République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Abderahmane Mira de Béjaia
Faculté des Sciences Exactes
Département de Recherche Opérationnelle

MÉMOIRE DE FIN DE CYCLE

EN VUE DE L'OBTENTION DU DIPLÔME DE MASTER EN MATHÉMATIQUES APPLIQUÉES

Option : Modélisation Mathématique et Évaluation des Performances des Réseaux

Présenté par

AIT-AMARA IKHLEF

Thème :

Évaluation et Amélioration de la Disponibilité des Services *Cloud Data Center* par Différentes Techniques de Redondance Chez ICOSNET (Alger)

Soutenu : le 06/07/2019 Devant le Jury composé de :

Mr	ADJABI Smail	Professeur	Univ. de Bejaia	Président
Mr	AÏSSANI Djamil	Professeur	Univ. de Bejaia	Rapporteur
Mlle	OUTAMAZIRT Assia	Docteur	Univ. de Bejaia	Co-Promotrice
Mr	CHERFAOUI Bachir	Doctorant	Univ. de Bejaia	Examinateur
Mme	DEHDOUH Amel	Ingénieur	Univ. de Bejaia	Examinatrice
Mr	MORSLI Ahmed	Ingénieur	Entr. ICOSNET	Invité

Année Universitaire : 2018/2019

Remerciements

J*e remercie, en premier lieu,* Dieu *le tout puissant pour m'avoir donner la force et le courage afin d'accomplir ce travail.*

J *e tiens à exprimer ma profonde gratitude à Monsieur Djamil AÏSSANI, Professeur à l'Université de Béjaïa, et à Mademoiselle* Assia OUTAMAZIRT, *Docteur à l'Université de Béjaïa, qui m'ont fait l'honneur d'être les rapporteurs de mon manuscrit de Master. Je les remercie pour leurs grandes qualités humaines, leur précieuse attention et particulièrement pour leurs conseils et leurs orientations qui ont contribué à l'aboutissement de ce travail.*

M*es sincères remerciements et ma gratitude vont aussi à Monsieur* ADJABI Smail, *Professeur à l'Université de Béjaïa, pour avoir accepté de juger ce travail et de présider le jury de soutenance. Que vous soyez assurer de mon entière reconnaissance.*

J*e remercie également tous les autres membres de jury, Monsieur* CHERFAOUI Bachir, *Doctorant à l'Université de Béjaïa, Madame* DEHDOUH Amel, *ingénieur, d'avoir bien voulu donner de leurs temps pour lire ce mémoire et d'avoir juger mon travail.*

J*e tiens à remercier mon tuteur de stage* Ahmed MORSLI, *Directeur d'Ingénierie et Infrastructure Cloud à l'entreprise ICOSNET, de m'avoir d'abord accueilli, mais surtout accompagné durant toute la durée du stage. Son soutien, ses conseils et sa disponibilité auront été précieux pour mener à bien mon travail.*

U*n grand merci à toute l'équipe de l'entreprise ICOSNET, ingénieurs, techniciens et administratifs, pour l'accueil chaleureux et cordial qui m'a été réservé.*

J*e n'oublierai pas non plus de remercie tous les enseignants du Département de Recherche Opérationnelle qui ont assuré ma formation universitaire, en particulier : Professeur* ADJABI Smail.

J*'ai une pensée particulière pour ma chère famille et ma chère petite amie qui m'ont toujours soutenus et encouragés tout au long de mes études, ce dont je suis très reconnaissant.*

M*erci aussi à tous mes amis, mes collègues et toutes les personnes que j'ai pu côtoyer pendant ces cinq ans à l'université. Je leur exprime ma profonde sympathie et leur souhaite beaucoup de bien.*

J*e tiens en dernier lieu à exprimer ma reconnaissance et ma gratitude à toutes les personnes qui ont contribué de près ou de loin à l'aboutissement de ce travail.*

Dédicaces

❝ Je dédie ce travail à toutes les personnes que j'aime et qui m'aiment ❞

Ikhlef. A.. ✍

Table des Matières

TABLE DES MATIÈRES **II**

LISTE DES TABLEAUX **IV**

LISTE DES FIGURES **V**

LISTE DES ABRÉVIATIONS **VIII**

INTRODUCTION GÉNÉRALE **1**

1 l'Organisme d'Accueil : l'Entreprise ICOSNET **4**

1.1 Présentation de l'entreprise ICOSNET 4

1.1.1 Historique de l'entreprise 5

1.2 Couverture géographique 5

1.3 Organigramme de l'entreprise 6

1.4 Services proposés par ICOSNET 6

1.4.1 Solutions Accès Internet 7

1.4.2 Solutions Communications unifiées 8

1.4.3 Solutions Cloud 10

1.5 Atouts de l'entreprise 13

1.6 Position du problème 13

2 Généralités sur le Cloud Computing **14**

2.1 Qu'est-ce que le Cloud Computing ? 14

2.1.1 Définitions 14

2.1.2 Caractéristiques 15

2.1.3 Modèles de services 16

2.1.4 Modèles de déploiement 18

2.1.5 Avantages et inconvénients 19

2.1.6 Acteurs 20

2.2 Virtualisation 21

2.3 Data Center 23

2.3.1 Composition d'un Data Center 23
2.3.2 Caractéristiques des Data Centers d'aujourd'hui 24
2.3.3 Topologie réseau d'un Data Center 25
2.3.4 Classification des Data Centers 25
2.4 Accord de niveau de service (SLA) 26

3 Généralités sur la Disponibilité et de la Haute Disponibilité 28
3.1 Définition 28
3.2 Fiabilité 29
3.3 Maintenabilité 31
3.4 Disponibilité 32
3.4.1 Types de disponibilité 34
3.4.2 Disponibilité des systèmes multi-composants 35
3.4.3 Degrés de disponibilité d'un système 39
3.5 Mécanismes de Haute Disponibilité 41
3.5.1 Redondance et tolérance aux pannes 41
3.5.2 Sécurisation des données : Technologies RAID 45

4 Modélisation de la Disponibilité de l'Infrastructure Technique du Data Center 49
4.1 Collecte des données 50
4.2 Architecture globale du Data Center d'ICOSNET 51
4.3 Application sur les systèmes de stockage RAID 52
4.3.1 Redondance par duplication 52
4.3.2 Redondance par contrôle de parité 55
4.3.3 Redondance par double contrôle de parité 57
4.4 Application sur le Cluster Cloud 60
4.5 Application sur le réseau LAN 64
4.6 Application sur l'architecture globale du Data Center 66

Bibliographie 70

Liste des Tableaux

2.1 *Récapitulatif des niveaux de tiers dans un Data Center* 26

3.1 *Degrés de disponibilité d'un système. [5]* 40

4.1 *Valeurs MTTF, MTTR et la disponibilité des composants du Data Center* 50
4.2 *Les résultats obtenus pour la structure RAID-0* 52
4.3 *Les résultats obtenus pour la structure RAID-1* 53
4.4 *Les résultats obtenus pour la structure RAID-0+1* 54
4.5 *Les résultats obtenus pour la structure RAID-10* 55
4.6 *Les résultats obtenus pour la structure RAID à parité unique* 57
4.7 *Les résultats obtenus pour la structure RAID à double parité* 58
4.8 *Classement par niveau de disponibilité pour différents types de RAID* 59
4.9 *Les résultats obtenus pour le service Cloud* 61
4.10 *Les résultats obtenus pour la configuration HA Cluster d'ICOSNET* 62
4.11 *Les résultats obtenus pour la configuration HA Cluster (C2)* 63
4.12 *Les résultats obtenus pour l'infrastructure réseau du DC d'ICOSNET* 64
4.13 *Les résultats obtenus pour l'infrastructure réseau du DC avec LAN (A2)* 65
4.14 *Les résultats obtenus pour l'architecture globale du DC* 66
4.15 *Les résultats obtenus pour l'architecture globale du DC (A2)* 68
4.16 *Les résultats obtenus pour l'architecture globale du DC (A3)* 68

Liste des Figures

1.1 *Historique de l'entreprise ICOSNET* 5
1.2 *La couverture géographique de l'entreprise ICOSNET* 5
1.3 *Organigramme de l'entreprise ICOSNET* 6
1.4 *Direction d'ingénierie et Infrastructures Cloud* 6
1.5 *Accès Internet Filaire* 7
1.6 *Accès Internet Sans Fil* 7
1.7 *Interconnexion des Sites Distants* 8
1.8 *Accès Internet WIFI* 8
1.9 *Instalation Client de SCC* 9
1.10 *Téléphonie IP* 9
1.11 *Visio/Call Conférence* 10
1.12 *Hébergement des données* 10
1.13 *Hébergement des serveurs* 11
1.14 *Serveur Virtuel* 11
1.15 *Cértificat SSL* 12
1.16 *Messagerie Pro avec ICOSNET* 12
1.17 *Nom de domaine* 12

2.1 *L'environnement du Cloud Computing* 15
2.2 *Caractéristiques du Cloud Computing* 16
2.3 *Types de service du* Cloud Computing 17
2.4 *Modèles de déploiement du Cloud Computing* [29] 19
2.5 *L'écosystème du* Cloud Computing 21
2.6 *Principe de la virtualisation et de la consolidation* 22
2.7 *Architecture globale d'un Data Center* 24
2.8 *Exemples de Data Centers : Google, Facebook et Microsoft* 24
2.9 *L'infrastructure de réseau du Data Center [64]* 25

3.1 *Fiabilité R, dé-fiabilité* $\overline{R}$ 29
3.2 *MTTF* 30

3.3 *MTTFF, MTBF, MTTF* . . . 31
3.4 *L'état du système* . . . 33
3.5 *Disponibilité, indisponibilité* . . . 33
3.6 *MUT, MDT* . . . 34
3.7 *Disponibilités intrinsèque et opérationnelle* . . . 35
3.8 *Diagramme de fiabilité d'un système avec structure série* . . . 36
3.9 *Diagramme de fiabilité d'un système avec structure parallèle* . . . 36
3.10 *Diagramme de fiabilité d'un système avec structure série-parallèle* . . . 37
3.11 *Diagramme de fiabilité d'un système avec structure parallèle-série* . . . 37
3.12 *Diagramme de fiabilité d'un système avec structure mixte* . . . 38
3.13 *Diagramme de fiabilité d'un système avec structure redondant k/n* . . . 38
3.14 *Diagramme de fiabilité d'un système avec structure de pont* . . . 39
3.15 *Décomposition d'un système en pont* . . . 39
3.16 *Le principe de tolérance aux pannes* . . . 41
3.17 *HA Cluster* . . . 42
3.18 *Configuration de cluster à quatre nœuds avec disque quorum* . . . 42
3.19 *Configuration de quorum peut survivre à deux pannes de serveur à la fois* . . . 43
3.20 *Reprise après sinistre d'un Data Center* . . . 43
3.21 *Mouvement de machine virtuelle - migration d'un serveur physique vers d'autres serveurs.* . . . 44
3.22 *Trois emplacements de stockage différents : stockage principal, sur site et hors site* . . . 44
3.23 *Périphériques réseau redondants* . . . 44
3.24 *Schéma de principe d'une grappe de disques en RAID-0* . . . 45
3.25 *Schéma de principe d'une grappe de disques en RAID-1* . . . 46
3.26 *Schéma de principe d'une grappe de disques en RAID-0+1 et RAID-10* . . . 46
3.27 *Schéma de principe d'une grappe de disques en RAID-3* . . . 47
3.28 *Schéma de principe d'une grappe de disques en RAID-4* . . . 47
3.29 *Schéma de principe d'une grappe de disques en RAID-5* . . . 48
3.30 *Schéma de principe d'une grappe de disques en RAID-6* . . . 48

4.1 *L'infrastructure globale du Data Center d'ICOSNET* . . . 51
4.2 *Diagramme de fiabilité pour la structure RAID-0* . . . 52
4.3 *Diagramme de fiabilité pour la structure RAID-1* . . . 53
4.4 *Diagramme de fiabilité pour la structure RAID-0+1* . . . 54
4.5 *Diagramme de fiabilité pour la structure RAID-10* . . . 54
4.6 *Diagramme de fiabilité pour les structures RAID-3 et RAID-4* . . . 56
4.7 *Diagramme de fiabilité pour la structure RAID-5* . . . 56
4.8 *Présentation graphique des résultats* . . . 57
4.9 *Diagramme de fiabilité pour la structure RAID-6* . . . 58

4.10 *Présentation graphique des résultats* 58
4.11 *Diagrammes montrent les résultats obtenus pour différents types de RAID* 59
4.12 *Classement par niveau de disponibilité pour trois types de RAID. [4]* 60
4.13 *La configuration de la virtualisation dans un serveur Cloud* 60
4.14 *Digramme de fiabilité du système de base d'un service Cloud* 61
4.15 *Digramme de fiabilité pour la configuration HA Cluster d'ICOSNET* 62
4.16 *Diagramme de fiabilité pour la configuration HA Cluster (C2) suggérée* 63
4.17 *Diagramme de fiabilité pour l'infrastructure réseau du DC d'ICOSNET* 64
4.18 *Diagramme de fiabilité pour LAN (A2) suggérée* 65
4.19 *Diagramme de fiabilité pour l'architecture globale du DC d'ICOSNET* 66
4.20 *Diagramme de fiabilité pour l'architecture du DC (A2) suggérée* 67
4.21 *Diagramme de fiabilité pour l'architecture du DC (A3) suggérée* 67

Liste des Abréviations

- **BDF** : Blocs Diagramme de Fiabilité.
- **CATV** : Community Antenna Television.
- **CPU** : Central Processing Unit.
- **DC** : Data Center.
- **Gbps** : Gigabits par seconde.
- **HA** : High Availability.
- **HDD** : Hard Disk Drive.
- **HW** : Hardware.
- **IaaS** : Infrastructure as a Service.
- **IBM** : International Business Machines.
- **IDE** : Integrated Drive Electronics.
- **IEEE** : L'Institute of Electrical and Electronics Engineers.
- **IP** : Internet Protocol.
- **ISP** : Internet Service Provider.
- **KVM** : Kernel-based Virtual Machine.
- **LAN** : Local Area Network.
- **LS** : Ligne Spécialisée.
- **Mbps** : Mega bytes per seconds.
- **MDT** : Mean Down Time.
- **MPLS** : Multiprotocol Label Switching.
- **MTBF** : Mean Time Between Failures.
- **MTTF** : Mean Time To Failure.

- **MTTFF** : Mean Time To First Failure.
- **MTTR** : Mean Time To Repair.
- **MUT** : Mean Up Time.
- **NIC** : Network Interface Card.
- **NIST** : National Institute of Standards and Technology.
- **PaaS** : Plateform as a Service.
- **PME/PMI** : Petites et Moyennes Entreprises / Industries.
- **RAID** : Redundant Array of Inexpensive Disks.
- **RAM** : Random Access Memory.
- **SaaS** : Software as a Service.
- **SAS** : Serial Attached SCSI.
- **SATA** : Serial Advanced Technology Attachment.
- **SCC** : Solution centre de contact.
- **SCSI** : Small Computer System Interface.
- **SOA** : Service Oriented Architecture.
- **SLA** : Service Level Agreement.
- **SMS** : Short Message Service.
- **SSL** : Secure Socket Layer.
- **TIC** : Technologies de l'Information et de la Communication.
- **VM** : Virtual Machine.
- **VMM** : Virtual Machine Monitor.
- **VOIP** : Voix sur IP.
- **VPN** : Virtual Private Network.
- **WAN** : Wide Area Network.
- **WIFI** : Wireless Fidelity.
- **WiMAX** : Worldwide Interoperability for Microwave Access.
- **WSDL** : Web Services Description Language.
- **xDSL** : Digital Subscriber Line.

Introduction Générale

Le *Cloud Computing* ou l'informatique en nuage, est un nouveau modèle économique hébergeant les applications de la technologie de l'information. Il répond aux besoins exponentiellement croissants en ressources physiques et logicielles. Il permet d'approvisionner ces ressources et de les partager sous forme de ressources virtuelles à travers le réseau Internet. Le passage au Cloud devient un enjeux important des entreprises pour des raisons essentiellement économiques. En effet, le Cloud fournit des services à la demande ce qui permet aux utilisateurs d'allouer les ressources virtuelles nécessaire pour leurs processus métier. Ils n'ont plus donc besoin d'installer des infrastructures couteuses et d'assurer leurs mis à jours ce qui permet de réduire les coûts de l'exploitation et de l'entretien.

Aujourd'hui'hui il existe plusieurs fournisseurs de service Cloud public, privé et hybride. Étant donné la diversité des fournisseurs et des services Cloud, l'utilisateur doit être capable de sélectionner celui qui répond au mieux à ses besoins. Du point de vue du fournisseur de Cloud, de nombreux défis doivent être surmontés pour fournir des services Cloud qui répondent à toutes les exigences définies dans les accords de niveaux de service (SLA).

La haute disponibilité a été l'un des plus grands défis pour les fournisseurs de service Cloud. Ceci est étroitement lié à la gestion des défaillances de *Data Centers* (sur l'ensemble du réseau, du matériel au logiciel). Les pannes non planifiées de *Data Center* sont coûteuses (des deux côtés, fournisseurs et utilisateurs) et nécessitent une attention particulière. Une disponibilité élevée est atteinte lorsque le service en question est indisponible moins de 5.25 minutes par an, ce qui correspond à une disponibilité d'au moins 99.999% (cinq neuf) [38]. Avant de valider un contrat de niveau de service avec les clients du Cloud, le fournisseur de services doit procéder à une évaluation de la disponibilité de l'infrastructure sur laquelle le service Cloud est hébergé.

La plupart des fournisseurs de service Cloud offrent environ 99,999 % de la disponibilité de leur contrat de niveau de service. Toutefois, les données réelles montrent que la valeur réelle de la disponibilité de ces fournisseurs est beaucoup plus faible. Par conséquent, pour réduire les temps d'arrêt globaux dans le Cloud et fournir une estimation fiable de la disponibilité du service, les fournisseurs de services Cloud doivent évaluer régulièrement leur infrastructure pour détecter les défaillance probables et réduire le temps nécessaire à la résolution de ces défaillance ou de faire face aux mécanismes de haute disponibilité basées sur les techniques de redondance

pour assurer une disponibilité de service en permanence. En d'autre terme, lorsque un composant système tombe en panne, cela ne provoque pas nécessairement la fin du service fourni par ce composant.

L'utilisation de plusieurs mécanismes permet d'atteindre la haute disponibilité de service dans le *Cloud Data Center*. En effet, la redondance permet une duplication de l'information qui peut ainsi rester disponible en cas de panne. Il est possible de faire de la redondance au niveau du stockage via la technologie RAID (Redundant Array of Independent Disks) ; elle permet aussi d'améliorer les temps d'accès en dupliquant les données des disques durs physiques. D'autre part, le fait de répliquer un *Data Center* situé dans une zone géographique A vers une zone géographique B constitue également une forme de redondance. Un haut niveau de disponibilité ne s'obtient pas uniquement par le biais de l'informatique. Il est possible de faire appel à des équipements de secours comme les circuits électriques, les systèmes de climatisation ou les groupes électrogènes pour assurer la continuité du service. Ces mises en application impliquent une gestion rigoureuse du *Data Center* notamment une bonne gouvernance du système d'informations.

Le *Cloud Computing* a été étudié à l'aide de diverses techniques issues de la théorie de la fiabilité, notamment les Blocs Diagramme de Fiabilité (BDF), les Réseaux de Petri Stochastiques (RDPS), les Arbres de Défaillances (ADD) et les Chaînes de Markov (CM). La disponibilité de l'architecture du *Cloud Computing* a été modélisée de différentes manières à l'aide de techniques de Blocs Diagramme de Fiabilité (BDF) [20, 25, 54]. En outre, la modélisation analytique a été utilisée pour estimer la disponibilité des architectures de systèmes du *Cloud Computing*, notamment une architecture simple virtualisée et une architecture redondante virtualisée [5].

En ce qui concerne les études effectués sur le sujet du *Cloud Computing* au sein de l'entreprise ICOSNET, citons : La modélisation et l'évaluation des performances de la solution *Cloud Computing* (l'évaluation de l'enchaînement de la requête depuis son lancement de la part du client jusqu'à sa supervision finale de la part de l'entreprise), par les réseaux de files d'attente [11].

L'objectif principale de notre étude est d'évaluer la disponibilité de l'infrastructure sous-jacente sur laquelle les services Cloud offerts par le fournisseur ICOSNET sont hébergés (*Data Center*, stockage, serveurs, réseau interne, réseau externe) par la méthode des Blocs Diagramme de Fiabilité (BDF) afin de voir l'impact des différentes mécanismes de haute disponibilité que nous allons introduire dans chaque système de l'infrastructure technique sur la disponibilité des données et des services *Cloud*.

Plan du mémoire

Après une introduction générale, le reste de ce mémoire est structuré autour de quatre chapitres, une conclusion générale et s'achève par une bibliographie.

Chapitre 1 : Ce chapitre est consacré à la présentation de l'entreprise d'accueil « ICOSNET »,

dans laquelle s'est déroulé mon stage, ainsi que la problématique de notre travail.

Chapitre 2 : Dans ce chapitre, nous présentons brièvement l'état de l'art des deux principaux sujets de notre mémoire qui sont le *Cloud Computing* et le *Data Center*. L'objectif était de s'assurer que le lecteur aurait une compréhension des concepts de base manipulés dans le reste du manuscrit.

Chapitre 3 : Ce chapitre se focalise dans la première partie sur les notions relatives au concept de modélisation de la disponibilité. Dans la deuxième partie nous décrirons les mécanismes permettant d'assurer la haute disponibilité dans les systèmes informatiques du *Cloud Data Center*.

Chapitre 4 : Dans ce chapitre, nous introduisons l'analyse de disponibilité de l'infrastructure technique du *Cloud Data Center* d'ICOSNET en utilisant plusieurs techniques de redondance. Ensuite, nous interpréterons les résultats obtenus. Enfin, nous recommandons les meilleurs solutions évaluées en terme de disponibilité pour chaque système de l'infrastructure.

Chapitre 1

l'Organisme d'Accueil : l'Entreprise ICOSNET

Introduction

Mon stage de fin de cycle s'est déroulé au sein de l'entreprise ICOSNET, qui est un opérateur multiservices d'accès Internet. Elle est située à Centre d'Affaires El Qods, Chéraga, Alger.

J'ai été accueilli au sein de l'équipe responsables du *Cloud Data Center*, qui se charge des ressources matériels et logiciels tels que les serveurs, le stockage, les logiciels de réseau et de virtualisation (sécurité, machines virtuelles..etc), nécessaires à la prise en charge des besoins informatiques pour le *Data Center*. L'objectif du stage était d'enrichir mes connaissances sur le *Cloud Data Center* dans l'état pratique afin de mieux comprendre son architecture et son fonctionnement, et de réaliser une étude mathématique sur la disponibilité et l'accessibilité de ses services.

Dans ce premier chapitre, je présenterai l'entreprise ICOSNET dans laquelle s'est déroulé mon stage ainsi que la problématique fixée.

1.1 Présentation de l'entreprise ICOSNET

L'entreprise ICOSNET, est un opérateur Algérien d'accès Internet haut débit, de solutions de télécommunications convergentes et de solutions *Cloud*. Créé en 1999, et doté d'une équipe pluridisciplinaire, ICOSNET a su capitaliser une expérience importante et nouer des relations considérables avec les différents acteurs du secteur des TIC à l'échelle nationale et internationale.

Sur le marché algérien, ICOSNET est un opérateur à part entière (autorisations ISP, VoIP et Wimax). Ce positionnement lui permet de s'adresser à une clientèle large, de convaincre des clients de taille significative et de pouvoir proposer des solutions de connexion et de communi-

cation économiquement plus avantageuses et plus abouties.

1.1.1 Historique de l'entreprise

La Figure [1.1], résume l'histoire de l'entreprise ICOSNET.

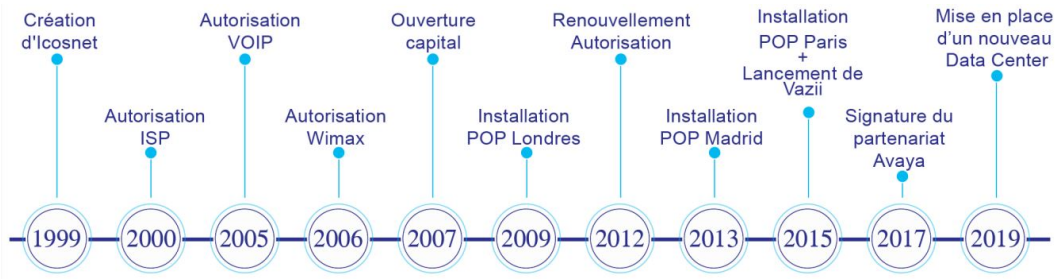

FIGURE 1.1 – *Historique de l'entreprise ICOSNET*

1.2 Couverture géographique

ICOSNET possède un large réseau de distribution au niveau national et international ce qui lui permet de garantir une fourniture d'accès Internet performante sous les différentes technologies. La carte suivante [Fig. 1.2] représente la localisation géographique de l'entreprise ICOSNET dans le monde :

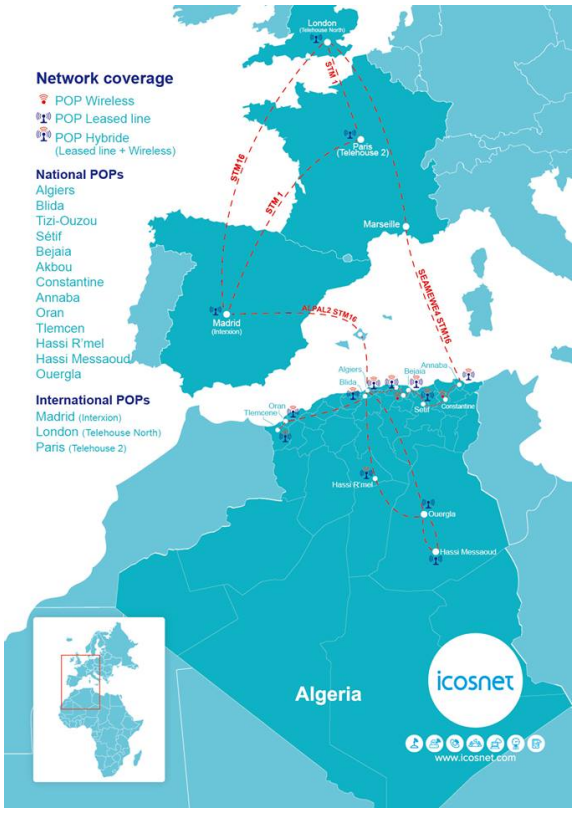

FIGURE 1.2 – *La couverture géographique de l'entreprise ICOSNET*

1.3 Organigramme de l'entreprise

L'organigramme de l'ICOSNET s'établit comme suit :

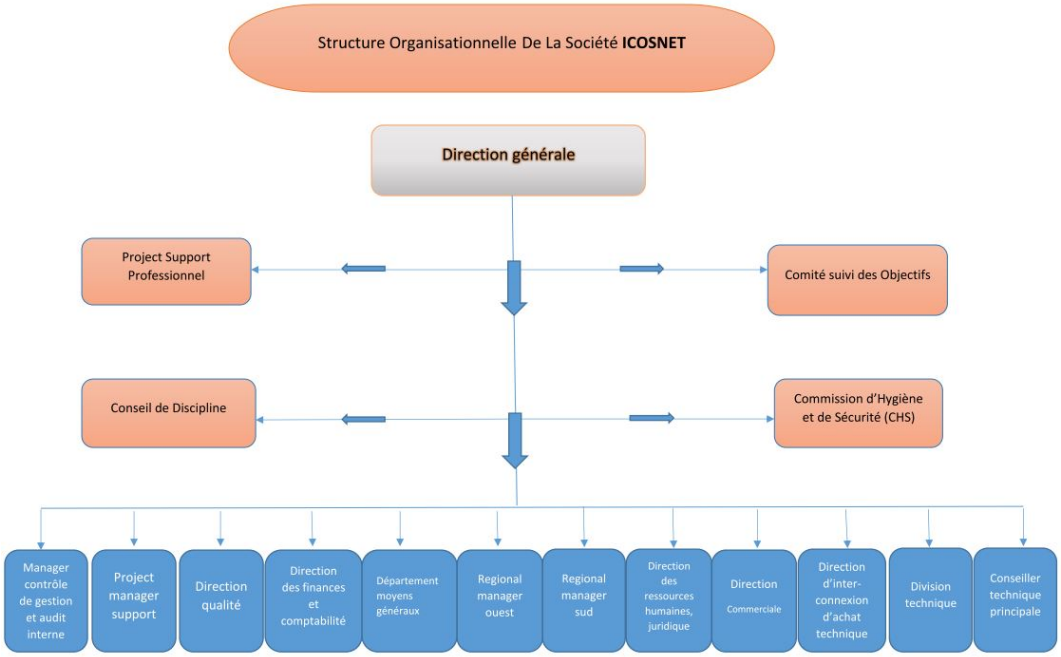

FIGURE 1.3 – *Organigramme de l'entreprise ICOSNET*

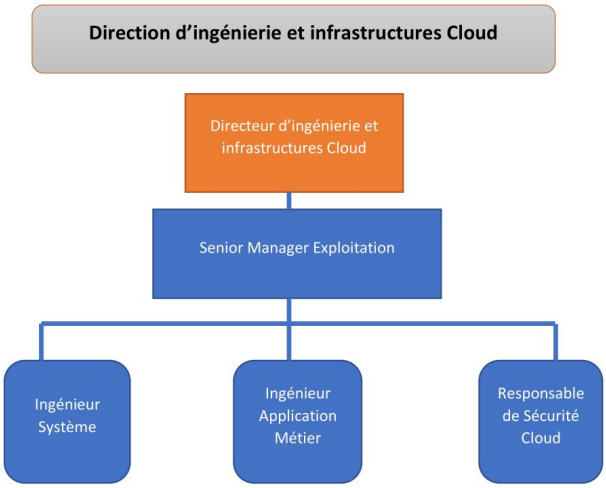

FIGURE 1.4 – *Direction d'ingénierie et Infrastructures Cloud*

1.4 Services proposés par ICOSNET

ICOSNET SPA est un fournisseur algérien de solutions de communication d'entreprise et un opérateur multiservices destiné aux PME/PMI et les grands comptes multinationaux installés en Algérie.

Parmi les services proposées par ICOSNET, citons :

1.4.1 Solutions Accès Internet

- **Accès Internet Filaire**

La solution d'accès préconisée au client mono-site (entreprise, administration, ...) est constituée d'un ou de plusieurs tronçons filaires de transmission, à base de cuivre torsadé ou fibre optique d'un réseau privé ou public mis bout à bout pour assurer une connexion fiable à un ou plusieurs points de présence du réseau ICOSNET.
C'est une liaison offrant au Client la possibilité d'échanger tous types de données (voix, data, vidéo, ..) sur la toile Internet à des débits de connexion symétriques, garantis en émission et en réception de données et allant jusqu'à des dizaines de Mbps. Cette solution d'accès est proposée avec des outils de mesure de bande passante et de statistiques en temps réel.

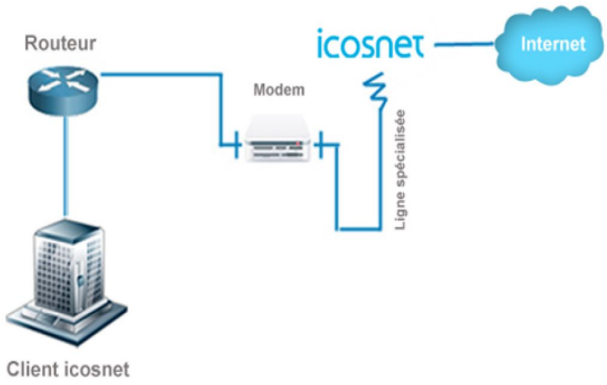

FIGURE 1.5 – *Accès Internet Filaire*

- **WDSL : Internet Sans Fil**

« *WDSL* » est le nom commercial des technologies basées sur le standard *IEEE* 802.16 et aujourd'hui'hui labellisées sous le nom de *WiMAX*. Comme son nom l'indique, *WDSL* vise à concurrencer les connexions filaires *xDSL* et le câble de télévision *(CATV)* par des réseaux sans fil. La technologie utilise des antennes de diffusion classiques, mais aussi des antennes qui ne couvrent qu'un angle de 90, ainsi que des antennes point à point.
C'est une solution offrant au client la possibilité d'échanger tous types de données (voix, data, vidéo, ..) sur la toile Internet à des débits de connexion asymétriques, allant jusqu'à 2 de Mbps.

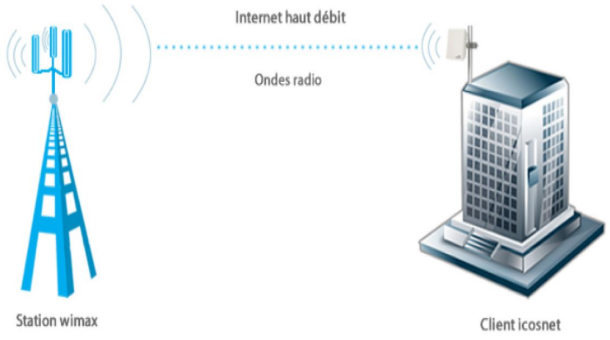

FIGURE 1.6 – *Accès Internet Sans Fil*

- **Réseau Privé**

Une solution sur-mesure pour l'interconnexion de multi-sites d'une entreprise ou d'une administration. Le tout en s'appuyant sur un Réseau Privé Virtuel *IP VPN* de type *MPLS* composé d'une plateforme technique de dernière génération ainsi que sur ceux de ses partenaires locaux et internationaux.

L'objectif à vouloir atteindre derrière cette offre de service est de proposer des connexions sécurisées en *xDSL* ou fibre optique à débit garanti variant de 2 Mbps à 10 Gbps pour donner la possibilité aux utilisateurs finaux d'échanger tous types de données (voix, data, vidéo,..) sur un Réseau Privé Virtuel *IP VPN* de type *MPLS* haut débit sécurisé de bout en bout.

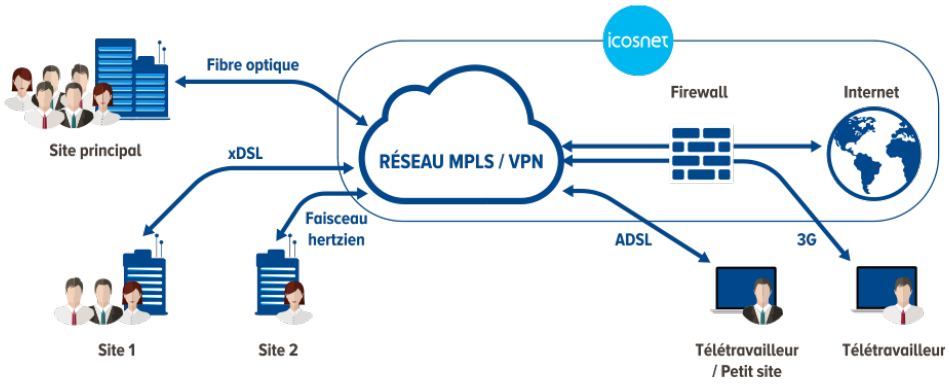

FIGURE 1.7 – *Interconnexion des Sites Distants*

Il existe aussi d'autres services d'accès Internet offerts par ICOSNET, tel que *l'Accès large bande Sans Fil*, et le *WIFI*.

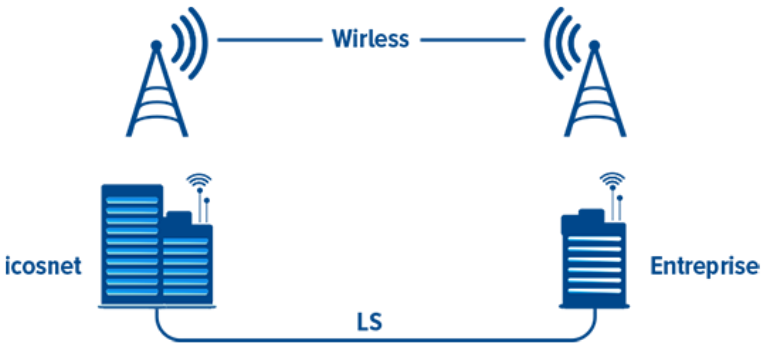

FIGURE 1.8 – *Accès Internet WIFI*

1.4.2 Solutions Communications unifiées

La communication unifiée en *Cloud* offre une approche différente aux communications de l'entreprises en transformant les solutions : VOIX, Vidéo, messagerie instantanée en une véritable architecture qui correspond le mieux aux clients. Nous en citons quelques-unes :

- **Solution Centre de Contacts**

Un centre de contacts est une structure centralisée dont la vocation est de gérer à distance les relations des entreprises avec leurs clients et prospects, par une communication directe, basée sur le couplage de la téléphonie et de l'informatique. Il est appelé également Centre d'appels (*call center*). Les différentes fonctionnalités de la solution centre de contacte *SCC* sont :

– La gestion et l'enregistrement des appels entrants et sortants ;
– La gestion interface unifiée multicanal (réseaux sociaux, mail, chat, SMS) ;
– Un outil de supervision sur site et à distance ;
– Des statistiques en temps réel /rapports historiques.

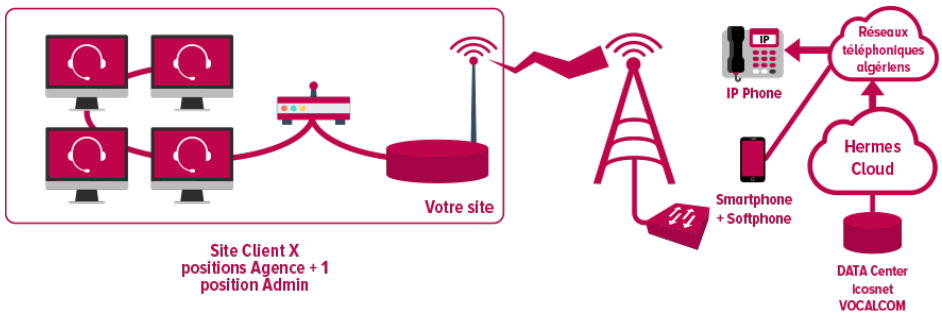

FIGURE 1.9 – *Instalation Client de SCC*

- **Téléphonie IP**

Une ligne téléphonique IP qui fonctionne avec une connexion Internet portant un numéro 098240xxxxxx. Cette ligne de téléphonie, permet :

– L'acquisition des numéros : 098240xxxxxx offerts sans frais d'abonnement ;
– Une configuration sur différents supports (*IP PHONE,Smartphone,..*) selon le besoin du client ;
– La communication en Algérie et vers l'international avec des tarifs préférentiels ;
– La réception de plusieurs appels en simultané et accès à plusieurs fonctionnalités de télépho.

FIGURE 1.10 – *Téléphonie IP*

- **Call/Visio Conférence**

Un service qui permet d'organiser des conférences téléphoniques simultanément avec des collaborateurs ou des clients sans avoir à se déplacer. Cette solution s'organise aisément avec autant de participants souhaités, elle propose un service professionnel et elle garanti une excellente qualité d'écoute et/ou de vision pour les communications.

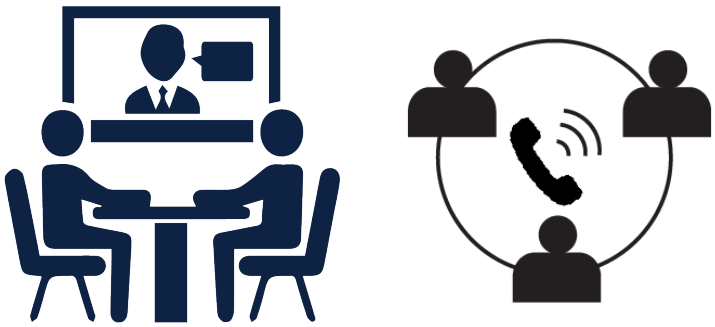

FIGURE 1.11 – *Visio/Call Conférence*

Il existe aussi d'autres services de Communications unifiées offertes par ICOSNET, tel que le *Standard virtuel IP Aura*, *E-Fax*, et *SMS Pro*.

1.4.3 Solutions Cloud

ICOSNET propose une multitude de services hébergés au niveau de son *Data Center* basé en Algérie, citons :

- **Hébergement Mutualisé**

L'hébergement mutualisé est un mode d'hébergement Internet destiné principalement à des sites web, dans un environnement technique dont la caractéristique principale est d'être partagé par plusieurs utilisateurs. Cette architecture est adaptée pour des sites d'importance et d'audience faibles ou moyennes, ne sollicitant que ponctuellement les ressources du ou des serveurs informatiques assurant l'hébergement (processeur, mémoire vive, espace disque, débit). L'administration de ces derniers est assurée par le titulaire de l'hébergement ICOSNET.

FIGURE 1.12 – *Hébergement des données*

- **Hébergement Co-localisé**

Il s'agit d'avoir votre propre serveur, mais il est situé à un endroit différent spécialement conçu pour cela. L'entreprise apporte le serveur et loue l'espace de stockage, et le fournisseur de services offre la sécurité physique, l'alimentation, les connexions Internet dédiées et le refroidissement. En outre, l'entreprise est responsable de son propre stockage de données, de son système de sauvegarde et de son logiciel serveur. Dans tous les cas, si le matériel tombe en panne, il est de la responsabilité de l'entreprise de le remplacer ou de le réparer pour que le serveur fonctionne. Cette solution d'hébergement offre :

– Une réduction des coûts et des risques liée à l'hébergement et la gestion interne ;

– Une haute disponibilité et une meilleure sécurité.

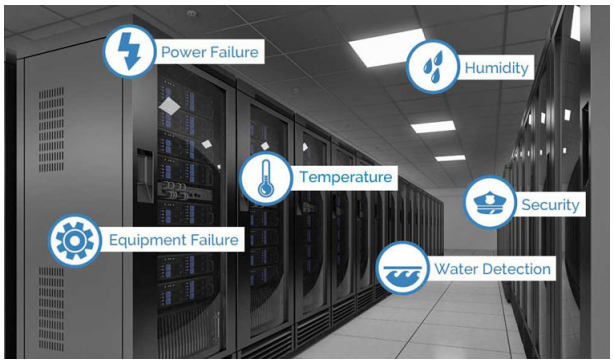

FIGURE 1.13 – *Hébergement des serveurs*

- **Serveur Virtuel Privé**

Un serveur virtuel ou serveur dédié virtuel, est une machine physique découpée en plusieurs serveurs virtuels indépendants et autonomes, et qui communiquent avec d'autres entités virtuelles. Chacun de ces serveurs possède les caractéristiques générales d'un serveur dédié classique.

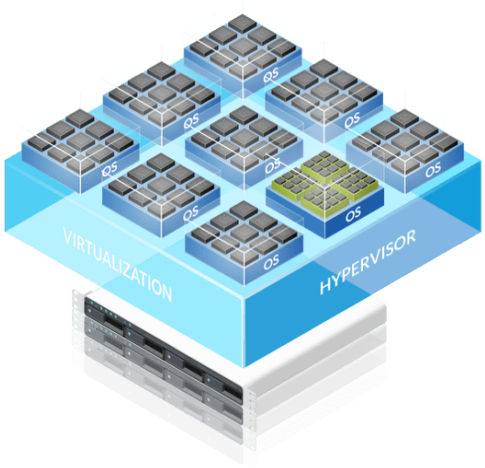

FIGURE 1.14 – *Serveur Virtuel*

- **Cértificat SSL**

Un certificat *SSL* est un fichier de données qui lie une clé cryptographique aux informations d'une organisation ou d'un individu. Installé sur un serveur, le certificat active le cadenas et le

protocole « *https* » dans les navigateurs, afin d'assurer une connexion sécurisée entre le serveur web et le navigateur. Généralement, le *SSL* est utilisé pour sécuriser les transactions bancaires, le transfert de données et les informations de connexions, telles que les noms d'utilisateurs et les mots de passe. C'est la norme pour sécuriser l'utilisation de sites de réseaux sociaux.

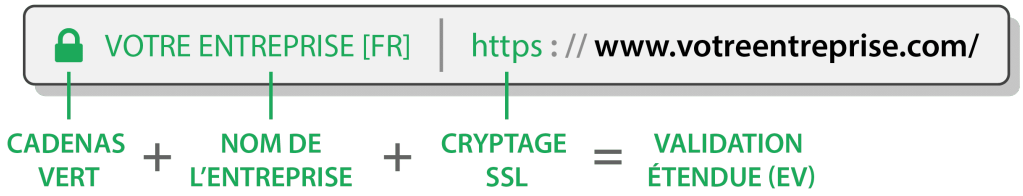

FIGURE 1.15 – *Cértificat SSL*

- **Messagerie Pro**

La Messagerie pro est une suite de communication, regroupant sous une même interface, les outils de communication indispensables à l'activité professionnelle du client. Avec la Messagerie pro, les clients bénéficient d'un(e) :

– Communication simplifiée avec leur partenaires ;
– Organisation plus pratique ;
– Image plus professionnelle de leur activités ;
– Haut niveau de sécurité des données et des échanges.

FIGURE 1.16 – *Messagerie Pro avec ICOSNET*

- **Nom de domaine**

Le nom de domaine est ce qui permet d'identifier de manière simple un site Internet. Il est composé d'un nom et de son extension de domaine, en fonction de son activité. Le nom de domaine est indispensable à l'identité de toute marque, société, personne morale ou physique, souhaitant se positionner sur le réseau Internet.

FIGURE 1.17 – *Nom de domaine*

1.5 Atouts de l'entreprise

Les principaux atouts de l'entreprise ICOSNET sont :

- Un accès permanent et un support technique performant ;
- Un hébergement assuré en Algérie suivant la règlementation en vigueur ;
- Une expertise confirmée sur le marché ;
- Une réduction de coûts conséquente avec des solutions à la demande ;
- Des solutions innovantes et adaptées aux attentes des clients pour de meilleures performances ;
- Un personnel bien formé et motivé.

1.6 Position du problème

La haute disponibilité est un problème critique pour le *Cloud Data Center*. Les infrastructures de *Data Centers* doivent offrir une haute disponibilité de leurs services. L'indisponibilité des services n'affecte pas uniquement l'expérience utilisateur, elle est également traduite en coûts directs pour les fournisseurs de service *Cloud* et les entreprises. Une partie des coûts est due à des violations de SLA, dès lors que des interruptions plus longues que celles signées dans le contrat génèrent des pénalités financières. Étant donné la multitude de raisons menant à l'indisponibilité d'un service et des données (panne, coupure électrique, arrêt du serveur pour maintenance), la problématique qui se pose est la suivante : comment faire en sorte d'assurer un fonctionnement en régime permanent dans une infrastructure *Cloud Data Center* (une disponibilité de service maximale) ?.

Afin de répondre à ce besoin, les fournisseurs de service *Cloud* se sont tournés vers les techniques de redondance. Il s'agit donc de doubler un maximum d'éléments matériels du système et de prévoir les mécanismes de basculement automatiques qui doit être déclenché immédiatement après la détection de la panne.

C'est pourquoi, il nous semble intéressant d'évaluer chez le fournisseur ICOSNET la disponibilité de l'infrastructure sous-jacente du *Cloud Computing* configurée avec certaines techniques de redondance qui sont largement utilisées dans les *Data Centers* afin de voir comment ces différentes techniques améliorent la disponibilité en régime permanent des données et des services Cloud.

Conclusion

Dans ce chapitre, nous avons présenté brièvement l'entreprise d'accueil ICOSNET ainsi que la problématique posée. Dans le chapitre suivant, nous détaillerons les éléments essentiels autour du *Cloud Computing* et du *Data Center*.

Chapitre 2

Généralités sur le Cloud Computing

Introduction

Dans ce chapitre, nous aborderons l'état de l'art sur l'environnement du *Cloud Computing*, ses caractéristiques, ses modèles de service et de déploiement ainsi que ses avantages et ses inconvénients. Ensuite, nous décrivons aussi la virtualisation qui est une partie essentielle dans le *Cloud Computing*. Enfin, nous définissons le *Data Center*, sa conception architecturale, ses caractéristiques et ses classifications selon la norme de niveau.

2.1 Qu'est-ce que le Cloud Computing ?

2.1.1 Définitions

Il existe de nombreuses définitions du terme *Cloud Computing* (CC) et il y a peu de consensus sur une seule et universelle définition. Cette multitude de définitions reflète en soi la diversité et la richesse technologique du *Cloud Computing*. Dans ce qui suit, nous citons quelques une des plus pertinentes.

Selon [26, 28, 30, 35, 45], qui se basent sur une vision rapprochée des grilles de calcul *'Grid Computing'*, le *Cloud Computing* se base principalement sur le paradigme de l'informatique distribuée à grande échelle afin d'assurer un service à la demande accessible à travers Internet. Une deuxième définition, proposée dans [13, 42] et qui est plus abstraite, définit le *Cloud Computing* par l'utilisation des ressources informatiques (matériels et logiciels) qui sont offertes en tant que service à travers un réseau (typiquement Internet). Une troisième définition, élaborée par un groupe de travail de la commission européenne [37], considère le *Cloud Computing* comme un environnement d'exécution élastique de ressources impliquant de multiples acteurs pour offrir un service tarifé avec un certain niveau de qualité de service. Cette définition a été étendue dans [36] en prenant en considération les perspectives des différents acteurs de l'écosystème *Cloud Computing* (fournisseur, développeur, utilisateur).

Cependant, la définition proposée par la *National Institute of Standards and Technology (NIST)* dans [44], qui a été reprise par plusieurs travaux [6, 17, 23, 33, 34, 41, 47], est devenue quasi la référence et communément acceptée par le public. NIST définit le *Cloud Computing* comme étant un modèle qui permet l'accès via un réseau d'une façon simple et à la demande à un ensemble de ressources informatiques mutualisées et configurables (ex réseaux, serveurs, stockage, applications et services). Ces ressources informatiques peuvent être allouées et libérées rapidement avec le minimum d'effort de gestion ou d'interaction avec les fournisseurs de services. De plus, NIST précise que le *Cloud Computing* est composé de cinq caractéristiques essentielles, trois modèles de services et quatre modèles de déploiement. Ces éléments sont énumérés par la suite [29].

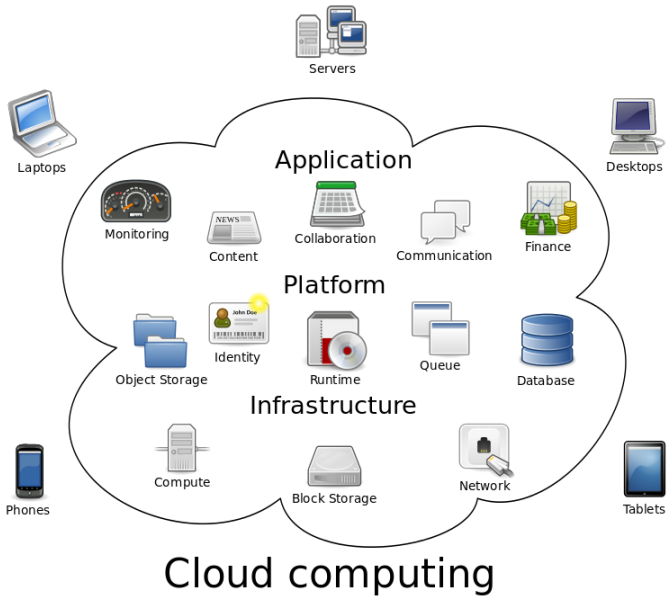

FIGURE 2.1 – *L'environnement du Cloud Computing*

2.1.2 Caractéristiques

Généralement, un service, une solution ou un environnement d'exécution devrait satisfaire une liste de caractéristiques pour qu'il soit considéré comme étant du *Cloud Computing* . Parmi ces caractéristiques, il y a celles qui sont reconnues comme fondamentales. Par exemple, *NIST* définit cinq caractéristiques essentielles qui sont [23, 44, 48] [29] :

- **Ressources à la demande**

Un utilisateur peut allouer unilatéralement des ressources informatiques (serveurs, réseau, stockage, environnement d'exécution, application) au besoin, de façon automatique et sans nécessité d'interaction humaine avec chaque fournisseur de services.

- **Large accès réseau**

Les ressources *Cloud Computing* sont disponibles à travers le réseau et accessibles via des mécanismes standards qui favorisent leurs utilisations à partir des appareils clients hétérogènes,

voire légères (ex ordinateurs portables, téléphones, tablettes).

- **Mutualisation des ressources**

Les ressources informatiques du fournisseur *Cloud Computing* sont mutualisées pour servir plusieurs clients en utilisant un modèle multi-tenant. Ces ressources, physiques ou virtuelles, sont allouées et libérées dynamiquement selon la demande du consommateur. Généralement, l'utilisateur n'a ni le contrôle ni la connaissance de l'emplacement exact des ressources allouées. Dans certains cas, il peut choisir l'emplacement géographique à un niveau haut (ex par pays, continent ou *Data Center*).

- **Élasticité rapide**

Les ressources sont allouées et libérées d'une façon élastique, idéalement d'une façon automatiquement, pour s'adapter rapidement à la demande qu'elle soit croissante ou décroissante. Pour le consommateur, les ressources disponibles à l'allocation apparaissent comme illimitées et peuvent s'allouer à tout moment.

- **Services mesurés**

Toutes les ressources allouées peuvent être surveillées et contrôlées afin de mesurer leurs consommations avec un niveau d'abstraction approprié selon le type du service (ex stockage, temps de calcul, bande passante).

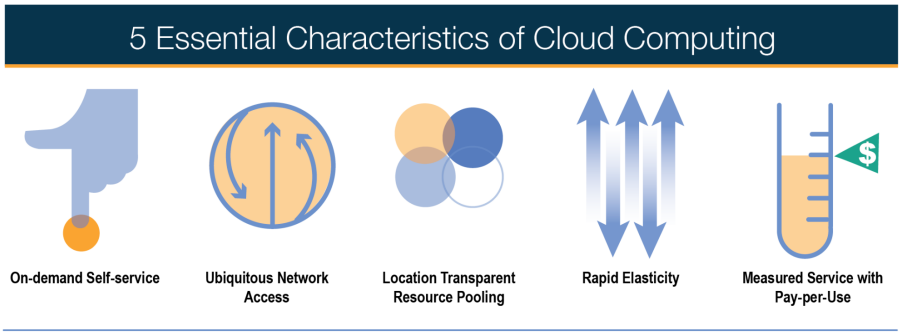

FIGURE 2.2 – *Caractéristiques du Cloud Computing*

2.1.3 Modèles de services

Afin de mieux définir la classification selon le type du service *Cloud Computing* et comme illustré dans la [Fig. 2.3], un environnement informatique standard peut être composé par plusieurs couches qui partent du bas niveau (le matériel physique) vers le haut niveau (l'application à utiliser). Ces couches sont : Matériel serveur, Réseau, Stockage, Virtualisation, Système d'exploitation, Bases de données, Intégration SOA, Moteur d'exécution, Données et Applications. La classification selon le type du service correspond au niveau de responsabilité dans la gestion de ces couches que ce soit par les fournisseurs ou par les utilisateurs. Traditionnellement, toutes les couches sont gérées par l'utilisateur lui-même. Avec le *Cloud Computing*, l'utilisateur n'a plus en charge la totalité des couches et en fonction du niveau des sous-ensembles de couche nous

distinguons le type de service. Selon NIST [34, 44] et d'autres travaux [10, 15, 28, 36, 37, 41, 56] et comme illustré dans la [Fig. 2.3] , il y a principalement trois types de services *Cloud Computing* [29] :

- **Infrastructure as a Service *(IaaS)***

Les services *Cloud Computing* de type *IaaS* correspondent à des ressources infrastructures offertes à la demande. Ces ressources sont des ressources de calculs, de stockage ou de réseau et peuvent être soit virtuelles, soit physiques. Le fournisseur a la gestion des couches Calcul, Stockage, Réseau et Virtulisation. L'utilisateur des ressources *IaaS* est responsable de la gestion de toutes les couches à partir et au-dessus du système d'exploitation. L'utilisateur n'a ni le contrôle, ni la gestion, ni la visibilité de l'infrastructure sous-jacente ;

- **Platform as a Service *(PaaS)***

Les services *Cloud Computing* de type *PaaS* correspondent principalement à des environnements de développement offerts à la demande. L'utilisateur n'a plus en charge que les couches de données et d'applications. Pour ce faire, il y a utilisation des librairies, langages et outils offerts par le fournisseur pour structurer ses données et développer ses applications. Une fois développé, le fournisseur doit déployer et maintenir le bon fonctionnement de l'application et cela en gérant toutes les couches basses allant de l'infrastructure jusqu'aux environnements d'exécution ;

- **Software as a Service *(SaaS)***

Les services *Cloud Computing* de type *SaaS* correspondent tout simplement à des applications prêtes à l'utilisation offertes à la demande. L'utilisateur n'a qu'à utiliser le service *Cloud Computing* offert. Il n'a rien à gérer et c'est le fournisseur qui a toute la responsabilité de maintenir le service en gérant toutes les couches.

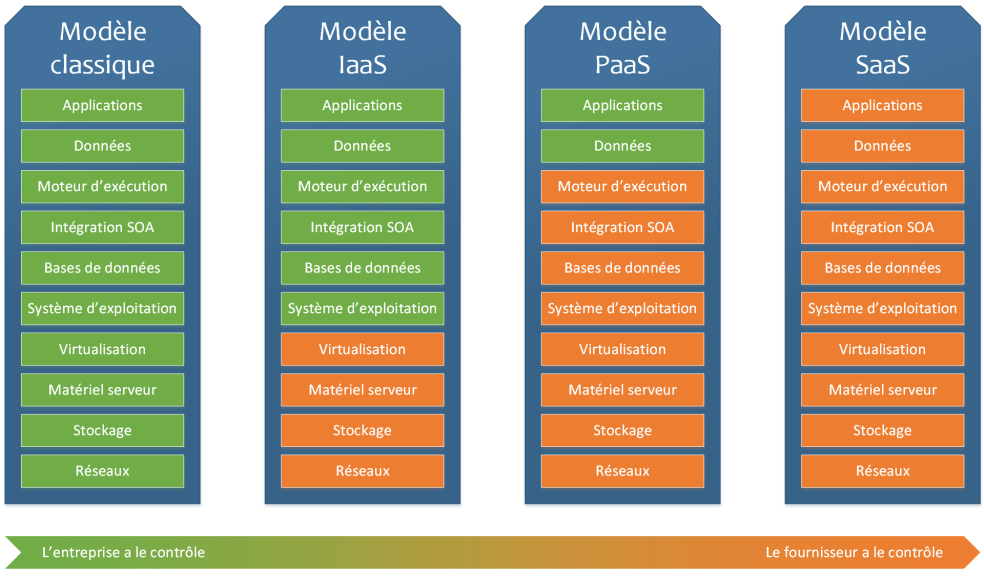

FIGURE 2.3 – *Types de service du* Cloud Computing

2.1.4 Modèles de déploiement

Pour classifier les modèles de déploiement *Cloud Computing*, il faut juste répondre à deux questions [6] : qui utilise le *Cloud* ? Et qui gère et possède l'infrastructure hébergeant le service *Cloud* ? Dans [34, 44], NIST a défini quatre modèles de déploiement. Ces modèles ont été aussi mentionnés dans plusieurs autres travaux [6, 17, 36, 42, 53]. Comme nous l'avons illustré dans la [Fig. 2.4], les quatre modèles sont [29] :

- **Cloud Public**

Dans un *Cloud Public*, le fournisseur gère l'infrastructure et offre ses services aux utilisateurs *Cloud* grand public d'une façon complètement ouverte. Les ressources informatiques sont partagées entre les utilisateurs. Ces derniers n'ont aucun contrôle ou visibilité sur l'infrastructure qui est gérée par un tiers (le fournisseur de *Cloud*).

- **Cloud Privé**

Dans un *Cloud Privé*, l'utilisateur des ressources *Cloud Computing* contrôle, voire possède, l'infrastructure d'hébergement. Les ressources disponibles ne sont pas destinées au grand public, mais pour une utilisation privée. Dans ce type de déploiement, l'infrastructure est gérée avec des solutions (Open Source ou propriétaire) de type *Cloud* pour offrir les ressources et services par le biais d'interface *Cloud*.

- **Cloud Hybride**

Dans un *Cloud Hybride*, les ressources peuvent être allouées à partir d'un *Cloud Privé* et d'un *Cloud Public*. C'est un environnement qui combine les deux modèles Public et Privé. Comme utilisation de ce type de *Cloud Hybride*, il est possible de stocker et gérer les données confidentielles dans l'environnement privé et celles qui sont moins confidentielles dans un *Cloud Public*. Une autre utilisation est d'avoir recours aux ressources *Cloud* publiques d'une façon ponctuelle, lors des pics d'activité.

- **Cloud Communautaire**

Dans un *Cloud Communautaire*, l'infrastructure de *Cloud* est provisionnée à l'usage exclusif d'une communauté d'utilisateurs, par exemple les organismes gouvernementaux. L'infrastructure peut être détenue, gérée et exploitée par un ou plusieurs des organismes de la communauté, un tiers, ou une combinaison d'entre eux.

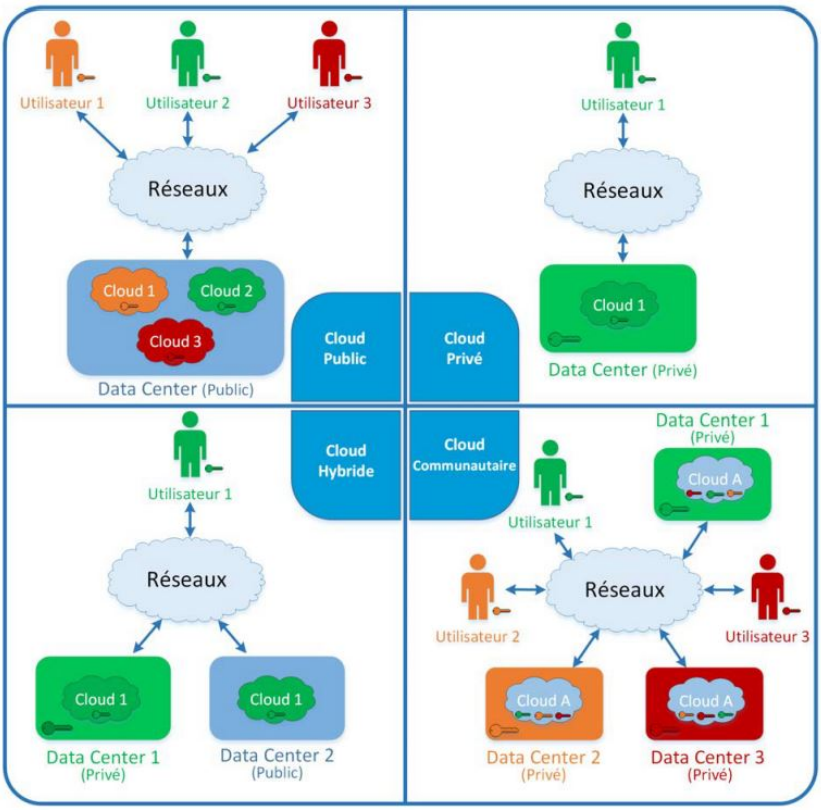

FIGURE 2.4 – *Modèles de déploiement du Cloud Computing* [29]

2.1.5 Avantages et inconvénients

Le *Cloud Computing* offre de nombreux avantages que plusieurs travaux ont listés [33, 37, 47, 50, 53, 56]. Parmi ces avantages, il y a [29] :

- Réduction des coûts d'infrastructure, de développement, des logiciels ;
- Des ressources et services plus rapide à allouer et plus simple à utiliser ;
- Augmentation de la puissance de calcul ;
- Grande capacité de stockage (quasi illimitée) ;
- Moins de problèmes d'entretien ;
- Gestion des mises à jour plus simple et rapide ;
- Pas de perte de données ;
- Tout est considéré comme un service défini par un SLA ;
- Infrastructure allouée et disponible juste à temps ;
- Réduction du temps de mise sur le marché.

Le *Cloud Computing* n'a pas que des avantages, il possède quelques obstacles et désavantages qui sont abordés dans [7, 33, 53]. Parmi ces inconvénients, il y a [29] :

- Confidentialité et Chiffrement des données ;

- Nécessité d'un accès réseau constant ;
- Mauvais fonctionnement avec les connexions à basse vitesse ;
- Faible niveau de la qualité de service dans le réseau ;
- Risque d'engorgements lors des transferts de données ;
- Problème d'interopérabilité et de de portabilité ;
- Faible contrôlabilité ;
- Manque de fonctionnalités d'audit ;
- Des contrats de service SLAs non normalisés.

2.1.6 Acteurs

Comme mentionné dans [19, 41] et comme illustré dans la [Fig. 2.5], l'écosystème du *Cloud Computing* est composé principalement par cinq acteurs majeurs (*Cloud Provider*, *Cloud Consumer*, *Cloud Carrier*, *Cloud Broker*, *Cloud Auditor*) [29] :

- **Cloud Provider** :

Le fournisseur des ressources *Cloud Computing*. Il est responsable de fournir un service *Cloud Computing* qui satisfait les caractéristiques définies dans la Section 2.1.2, tout en respectant les *Service Level Agreements* (SLAs) établies avec les autres acteurs (en particulier le *Cloud Consumer*). Le *Cloud Provider* a comme activité l'allocation, l'orchestration et la gestion des ressources qu'il offre tout en assurant le bon niveau de sécurité.

- **Cloud Consumer** :

L'utilisateur des ressources *Cloud Computing*. Cet utilisateur peut être un utilisateur final ou un développeur selon le type du service *Cloud* alloué. Cet utilisateur peut être une personne, un groupe de personnes, les petites et moyennes entreprises, les multinationales ou les gouvernements.

- **Cloud Carrier** :

Le fournisseur de réseau est l'intermédiaire qui assure principalement la connectivité entre les ressources *Cloud Computing* et la liaison entre les acteurs de l'écosystème *Cloud Computing* (en particulier entre le *Cloud Provider* et le *Cloud Consumer*). Cet utilisateur peut jouer un simple rôle d'acheminements des paquets, comme il peut jouer un rôle plus important en offrant des fonctionnalités avancées dans le réseau. Ces fonctionnalités sont basées sur des SLAs établies avec les autres acteurs de l'écosystème.

- **Cloud Broker** :

Le courtier *Cloud* est un intermédiaire qui négocie la relation entre les *Cloud Providers* et les *Cloud Consumers*. Il peut offrir de nouveaux services qui simplifient les tâches de gestion du *Cloud Consumer*. Ce dernier peut demander les ressources *Cloud Computing* auprès du *Cloud*

Broker au lieu du *Cloud Provider* directement. Pour récapituler, le *Cloud Broker* peut assurer l'orchestration, l'agrégation et l'arbitrage des services *Cloud Computing*.

- **Cloud Auditor** :

L'auditeur *Cloud* s'occupe de la vérification et l'audition des services *Cloud Computing*. Il évalue les services offerts par les *Cloud Providers*, *Cloud Carriers* et *Cloud Brokers* du point de vue performances et sécuritaires. Le but principal est de vérifier que les fournisseurs respectent bien les SLAs qu'ils proposent.

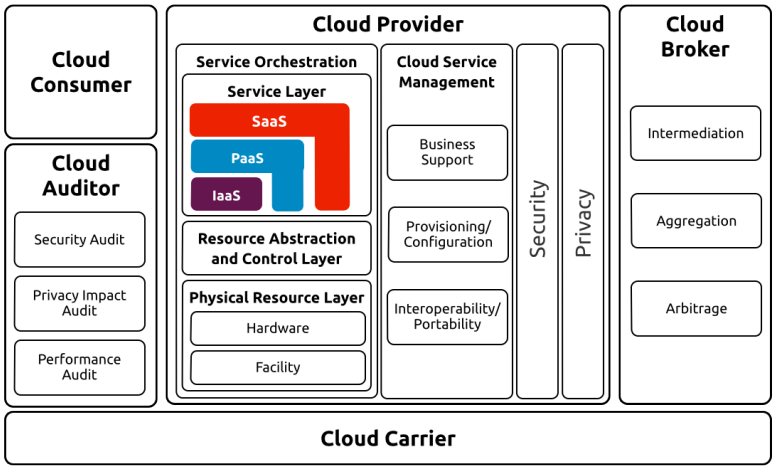

FIGURE 2.5 – *L'écosystème du* Cloud Computing

2.2 Virtualisation

La virtualisation consiste à utiliser une version émulée ou simulée (version virtuelle) d'une ressource (ex. un serveur) au lieu de la version réelle. Dans un *Data Center*, la virtualisation se symbolise par l'utilisation de machines virtuelles comme environnements d'exécution des applications au lieu d'un système d'exploitation fonctionnant directement sur un vrai matériel [3, 31, 59].
Virtualiser un serveur [31] consiste à faire fonctionner plusieurs systèmes d'exploitation, appelés systèmes invités, au dessus du système d'exploitation de ce serveur appelé serveur hôte, serveur physique ou encore machine hôte [Fig. 2.6]. Les différents systèmes virtuels aussi appelés instances virtuelles, machines virtuelles, serveurs virtuels, ou encore systèmes invités se partagent les ressources physiques du serveur (mémoire, CPU, disque, réseau ...), mais la virtualisation doit satisfaire une propriété essentielle : l'isolation entre eux. Les serveurs virtuels doivent en effet être isolés mutuellement l'un de l'autre. Autrement dit, aucune des instances virtuelles ne doit pouvoir accéder directement ou indirectement aux ressources réservées à une autre instance.

La virtualisation d'un serveur nécessite un outil spécifique, à l'instar de KVM, Microsoft Hyper-V, VMware ESXi/ESX (de la suite VMware vSphere) ou Xen, pour gérer le cycle de vie des machines virtuelles. Appelé hyperviseur ou un gestionnaire de machine virtuelle.

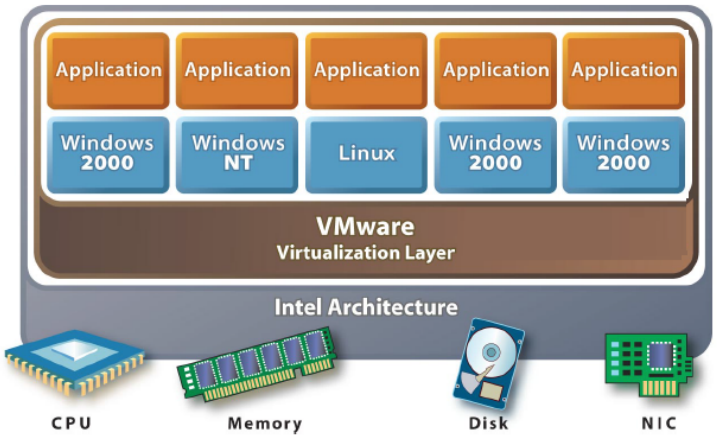

FIGURE 2.6 – *Principe de la virtualisation et de la consolidation*

Machine Virtuelle (MV)

Une machine virtuelle, également appelé *Virtual Machine (VM)*, est un système d'exploitation isolé par son hyperviseur physique hôte. Le client exécute ces taches sur les machines virtuelles comme s'il était sur une machine hôte physique. Une MV est généralement crée à partir de plusieurs paramètres : un hôte configuré qui émule un hôte physique avec CPU virtuel, RAM, et disques de stockage virtuels ; et une image qui donne un aperçu du système exploitation.

Hyperviseur

L'hyperviseur, également appelé *Virtual Machine Monitor (VMM)*, est le composant essentiel de la couche de virtualisation. L'hyperviseur est une plate-forme de virtualisation qui permet d'activer et exécuter plusieurs systèmes d'exploitation invités (ou *machine virtuelle*) simultanément sur une seule machine hôte. C'est l'hyperviseur qui alloue, multiplexe, partage et partitionne dynamiquement les ressources physiques entre toutes les *VMs*.

Il ne faut cependant pas confondre virtualisation et *Cloud Computing*, car le dernier consiste essentiellement à fournir des ressources informatiques partagées, à la demande via Internet selon des modèles de services ; ce qui est justement réalisable grâce à la virtualisation. Que l'on soit ou non dans le *Cloud*, il est toujours possible de virtualiser son infrastructure.

Avantages de la virtualisation dans les entreprises

La virtualisation permet de faire fonctionner plusieurs machines virtuelles dans un seul serveur physique. Cette technique convient aux petites et grandes entreprises qui voient plusieurs avantages à la virtualisation [22] :

- **Le nombre de serveurs physiques est réduit**

Le nombre de machines nécessaires au bon fonctionnement du serveur informatique diminue

grâce à la virtualisation. Ainsi, la virtualisation diminue le coût d'achat de serveurs et l'entretien de ces derniers.

- **Des machines virtuelles disponibles**

Grâce à la virtualisation, il est possible de déplacer une machine virtuelle d'un serveur physique à un autre, ce qui garantit un meilleur taux de disponibilité des services.

- **Des performances optimales**

La virtualisation à l'avantage de répartir la charge de travail si une machine virtuelle monte en charge de manière inhabituelle, les autres machines virtuelles pourront ainsi fonctionner sur un serveur physique moins sollicité.

- **Une sécurité accrue**

Dans une structure traditionnelle, si un malware infecte la messagerie, l'ensemble des applications sont vulnérables. Avec la virtualisation, les tâches d'un serveur physique sont isolées et les services sont cloisonnés.

- **Un impact environnemental moindre**

La virtualisation permet de réduire la consommation électrique d'une infrastructure informatique.

2.3 Data Center

Un *Data Center*, ou centre de données, est un site physique sur lequel se trouvent regroupés des équipements constituant le système d'information de l'entreprise (ordinateurs centraux, serveurs, baies de stockage, équipements réseaux et de télécommunications, etc.). Il peut être interne et/ou externe à l'entreprise, exploité ou non avec le soutien de prestataires. [8] C'est un service généralement utilisé pour remplir une mission critique relative à l'informatique. Il sert à traiter l'information nécessaire aux activités de l'entreprise mais aussi aux activités du grand public.

2.3.1 Composition d'un Data Center

Après avoir défini ce qu'était un *Data Center*, nous allons maintenant voir de quoi il est composé. Celui-ci comprend des ressources informatiques (serveurs + disques + réseau) dans un bâtiment dédié. Une infrastructure technique assurant la continuité de l'alimentation électrique, du refroidissement et de l'accès télécommunication afin que ces ressources informatiques soient toujours disponibles. Le tout se trouvant dans le bâtiment dont la salle informatique est le plus souvent sécurisée (caméras de surveillance, etc.) pour ne pas permettre l'accès à des personnes non-autorisées. De par son utilisation électrique intense, un *Data Center* est souvent situé près d'un point d'accès de très forte puissance électrique et situé près d'un point d'accès à large bande passante [Fig. 2.7].

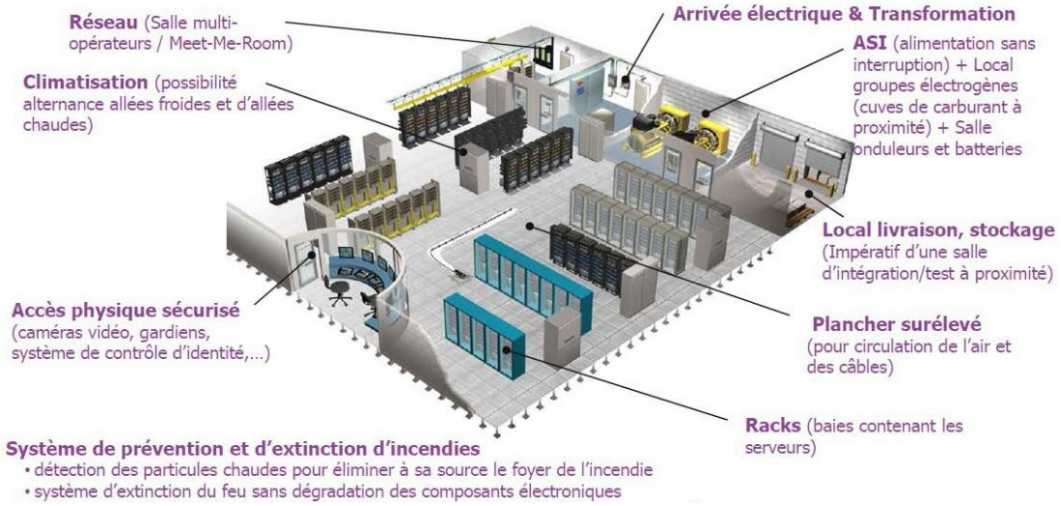

FIGURE 2.7 – *Architecture globale d'un Data Center*

2.3.2 Caractéristiques des Data Centers d'aujourd'hui

Les *Data Centers* sont des bâtiments qui doivent se plier aux contraintes du processus informatique et constituer un socle durable pour contribuer au développement de l'entreprise. Ils doivent répondre à des défis sans précédents. En effet, ils doivent pouvoir être flexibles, avoir un taux de disponibilité de plus de 99% et être sûrs. En plus de ces qualités, ils doivent être aussi de plus en plus «green» pour répondre à l'enjeu environnemental.

Selon Tetreau [57], la liste des caractéristiques que l'on peut attendre des *Data Centers* de nos jours est la suivante :

• **Flexibilité** : dynamisme pour intégrer de nouvelles données business, techniques ou environnementales ;

• **Disponibilité** : continuité opérationnelle en cas de défaillances techniques ou humaines ;

• **Sûreté** : résistance phénomènes naturels ou tout autre problème (incendies, etc.) ;

• **Green** : limitation de l'empreinte carbone, une optimisation du coût global de possession et une vision transversale de tous les domaines du green (le bâtiment, les économies d'énergie, la gestion des déchets, l'approvisionnement en eau et en électricité).

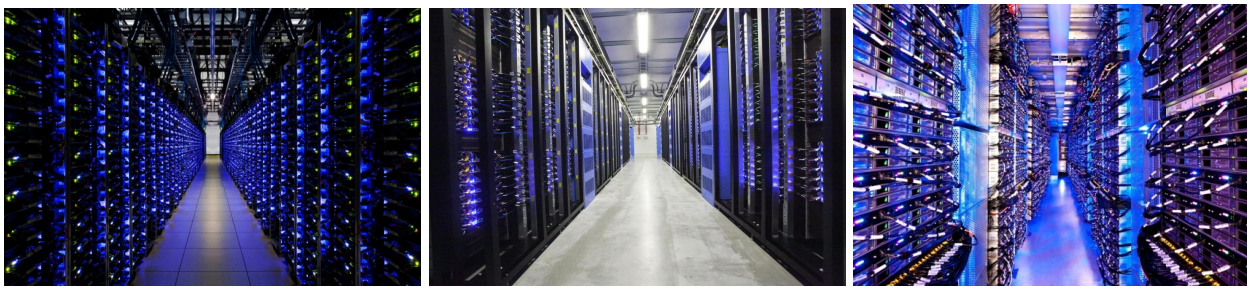

FIGURE 2.8 – *Exemples de Data Centers : Google, Facebook et Microsoft*

2.3.3 Topologie réseau d'un Data Center

Sur la [Fig. 2.9], nous retrouvons le modèle hiérarchique mis de l'avant et diffusé par Cisco [64] ; cette topologie est largement utilisée dans les *Data Centers*.

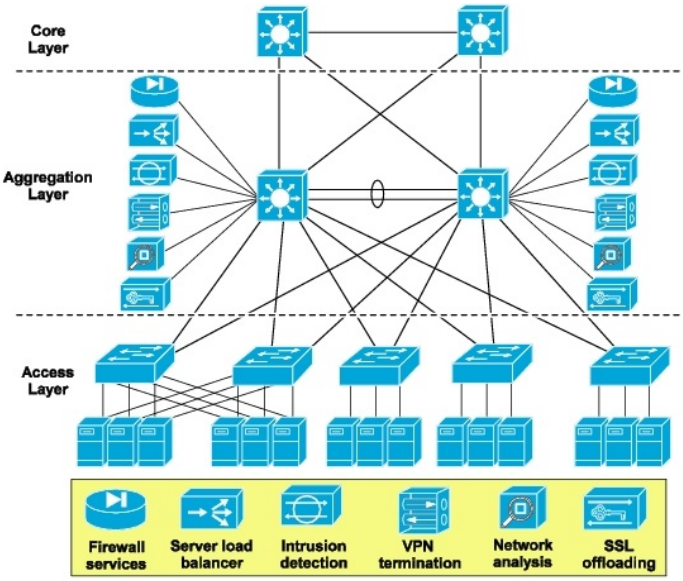

FIGURE 2.9 – *L'infrastructure de réseau du Data Center [64]*

Cisco préconise l'utilisation d'une topologie hiérarchique en trois couches pour garantir une haute-disponibilité des services :

• **La couche d'accès** (*Access Layer*) Permet de connecter des commutateurs aux périphériques de bout de réseau, dans le cas présent, les serveurs.

• **La couche d'agrégation** (*Aggregation Layer*) Joue un triple rôle : filtrer, router et autoriser les paquets (le rôle d'un pare-feu en somme). Le premier niveau de segmentation de sécurité, intervient à cet endroit précis. Cette couche fait la liaison entre le cœur de réseau et la couche d'accès.

• **La couche cœur de réseau** (*Core Layer*) Connecte le *Data Center* à Internet et à d'autres réseaux externes ; les routeurs se veulent très rapides pour supporter la charge du réseau.

2.3.4 Classification des Data Centers

Les *Data Centers* sont conçus sur deux critères principaux qui sont la haute disponibilité, pour que les applications informatiques ne s'arrêtent jamais et l'efficacité énergétique pour minimiser la facture énergétique et l'empreinte carbone de cette activité [8]. C'est pourquoi, l'organisme Uptime Institut [58] a défini une classification qui est reconnue internationalement par les *Data Centers* et qui se compose de quatre catégories, appelées « Tier ». Chaque Tier correspond

à des niveaux d'équipements et de disponibilités différents.

Niveau Tiers I : Un *Data Center* Tiers 1 ne dispose de capacité de redondance (alimentation électrique et système de refroidissement) et peu ou pas de redondance matérielle. Ce niveau de note (N). Cette certification correspond généralement à un taux de disponibilité de 99.671 %, une mesure qui est considérée comme acceptable des applications peu critiques.

Niveau Tiers II : Cette certification accorde une redondance de niveau (N+1) ; en revanche, elle ne fournit pas de redondance d'ordre électrique ou du système de refroidissement. Par conséquent, le taux de disponibilité atteint environ 99.75% ; ce pourcentage est satisfaisant pour la majorité des applications.

Niveau Tiers III : Ce niveau vise un taux de disponibilité de 99,982% via la redondance (N+1) des équipements informatiques en plus d'une redondance des matériels électriques et de refroidissement. Cette certification à l'inverse des niveaux 1 et 2 n'a pas d'impact sur la disponibilité lors des opérations sur les données.

Niveau Tiers IV : Nous arrivons au plus haut niveau de certification avec un minimum de 99,995% de disponibilité via la redondance 2(N+1) des équipements (informatiques, électriques, et de refroidissement). La sagesse serait de recommander cette mesure aux applications ultra-critiques (bourses, finances, applications critiques temps réel, etc.).

Type de Tier	Caractéristiques	Niveau de redondance	Taux de disponibilité	Arrêt annuel	Maintenance à chaud possible	Tolérance aux pannes
Tier 1	Non redondant	N	99,671%	28,8 h	Non	Non
Tier 2	Redondance partielle	N+1	99,749 %	22 h	Non	Non
Tier 3	Redondance actif/passif	N+1	99,982%	1.6 h	Oui	Non
Tier 4	Redondance actif/passif	2(N+1)	99,995%	0.4 h	Oui	Oui

TABLE 2.1 – *Récapitulatif des niveaux de tiers dans un Data Center*

2.4 Accord de niveau de service (SLA)

Accord de niveau de service ou *Service-Level Agreement*, est un contrat par lequel un prestataire informatique s'engage à fournir un ensemble de services à un ou plusieurs clients. Autrement dit, il s'agit d'une clause contractuelle qui définit les objectifs précis et la qualité du service à attendre de la part du prestataire signataire.

Le SLA est intimement lié à l'univers du *Cloud*. Il permet de garantir aux clients certains niveaux de sécurité dans le stockage et la gestion de leurs données à caractère personnel. Il faut alors définir de façon très précise différents indicateurs de qualité pouvant être mesurés, analysés et contrôlés régulièrement. Il convient enfin de prévoir des sanctions qui seront appliquées si le prestataire ne répond pas à ses obligations mentionnées dans le SLA.
Les SLA calculent les performances en spécifiant les éléments de mesure ou indicateurs suivants [39] :

- La disponibilité (Pourcentage de temps durant lequel les services sont disponibles) ;
- La fiabilité (Définit par exemple le nombre d'échecs par semaine) ;
- Le nombre d'utilisateurs pris en charge simultanément ;
- Le temps de réponse des applications ;
- La pérennité des Données ;
- Le périmètre de responsabilité ;
- Le dédommagement ;
- Le délai de réponse du service d'assistance pour différentes catégories de problèmes ;
- Des statistiques d'utilisation ;
- Un calendrier des notifications préalables à des modifications du réseau susceptibles d'affecter les utilisateurs.

Conclusion

Ce chapitre a permis de nous familiariser avec le paradigme du *Cloud Computing*, ses concepts et ses différentes technologies. Nous avons également pu voir quelques généralités essentielles sur les *Data Centers* pour une meilleure compréhension du sujet traité dans notre travail qui sera présenté dans le chapitre 4.

Dans le chapitre qui suit, nous allons présenter les concepts théoriques liés au sûreté de fonctionnement (fiabilité, maintenabilité, disponibilité), ainsi que les mécanismes qui permettent d'assurer la haute disponibilité.

Chapitre 3

Généralités sur la Disponibilité et de la Haute Disponibilité

Introduction

Pour mener à bien notre étude et afin de mieux cerner et de répondre précisément à notre problématique, nous présentons à travers ce chapitre quelques concepts de base mathématiques nécessaires à une meilleure compréhension de la notion du disponibilité et l'état de l'art des solutions de haute disponibilité actuellement utilisées par les fournisseurs de service *Cloud* dans le biais de l'informatique.

3.1 Définition

La disponibilité est définie comme étant la probabilité qu'un système soit opérationnel à chaque fois que son utilisation est requise [16]. Elle constitue ainsi l'un des indicateurs clés de performance d'un système de stockage *infonuagique*, indiquant la fréquence à laquelle un système est en état de fonctionnement et permet, en outre, de renseigner sur la rentabilité du système à la fois pour l'opérateur de stockage *infonuagique* qui cherche à éviter de payer des pénalités suite à une incapacité à satisfaire une exigence SLA mais également pour les clients dont la rentabilité économique dépend de la continuité de leurs services.
Par définition, le concept de disponibilité combine, en son sein, les concepts de fiabilité et de maintenabilité, quantifiant respectivement la durabilité et la quantité de maintenance/ réparations envisageable pour la durée de vie du système.
Dans ce cadre, il convient alors de définir au préalable les notions de fiabilité et de maintenabilité pour mieux comprendre la modélisation de la disponibilité [14].

3.2 Fiabilité

La fiabilité est la probabilité qu'un produit ou un service fonctionne adéquatement et sans panne durant une période de temps spécifiée et dans des conditions spécifiques [16].
D'un point de vue mathématique, la fiabilité est définie par la probabilité qu'une entité soit non défaillante sur une durée prédéfinie $[0, t]$ cela veut dire que l'entité doit être en état de bon fonctionnement à $\tau = t$ sachant qu'elle était en bon état à l'instant d'être mise en service $\tau = 0$; cela représente la période de temps durant laquelle le fonctionnement est assuré. Si on considère t_f une variable aléatoire qui représente le temps jusqu'à la première défaillance (*time to first failure*), et t le temps actuel, nous avons [61] :

$$R(t) = \Pr(\text{Système non défaillant à } \tau = t | \text{ il n'est pas défaillant à } \tau = 0) \tag{3.1}$$

$$R(t) = \Pr(\text{Système non défaillant sur} [0, t]) \tag{3.2}$$

$$R(t) = \Pr(t_f > t); t > 0; \tag{3.3}$$

L'aptitude contraire qui représente la probabilité de défaillances est appelée la dé-fiabilité (*unreliability*), c'est le complément de la fiabilité, et il est défini par la probabilité qu'une entité ne réussisse pas à fournir sa mission pendant au moins une phase $\overline{R}(t)$, où :

$$\overline{R}(t) = 1 - R(t) \tag{3.4}$$

$$\overline{R}(t) = \Pr(t_f \leqslant t); t > 0 \tag{3.5}$$

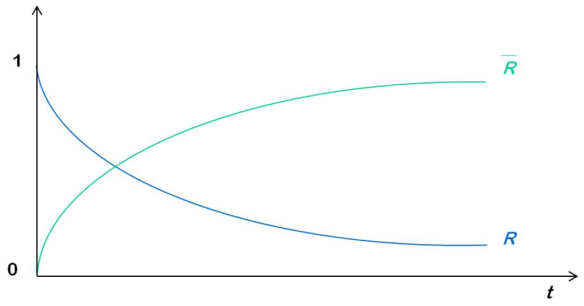

FIGURE 3.1 – *Fiabilité R, dé-fiabilité* $\overline{R}$

La fiabilité est donc concernée par un fonctionnement sans défaillance du système pendant une durée donnée, alors que la fonction ou le terme $\overline{R} = 1 - R(t)$ représente la fonction de répartition $F(t)$ qui est définie par la probabilité que la défaillance se produise pendant $[0, t]$. En dérivant la fonction de répartition à l'instant de la défaillance, on obtient la densité de probabilité $f(t)$ ou la densité des défaillances.

$$\Pr(t < t_f < t + dt) = F(t + dt) - F(t) = f(t)dt \tag{3.6}$$

$$f(t) = \lim_{dt \to 0} \frac{F(t + dt) - F(t)}{dt} = \frac{dF(t)}{dt} = -\frac{dR(t)}{dt} \tag{3.7}$$

$$R(t) = -\int_0^t f(t)dt = \int_t^\infty f(t)dt \tag{3.8}$$

La fonction de densité $f(t)$ représente le nombre des défaillances ; et la fonction $R(t)$ représente le nombre des entités survivantes ; et dans ce sens, on présente la notion de taux des défaillances *(Failure rate)* $\lambda(t)$ qui peut être calculé à partir de ces deux fonctions :

$$\lambda(t) = \frac{\text{Nombre des défaillances}}{\text{Nombre des entités survivantes}} \tag{3.9}$$

$$\lambda(t) = \frac{f(t)}{R(t)} \tag{3.10}$$

Le taux de défaillance $\lambda(t)$ peut être défini par la probabilité d'avoir une défaillance sur $[t, t+dt]$ sachant qu'il n'y a pas eu de défaillance sur $[0, t]$.

$$\frac{\Pr(\text{Déf sur } [t, t+dt] \text{et non déf sur } [0, t])}{\Pr(\text{Non déf sur } [0, t])} \tag{3.11}$$

$$\lambda(t) = \lim_{dt \to 0} \frac{F(t+dt) - F(t)}{dt} \frac{1}{R(t)} = \frac{f(t)}{R(t)} \tag{3.12}$$

$$\lambda(t) = -\frac{1}{R(t)} \frac{dR(t)}{dt} \tag{3.13}$$

Le taux de défaillances permet de définir la probabilité instantanée de tomber en panne. On s'intéresse aussi à la vie complète du système en présentant un paramètre associé à la fiabilité, c'est une grandeur statistique finie qui exprime la durée moyenne jusqu'à la défaillance MTTF (*mean time to failure*) illustrée dans la Figure ci-dessous [3.2] et qui est définie par :

$$MTTF = \int_0^\infty R(t)dt \tag{3.14}$$

Dans la Figure [3.2], on calcule le MTTF à partir de la moyenne statistique de toutes les défaillances, t_{fi} est le temps avant défaillance de l'élément i et n est le nombre des défaillances.

$$MTTF = \frac{t_{f1} + t_{f2} + t_{f3} + ... + t_{fn}}{n} \tag{3.15}$$

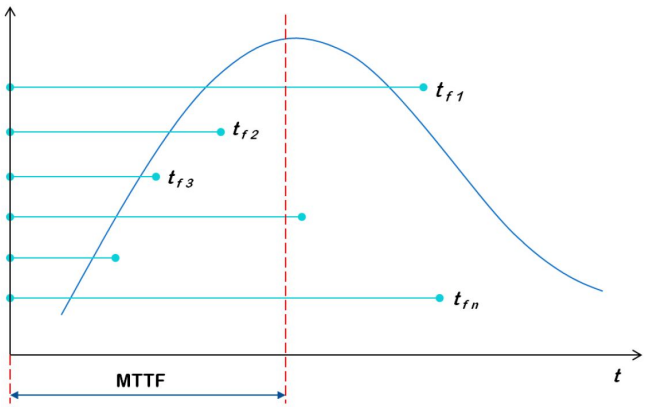

FIGURE 3.2 – *MTTF*

Il est impératif de ne pas confondre avec la durée moyenne jusqu'à la première défaillance MTTFF (*mean time to first failure*). Il reste enfin à évoquer une grandeur de fiabilité qui exprime le temps moyen entre défaillances MTBF (*mean time between failures*) qui représente la durée de vie moyenne utile d'une entité jusqu'à sa prochaine défaillance. La Figure suivante [3.3] illustre la notion de ces trois paramètres associés à la fiabilité.

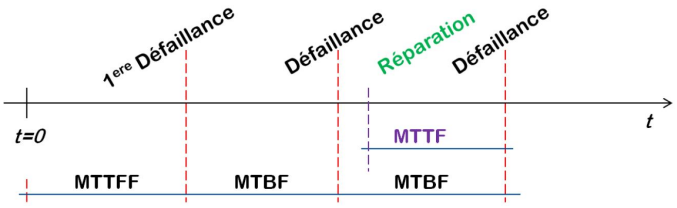

FIGURE 3.3 – *MTTFF, MTBF, MTTF*

En conclusion, on peut associer à la fiabilité les paramètres suivants :

- MTTF
- Taux de défaillance
- La probabilité que l'entité ne tombe pas en panne sur $[0, t]$
- La probabilité que l'entité soit capable de fournir sa fonction à l'instant t

Blocs Diagramme de fiabilité (BDF)

La méthode des blocs diagrammes de fiabilité est une des premières méthodes a avoir été utilisée pour analyser les systèmes et elle permet des calculs de fiabilité. Elle est aussi appelée la Méthode du Diagramme de Succès (MDS). C'est une représentation de la logique de fonctionnement des systèmes car elle est souvent proche de leur schéma fonctionnel. Cette méthode est basée sur l'utilisation de blocs pour représenter les composants, les sous-systèmes ou les fonctions. La modélisation consiste à rechercher les liens existant entre ces blocs. Un diagramme de fiabilité est défini par :

- Une entrée E, un corps de diagramme et un sortie. S
- Un flux est transmis de E jusqu'à S en passant par les différents chemins.
- Défaillance d'une entité arrête le flux au niveau du composant.
- S'il n'existe pas de chemin jusqu'à S, le système est défaillant, sinon il fonctionne.
- Configuration série ou/et parallèle.

3.3 Maintenabilité

La maintenabilité est un concept faisant référence à la capacité de maintenir le fonctionnement ou de réparer l'équipement en accord avec les conditions de fonctionnement et d'intervalle de temps limite définies. La maintenabilité est exprimée par : [14]

$$M(t) = \Pr(\text{ La maintenance d'un système soit achevée au temps t }) \tag{3.16}$$

L'aptitude contraire est appelée "immaintenabilité", c'est la probabilité que le système ne soit pas réparé sur la durée [0, t].

$$\overline{M}(t) = 1 - M(t) \tag{3.17}$$

Parmi les grandeurs associées à la maintenabilité, on appelle taux de réparation $\mu(t)$, d'un système réparable, la probabilité que le système soit réparé entre t et $t + dt$ sachant qu'il n'était pas réparé sur l'intervalle $[0, t]$.

$$\mu(t) = \Pr(\text{ Système réparé sur}[t, t + dt]|\text{non réparé sur}[0, t]) \tag{3.18}$$

$$\mu(t) = \frac{1}{1 - M(t)} \frac{dM(t)}{dt} \tag{3.19}$$

L'indice de la maintenabilité est la durée moyenne de maintenance ou de réparation, elle représente le temps technique moyen de réparation MTTR *(Mean time to repair)*.

$$MTTR = \frac{\text{Le temps total d'arrêt}}{\text{Le nombre d'arrêts}} \tag{3.20}$$

$$MTTR = \int_0^\infty (1 - M(t))dt \tag{3.21}$$

Le MTTR englobe le temps de :

- La détection du problème
- La durée pour préparer une équipe de maintenance
- Le diagnostic et l'identification des pannes
- L'obtention des pièces de rechange
- La durée de réparation
- Les tests et les contrôles après réparation
- Le démarrage de l'équipement pour reprendre le service.

3.4 Disponibilité

La disponibilité selon la norme *(NF X 60-500)* est l'aptitude d'un bien à être en état d'accomplir une fonction requise dans des conditions données, à un instant donné ou pendant un intervalle de temps donné, en supposant que la fourniture des moyens extérieurs nécessaires soit assurée [63]. À ce titre, elle représente un indicateur de performance plus réaliste d'un système tel que celui du stockage *infonuagique*. En somme, maintenir la disponibilité d'un équipement se résume à deux aspects : Le premier consiste à s'assurer que l'équipement ne tombe pas en panne aussi longtemps que possible. Le deuxième étant de réparer l'équipement aussi rapidement que possible. Alors que l'indisponibilité $\overline{A}(t)$ est l'aptitude contraire, c'est la probabilité que le système soit défaillant à l'instant t.

$$A(t) = \Pr(\text{Système est non défaillant à l'instant} t) \tag{3.22}$$

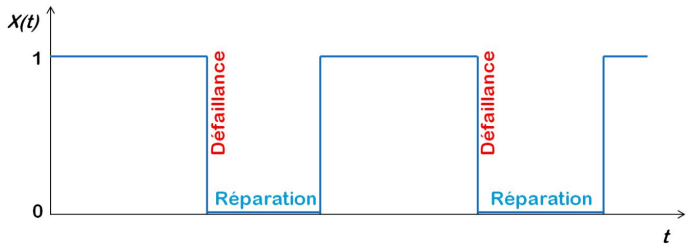

FIGURE 3.4 – *L'état du système*

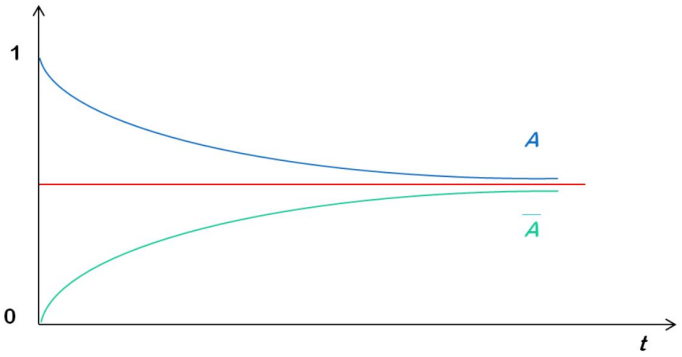

FIGURE 3.5 – *Disponibilité, indisponibilité*

Si $X(t)$ était un indicateur qui dénote l'état [Fig. 3.4] d'une entité ou d'un système à l'instant t donc [62] :

$$X(t) = \begin{cases} 1 & \text{Si le système est en état de fonctionnement à l'instant } t \\ 0 & \text{Si le système est en panne} \end{cases}$$

$$A(t) = \Pr(X(t) = 1) \tag{3.23}$$

$$\overline{A}(t) = \Pr(X(t) = 0) = 1 - A(t) \tag{3.24}$$

De la même façon, la disponibilité instantanée $A_i(t)$ est définie comme la probabilité que le système soit en état de fonctionnement à l'instant t, et pas forcément en cet état pendant toute la durée de mission sur $[0, t]$. Pour les systèmes non réparables, la fiabilité et la disponibilité sont les mêmes $A(t) \equiv R(t)$, alors que dans les systèmes réparables $A(t) \geqslant R(t)$, cela est dû à la possibilité d'effectuer les réparations ; la seule différence est que la fiabilité est la probabilité que le système fonctionne sans avoir des défaillances jusqu'à l'instant t [62]. Dans les systèmes qui possèdent des comportements qui peuvent être décrits par des processus markoviens (lorsqu'on utilise les probabilités pour modéliser l'état du système), on peut présenter la disponibilité stationnaire comme :

$$A_s = \lim_{t \to \infty} A(t) \tag{3.25}$$

La disponibilité peut tout simplement signifier la capacité d'une entité d'être dans l'état de fonctionnement pendant une durée de temps donnée. Les grandeurs moyennes associées à la disponibilité sont les suivantes [Fig. 3.6] :

• **MUT** (*mean uptime*) : Le temps moyen de la disponibilité, ou la durée de bon fonctionnement après réparation et avant la défaillance.
• **MDT** (*mean downtime*) : Le temps moyen d'indisponibilité ou la durée moyenne d'indisponibilité entre la défaillance et la remise en état suivante. Ces deux grandeurs permettent le calcul de MTBF *(Mean Time Between Failure)* :

$$MTBF = MUT + MDT \tag{3.26}$$

$$MTBF = \frac{\text{Somme des temps de bon fonctionnement}}{\text{Le nombre des défaillances}} \tag{3.27}$$

La relation de base qui décrit la disponibilité est la suivante :

$$Disponibilité = \frac{\text{Durée moyenne de fonctionnement après réparation}}{\text{Le temps total}} \tag{3.28}$$

$$A(t) = \frac{\text{Uptime}}{\text{Uptime + Downtime}} = \frac{\text{MUT}}{\text{MUT + MDT}} \tag{3.29}$$

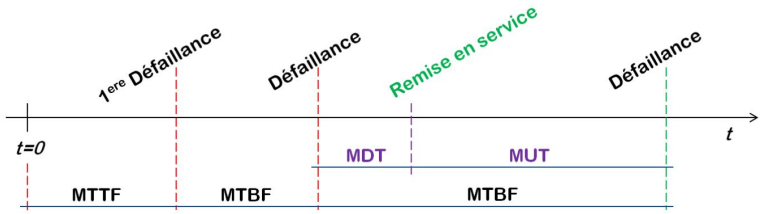

FIGURE 3.6 – *MUT, MDT*

Les paramètres déterministes de la disponibilité sont la fréquence des pannes et le temps de réparation ; plus le temps de réparation est court, plus la disponibilité est haute.

3.4.1 Types de disponibilité

On va citer dans ce paragraphe les deux types de disponibilité les plus connus [18] :

• **La disponibilité intrinsèque** :

C'est la probabilité qu'un système ou un équipement fonctionne de manière satisfaisante à tout instant durant le temps de fonctionnement dans des conditions données. La disponibilité intrinsèque représente le point de vue du constructeur, elle ne prend en compte que la disponi-

bilité pendant la période de fonctionnement et elle s'exprime de la façon suivante, en notant que *MTTR* est le temps moyen de réparation *(Mean time to repair)* : [61]

$$A_i = \frac{\text{Temps de disponibilité}}{\text{Temps de disponibilité} + \sum \text{Temps d'arrêt pour la réparation}} \tag{3.30}$$

$$A_i = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}} = \frac{1}{1 + \frac{\text{MTTR}}{\text{MTBF}}} \tag{3.31}$$

• **La disponibilité opérationnelle** :

C'est la probabilité qu'un système ou un équipement fonctionne de façon satisfaisante, à tout instant, durant le temps d'utilisation opérationnelle, dans des conditions déterminées. La disponibilité opérationnelle représente le point de vue de l'utilisateur, elle prend en compte tous les événements reliés à l'exploitation et elle s'exprime de la façon suivante :

$$A_o = \frac{\text{MTBM}}{\text{MTBM + MDT}} \tag{3.32}$$

Où MTBM (*Mean Time Between Maintenance*) est le temps moyen entre les actions de maintenance préventive ou corrective et MDT (*Mean Down Time*) est la moyenne de des temps d'arrêts (administratifs, logistiques et maintenance).

Le graphe ci-dessous [Fig. 3.7] montre la relation entre la disponibilité intrinsèque et la disponibilité opérationnelle.

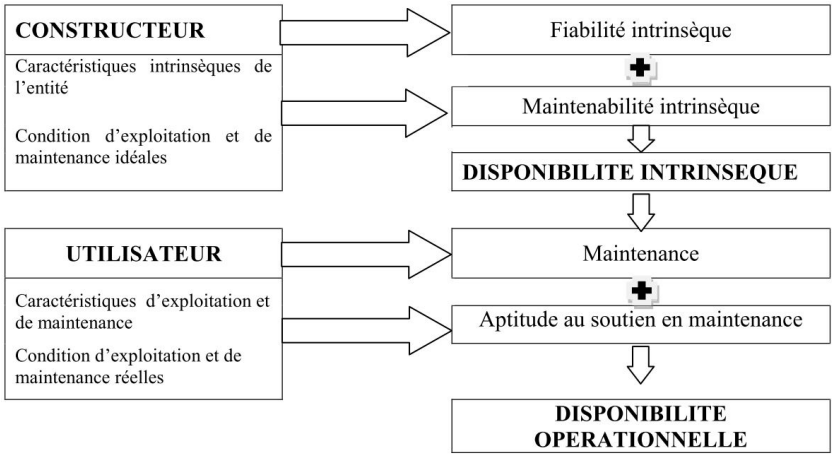

FIGURE 3.7 – *Disponibilités intrinsèque et opérationnelle*

3.4.2 Disponibilité des systèmes multi-composants

Le terme système est présent dans tous les domaines : mécanique, électronique, informatique, etc. Ce terme se réfère généralement à toute entité formée d'un ensemble ordonné d'éléments indépendants. De plus, tout système est conçu pour assurer une fonction bien déterminée. Cette dernière est définie par les relations que ces composants entretiennent entre eux [32].

Une fois la disponibilité de tous les composants d'un système calculée, nous pouvons appliquer les relations issues des blocs diagrammes fonctionnels (BDF) pour calculer la disponibilité de tout le système [24]. Dans cette partie, nous allons mettre en œuvre les différentes configurations de systèmes.

Système série :

Un système série se caractérise par l'enchaînement linéaire de n éléments [Fig. 3.8]. D'après sa structure, la défaillance de l'un de ses n composants entraîne la défaillance du système complet car chaque élément dépend de l'élément qui le précède [32].

FIGURE 3.8 – *Diagramme de fiabilité d'un système avec structure série*

La disponibilité du système complet A_S est égale au produit des disponibilités de chaque composant :

$$A_S(t) = \prod_{i=1}^{n} A_i(t) \tag{3.33}$$

Système parallèle :

Un système parallèle se caractérise par une association parallèle de tous les composants [Fig. 3.9]. Généralement, la défaillance de l'un ou de plusieurs éléments n'entraine pas la panne du système, ce dernier ne tombe en panne que si l'ensemble des éléments tombe en panne.

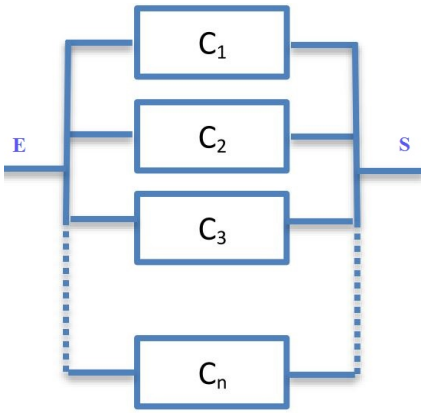

FIGURE 3.9 – *Diagramme de fiabilité d'un système avec structure parallèle*

La probabilité de panne du système P_S est égale au produit de la probabilité de panne de chaque composant :

$$P_S(t) = \prod_{i=1}^{n} P_i(t) = \prod_{i=1}^{n} (1 - A_i(t)) \tag{3.34}$$

Alors la disponibilité A_s du système est :

$$A_S(t) = 1 - \prod_{i=1}^{n}(1 - A_i(t)) \tag{3.35}$$

Système série-parallèle :

Le système série-parallèle est constitué de n sous-systèmes connectés en parallèle tel que chaque sous-système est composé de k éléments placés en série [Fig. 3.10].
Un système série-parallèle est le résultat de l'association des deux systèmes série et parallèle. Pour calculer sa disponibilité, on réduit le système complet en un système parallèle en modélisant chaque sous-système en série par un seul composant.

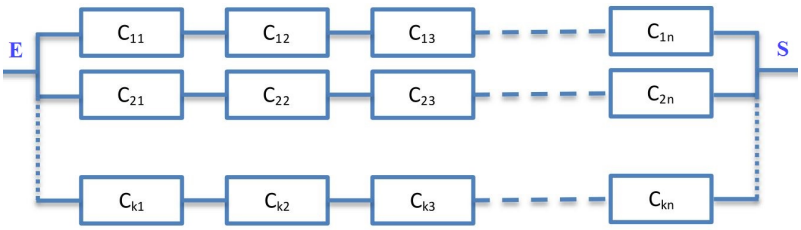

FIGURE 3.10 – *Diagramme de fiabilité d'un système avec structure série-parallèle*

La disponibilité d'un sous-système en série i est :

$$A_i(t) = \prod_{j=1}^{n} A_{ij}(t) \tag{3.36}$$

Alors la disponibilité A_S du système complet est :

$$A_S(t) = 1 - \prod_{i=1}^{k}(1 - \prod_{j=1}^{n} A_{ij}(t)) \tag{3.37}$$

Système parallèle-série :

Le système parallèle-série est constitué de n sous-systèmes connectés en série tel que chaque sous-système est composé de k éléments placés en parallèle [Fig. 3.11].
De même, un système parallèle-série est le résultat de l'association des deux systèmes série et parallèle. Pour calculer sa disponibilité, on réduit le système complet en un système série en modélisant chaque sous-système en parallèle par un seul composant [32].

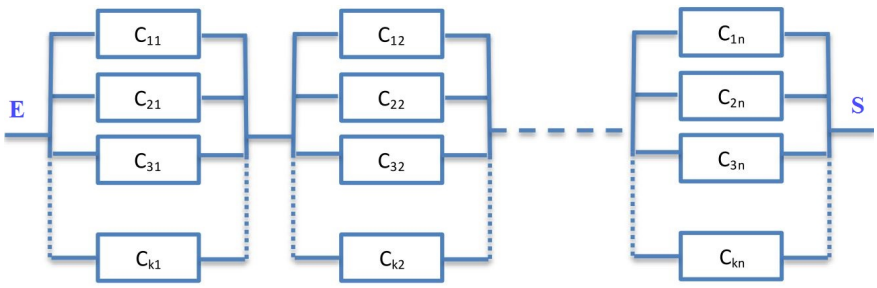

FIGURE 3.11 – *Diagramme de fiabilité d'un système avec structure parallèle-série*

La disponibilité d'un sous-système en parallèle j est :

$$A_i(t) = 1 - \prod_{i=1}^{k}(1 - A_{ij}(t)) \tag{3.38}$$

Alors la disponibilité A_S du système complet est :

$$A_S(t) = \prod_{j=1}^{n}[1 - \prod_{i=1}^{k}(1 - A_{ij}(t))] \tag{3.39}$$

Système mixte :

Un système mixte est la combinaison de structures séries et de structures parallèles (exemple [Fig. 3.12]). La disponibilité du système complet est évaluée en décomposant le système en plusieurs sous-systèmes séries et sous-systèmes parallèles, ensuite chaque sous-système est réduit en un seul composant.

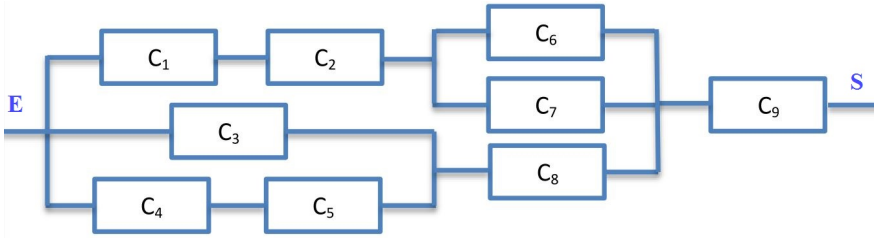

FIGURE 3.12 – *Diagramme de fiabilité d'un système avec structure mixte*

Système redondant k/n :

Un système redondant k parmi n fonctionne seulement si au moins k composants des n composants en parallèles fonctionnent (voir [Fig. 3.13]).

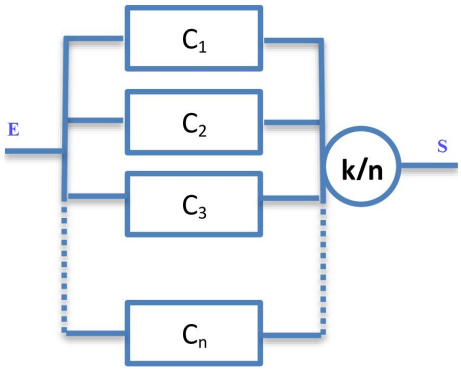

FIGURE 3.13 – *Diagramme de fiabilité d'un système avec structure redondant k/n*

la disponibilité du système A_S est égale à la somme des probabilités de toutes les configurations avec au moins k composants opérationnels :

$$A_S(t) = \sum_{i=k}^{n} C_n^i A^i (1 - A)^{n-i}, \qquad C_n^i = \frac{n!}{i!(n-i)!} \tag{3.40}$$

Structure de pont :

Il s'agit d'une structure de pont lorsque le système ne peut être décomposé à des combinaisons séries et parallèles (exemple [Fig. 3.14]). Ce système fonctionne en mode parallèle-série sous le contrôle du composant pont (composant 3 [Fig. 3.14]). Si ce composant tombe en panne, le système passe en mode série-parallèle considéré comme mode dégradé.
Pour calculer la disponibilité du système A_S, on utilise soit la table booléenne énumérant tous les combinaisons possibles des états des composants, soit en réduisant le système par itération [Fig. 3.15] en utilisant le théorème des probabilités conditionnelles [32].

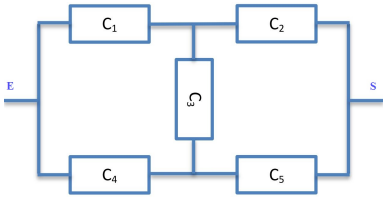

FIGURE 3.14 – *Diagramme de fiabilité d'un système avec structure de pont*

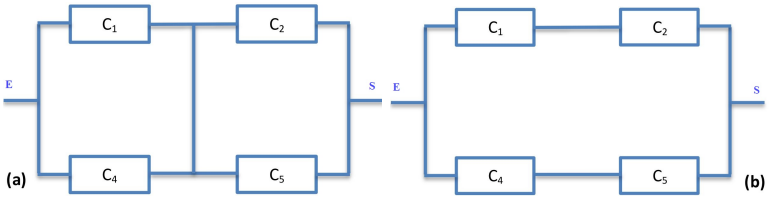

FIGURE 3.15 – *Décomposition d'un système en pont*

Le calcul de la disponibilité en utilisant les probabilités conditionnelles nécessite la prise en considération des deux configurations [Fig. 3.15] en conditionnant sur l'état du composant pont (composant 3).
Le composant pont est en marche ([Fig. 3.15] (a)) :

$$A_S = [1 - (1 - A_1)(1 - A_4)][1 - (1 - A_2)(1 - A_5)] \tag{3.41}$$

Le composant pont est défaillant ([Fig. 3.15] (b)) :

$$A_S = 1 - [(1 - A_1.A_2)][(1 - A_4.A_5)] \tag{3.42}$$

On déduit donc la disponibilité A_s du système complet :

$$A_S = A_3.A_a + [(1 - A_3).A_b] \tag{3.43}$$

3.4.3 Degrés de disponibilité d'un système

La disponibilité d'un système est généralement décrite à travers le nombre de "9" obtenus ou par un qualificatif dénotant la criticité du système ainsi que l'étendue de la durée d'indisponibilité envisageable [5] que nous présentons dans le tableau 3.1.

En effet, au-delà du fonctionnement ou non du système, la disponibilité constitue également une métrique quantifiant l'importance du système par rapport à l'accomplissement d'une tâche. Ainsi, selon [5], on peut distinguer trois niveaux de criticité :

• **Usuel** (99%) : l'indisponibilité du système a un impact mineur dans l'accomplissement de la tâche considérée.
• **Essentiel** (99.9%) : l'indisponibilité a un impact significatif quant à l'exécution de la tâche.
• **Critique** (99.999%) : l'indisponibilité mettrait de façon inacceptable en danger la matérialisation de la tâche considérée.

Quant. de 9 / (%)	Qualification du système	Indispo. à l'année (min.)	Indispo. au mois (min.)	Signification pratique
1 / 90	Disponibilité non maitrisée	52 596	4 383	Indisponibilité de 5 minutes par an
2 / 99	Disponibilité maitrisée	5 259	438.3	Indisponibilité de 4 jours par an
3 / 99.9	Disponibilité bien maitrisée	525.9	43.83	Indisponibilité de 9 heures par an
4 / 99.99	Tolérant aux pannes	52.6	4.38	Indisponibilité de 1 heure par an
5 / 99.999	Hautement disponible	5.26	0.44	Indisponibilité de 5 minutes par an
6 / 99.9999	Très hautement disponible	0.53	0.04	Indisponibilité de 30 secondes par an
7 / 99.9999	Ultra disponible	0.05	-	Indisponibilité de 3 secondes par an

TABLE 3.1 – *Degrés de disponibilité d'un système. [5]*

NB :
La formule utilisée pour calculer le temps d'indisponibilité D (Downtime), en heure/année, est indiquée dans l'équation [3.44].

$$D = (1 - A) * 8760, \qquad 1\ an = 8760\ heures \tag{3.44}$$

3.5 Mécanismes de Haute Disponibilité

La haute disponibilité (abrégée HA « *High Availability* ») consiste à réduire les points de défaillances détectés du système par la mise en place de techniques de redondance et/ou de réplication afin d'assurer la continuité de service en permanence [49].

Il existe plusieurs solutions pouvant être déployés aujourd'hui pour obtenir une haute disponibilité des systèmes. Nous décrivons, à titre non exhaustif certaines technologies et solutions les plus couramment utilisées dans le biais de l'informatique pour atteindre une haute disponibilité dans les services *Cloud Data Center*.

3.5.1 Redondance et tolérance aux pannes

Lorsque l'une des ressources tombe en panne, d'autres ressources redondés peuvent prendre le relais afin d'assurer la continuité opérationnelle du système et donner aux administrateurs le temps de résoudre le problème. Ce processus s'appelle basculement (*Failover*). Les services basculent vers le périphérique de sauvegarde qui continuera à partir de l'endroit où le périphérique principal s'est arrêté (sans interruption de service) [21].

FIGURE 3.16 – *Le principe de tolérance aux pannes*

Cluster à Haute Disponibilité

Un cluster à haute disponibilité (*High Availability (HA) Cluster*) également appelés cluster de basculement (*Failover Cluster*), est un groupe d'ordinateurs indépendants qui travaillent conjointement pour accroître la disponibilité et l'extensibilité des rôles en cluster. Les serveurs en cluster (appelés « *nœuds* ») sont connectés par des câbles physiques et par des logiciels. En cas de défaillance d'un ou plusieurs nœuds, d'autres nœuds prennent le relais pour fournir les services requis (processus appelé « *basculement* »). En outre, les rôles en cluster sont surveillés de manière proactive pour vérifier qu'ils fonctionnent correctement. S'ils ne fonctionnent pas, ils sont redémarrés ou déplacés vers un autre nœud [12]. Le cluster nécessite généralement plus de la moitié des nœuds pour s'exécuter, ce qui est appelé quorum [43].

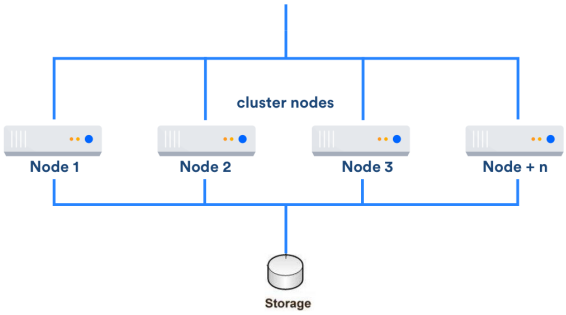

FIGURE 3.17 – *HA Cluster*

Configuration du mécanisme de quorum

Une configuration de quorum de cluster de basculement (HA Cluster) spécifie le nombre d'échecs qu'un cluster peut prendre en charge pour continuer à fonctionner. Une fois le seuil atteint, le cluster cesse de fonctionner. Les échecs les plus courants dans un cluster sont les nœuds qui ne fonctionnent plus ou ceux qui ne peuvent plus communiquer. nous avons présenté ci-dessous la configuration de quorum la plus couramment utilisée et qui offre une haute disponibilité [43].

• **Nœud et disque majoritaire** :
Cette configuration de quorum est la plus couramment utilisée car elle fonctionne bien avec les clusters à 2 et 4 nœuds, qui sont les déploiements les plus courants. Ce mode est préférable dans les situations avec un nombre pair de nœuds pour lesquels un stockage partagé est disponible car, dans les modes nœud et disque majoritaire, chaque nœud dispose d'un vote ainsi que d'un disque partagé appelé disque témoin (également appelé disque quorum). Comme il y a un nombre pair de nœuds et 1 vote additionnel de témoin de disque, le nombre total de votes sera impair. Le groupe ne fonctionne qu'à la majorité des voix, soit plus de la moitié.

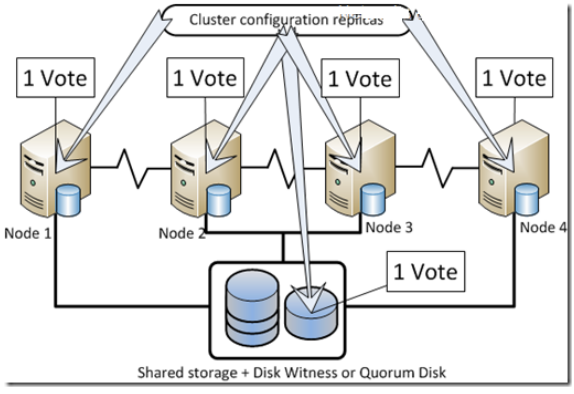

FIGURE 3.18 – *Configuration de cluster à quatre nœuds avec disque quorum*

Ce disque témoin (Disk Witness) est simplement un petit disque en cluster qui fait partie du groupe stockage disponible en cluster. Il est donc hautement disponible et peut basculer entre les nœuds. Il est considéré comme faisant partie du groupe des ressources principales du cluster. Ce mode peut supporter des défaillances de la moitié des nœuds (arrondi) si le témoin de

disque reste en ligne ou des défaillances de la moitié des nœuds (arrondi) moins un si le témoin de disque se déconnecte ou échoue [20].

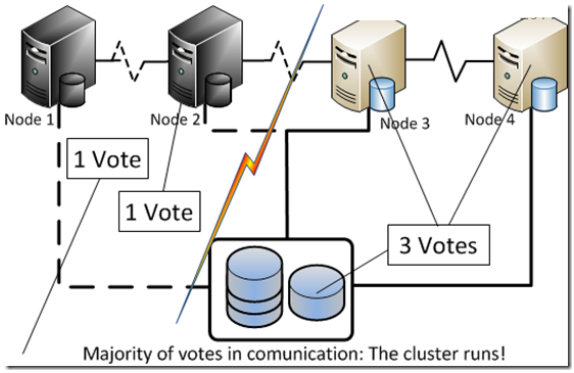

FIGURE 3.19 – *Configuration de quorum peut survivre à deux pannes de serveur à la fois*

Reprise après sinistre (Disaster Recovery)

La reprise après sinistre (*Disaster Recovery*) est un ensemble de règles et procédures visant à protéger une organisation de tout effet important (la perte de données par exemple) en cas d'événement négatif, pouvant inclure des cyberattaques, des catastrophes naturelles ou des défaillances de bâtiments ou de périphériques. Le fait de répliquer un *Data Center* situé dans une zone géographique A vers une zone géographique B constitue une solution de reprise après sinistre.

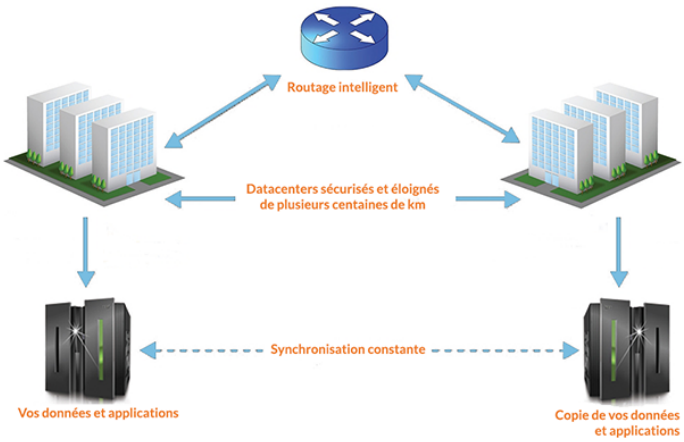

FIGURE 3.20 – *Reprise après sinistre d'un Data Center*

Migration de machines virtuelles

La migration de machine virtuelle est une méthode efficace pour assurer la tolérance aux pannes. Une machine virtuelle peut facilement être déplacée d'une machine physique et déplacée vers une autre, si nécessaire. Des exemples typiques de mouvements de machines virtuelles sont : le clonage de machine virtuelle (pour copier plusieurs instances de la même machine virtuelle sur un autre serveur), le déplacement de la machine virtuelle (pour libérer la machine d'origine

hébergeant la machine virtuelle), en cas de maintenance ou de rupture [21].

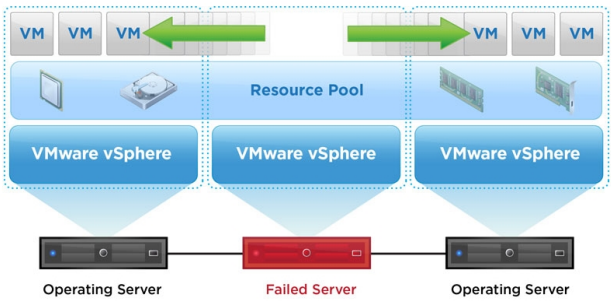

FIGURE 3.21 – *Mouvement de machine virtuelle - migration d'un serveur physique vers d'autres serveurs.*

Sauvegarde (Backup)

La sauvegarde (Backup) est un processus qui consiste à conserver les données, par une duplication, sur un support externe du système informatique. Cela permet de garantir que les données ne seront pas perdues si un sinistre venait de se produire. Une fois les données sauvegardées il est impératif de pouvoir les restituer en état lorsque c'est nécessaire. Les données d'une heure antérieure ne peuvent être récupérées que si elles ont été sauvegardées.

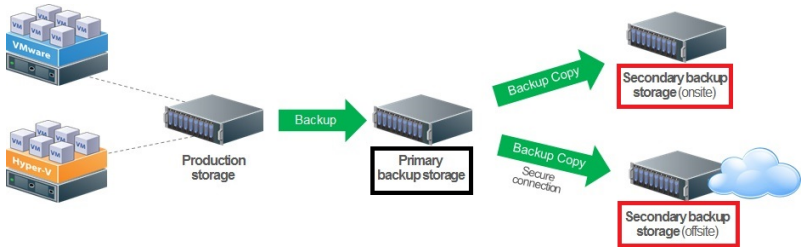

FIGURE 3.22 – *Trois emplacements de stockage différents : stockage principal, sur site et hors site*

Redondance des matériels d'accès au réseau

À l'interface avec le réseau Internet (LAN), les matériels (routeur, pare-feu, switchs et le câblage principalement) peuvent être redondés. Cette approche assure, d'une part une meilleure tolérance à la défaillance d'un composant, d'autre part, la possibilité de mettre en œuvre une répartition de charge sur le réseau, et d'assurer une haute disponibilité [40].

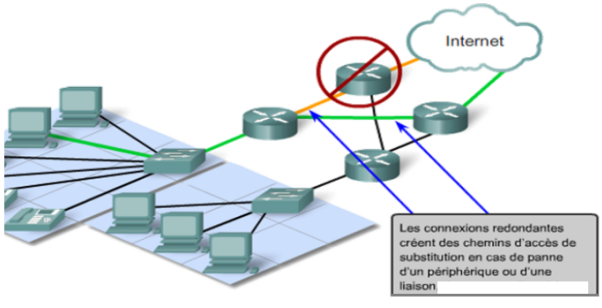

FIGURE 3.23 – *Périphériques réseau redondants*

3.5.2 Sécurisation des données : Technologies RAID

Les disques RAID (acronyme de *Redundant Arrays of Independent Disks*) ont été conçus en 1987 par trois chercheurs de l'université de Berkeley D.A. Patterson, G. Gibson et R.H. Katz [9]. Un système RAID est une matrice de disques dans laquelle une partie de la capacité physique est utilisée pour stocker de l'information redondante. Le système d'exploitation et les applications voient la matrice de disques comme étant un seul disque. Un système RAID permet de :

• Augmenter la capacité : RAID permet de mettre «bout à bout » des disques durs, ce qui permet d'accroître le volume de stockage.

• Améliorer les performances : les données sont écrites sur plusieurs disques à la fois. Ainsi, chacun des disques n'a qu'une partie de données à inscrire.

• Assurer la tolérance de panne : le système RAID permet de se prémunir contre les défaillances d'un disque.

Plusieurs niveaux RAID existent. Toutes les architectures de disques RAID sont en fait une combinaison des deux facteurs suivants :

• La manière dont les informations de redondance sont distribuées sur l'ensemble des disques.

• Le type de redondance utilisé (réplication, parité).

Il y'a deux façons de mettre en œuvre le RAID : soit niveau logiciel (*software*) géré par le système d'exploitation ou niveau matériel (*hardware*) [46].

RAID 0 : Segmentation

Ce niveau de RAID combine au moins deux disques durs qui forment un seul volume. Les données à stocker sont découpées par "bandes" ("stripes") puis réparties sur les unités de disque mais sans redondance. Les accès deviennent alors plus rapides qu'avec un seul disque puisque les contrôleurs des différents disques sont utilisés simultanément. Son utilisation n'est acceptable que si la perte de toutes les données de l'ensemble RAID ne pose aucun problème (par exemple pour les données temporaires) [60].

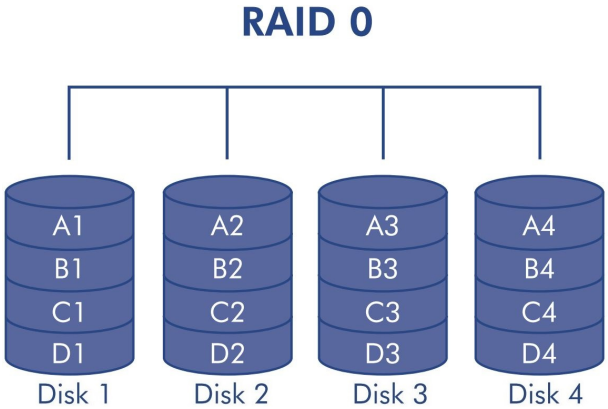

FIGURE 3.24 – *Schéma de principe d'une grappe de disques en RAID-0*

RAID 1 : Mise en miroir

Ce niveau de RAID utilise la mise en miroir de disque afin que les données écrites sur un disque physique soient simultanément écrites sur un autre disque physique (une redondance complète des données), d'où une formidable tolérance aux pannes mais pas de véritable augmentation des performances par rapport à un disque unique. Le RAID-1 composé de deux disques (la capacité est celle d'un disque).

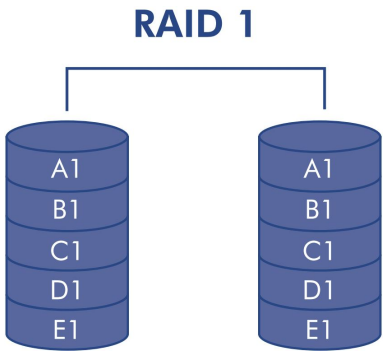

FIGURE 3.25 – *Schéma de principe d'une grappe de disques en RAID-1*

RAID 10 et RAID 01 : RAID Combinés

Aussi appelé RAID 1/0, RAID 0/1, RAID0+1 ou RAID1+0, c'est la combinaison du RAID 0 et du RAID 1. Ce type de RAID est composé de quatre disques durs répartis soit en deux volumes RAID 0 montés en miroir, soit en deux volumes RAID 1 montés en striping. On cumule alors les avantages de ces deux modes (Performances et redondance) mais ce système est l'un des plus onéreux car un grand nombre de disques est requis et seulement 50% de la capacité totale de ceux-ci est exploitable [60].

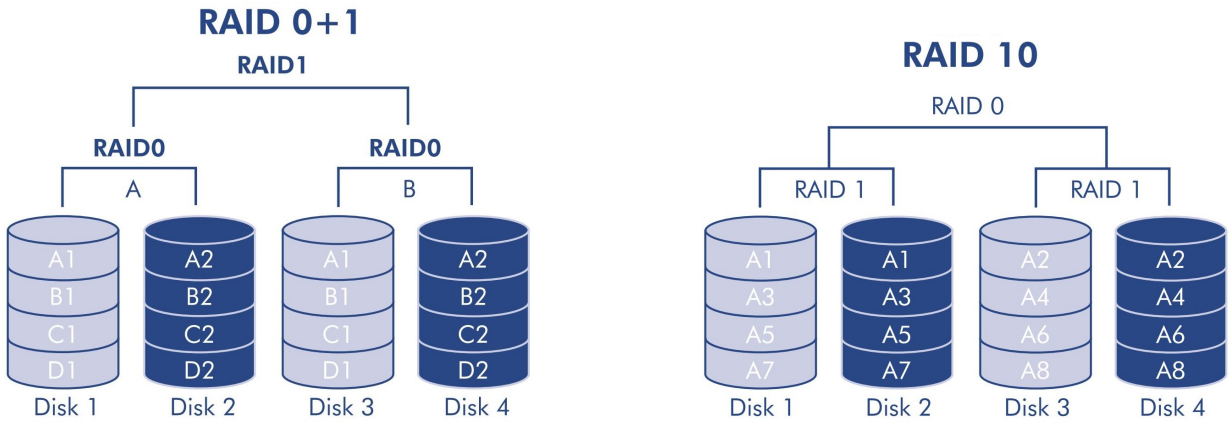

FIGURE 3.26 – *Schéma de principe d'une grappe de disques en RAID-0+1 et RAID-10*

RAID 3 : Segmentation avec parité

Le RAID 3 basé sur une grappe de disques durs identique au RAID 0 mais on ajoute un disque de parité pour obtenir une tolérance de panne qui permet jusqu'à une panne de disque. RAID 3

nécessite un contrôleur spécial permettant la rotation synchronisée de tous les disques. Au lieu de répartir les blocs de données dans différents disques, RAID 3 répartit les bits en bande, qui sont stockés sur des unités de disque différentes. Nécessite un minimum de trois disques (deux ou plus pour les données et un pour la parité).

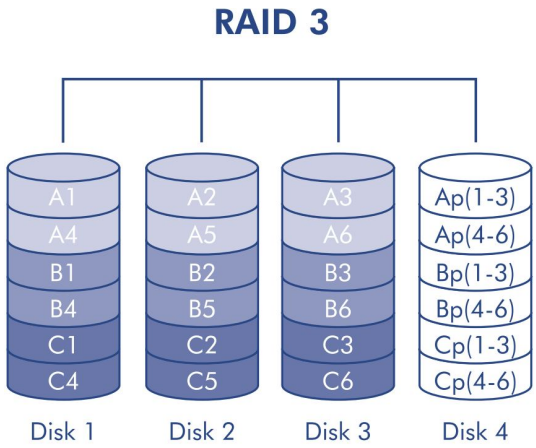

FIGURE 3.27 – *Schéma de principe d'une grappe de disques en RAID-3*

RAID 4 : Données bloquées avec parité

S'appuyant sur le RAID 3, il répartit les données comme le RAID 0 et est donc plus performant. Néanmoins, toutes les données de parité étant enregistrées sur une même unité, le disque correspondant devra aussi rapide que la somme de tous les autres pour éviter un goulot d'étranglement. Nécessite un minimum de trois disques (deux ou plus pour les données et un pour la parité). [52].

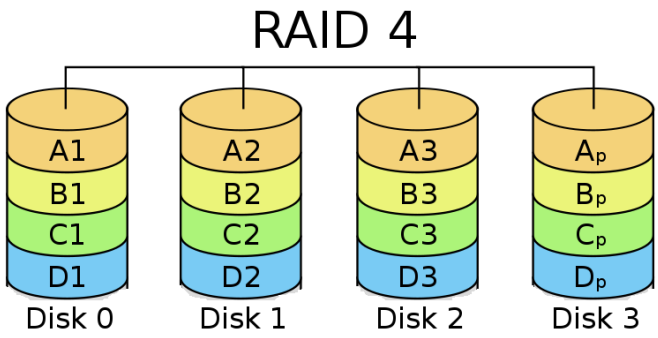

FIGURE 3.28 – *Schéma de principe d'une grappe de disques en RAID-4*

RAID 5 : Données bloquées avec parité distribuée

Ce niveau fonctionne comme le RAID 4, mais ici les données de parité sont réparties sur tous les disques (parité distribuée) pour fournir un débit de données élevé et une redondance des données. Le système tourne donc au maximum des capacités matérielles et l'espace disque final utilisable est de (n-1) disques. C'est le type RAID le plus abouti et le plus répandu actuellement.

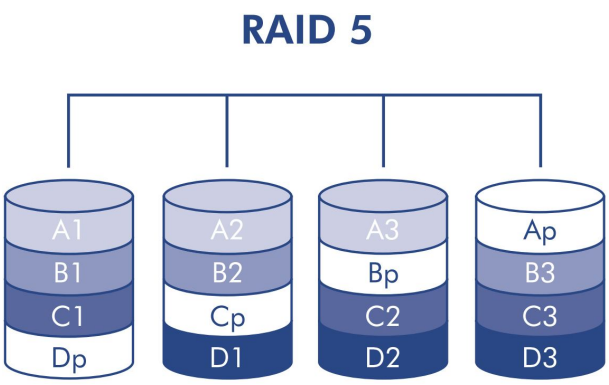

FIGURE 3.29 – *Schéma de principe d'une grappe de disques en RAID-5*

RAID 6 : Données bloquées avec double parité distribuée

Est une extension de RAID 5 et utilise un bloc de parité supplémentaire. RAID 6 utilise une segmentation au niveau des blocs avec deux blocs de parité répartis sur tous les disques membres. RAID 6 offre une protection contre les défaillances de double disque et les défaillances lors de la reconstruction d'un seul disque. Nécessite un minimum de quatre disques (deux ou plus pour les données et deux pour la parité) [52].

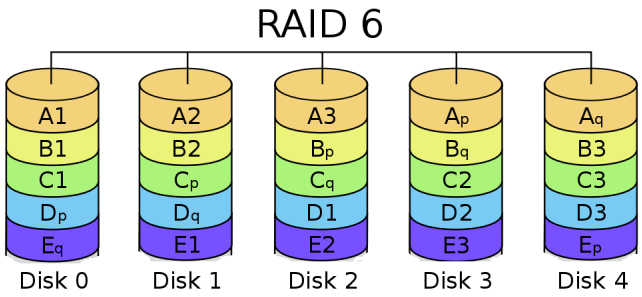

FIGURE 3.30 – *Schéma de principe d'une grappe de disques en RAID-6*

Contrôleur RAID

Un paramètre à ne pas oublier dans la conception d'un RAID est le nombre d'interfaces contrôlant les disques (cartes IDE, SCSI, SATA ou SAS). En effet, le contrôleur RAID est un élément indispensable au fonctionnement de l'ensemble, s'il vient à défaillir, il entraîne l'indisponibilité de tous les éléments du RAID.

Conclusion

A travers ce chapitre, nous avons pu découvrir plusieurs concepts liés à la disponibilité des systèmes ainsi que plusieurs mécanismes qui permettent d'atteindre la haute disponibilité des données et de service dans le *Cloud Data Center*. Ceci fait l'objet essentiel de notre travail qui sera présenté dans le chapitre qui suit.

Chapitre 4

Modélisation de la Disponibilité de l'Infrastructure Technique du Data Center

Introduction

Dans ce chapitre, nous nous intéressons à la modélisation et l'évaluation de la disponibilité par la méthode des blocs diagramme de fiabilité pour les systèmes informatiques exécutés sous l'infrastructure sous-jacente du *Cloud Computing*, tel que le stockage, les serveurs et le réseau, tout en considérant dans chaque système les mécanismes de haute disponibilité utilisés actuellement par ICOSNET afin de voir comment ces différents mécanismes contribue à l'amélioration de la disponibilité en régime permanent des données et des services Cloud et afin d'identifier les points critiques qui diminue cette dernière. Puis, nous suggérons dans chaque système d'autres configurations ou architectures basées aussi sur les techniques de haute disponibilité mais qui réduit le maximum les temps d'arrêt moyen de service pour l'entreprise. Enfin, nous interprétons les résultats obtenus en vérifiant qu'elles répondent bien au besoin de haute disponibilité pour le fournisseur ICOSNET.

4.1 Collecte des données

Les données que nous avons utilisées dans notre rapport sur l'évaluation de la disponibilité des services *Cloud Data Center* proviennent de quatre sources [27, 51, 54, 55]. Le Tableau [4.1] détaille les valeurs du temps moyen avant défaillance (MTTF) et du temps moyen de réparation (MTTR) pour chaque périphérique de l'infrastructure du *Data Center* que nous avons besoin dans notre étude. Il est important de comprendre comment ces chiffres sont calculés. Le temps requis pour effectuer l'analyse de disponibilité était de 8760 heures (1an) et il a été calculé pour l'état stable. Les données sur les défaillances et les réparations de plusieurs composants sont modélisées et analysées à l'aide de distributions de probabilité et d'inférences statistiques. Ensuite, des mesures opérationnelles (MTTF et MTTR) sont dérivées et utilisées pour estimer la disponibilité des composants.

Nous avons augmenté la valeur de (MTTR) pour les matériels réseau afin d'obtenir des résultats approximativement égale à celles du *Data Center* d'ICOSNET.

Composants	$\frac{1}{\lambda}$ = MTTF (h)	$\frac{1}{\mu}$ = MTTR (h)	Disponibilité
Alimentation serveur (Power)	67 * 10^4	1	0.999998507
CPU (Central Processing Unit	25 * 10^5	1	0.9999996
CNI (Network Interface Card	62 * 10^5	1	0.999999839
RAM (Random Access memory)	48 * 10^3	1	0.999979167
VMM (Virtual Machine Monitor)	2893	2	0.999309154
VM (Virtual Machine)	2880	2	0.999306037
TOR Switch	145 * 10^3	8	0.999944831
Aggregation Switch	2 * 10^5	6	0.999970001
Routeur	22 * 10^4	6	0.999972728
Firewall	14 * 10^4	8	0.99994286
Link	19996	14	0.99930035

TABLE 4.1 – *Valeurs MTTF, MTTR et la disponibilité des composants du Data Center*

4.2 Architecture globale du Data Center d'ICOSNET

L'architecture globale du *Data Center* d'ICOSNET que nous avons utilisée par la suite pour la modélisation de la disponibilité par les blocs diagramme de fiabilité (BDF) est illustrée dans la Figure [4.1].

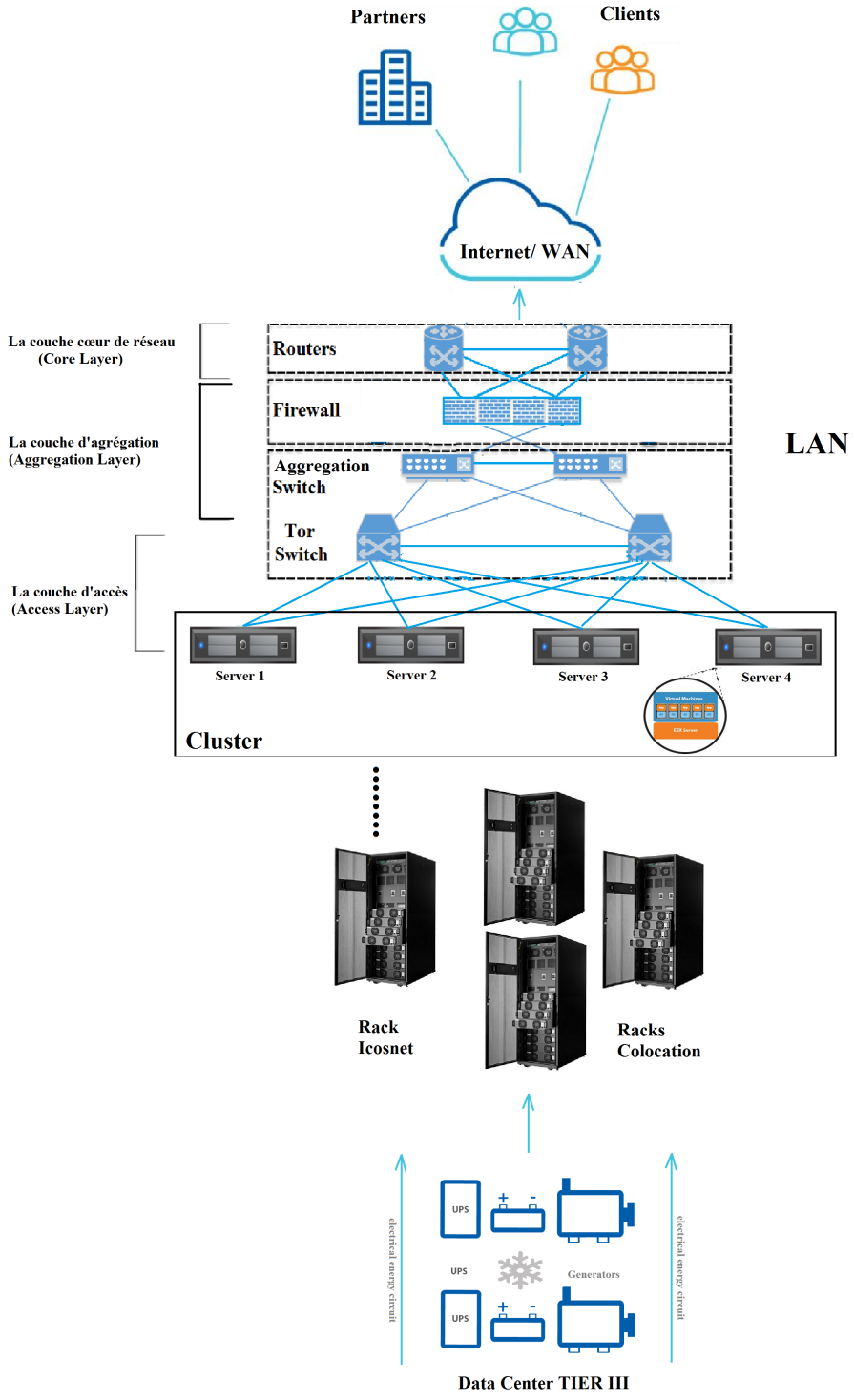

FIGURE 4.1 – *L'infrastructure globale du Data Center d'ICOSNET*

4.3 Application sur les systèmes de stockage RAID

Pour déterminer la disponibilité globale d'un système de stockage basé sur RAID, il est important d'évaluer avec précision la disponibilité du sous-système RAID. En utilisant la méthode des blocs diagramme de fiabilité (BDF) nous allons déterminer la probabilité que les données sur différentes configurations RAID soient disponible en régime permanent.
Afin de déterminer la différence de disponibilité entre les différents niveaux de configuration RAID, une valeur de disponibilité de A_{HDD} = 0.99952023 est attribuée aux disques durs utilisés dans notre évaluation (MTTF=200000 (h), MTTR= 96 (h)), soit une indisponibilité de quatre jours dans une durée de 22 ans de fonctionnement, car les lecteurs de disque individuels sont moyennement fiables. Le temps moyen de réparation (MTTR) est égal au temps de reconstruction du système (reconstituer le stockage plus restaurer les données).

4.3.1 Redondance par duplication

RAID-0 : Répartition de données (Striping)

RAID-0 ne fournit aucune redondance des données. En d'autres termes, si un lecteur de l'ensemble RAID tombe en panne, toutes les données seront perdues. La Figure [4.2] illustre le diagramme de fiabilité d'un ensemble de disques RAID-0. Les disques durs sont considérés comme étant en série. La relation mathématique qui évalue la disponibilité d'une matrice RAID-0 est écrite dans l'équation [3.33].

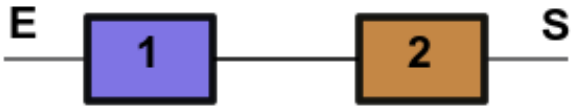

FIGURE 4.2 – *Diagramme de fiabilité pour la structure RAID-0*

La disponibilité et le temps d'arrêt moyen du système qui en résultent sont :

Nombre de disques HDD	2
A_{RAID-0}	0.99904069
A_{RAID-0} (%)	99.90 %
Temps d'arrêt moyen (h) / an	8.40

TABLE 4.2 – *Les résultats obtenus pour la structure RAID-0*

Cette configuration n'est pas recommandée pour du stockage de données importantes. Le RAID-0 n'est pas utilisé par les fournisseurs *Cloud*, car son fonctionnement ne permettre pas la tolérance de panne et contient un risque trop important sur les données des clients.

RAID-1 : Mise en miroir (Mirroring)

Le RAID-1 est le type de RAID utilisé par ICOSNET. RAID-1 fournit une redondance complète des données. Un disque dur peut échouer dans un ensemble couplé sans perte de données. Toutefois, si les deux lecteurs du même ensemble lié échouent, les données seront perdues. La Figure [4.3] illustre le diagramme de fiabilité d'un ensemble de disques RAID-1. Les disques durs sont considérés comme étant en parallèle. La relation mathématique qui évalue la disponibilité d'une matrice RAID-1 est écrite dans l'équation [3.35].

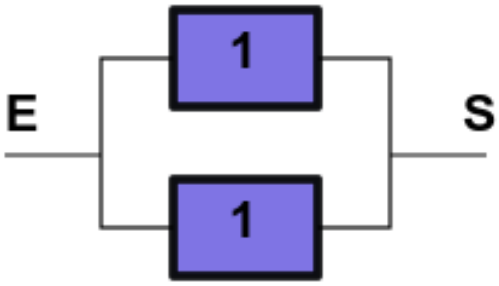

FIGURE 4.3 – *Diagramme de fiabilité pour la structure RAID-1*

La disponibilité et le temps d'arrêt moyen du système qui en résultent sont :

Nombre de disques HDD	2
A_{RAID-1}	0.999999769
A_{RAID-1} (%)	99.99997 %
Temps d'arrêt moyen (sec) / an	7.28

TABLE 4.3 – *Les résultats obtenus pour la structure RAID-1*

D'après le résultat obtenu (l'indisponibilité de 7 seconde/an), nous constatons que le RAID-1 fournit une sécurité maximale des données en cas de panne d'un seul disque. Cette configuration est recommandée lorsque la sécurité est plus importante que la vitesse, comme le cas chez ICOSNET.

RAID Combinés

RAID-0+1 : Miroir de grappes (Mirror of stripes)

En RAID-0+1, les données sont agrégées par deux grappes sur un jeu de disques, puis mises en miroir sur un autre jeu de disques. Si un lecteur dans un jeu de disques échoue, ce jeu de disques est perdu, mais toutes les données resteront disponibles à partir du jeu de disques mis en miroir. Cependant, si l'un des disques durs du jeu de disques restant (le miroir) tombe en panne avant la restauration du premier jeu de disques, toutes les données sont perdues. La

Figure [4.4] illustre le diagramme de fiabilité d'un ensemble de disques RAID-0+1. Les disques durs sont considérés comme étant en série-parallèle. La relation mathématique qui évalue la disponibilité d'une matrice RAID-0+1 est écrite dans l'équation [3.37].

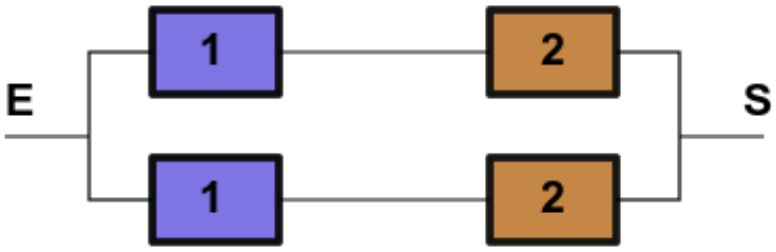

FIGURE 4.4 – *Diagramme de fiabilité pour la structure RAID-0+1*

La disponibilité et le temps d'arrêt moyen du système qui en résultent sont :

Nombre de disques HDD	4
$A_{RAID-0+1}$	0.999999079
$A_{RAID-0+1}$ (%)	99.99990 %
Temps d'arrêt moyen (sec) / an	29.04

TABLE 4.4 – *Les résultats obtenus pour la structure RAID-0+1*

RAID 10 : Grappe de miroirs (Stripe of mirrors)

RAID 10 combine la mise en miroir de RAID-1 avec la répartition des données de RAID-0 ; en particulier, les données sont réparties sur des ensembles de disques en miroir. Un seul disque dur dans un ensemble en miroir d'une matrice RAID 10 peut échouer sans aucune perte de données. Cependant, si les deux disques durs d'un ensemble en miroir échouent, toutes les données sont perdues. La Figure [4.1] illustre le diagramme de fiabilité d'un ensemble de disques RAID-10. Les disques durs sont considérés comme étant en parallèle-série. La relation mathématique qui évalue la disponibilité d'une matrice RAID-1+0 est écrite dans l'équation [3.39].

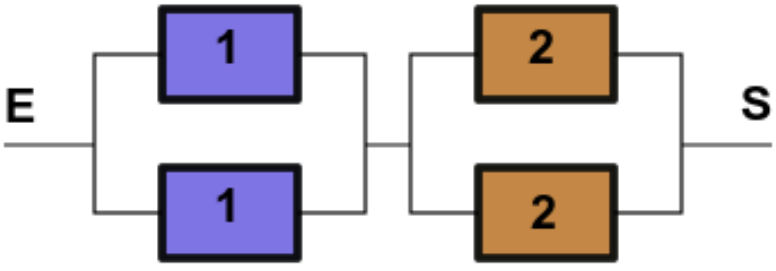

FIGURE 4.5 – *Diagramme de fiabilité pour la structure RAID-10*

La disponibilité et le temps d'arrêt moyen du système qui en résultent sont :

Nombre de disques HDD	4
$A_{RAID-10}$	0.999999538
$A_{RAID-10}$ (%)	99.99995 %
Temps d'arrêt moyen (sec) / an	14.56

TABLE 4.5 – *Les résultats obtenus pour la structure RAID-10*

Les résultats obtenus, montrent que les RAIDs combinés fournit une indisponibilité supérieure à celle de RAID-1, tel que RAID-0+1 environ quatre fois supérieure, et le RAID-10 environ deux fois dans une durée de 1 an. C'est pour cette raison essentielle que le RAID-10 est préféré au RAID-01 dans la pratique.

Cependant, une disponibilité du système de six 9 (moins de trente secondes d'indisponibilité par an en moyenne) peut être suffisante pour les fournisseurs *Cloud* qui nécessitant une sécurité très élevée des données. Ces configurations RAIDs sont recommandées quand à la fois haute performance et haute sécurité est requise.

Pour optimiser la haute disponibilité, il est recommandé de placer les disques miroirs dans un boîtier séparé (et de préférence dans un rack séparé) et d'utiliser des contrôleurs de disque redondants.

4.3.2 Redondance par contrôle de parité

RAID-3 et **RAID-4** utilisent tous les deux la méthode de « stripping » associé à un disque dur dédié à la parité. La différence entre les deux est que RAID 3 travaille par octets tandis que RAID 4 agit par blocs, comme expliqué précédemment dans le chapitre (3). Les deux configurations peut tolérant une seule défaillance du disque dur dans un tableau de **N** disques durs. Par exemple, en cas de défaillance du disque dur de parité, les disques durs de données restants ne sont pas affectés, mais la redondance est perdue. Si un disque dur de données échoue, le contrôleur RAID utilise les disques durs de données restants et le disque dur de parité pour recalculer les données manquantes à la volée. Toutes les données de l'ensemble RAID seront perdues si un autre disque dur tombe en panne avant que le disque dur défaillant ne soit restauré. La Figure [4.6] illustre le diagramme de fiabilité d'un ensemble de disques RAID-3 et RAID-4. Les disques durs sont considérés comme étant un système redondant k/n. La relation mathématique qui évalue la disponibilité de **N** disques durs dans les matrices **RAID-3**, **RAID-4**, est écrite dans l'équation [3.40].

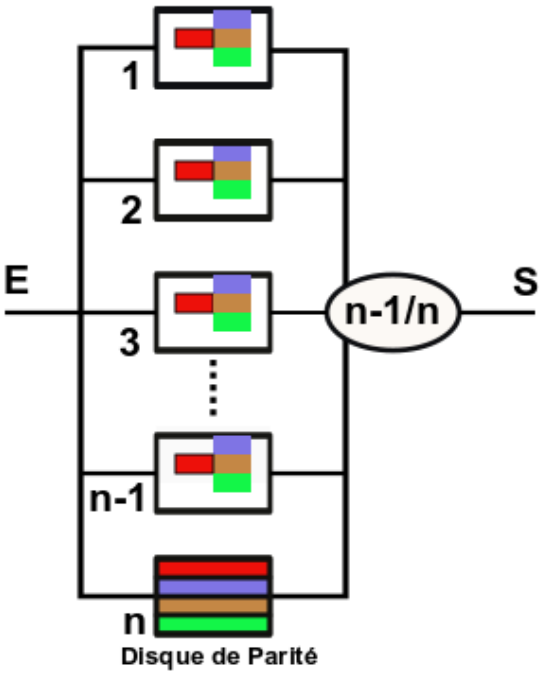

FIGURE 4.6 – *Diagramme de fiabilité pour les structures RAID-3 et RAID-4*

RAID-5 est similaire à RAID-4, à la différence que les données de parité sont réparties sur tous les disques durs. Là encore, lorsqu'un disque dur tombe en panne, toutes les données sont toujours disponibles. les données manquantes sont recalculées à partir des disques durs restants et des informations de parité. La Figure [4.7] illustre le diagramme de fiabilité d'un ensemble de disques RAID-5. Les disques durs sont considérés aussi comme étant un système redondant k/n. La relation mathématique qui évalue la disponibilité de **N** disques durs dans une configuration RAID-5 est identique à ceux de RAID-3 et RAID-4.

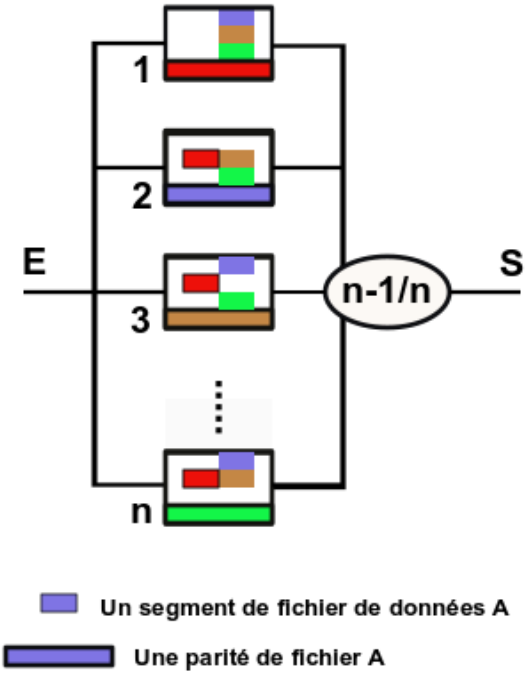

FIGURE 4.7 – *Diagramme de fiabilité pour la structure RAID-5*

Les résultats de disponibilité et d'indisponibilité obtenus pour les configurations RAID avec parité en fonction de n disques durs sont présentés dans le Tableau et la Figure ci-dessous :

Nombre de disques HDD	3	4	5	6	7
$A_{RAID-3,4,5}$	0.99999930	0.999998619	0.99999770	0.999996551	0.999995173
$A_{RAID-3,4,5}$ (%)	99.99993 %	99.9998 %	99.9997 %	99.9996 %	99.9995 %
Temps d'arrêt moyen (sec) / an	22.07	43.55	72.53	108.76	152.22

TABLE 4.6 – *Les résultats obtenus pour la structure RAID à parité unique*

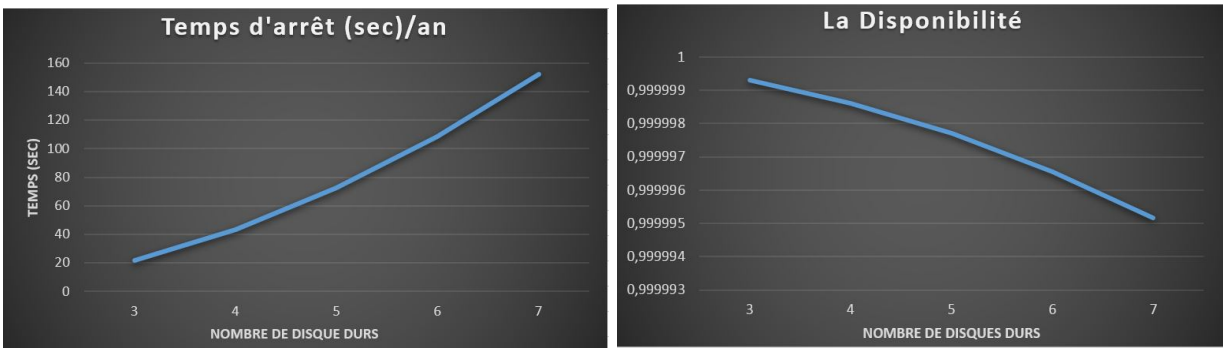

FIGURE 4.8 – *Présentation graphique des résultats*

D'après les résultats obtenus, nous avons constaté que plus le nombre de périphériques de stockage augmente, plus la disponibilité du système diminue. Cela est dû à la grande probabilité de subir des dommages matérielles avec un système comportant plusieurs lecteurs (6 par exemple) qu'un système à trois lecteurs (taux de défaillance augmente avec l'augmentation de nombre de disques).

En outre, nous pouvons constaté que les niveaux de RAID utilisant la mise en miroir risquent moins d'indisponibilité que ceux utilisant la parité.

Parmi les différentes configurations RAID avec parité, le RAID 5 est recommandé pour un bon équilibre entre protection des données et vitesse.

4.3.3 Redondance par double contrôle de parité

RAID-6 est similaire à RAID-5, à la différence que les données de parité sont réparties en deux fois sur tous les disques durs. Ce mode de RAID peut prendre en charge une défaillance jusqu'à deux disques sans aucune perte de données. La Figure [4.9] illustre le diagramme de fiabilité d'un ensemble de disques RAID-6. Les disques durs sont considérés aussi comme étant un système redondant k/n. La relation mathématique qui évalue la disponibilité de **N** disques durs dans une configuration RAID-6 est identique à ceux de RAID-3, RAID-4 et RAID-5.

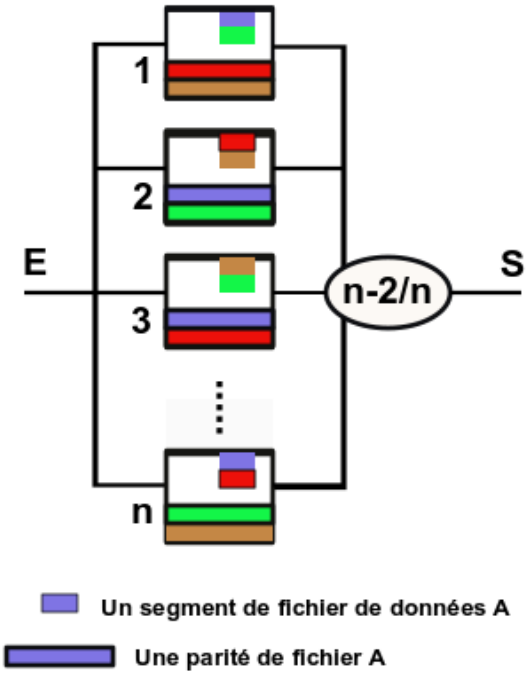

FIGURE 4.9 – *Diagramme de fiabilité pour la structure RAID-6*

Les résultats de disponibilité et d'indisponibilité obtenus pour la configuration RAID avec double parité en fonction de n disques durs sont présentés dans le Tableau et la Figure ci-dessous :

Nombre de disques HDD	4	5	6	7	8
A_{RAID-6}	0.999999999	0.999999998	0.999999997	0.999999996	0.999999993
A_{RAID-6} (%)	99.9999999 %	99.9999998%	99.9999997%	99.9999996%	99.9999993%
Temps d'arrêt moyen (sec) / an	0.031	0.063	0.094	0.126	0.220

TABLE 4.7 – *Les résultats obtenus pour la structure RAID à double parité*

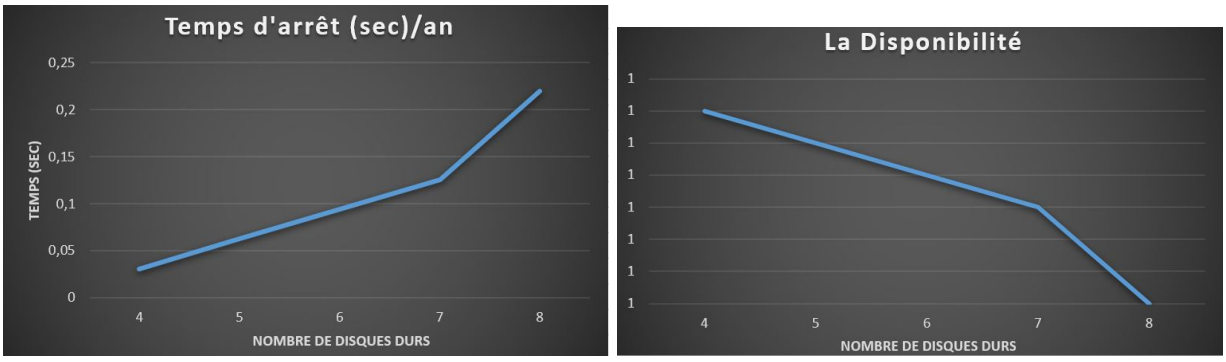

FIGURE 4.10 – *Présentation graphique des résultats*

Les résultats indiquent que le RAID-6 offre une excellente disponibilité des données (100%) avec une indisponibilité nulle, même avec une configuration de huit disques durs.

Cependant, en RAID-5 comme en RAID-6, plus le nombre de périphériques de stockage augmente, plus la disponibilité du système diminue. Car en règle générale, plus le nombre de disques contenus dans un système est grand, plus il est probable d'y avoir une défaillance.

Le système RAID 6 est fortement recommandé à cause de son niveau de protection et de disponibilité de données très élevé et sa bonne performance.

La Figure [4.11] résume en diagrammes à bandes les résultats obtenus sur la disponibilité et l'indisponibilité des systèmes RAID les plus couramment utilisés dans les entreprises.

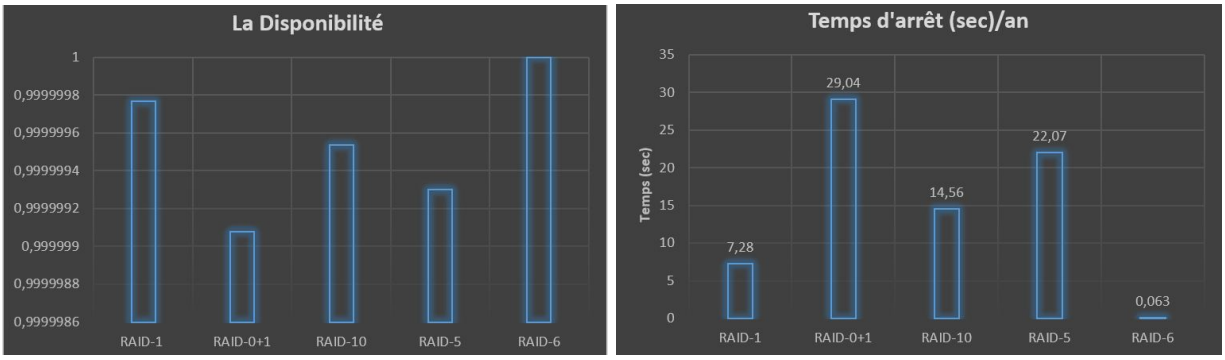

FIGURE 4.11 – *Diagrammes montrent les résultats obtenus pour différents types de RAID*

L'analyse des résultats conduit à la conclusion suivante : les matrices RAID sont conçues pour assurer une disponibilité de six neuf (99,9999) (soit environ de moins de trente seconde d'indisponibilité par an en moyenne), lorsque on utilise le minimum de disques exigés.

Le Tableau [4.8] décrit un classement des différentes configurations RAID qu'on a étudié dans cette Section par niveau de disponibilité avec un ordre croissant.

RAIDs	RAID-1	RAID-0+1	RAID-10	RAID-5	RAID-6
Niveau de disponibilité	2	6	3	4	1

TABLE 4.8 – *Classement par niveau de disponibilité pour différents types de RAID*

La Figure [4.12] montre un classement par niveau de disponibilité de trois types de RAID (RAID-5, RAID-6 et RAID-10) trouvée sur un document officiel (REDP-4484-00) publié par Redbooks IBM [4] (Une société multinationale américaine présente dans les domaines du matériel informatique, du logiciel et des services informatiques). Ce classement de trois types de RAID est identique au celle qu'on avait classés, ce qui nous a permis de confirmer les résultats que nous avions pu obtenir.

Factor	RAID-5	RAID-6	RAID-10
Random write performance	2	3	1
Sequential write performance	1	2	3
Availability	3	1	2
Space efficiency	1	2	3

FIGURE 4.12 – *Classement par niveau de disponibilité pour trois types de RAID. [4]*

4.4 Application sur le Cluster Cloud

Nous examinons maintenant la disponibilité du Cluster *Cloud* d'ICOSNET, en commençant tout d'abord par le serveur *Cloud*. La Figure [4.13] illustre la configuration de la virtualisation dans un serveur *Cloud* qui se trouve dans un système Cluster tolérant aux pannes (HA Cluster).

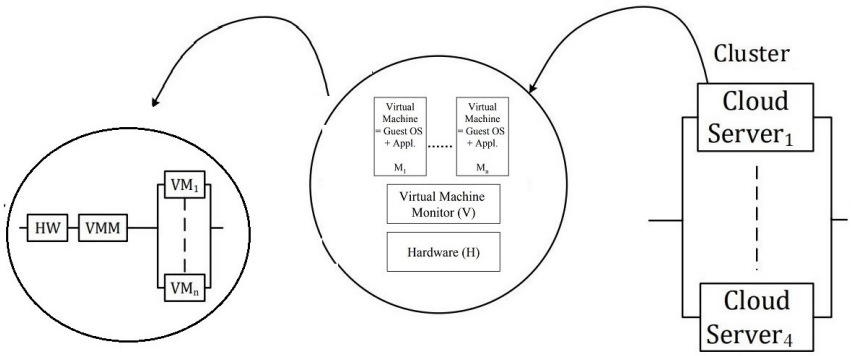

FIGURE 4.13 – *La configuration de la virtualisation dans un serveur Cloud*

Chaque serveur est composé d'une unité centrale de traitement (CPU), des disques durs (HDDs), d'une carte d'interface réseau (NIC), d'une mémoire (RAM), d'une alimentation (POW), des machines virtuelles (VMs) et d'un hyperviseur (VMM). L'échec d'un composant (CPU ou RAM ou HDD ou NIC ou POW ou VMM) à exécuter ses fonctions requises peut entraîner une défaillance de serveur.

La Figure [4.14] illustre le diagramme de fiabilité du système de base d'un service *Cloud* (système géré par le fournisseur). Les composants du serveur sont considérés comme étant un système en série. Nous avons présenté les disques durs (HDD) et la machine virtuelle par des systèmes en parallèle, car les machines virtuelles sont redondées par réplication synchrone sur le sauvegarde (backup) (si une VM tombe en panne sur un serveur, son duplicata démarre sur l'autre hôte et accède aux mêmes données), et le système de stockage utilise la configuration RAID-1.

La disponibilité du serveur est déterminé en substituant les valeurs des disponibilités de composants concernés présentés dans le Tableau [4.1] dans les équations [3.33] [3.35]. Les résultats sont présentées dans le Tableau [4.9] :

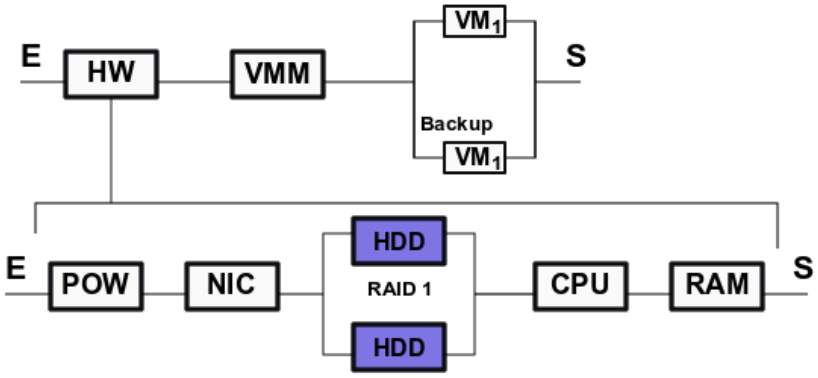

FIGURE 4.14 – *Digramme de fiabilité du système de base d'un service Cloud*

	Disponibilité
Hardware	0.999976882
VMM	0.999309154
Machine virtuelle avec redondance	0.999999518
Cloud serveur	**0.99928557**

TABLE 4.9 – *Les résultats obtenus pour le service Cloud*

La disponibilité de tout le serveur *Cloud* est : 99.928557 %. Ceci est inférieur à la disponibilité de chaque composant du serveur. Il est clair que le composant qui a le plus d'impact sur la disponibilité du serveur était le VMM (le point critique qui peut tomber en panne), car sa disponibilité est très faible par rapport à d'autres composants, mais les serveurs placés dans le cluster ne sont pas autonomes (isolés). Dans un cluster si un hyperviseur (VMM) tombe en panne, les machines virtuelles se déplacent automatiquement dans un autre hyperviseur de l'autre serveur qui appartenant à le même cluster. De même si un serveur tombe en panne alors qu'il est en train de traiter des requêtes, d'autres serveurs du cluster prends automatiquement la relève d'une manière aussi transparente que possible.

Le HA cluster d'ICOSNET dispose de quatre serveurs et chaque serveur est relié par deux liens (Link) à deux commutateurs (Switchs). Le cluster peut prendre en charge une seule défaillance de serveur sans interruption de service. La Figure [4.15] illustre le diagramme de fiabilité du HA Cluster d'ICOSNET. Les serveurs sont considérés comme étant un système redondant k/n. La relation mathématique qui évalue la disponibilité de système, est écrite dans l'équation [3.40].

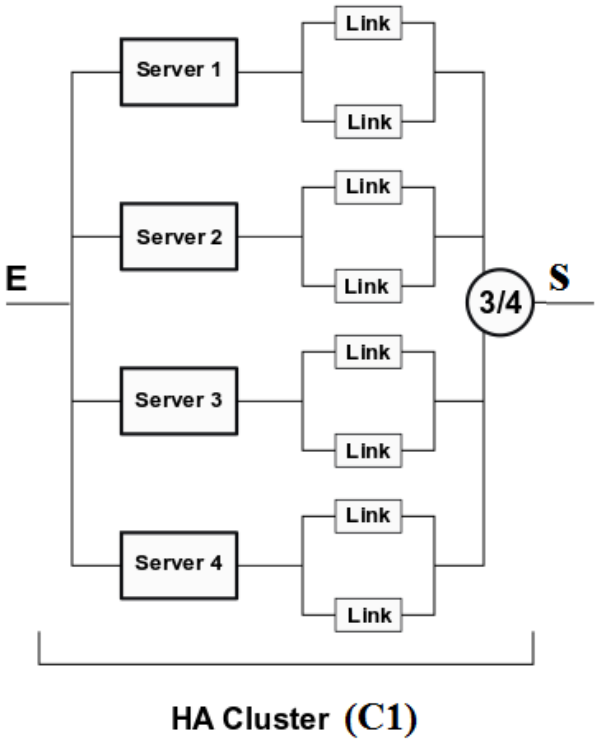

FIGURE 4.15 – *Digramme de fiabilité pour la configuration HA Cluster d'ICOSNET*

HA Cluster	C1
Disponibilité	**0.9999969362**
Temps d'arrêt moyen (sec)/an	96.61

TABLE 4.10 – *Les résultats obtenus pour la configuration HA Cluster d'ICOSNET*

Les résultats du cluster sont satisfaisants, d'où la disponibilité du service *Cloud* est spectaculairement améliorée. Cela est principalement dû aux mécanismes de redondance et de basculement des serveurs (mise en place d'un HA Cluster). Ce rendement pourrait encore être amélioré en proposant une configuration (C2) de quorum (nœud et disque majoritaire)(voir la Section [3.5.1]) évolutive plus fiable capable de supporter une charge de deux défaillance de serveurs (la moitié des nœuds) en même temps et qui peut atteindre plus de six (9) de disponibilité (environ moins trente secondes d'indisponibilité par an en moyenne). La Figure [4.16] illustre le diagramme de fiabilité du HA Cluster (C2).

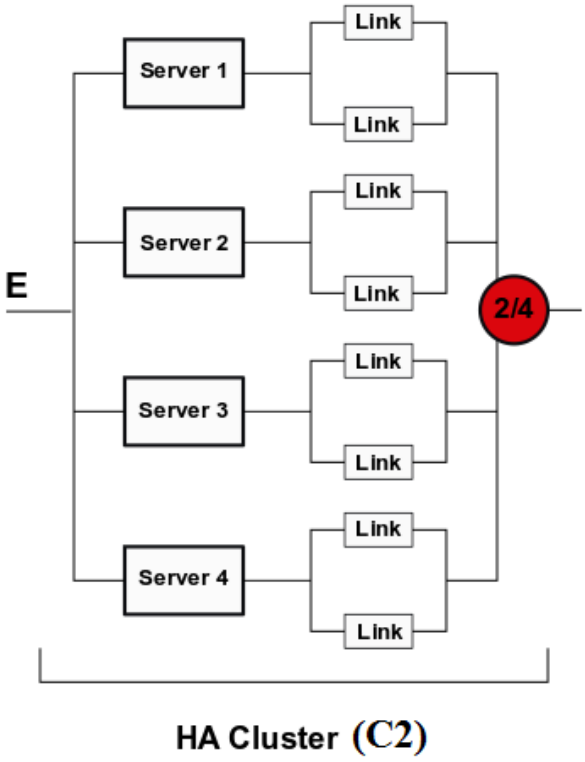

FIGURE 4.16 – *Diagramme de fiabilité pour la configuration HA Cluster (C2) suggérée*

HA Cluster	C2
Disponibilité	**0.9999999985**
Temps d'arrêt moyen (sec)/an	0.047

TABLE 4.11 – *Les résultats obtenus pour la configuration HA Cluster (C2)*

Le résultat de la disponibilité du HA Cluster avec la configuration (C2) est hautement satisfaisant. On peut dire qu'elle offre une disponibilité de 100% et une indisponibilité nulle de service. Il s'agit là d'une amélioration majeure. Cela est dû au mécanisme de quorum.

4.5 Application sur le réseau LAN

Nous examinons maintenant la disponibilité du réseau LAN d'ICOSNET. La Figure [4.17] illustre le diagramme de fiabilité de l'infrastructure réseau du *Data Center* d'ICOSNET.

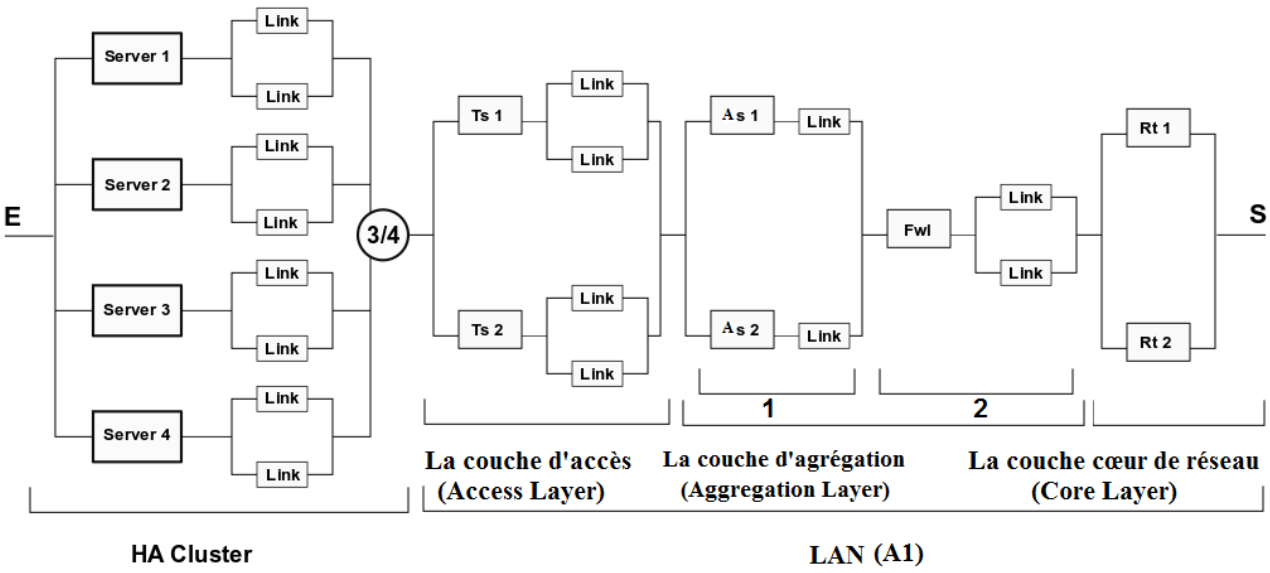

FIGURE 4.17 – *Diagramme de fiabilité pour l'infrastructure réseau du DC d'ICOSNET*

En décomposant le système (LAN) en une série de sous-systèmes parallèles et en série, la disponibilité de l'ensemble du système peut être facilement déterminée en substituant les valeurs des disponibilités de composants (Tor switch, Aggregation switch, firewall, routeur et link) présentés dans le Tableau [4.1] dans les équations [3.33] [3.35]. Les résultats sont présentées dans le Tableau ci-dessous :

	Disponibilité	Temps d'arrêt moyen **(min)**/an
Access Layer	0.999999996	0.0021
Aggregation Layer 1	0.999999467	0.280
Aggregation Layer 2	0.99994237	30.29
Core Layer	0.999999999	0.0005
LAN (A1)	0.999941832	30.57
LAN (A1) + HA Cluster (C1)	**0.999938768**	**32.18**
LAN (A1) + HA Cluster (C2)	0.999941830	30.57

TABLE 4.12 – *Les résultats obtenus pour l'infrastructure réseau du DC d'ICOSNET*

Nous avons également effectué une analyse de disponibilité sur différentes couches de réseau LAN, ainsi ce dernier avec les deux configurations HA Cluster afin de déterminer les paramètres qui affectent le plus sur la disponibilité globale du l'infrastructure réseau.

Les résultats indiquent que la couche d'agrégation 2 où il y a le pare-feu (Firewall) a le plus grand impact sur la disponibilité du l'infrastructure réseau, car sa disponibilité est très faible si on le comparant avec d'autres composants qui atteintes une disponibilité de plus de cinq ou de six (9). La panne de ce composant (Firewall) entraînera la perte de service.

Une disponibilité de quatre (9) n'est pas satisfaisante, mais peut être considérablement améliorée grâce au principe de redondance de toutes les éléments critiques. En proposant une architecture LAN (A2) avec redondance dans les périphériques pare-feu (Firewall) et liens (Links). La Figure [4.18] illustre le diagramme de fiabilité de l'architecture réseau LAN (A2). Les résultats sont présentées dans le Tableau [4.13] :

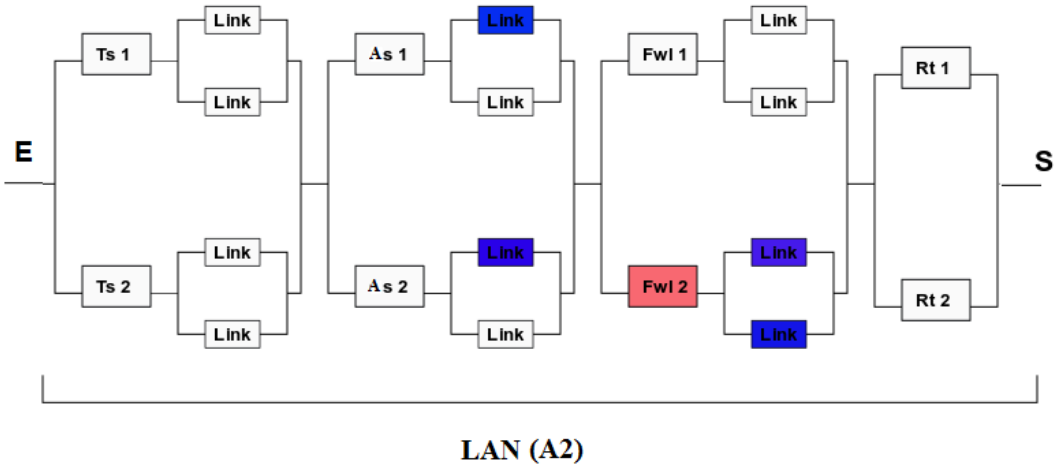

FIGURE 4.18 – *Diagramme de fiabilité pour LAN (A2) suggérée*

	Disponibilité	Temps d'arrêt moyen **(sec)**/an
Access Layer	0.999999996	0.1261
Aggregation Layer 1	0.999999999	0.0005
Aggregation Layer 2	0.999999996	0.1261
Core Layer	0.999999999	0.0005
LAN (A2)	0.99999999	0.3153
LAN (A2) + HA Cluster (C1)	**0.999996926**	**96.93**
LAN (A2) + HA Cluster (C2)	0.999999988	0.3626

TABLE 4.13 – *Les résultats obtenus pour l'infrastructure réseau du DC avec LAN (A2)*

la disponibilité qu'elle offre la deuxième architecture du LAN varie énormément par rapport au première architecture (A1). On peut dire qu'elle offre une disponibilité de 100% et une indisponibilité nulle de service. De même quand en le combinant avec la configuration HA Cluster (C2). Cela est dû au mécanisme de redondance des matériels d'accès au réseau.

A partir de cette évaluation sur le réseau LAN, nous avons pu répondre aux deux questions suivantes : Comment décider quel composant devrait être répliqué ? Comment améliorer la disponibilité du LAN en même temps pour réduire les coûts ?. Notre réponse est donc de faire redondés les points critiques individuelles disponibles.

L'indisponibilité de 96 secondes/an est dû à cause de la configuration HA Cluster (C1) (satisfaisante quand même). Il est fortement recommandé de faire combiné LAN (A2) avec HA Cluster (C2) ou avec HA Cluster (C1) pour garantit une disponibilité maximale de service *Cloud* et une sécurité extrême des données de clients.

4.6 Application sur l'architecture globale du Data Center

Nous examinons maintenant la disponibilité de l'architecture globale du *Data Center*. ICOSNET possède un *Data Center* de Tiers III qui offre une disponibilité de 99.982 % (voir la Section [2.3.4]). La disponibilité de la fibre optique WAN est estimé avec une disponibilité de 99.961 % (environ de 3h 30 min d'indisponibilité par an) par l'ingénieur d'infrastructure *Cloud* à l'entreprise ICOSNET en fonction de son expérience. La Figure [4.19] illustre le diagramme de fiabilité de l'architecture globale du DC. Le système est considéré comme étant en série. La relation mathématique qui évalue la disponibilité du système est écrite dans l'équation [3.33].

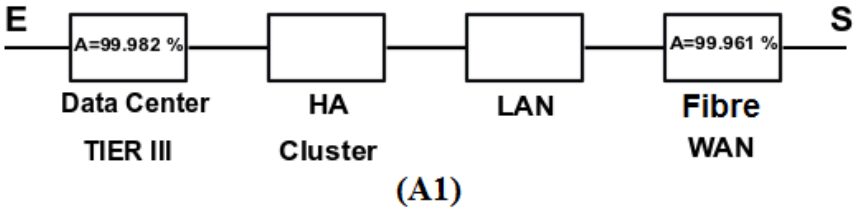

FIGURE 4.19 – *Diagramme de fiabilité pour l'architecture globale du DC d'ICOSNET*

Nous évaluons la disponibilité globale (A1) en fonction de configurations HA Cluster et architectures LAN vus auparavant. Les résultats sont présentées dans le Tableau ci-dessous :

	HA Cluster(C1) + LAN (A1)	HA Cluster(C2) + LAN (A2)	HA Cluster(C1) + LAN (A2)	HA Cluster(C2) + LAN (A1)
Disponibilité (A1)	0.999368873	0.999430058	0.999426998	0.999371933
Temps d'arrêt moyen (h)/an	5.52	4.99	5.01	5.50

TABLE 4.14 – *Les résultats obtenus pour l'architecture globale du DC*

La disponibilité globale du DC est autour de trois (9) (environ de 5 heures d'indisponibilité par an), et nous n'avons observé aucune amélioration significative avec les deux architectures fiables LAN (A2) et HA Cluster (C2). Dans ce cas, la disponibilité du système dépend entièrement d'un ou des points critiques.

Malheureusement, l'architecture globale du DC d'ICOSNET peut y aller jusqu'à 5 heures d'indisponibilité de service par an. Cela est dû notamment à la fibre WAN qui n'est pas redondée par un deuxième point d'adduction et qui rencontre souvent des problèmes de pannes durant l'année.

Nous suggérons deux architectures (A2) et (A3) qui permettent d'améliorer considérablement la disponibilité du système globale en régime permanent, mais qui sont très couteuses financièrement et complexes à mettre en place. Notre objectif est de voir la variation de la disponibilité en utilisant les deux mécanismes de haute disponibilité : la réplication sur site distant et la redondance des matériels d'accès au réseau. Les Figures [4.20] [4.21] illustrent les digrammes de fiabilité de l'architecture (A2) avec redondance dans la fibre WAN et l'architecture (A3) avec redondance d'un deuxième *Data Center* sur un autre site distant.

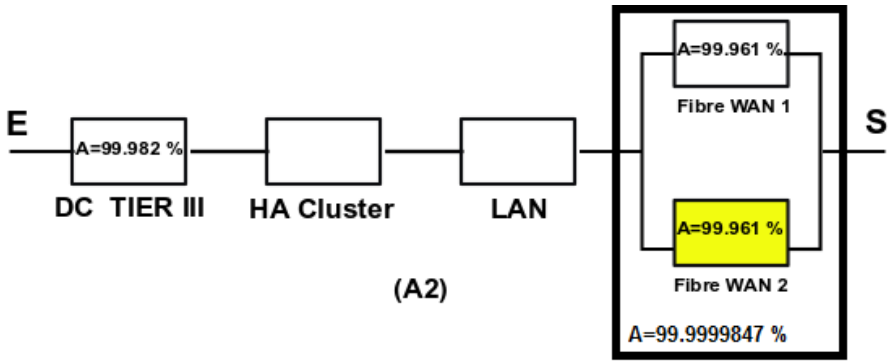

FIGURE 4.20 – *Diagramme de fiabilité pour l'architecture du DC (A2) suggérée*

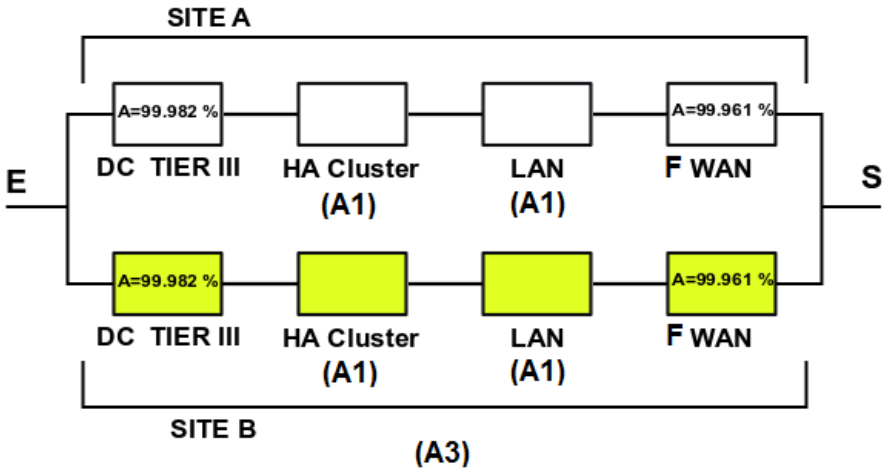

FIGURE 4.21 – *Diagramme de fiabilité pour l'architecture du DC (A3) suggérée*

Nous évaluons la disponibilité globale de (A2) en fonction de configurations HA Cluster et architectures LAN vus auparavant. Les résultats sont présentées dans les Tableaux ci-dessous :

	HA Cluster(C1) + LAN (A1)	HA Cluster(C2) + LAN (A2)	HA Cluster(C1) + LAN (A2)	HA Cluster(C2) + LAN (A1)
Disponibilité (A2)	0.999758627	0.999819835	0.999816773	0.999761687
Temps d'arrêt moyen (h)/an	2.11	1.57	1.60	2.08

TABLE 4.15 – *Les résultats obtenus pour l'architecture globale du DC (A2)*

Data Center global	Disponibilité	Temps d'arrêt moyen (sec)/an
A3	**0.999999601**	12.58

TABLE 4.16 – *Les résultats obtenus pour l'architecture globale du DC (A3)*

Les résultats indiquent une amélioration importante de la disponibilité du l'architecture (A2) par rapport à celle de (A1) (plus de deux fois supérieur). Cela est dû au mécanisme de redondance des matériels d'accès au réseau externe (la fibre WAN).

En ignorons le temps moyen de basculement d'un *Data Center* à un autre, la disponibilité de service est atteinte un niveau maximal (disponibilité de six (9)). Cela est principalement dû au mécanisme de redondance du *DC* sur un autre site distant (si le premier DC tombe en panne sur le site A, son duplicata démarre sur l'autre site B et les clients accèdent aux mêmes données).

Avec la mise en place d'une reprise après sinistre du *Data Center*, la probabilité que les deux systèmes (deux sites) soient indisponible au même moment est très faible (P= 3.98 * 10^{-7}).

Conclusion

A travers ce chapitre, nous pouvons conclure ce qui suit :

• Le RAID-6 est la technologie de stockage supérieur en terme de disponibilité, (la plus sûre qui permet une gestion redondante des données).

• La mise en place d'un HA Cluster utilisant la configuration du nœud majoritaire avec disque témoin dans l'environnement de machines virtuelles est la meilleure stratégie de haute disponibilité des données et de service.

• La redondance des matériels d'accès au réseau jugés critiques pour le fonctionnement du système est une solution certes évidente pour accroître la disponibilité du réseau et de service.

• La reprise après sinistre du *Data Center* est la solution ultime pour la haute disponibilité des données et des services Cloud. Son implémentation est très profitable à l'entreprise qui veut afficher une disponibilité applicative de 100 %.

Conclusion Générale

La violation de SLA et l'indisponibilité de services peuvent être converties en coûts directs pour le fournisseur de service Cloud ICOSNET. Pour cette raison, l'estimation de la disponibilité de l'infrastructure sous-jacente du *Cloud Computing* peut aider le fournisseur de service Cloud ICOSNET à minimiser ses coûts.

Dans ce travail nous avons présenté des modèles basés sur les blocs diagramme de fiabilité (BDF) afin d'évaluer la disponibilité du service exécuté sur l'infrastructure sous-jacente du *Cloud Computing* et d'évaluer l'impact de différentes stratégies de redondance et de tolérance aux pannes pour augmenter la disponibilité.

Dans la première partie, nous avons effectué une application sur les systèmes de stockage RAID y incluant celui qui est utilisé actuellement par ICOSNET (RAID-1) afin de voir la différence entre eux en terme de disponibilité des données. Nous avons constaté que le RAID-6 est le meilleur choix pour la sécurité extrême des données.

Dans la deuxième partie, nous avons effectué une application sur le Cluster Cloud, au terme duquel nous avons constaté que la disponibilité de ce dernier est suffisante. Mais nous avons quand même proposé une solution ultime pour le cluster contre les défaillance de double serveur et les défaillance lors de la reconstruction d'un seul serveur.

Dans la troisième et la quatrième partie, nous avons effectué une application sur le réseau interne et l'infrastructure globale du *Data Center*, respectivement. Les résultats montrent que la disponibilité des systèmes peut être améliorée de manière efficace et substantiel en se concentrant sur les composants qui ont le plus d'impact sur la disponibilité (les points critiques individuelles disponibles). Dans le contexte du l'architecture globale du *Data Center*, les résultats montrent que les systèmes très fiables (bien redondés) HA Cluster (C2) ou LAN (A2) sont moins pertinents que d'autres systèmes physiques lorsque l'objectif est de maximiser la disponibilité générale. Grâce à la redondance de point critique (fibre WAN), il est possible d'augmenter la disponibilité générale de l'infrastructure sous-jacente de plus de 180 heurs par an par rapport à un scénario sans redondance ou basé sur le mauvais choix de systèmes redondants.

Cette étude permettra à ICOSNET de voir approximativement l'état actuel de ses systèmes informatiques exécutés sous l'infrastructure sous-jacente du *Cloud Computing* (stockage, serveurs, réseau), et leurs taux de disponibilité, de savoir comment les solutions de haute disponibilité contribuer à l'augmentation du taux de disponibilité des systèmes informatiques ainsi que de modifier les stratégies de redondance adoptées actuellement au niveau de son *Data Center*.

A l'issue de l'étude effectuée, nous envisageons les perspectives suivantes :

• Valider notre approche de modélisation en nous servant des données réelles du fournisseur de service *Cloud* ICOSNET.

• Évaluer et optimiser les coûts liés aux solutions de haute disponibilité proposées.

• Effectuer une optimisation des performances de l'infrastructure sous-jacente du *Cloud Computing* sous contrainte d'énergie électrique consommée.

Bibliographie

[1] Aïssani D., Cours de Fiabilité, Master 1, Département de Recherche Opérationnelle, Université de Béjaïa, 2018.

[2] Aïssani A., et Aïssani D. *"Fiabilité des Systèmes et Systèmes de Files d'Attente non Fiables"*. U.E.R Math. - Info., ENITA (Ecole Militaire Polytechnique), Bordj-el-Bahri, 1986.

[3] Abbas A., and Mohammad H. D. *"Comparison of OS level and hypervisor server virtualization"*. In Proceedings of the 8th conference on Systems theory and scientific computation. World Scientific and Engineering Academy and Society (WSEAS), 2008.

[4] Alex O., Siebo F., and Michael D. R. *"Considerations for RAID-6 Availability and Format/Rebuild Performance on the DS5000"*. Redbooks, IBM, 2009.

[5] Baucr E., and Adams R. *"Reliability and availability of Cloud Computing"*. A John Wiley & Sons-IEEE Press, 2012.

[6] Borko F., and Armando E. *"Cloud Computing Fundamentals"*. In Borko Furht and Armando Escalante, Handbook of Cloud Computing, Springer US, 2010.

[7] By A., Rean G., Anthony. D. J., Randy K., Andy K., Gunho L., David P., and Ariel R.*"A view of Cloud Computing"*. Communications of the ACM, 2010.

[8] Cattier P. F., Combes M., Perrochat J., Besset G., Orifici S., Palen-gat J., Latreche A., Zerbib N., Durand R., Grosbost M., Philippe L., Le Calvé A., Rouyer A., Biscarat P., Galindo D., Stern E., Roche D., Manceau X., Sinapi S., and Brion S. *"Data Centers : Une chance pour la France"*. Livre blanc, 2010.

[9] David A. P., Garth G., and Randy H. K. *"A Case for Redundant Arrays of Inexpensive Disks"*, Proceeding. of ACM SIGMOD Conf, 1988.

[10] David H. *"Cloud Computing : A Taxonomy of Platform and Infrastructure-level Offerings"*. Technical Report April, Georgia Institute of Technology, 2009.

[11] Dehdouh A., et Drizi F. *"Modélisation et Évaluation des Performances de la Solution Cloud Computing de l'Entreprise ICOSNET (Alger)"*. Mémoire de master en Recherche Opérationnelle, Spécialité : Modélisation Mathématique et Évaluation des Performances des Réseaux, Université de Béjaïa, 2015.

[12] `https://docs.microsoft.com/fr-fr/windows-server/failover-clustering/failover-clustering-overview` (Consulté le 22/06/2019)

[13] Dharmender Singh K., and Ankit M. *"Cloud Computing-A Tool For Future"*. International Journal Of Mathematics and Computer Research, 2013.

[14] Dieye M. *"Disponibilité des données dans les centres de données a caractéristiques hétérogène"*. Mémoire de maîtrise en Informatique, Université du Québec à Montréal, 2016.

[15] Don B. *"Platform as a Service : The IBM point of view"*. Technical report, IBM Corporation, 2012.

[16] Elsayed E. *"Reliability Engineering"*. Numéro v. 1 de Reliability Engineering. Addison Wesley Longman, Inc., 1996.

[17] Equinix Group. Entreprise, *"Cloud et Data Centre"*. Technical report, 2013.

[18] Eriksen J., Nona R. A., and Chairman M. *"Guidance for Writing NATO R & M Requirements Documents"*. ARMP-4, 2001.

[19] Fang L., Jin T., Jian M., Robert B., John M., Lee B., and Dawn L. *"NIST Cloud Computing Reference Architecture"*. Technical Report 9, National Institute of Standards and Technology, 2011.

[20] Fatimah M. A., and Saad S. A. *"An analytical model for availability evaluation of cloud service provisioning system"*. Intern. Journ. of Advanced Computer Sciences and Applications, 2017.

[21] Federico C. *"High availability using virtualization"*. Thèse de doctorat de recherche en génie de l'information, Université de Pise, École doctorale Léonardo de Vinci en Ingénierie, 2006.

[22] `https://www.pexys.com/solutions-informatiques/systeme-virtualisation/` (Consulté le 20.05.2019)

[23] Gianmario M., Nicola S., and Daniele S. *"Cloud Computing : An Architectural and Technological Overview"*. In Service Sciences IJCSS-2012. International Joint Conference on Service Sciences, 2012.

[24] Gilbert M. *"Méthodologies appliquées : Adaptation au monde des réseaux"*. 1^{er} Édition. Ebook, 2017.

[25] Guto L. S., Patricia T. E., Glauco E. G., Daniel R., Demis G., Judith K., Djamel S., and Mozhgan M. *"Analyzing the IT subsystem failure impact on availability of cloud services"*. Symposium on Computers and Communications (ISCC), IEEE, 2017.

[26] Hassan R., and Jeffrey W. *"Clouds & grids : A network and simulation perspective"*. In Proceedings of the 14th Communications and Networking Symposium, CNS '11. Society for Computer Simulation International, 2011.

[27] Hlavacek J., and Bestak R. *"Availability Model for Virtualized Platforms"*. Advances in Electrical and Electronic Engineering, 2013.

[28] Höfer C. N., and Karagiannis G. *"Cloud Computing services : Taxonomy and comparison"*. Journal of Internet Services and Applications, 2011.

[29] Houssem M. *"Architectures et mécanismes de fédération dans les environnements Cloud Computing et Cloud Networking"*. Thèse de doctorat en Sciences, Spécialité : Informatique, École doctorale Informatique, Télécommunications et Électronique de Paris, 2015.

[30] Ian F., Yong Z., Ioan R., and Shiyong L. *"Cloud Computing and Grid Computing 360-Degree Compared"*. In 2008 Grid Computing Environments Workshop, IEEE, 2008.

[31] Jim S., and Ravi N. *"Virtual Machines : Versatile Platforms for Systems and Processes (The Morgan Kaufmann Series in Computer Architecture and Design)"*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2005.

[32] Kaoutar R. *"Optimisation de la disponibilité des systèmes multi-États"*. Projet industriel de fin d'études, Université Moulay Ismail, 2015.

[33] Keke G., and Saier L. *"Towards Cloud Computing : A Literature Review on Cloud Computing and Its Development Trends"*. In 2012 Fourth International Conference on Multimedia Information Networking and Security, IEEE, 2012.

[34] Lee B., Tim G., Robert P. C., and Jeff V. *"Cloud Computing Synopsis and Recommendations"*. Technical report, National Institute of Standards and Technology, 2011.

[35] Luis M. V., Luis R. M., Juan C., and Maik L. *"A break in the Clouds Towards a Cloud Definition"*. ACM SIGCOMM Computer Communication Review, 2009.

[36] Lutz S., and Keith J. *"Advances in Clouds : Research in Future Cloud Computing"*. Technical report, European Commission, 2012.

[37] Lutz S., Keith J., and Burkhard N. L. *"The Future of Cloud Computing : Opportunities for European Cloud Computing beyond 2010"*. Technical report, European Commission, 2010.

[38] Maria T., and Francis T. *"Service Availability : Principles and Practice"*. A John Wiley & Sons, 2012.

[39] Matallah H. *"Vers un nouveau modèle de stockage et d'accès aux données dans les Big Data et les Cloud Computing"*. Thèse de doctorat en Sciences, Spécialité : Informatique, Université Abou Bekr Belkaid Tlemcen, 2018.

[40] Matthieu B. *"Plan de continuité d'activité et système d'information"*. Dunod, Paris, 2006.

[41] Miha A., Dustin A., Patrick A., Andrew De A., and Joe A. *"Cloud Computing Use Cases"*. A White paper produced by the Cloud Computing Use Case Discussion Group Version 3, 2010.

[42] Mohiuddin A., Abu S., Raju C., Mustaq A., and Mahmudul H. R. *"An Advanced Survey on Cloud Computing and State of the art Research Issues"*. IJCSI International Journal of Computer Science Issues, 2012.

[43] `https://docs.microsoft.com/en-us/windows-server/storage/storage-spaces/understand-quorum` (Consulté le 13-06-2019)

[44] Peter M., and Timothy G. *"The NIST Definition of Cloud Computing"*. Technical Report 6, National Institute of Standards and Technology, 2011.

[45] Rajkumar B., Chee Shin Y., Srikumar V., James B., and Ivona B. *"Cloud Computing and emerging IT platforms : Vision, hype, and reality for delivering Computing as the 5th utility"*. Future Generation Computer Systems, 2009.

[46] Rim M. *"Contribution à la Conception et l'Implantation de la Structure de Données Distribuée & Scalable à Haute Disponibilité"*. Thèse de doctorat en Informatique. Université Paris Dauphine, 2004.

[47] Robert F. R., Tetiana B., and James R. C. *"Everyday Cloud Computing with SaaS"*. In The 2012 International Conference on Software Engineering Research and Practice SERP12, 2012.

[48] Salvatore. D. A., Miha A., Joe A., Rizwan A., and All. *"Moving to the Cloud"*. Technical Report February, Cloud Computing Use Cases Discussion Group, 2011.

[49] `http://www.haute-disponibilite.net/2009/09/24/la-haute-disponibilite/` (Consulté le 02/06/2019).

[50] Sameer R., and Apurva J. *"Cloud Computing : The Fifth Generation of Computing"*. In 2011 IEEE 3rd International Conference on Communication Software and Networks. Department of Computer science and technology, CUMT, China, IEEE, 2011.

[51] Sandra H., Xueli A., Wolfgang K., Sergio B., and Andreas K., *"Data Center architecture impacts on virtualized network functions service chain embedding with high availability requirements"*. In Proceedings of the IEEE Global Communications Conference, 2015.

[52] Scott M. *"Architecture, Maintenance et Mise à Niveau"*. Le PC, 18ème Édition. PEARSON, 2008.

[53] Shivaji M., and Kalyankar N. V. *"Cloud Computing"*. Journal of Computing, 2010.

[54] Souza R., Marcelo S., and Fernandes S. *"Importance Measures for NFV Data Center : An Availability Evaluation"*. 5º Workshop Pré-IETF-IRTF - CSBC, 2018.

[55] Stenio F., Eduardo T., Marcelo S., Victor L., and Paulo M. *"Dependability assessment of virtualized networks"*. In Communications (ICC), 2012 IEEE International Conference on, 2012.

[56] Sushil B., Leena J., and Sandeep J. *"Cloud Computing : A Study Of Infrastructure Aa A Service (IAAS)"*. International Journal of Engineering and Information Technology, 2010.

[57] Tetreau E. *"Les enjeux des Data Centers aujourd'hui et demain"*. La Journée Technologique, Bois Colombes, IBM, 2011.

[58] Uptime Institute. *"Data Center Site Infrastructure Tier Standard : Topology"*. `https://www.gpxglobal.net/wp-content/uploads/2018/11/Uptime-Tier-Standard-Topology.pdf`.

[59] VMware. *"Understanding Full Virtualization, Paravirtualization, and Hardware Assist"*. `http://www.vmware.com/resources/techresources/1008`, 2007.

[60] Yann L. T., and Nicolas P. *"Administration du système"*. GNU/Linux, version 3.1 (sarge). ENI, 2006.

[61] Ziad I. *"L'intégration des Activités de Maintenance dans la Conception des Systèmes"*. Thèse de doctorat en Automatique et Informatique Industrielle, Université de Lille 1, 2015.

[62] Zio E. *"An Introduction to the Basics of Reliability and Risk Analysis"*. World Scientific Publishing Co. Inc., Singapore, 2007.

[63] Zwingelstein G. *"Diagnostic Des Défaillances : Théorie et Pratique Pour Les Systèmes Industriels"*. HERMES, 1995.

[64] `https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/DC_BladeServer/DCBladServ/BSrv_Ch4.html` (Consulté le 11/06/2019)

Abstract

Cloud Computing is a major technological trend that continues to evolve and prosper. With the advent of the *Cloud*, ensuring high availability of *Cloud* service has become a critical issue for *Cloud* service providers. Providing highly available and reliable services in the *Cloud* is essential to maintain customer trust and satisfaction and avoid financial losses due to SLA contract violations. *Cloud Data Center* modeling is essential to assess and predict the availability of its internal connectivity. This paper presents an assessment of the availability of the underlying infrastructure on which ICOSNET's *Cloud* services are hosted. The work was conducted on the basis of models based on separate analytical Reliability Diagram Blocks (BDF) to assess the impact of different high availability strategies to increase the availability of data and *Cloud* services. The availability assessment helped us to identify critical points leading to lower system availability. Suggestions for improving the availability of *Cloud Data Center* services are provided on each system of the technical infrastructure. The results and conclusion of this study may be useful for the *Cloud* service provider ICOSNET to modify the redundancy and high availability strategies currently adopted for the underlying *Cloud Computing* infrastructure.

Keywords : *Cloud Computing* ; *Data Center* ; *Availability* ; *Reliability* ; *Redundancy* ; *High Availability*

Résumé

Le *Cloud Computing* est une tendance technologique majeure qui continue d'évoluer et de prospérer. Avec l'avènement du *Cloud*, l'assurance de haute disponibilité du service *Cloud* est devenue un problème critique pour les fournisseurs de services *Cloud*. Fournir des services hautement disponibles et fiables dans le *Cloud Computing* est essentiel pour maintenir la confiance et la satisfaction des clients et éviter les pertes financières dues à des violations du contrat SLA. La modélisation du *Cloud Data Center* est essentielle pour évaluer et prédire la disponibilité de sa connectivité interne. Ce mémoire présente une évaluation de la disponibilité de l'infrastructure sous-jacente sur laquelle les services *Cloud* offerts par ICOSNET sont hébergés. Le travail a été mené sur la base des modèles basés sur les Blocs Diagramme de Fiabilité (BDF) analytiques distincts afin d'évaluer l'impact de différentes stratégies de haute disponibilité pour augmenter la disponibilité des données et des services *Cloud*. L'évaluation de la disponibilité nous a aidé à identifier les points critiques conduisant à une disponibilité moindre des systèmes. Des suggestions sur l'amélioration de la disponibilité des services du *Cloud Data Center* sont proposées sur chaque système de l'infrastructure technique. Les résultats et la conclusion de cette étude pourront être utiles pour le fournisseur de service *Cloud* ICOSNET afin de modifier les stratégies de redondance et de haute disponibilité adoptées actuellement au niveau de l'infrastructure sous-jacente du *Cloud Computing*.

Mots clès : *Cloud Computing* ; *Data Center* ; *Disponibilité* ; *Fiabilité* ; *Redondance* ; *Haute Disponibilité*.