04 Les volumes de données**

Dans un Cloud public, le prix d'une offre est fonction du nombre de serveurs, de la bande passante utilisée et du volume de données stockées. En revanche, les opérateurs privatifs ont des coûts de fonctionnement plus élevés du fait de leur taille plus petite, mais sont généralement moins coûteux sur des usages à long terme. Selon le type de cloud public ou privée, l'entreprise aura le choix entre le service amazon aws Glacier pour l'archivage des données froides dites secondaires ou utiliser un Bucket S3 pour sauvegarder les données qui sont utiliser au quotidien. Le cloud privée OpenStack propose un service similaire qui est Swift pour le stockage à chaud et à froid.

#### **2.05 Les niveaux de service (SLA)**

Le prestataire de service mettra en place une stratégie lié à l'accès, à la disponibilité et un certain niveau de sécurité. Si l'entreprise souhaite une plus grande sécurisation de ses données, c'est à elle de prendre en charge cette sécurité en déployant les outils et services requis. La mise en place de la réplication active directory sera intégré dans le cloud avec le service AWS Directory service pour assurer la disponibilité du système au cas où un serveur tombe en défaillance. Une stratégie de mot de passe sera mise en place pour limiter limiter les attaques lié au craquage de mot de passe.

### **5.00 RECONNAISSANCE DES PARTIES LES PARTIES RECONNAISSENT QUE :**

1. LE PRÉSENT CONTRAT A FAIT L'OBJET DE NÉGOCIATIONS PRÉALABLES ENTRE ELLES ;
2. LE PRÉSENT CONTRAT REFLÈTE VÉRITABLEMENT ET COMPLÈTEMENT L'ENTENTE INTERVENUE ENTRE ELLES ;
3. TOUTES ET CHACUNE DES CLAUSES DU PRÉSENT CONTRAT SONT LISIBLES ;
4. LEUR COMPRÉHENSION NE LEUR A POSÉ AUCUNE DIFFICULTÉ ;
5. AVANT LA SIGNATURE DU PRÉSENT CONTRAT, CHAQUE PARTIE A EU L'OPPORTUNITÉ DE CONSULTER SON CONSEILLER JURIDIQUE POUR EN DISCUTER ;
6. CHAQUE PARTIE A PRIS POSSESSION D'UN EXEMPLAIRE DU PRÉSENT CONTRAT IMMÉDIATEMENT APRÈS LA SIGNATURE DE CELUI-CI PAR TOUTES LES PARTIES.