

**Institut Universitaire de Technologie,
Aix-Marseille Université**

**RAPPORT DE STAGE de fin de deuxième année
Bachelor Universitaire de Technologie
Spécialité Réseaux et Télécommunications
parcours cybersécurité**

**DECOUVERTE DU METIER DE
DATACENTER TECHNICIEN**

Auriane PLASENCIA

MICROSOFT France 1985

Responsable entreprise : Jacques ROSIN

Responsable académique : Damien MANOUKIAN

2024

Table des matières

1	Introduction.....	5
1	Présentation de l'entreprise.....	6
1.1	Présentation générale de Microsoft.....	6
1.2	Structure et organisation.....	6
1.3	Activités et Projets.....	6
2	Qu'est-ce qu'un Datacenter.....	8
2.1	Description Général.....	8
2.2	Les types de datacenter.....	9
2.3	Les datacenter Microsoft.....	11
2.4	Fonctionnement.....	12
2.5	Engagement.....	12
3	Break Fix.....	14
3.1	C'est quoi ?.....	14
3.2	Fonctionnement en ticket.....	16
3.3	Scrubbing.....	17
3.4	Ticket de maintenance.....	17
3.4.1	Exemple maintenance.....	18
3.5	Ticket d'investigation.....	19
3.5.1	Exemple investigation.....	19
4	Déploiement.....	20
4.1	Préparation pré-déploiement.....	20
4.2	Déploiement.....	21
5	Conclusion.....	23
6	Sitographie.....	30

1 Introduction

Ce rapport de stage, réalisé dans le cadre de mon BUT (Bachelor Universitaire et Technologique) Réseau et Télécommunication, explore mon immersion au sein d'un datacenter de Microsoft. En participant à des projets techniques et en assurant la maintenance des serveurs, j'ai pu appliquer mes connaissances académiques et acquérir une expérience précieuse dans un environnement hautement technologique et stratégique.

L'objectif de ce stage était d'apprendre le métier de technicien datacenter sous tous ses aspects. J'ai donc eu la chance d'accompagner les différents techniciens du datacenter dans leurs missions. Ces missions incluaient du Break Fix (réparation matériel) et du déploiement.

Mon rapport de stage est structuré de la manière suivante : dans un premier temps, je présenterai l'entreprise et son environnement, puis je détaillerai les différents aspects d'un datacenter, suivi des missions Break Fix qui m'ont été confiées et pour finir je détaillerai le processus de déploiement au sein d'un datacenter. Enfin, je conclurai par un bilan personnel de cette expérience enrichissante et des compétences acquises.

1 Présentation de l'entreprise

1.1 Présentation générale de Microsoft

L'entreprise Microsoft a été fondée le 4 avril 1975 par Bill Gates et Paul Allen. À l'origine, elle s'appelait "Micro-Soft". Au fil des années, Microsoft a lancé des produits emblématiques tels que MS-DOS et Windows. Elle a évolué pour devenir un acteur majeur dans les domaines des logiciels, des jeux vidéo, de la téléphonie mobile et des services cloud. De nos jours, Microsoft est une entreprise dominant le monde informatique.

Microsoft opère dans le secteur de l'informatique et de la micro-informatique. L'entreprise se concentre de plus en plus sur Microsoft Azure (les services cloud) et les technologies émergentes comme l'intelligence artificielle.

La mission de Microsoft est de permettre à chaque individu et chaque organisation sur la planète de réaliser leurs ambitions. L'entreprise vise à innover, à créer des solutions technologiques puissantes pour améliorer la vie des gens à travers ses produits et services.

1.2 Structure et organisation

Microsoft a une organisation dite divisionnaire, elle est basée sur des groupes fonctionnels et des groupes d'ingénierie. Depuis sa dernière restructuration en 2015, l'entreprise a maintenu une approche hybride entre la haute direction, les groupes fonctionnels et les groupes d'ingénierie.

Les groupes d'activités de Microsoft sont divisés en plusieurs domaines, avec le développement commercial, les ventes mondiales, le marketing, les ressources humaines et LinkedIn. Les groupes d'ingénierie, eux, se concentrent sur des domaines tels que l'intelligence artificielle, la sécurité et la recherche.

En 2023, Microsoft emploie plus de 221,000 personnes à travers le monde. L'entreprise est composée d'une équipe de direction plutôt restreinte, composé du PDG Satya Nadella, du président et vice-président, d'un directeur financier, d'un directeur de marketing et d'un directeur des ressources humaines.

La culture d'entreprise chez Microsoft est très présente et très important aux yeux des employés. Les valeurs et la culture interne de Microsoft mettent l'accent sur la diversité, l'inclusion, l'intégrité et l'engagement envers la communauté. Le bien être des employés compte beaucoup pour Microsoft, tout est fait pour que les employés puissent s'épanouir dans un environnement de travail positif et stimulant.

1.3 Activités et Projets

Microsoft propose une gamme étendue de produits et services. Voici les principaux :

- Microsoft 365 : Une suite d'applications et de services pour la productivité, comprenant Word, Excel, PowerPoint, Outlook, Teams et bien d'autres.
- Azure : Une plateforme cloud qui offre des services d'infrastructure, d'analyse, d'intelligence artificielle et de développement d'applications.
- Xbox : La célèbre console de jeux vidéo et les services associés.
- LinkedIn : Le réseau social professionnel.
- Microsoft Surface : Une gamme d'appareils hybrides entre tablette et ordinateur portable.

Microsoft se distingue par ses innovations dans l'intelligence artificielle, les données et les applications. Par exemple, ils ont développé des solutions de données modernes pour alimenter la transformation IA et créer des applications intelligentes combinant l'IA et les données à l'échelle du cloud.

En ce moment, Microsoft a beaucoup de projets en cours de réalisation on compte notamment un investissement de plus de 4 milliards d'euros pour développer une infrastructure cloud et IA de pointe, en France. Ils visent à former 1 million de personnes et à soutenir 2 500 startups françaises d'ici 2027.

Microsoft agrandi son partenariat avec OpenAI et investit plusieurs milliards de dollars dans cette startup axée sur l'intelligence artificielle. De plus Microsoft collabore avec divers partenaires stratégiques, notamment des entreprises de formation en IA, pour accélérer la préparation des organisations françaises et soutenir les startups françaises qui utilisent leur technologie en toute confiance. Ils continuent également à nouer des partenariats commerciaux pour garantir un large accès à leur technologie d'IA.

2 Qu'est-ce qu'un Datacenter

2.1 Description Général

Définition :

“ Un datacenter est une installation physique centralisée qui stocke les applications et données critiques des entreprises. Une définition courante d'un data center est un emplacement où l'équipement informatique et réseau est utilisé pour collecter, traiter et stocker des données, ainsi que pour distribuer et permettre l'accès aux ressources.”

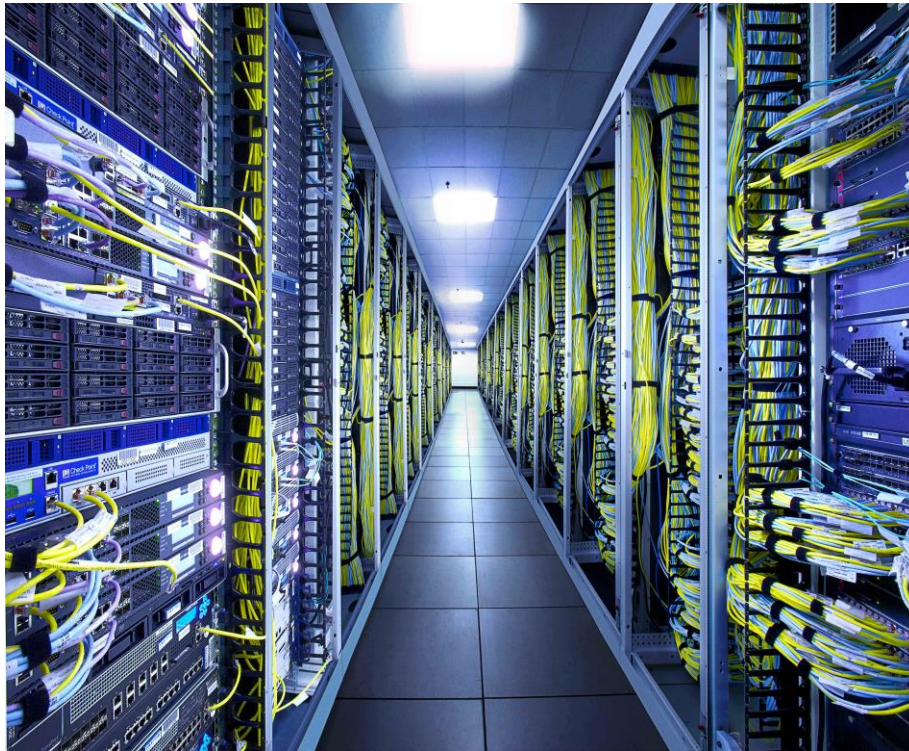


Figure 1 : Exemple d'allée dans un datacenter

Les Datacenters jouent un rôle essentiel dans le monde de l'informatique. Ils centralisent les opérations et les équipements informatiques des organisations, offrant un emplacement sécurisé pour stocker, partager et gérer d'énormes quantités de données. Ces installations permettent aux entreprises de visualiser, sauvegarder et stocker leurs données de manière flexible, tout en les protégeant contre les catastrophes naturelles et les incidents causés par l'homme. Les Datacenters sont responsables de la réception, du stockage et de l'envoi de données pour soutenir les applications métier critiques et alimenter des services de données intensifs comme :

1. Intelligence artificielle, big data et machine learning
2. Stockage, sauvegarde, restauration et gestion des données
3. Activité et transactions de commerce électronique
4. Partage de fichiers et e-mail
5. Outils de collaboration et de productivité en temps réel

Pour assurer le bon fonctionnement des composants d'un data center, une infrastructure étendue est nécessaire. Celle-ci prend en charge à la fois le matériel et les logiciels. Elle englobe les équipements d'alimentation et de refroidissement, ainsi que les connexions aux réseaux externes et les dispositifs de sécurité tels que les pare-feu et les systèmes de protection contre les intrusions. De plus, des mécanismes d'assurance de la livraison garantissent la disponibilité et la résilience des performances applicatives grâce à des basculements automatiques et à un équilibrage de charge.

2.2 Les types de datacenter

Aujourd'hui les datacenters sont séparés en plusieurs niveaux. L'Uptime Institute, une organisation de conseil spécialisé dans l'amélioration des performances, de l'efficacité et de la fiabilité de l'infrastructure critique des entreprises, a établi quatre niveaux de classification pour les installations de datacenter. Ces niveaux sont largement reconnus comme les normes de l'industrie en matière de performances des data centers. Investir dans ce processus de certification permet aux datacenters de démontrer leur conformité et leur expertise en matière de gestion des installations auprès de leurs clients.

Niveau 1:

Un data center de niveau 1 fournit la capacité de base nécessaire pour prendre en charge l'informatique d'un bureau. Il requiert une alimentation sans interruption (UPS, Uninterruptible power supply) pour faire face aux pannes de courant, aux creux de tension et aux pics. De plus, il doit disposer d'une zone dédiée aux systèmes informatiques, d'un équipement de refroidissement fonctionnant en dehors des heures de bureau et d'un générateur de secours en cas de coupure de courant. Cependant, une installation de niveau 1 offre une protection limitée contre les défaillances et les pannes inattendues. Elle devra être complètement arrêtée pour les réparations et la maintenance. En conséquence, sa disponibilité est de 99,671 %, sans redondance, et elle subira environ 28,8 heures d'arrêt par an.

Niveau 2:

Les data centers de niveau 2 offrent une protection accrue contre les événements physiques. Ils garantissent la maintenance et la sécurité face aux perturbations grâce à des équipements tels que les systèmes de refroidissement, les générateurs d'énergie, le stockage, les réservoirs de carburant et les pompes. Toutefois, comme pour une installation de niveau I, un arrêt inattendu affecte le système, entraînant une disponibilité de 99,749 % et 22 heures d'arrêt par an.

Niveau 3:

Contrairement aux data centers de niveau 1 et 2, un data center de niveau 3 ne nécessite pas d'arrêt complet lorsqu'une maintenance ou un remplacement d'équipement est nécessaire. Il est doté de composants redondants et de chemins de distribution multiples, ce qui permet de le maintenir en service simultanément. Un data center de niveau 3 convient davantage aux grandes entreprises et offre une protection contre la plupart des événements physiques. Sa disponibilité est de 99,982 %, il est tolérant aux pannes N+1 (fournissant au moins 72 heures de protection contre les pannes de courant) et subit moins de 1,6 heure d'arrêt par an.

Niveau 4:

Les data centers de niveau 4 sont dotés de systèmes indépendants et physiquement isolés, créant ainsi des composants de capacité et des chemins de distribution redondants. Cette conception garantit que les perturbations, qu'elles soient planifiées ou non, n'affecteront pas les opérations de l'installation et de l'informatique. Tous les équipements informatiques d'un datacenter de niveau 4 doivent être

conçus pour résister aux pannes électriques, et le bâtiment doit maintenir un refroidissement continu pour assurer un environnement stable.

Ces installations de niveau 4 sont généralement adaptées aux entreprises. Elles offrent une disponibilité de 99,995 %, avec seulement 26,3 minutes d'arrêt annuel. De plus, elles disposent d'une infrastructure entièrement redondante 2N + 1 et d'une protection contre les pannes de courant pouvant durer jusqu'à 96 heures.

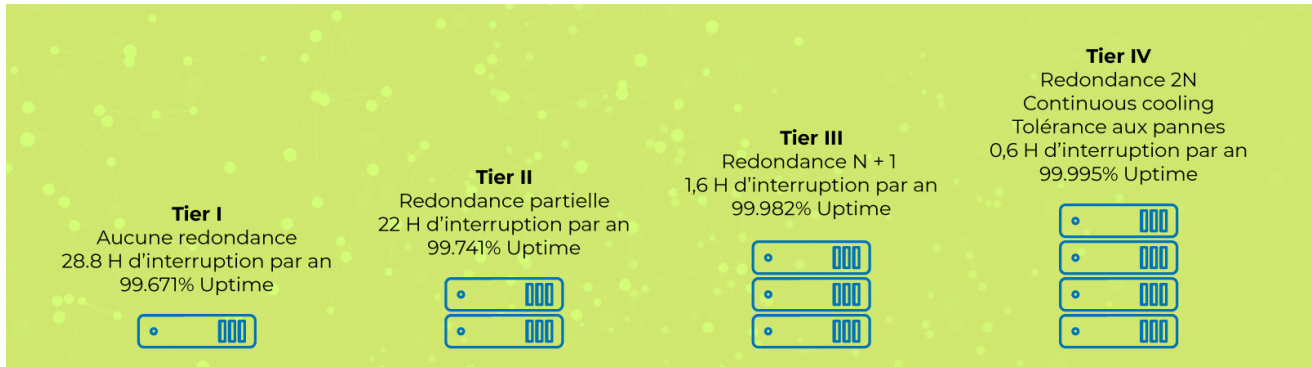


Figure 2 : Récapitulation des différents niveaux de datacenter

De plus les entreprises ont le choix entre plusieurs modes de cloud. On trouve notamment les clouds publics, les clouds privé et les clouds hybrides.

Les clouds publics sont des clouds où l'infrastructure finale n'appartient pas à l'utilisateur. Les entreprises louent ces services à de grandes entreprises telles que Alibaba Cloud, Microsoft Azure, Google Cloud, Amazon Web Services (AWS) et IBM Cloud. Un cloud est dit publique à partir du moment où le fournisseur loue ses services à plusieurs entités. C'est souvent une très bonne solution pour les entreprises voulant protéger et regrouper leurs données mais ayant un petit budget.

Les clouds privés sont administrés par l'utilisateur final ou par un groupe, généralement on les trouve au sein de l'entreprise derrière leur pare-feu. L'entreprise gère l'achat des serveurs, la mise en place des services et de la sécurité. Même si de nos jours, ces clouds privés là tendent à disparaître pour des clouds privés gérés par des tiers. Les groupes louent les services d'entreprises spécialisés dans la mise en place des services clouds qui leur fabriqueront leur espace dédié dans leur datacenter.

Les clouds hybrides fonctionnent à partir d'un mélange de réseaux interconnectés (LAN (Local Area Network), WAN (Wide Area Network), VPN (Virtual Private Network), etc.) pour créer un environnement unique. Comme son nom l'indique ces clouds comprennent au moins un cloud privé et un cloud public. Cette solution permet au client de disposer ses données là où il le souhaite, lui permettant de garder ses données les plus sensibles près de lui mais d'avoir un espace avec une plus grande disponibilité pour gérer les périodes de forte demande.

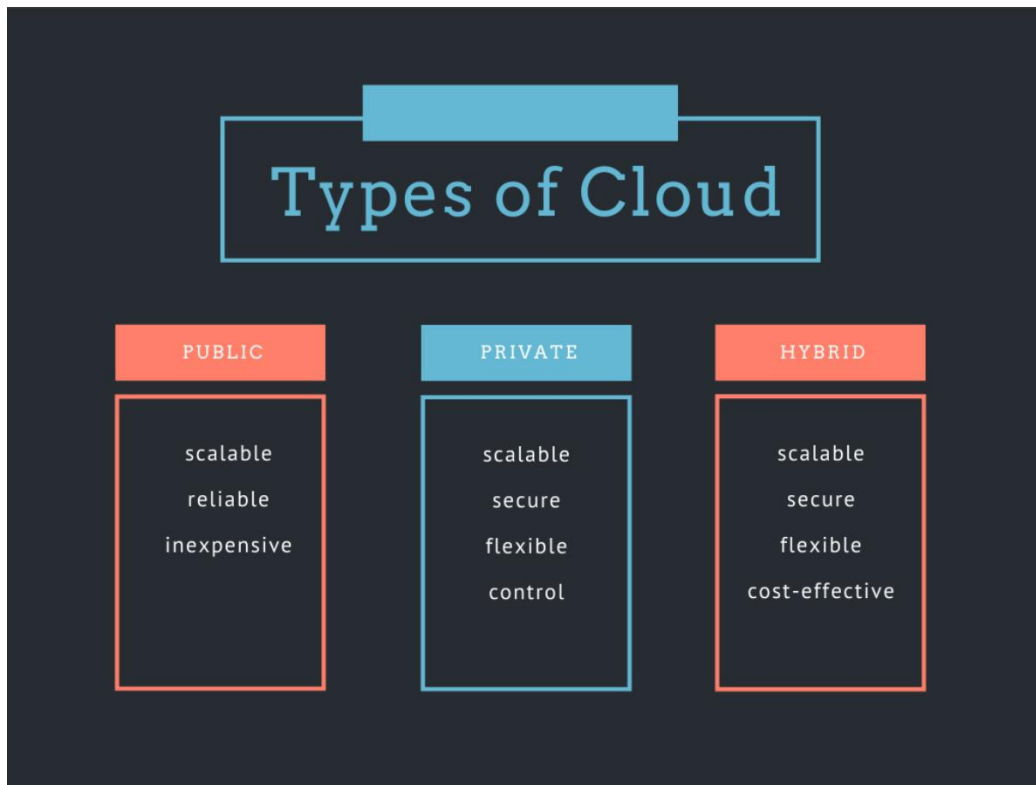


Figure 3 : Récapitulation des différents types de clouds

2.3 Les datacenter Microsoft

On retrouve des datacenters de Microsoft dans le monde entier, en Europe, Amérique, Afrique et Asie. Grâce à ça, Microsoft augmente encore sa disponibilité pour ses clients et sa capacité de résilience. Les datacenters de Microsoft sont de niveaux 4 avec un pourcentage de disponibilité de 99,999%.

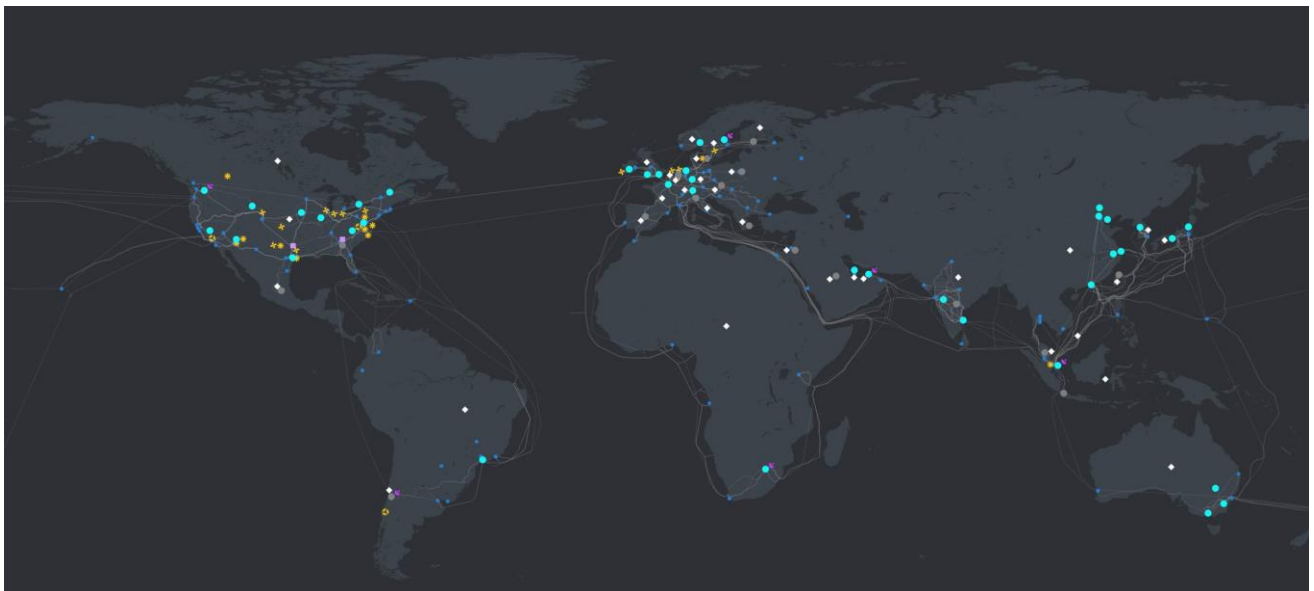


Figure 4 : Carte du monde des différents datacenter de Microsoft

Les datacenters de Microsoft servent à plusieurs fins essentielles, principalement liées à la fourniture de services cloud.

Le service principal est le « Services Cloud (Azure) ». Les datacenters hébergent majoritairement Microsoft Azure qui est la plateforme cloud de Microsoft. Azure offre une gamme de

services : le stockage, les bases de données, l'intelligence artificielle, l'Internet des objets (IoT), et bien d'autre chose. Les entreprises utilisent Azure pour héberger leurs applications, gérer leurs bases de données, ou encore déployer leurs services à grande échelle.

Mais les datacenters hébergent aussi les services de productivité en ligne de Microsoft, tels que Microsoft 365. Cela inclut des applications comme Outlook, Word, Excel, PowerPoint, Teams, et OneDrive que nous connaissons tous très bien. Ces services permettent aux utilisateurs d'accéder à leurs documents et communications de n'importe où, avec une disponibilité et une sécurité élevée. Dans la même idée on retrouve Dynamics 365 est une suite de gestion d'entreprise (des applications de gestion de la relation client (CRM, Client Relationship Management) et de gestion des ressources de l'entreprise (ERP, Enterprise Resource Planning)) qui aide les entreprises à gérer leurs opérations financières, leurs relations clients, leurs ventes, et plus encore. On compte aussi les services de jeu en ligne et les infrastructures pour les consoles Xbox (Xbox Live), ainsi que le service de streaming de jeux Xbox Game Pass.

En résumé, les datacenters de Microsoft sont des infrastructures critiques, elles soutiennent l'économie grâce à une vaste gamme de services numériques, permettant aux entreprises et aux particuliers d'accéder à des ressources informatiques puissantes, flexibles et tout en étant à l'abri d'une possible attaque.

2.4 Fonctionnement

Il existe plusieurs types de datacenter chez Microsoft. Certains sont administrés entièrement par Microsoft (le bâtiment, les arrivées d'électricité, la climatisation, la sécurité, les technologies, la connectivité), d'autre louent des espaces dans des datacenters déjà existant. Ces derniers peuvent avoir plusieurs niveaux, allant de louer un bâtiment entier jusqu'à ne louer qu'un ou deux racks dans des datacenters déjà existant.

J'ai eu la chance de travailler dans des sites dit en "colocation". Le fonctionnement en colocation un principal point :

- ➔ Infrastructure partagée : Ce n'est pas au client de s'occuper des arrivés d'énergies, de la climatisation, de la sécurité ou même de la connectivité avec l'extérieur.

Le fait d'être en colocation apporte beaucoup de points positifs, mais aussi de points négatifs. Avoir une infrastructure partagée permet d'avoir moins de choses à gérer mais dès qu'il y a une action à faire dans le datacenter comme un déploiement, le landlord (le propriétaire) doit être au courant et doit faire déplacer certains de ses techniciens pour intervenir. Alors que si le datacenter est totalement la propriété de Microsoft, les techniciens n'ont pas à faire appel à des entités extérieures pour faire des modifications dans leurs salles. Par exemple, si on fait tomber quelque chose à travers les dalles ventilées, nous devons appeler un technicien du landlord pour pouvoir récupérer ce qui était tombé.

2.5 Engagement

Au sein de leur datacenter, Microsoft s'engage notamment par rapport à la sécurité des données de leurs utilisateurs. Sur chaque site sur lequel Microsoft opère, il y a, de façon régulière, ce qui s'appelle un « DBD (Data Bearing Device) shred (destruction) », tous les disques durs ou SSD (Solid-state Storage Device) doivent être détruits. Cette destruction est très encadrée. De plus, Microsoft s'engage à protéger les données des clients avec d'autres mesures de sécurité avancées, comprenant le chiffrement des données au repos et en transit.



Figure 5 : Un DBD shredder

La sécurité des infrastructures est aussi très importante. Etant donné que nous sommes en colocation, toute l'infrastructure et la sécurité n'est pas assurée par Microsoft même. Tous les mois, les landlords doivent un rapport détaillé sur les colos (salle de colocation occupé par Microsoft), ce rapport comprend : l'énergie utilisé en pourcentage sur les deux voies d'arrivé de courant et les niveaux de température et d'humidité. Dès qu'un changement survient, Microsoft demande ce qu'il s'est passé tels jours à telles heures pour en comprendre les causes.

Mais Microsoft s'engage aussi auprès de ses employés qui travaillent dans les datacenters. Il existe un programme appelé "Safety & Security" visant à gérer la sécurité et la préservation de la santé de ses employés. Pour ça, Microsoft procure à tous ses employés des EPI (équipement de protection individuel). Ces EPI comprennent notamment un gilet de haute visibilité, des chaussures de sécurité, un casque anti bruit et un casque de protection). Aucune personne n'a le droit de rentrer en salle sans sa protection peu importe ce qu'elle va y faire. En plus des protections, tout le monde est amené à suivre des formations de préventions des risques dans un datacenter.



Figure 6 : Exemple de différents EPI

3 Break Fix

3.1 C'est quoi ?

La plupart des missions réalisées lors de mon stage étaient des missions de Break-Fix. Dans un datacenter avec autant d'équipements, il y a souvent des pannes et c'est aux techniciens de régler les problèmes. Tout ce qui se trouve dans le datacenter peut être audité ou changé. Voici une liste non exhaustive des composants pouvant être remplacé :

Carte mère : Une carte mère est le composant principal d'un ordinateur/serveur qui sert de plateforme de connexion pour tous les autres composants matériels qu'on va voir par la suite.



Figure 7 : Une carte mère

CPU : Un CPU (Central Processing Unit), ou processeur, est le composant d'un ordinateur/serveur qui effectue les calculs et exécute les instructions des programmes. Il agit comme le cerveau de l'ordinateur, interprétant et exécutant les commandes des logiciels.



Figure 8 : Un CPU

DIMM : Une DIMM (Dual In-line Memory Module) est un type de module de mémoire utilisé dans les ordinateurs pour stocker temporairement des données en cours de traitement. Elle se compose de plusieurs puces de mémoire vive (RAM (Random Access Memory)) montées sur un petit circuit imprimé.



Figure 9 : Une DIMM

NIC : Une NIC (Network Interface Card), ou carte réseau, est un composant matériel qui permet à un ordinateur de se connecter à un réseau, comme un réseau local (LAN) ou l'Internet. La NIC peut être intégrée à la carte mère ou être une carte d'extension installée dans un emplacement d'extension.



Figure 10 : Une NIC

DBD (HDD, SSD) : Un HDD (Hard Disk Drive) et un SSD sont des dispositifs de stockage utilisés pour conserver des données dans un ordinateur. Un HDD utilise des disques magnétiques rotatifs pour lire et écrire des données. Et un SSD utilise des puces de mémoire flash pour stocker les données, sans pièces mobiles.



Figure 11 : Un HDD et un SSD

Câbles :

- Cuivres : Les câbles en cuivre utilisés pour le management des réseaux et des systèmes informatiques sont essentiels pour la transmission de données.



Figure 12 : Un câble cuivre

- AOC : Les câbles AOC (Active Optical Cable) sont utilisés dans les réseaux pour la transmission de données à haute vitesse sur de longues distances. Les câbles AOC utilisent des fibres optiques et des composants électroniques actifs pour convertir les signaux électriques en signaux optiques et vice versa. Cela permet une transmission de données rapide, fiable et à haut débit, souvent sur des distances plus longues que les câbles en cuivre traditionnels. Les optiques des AOC sont très fragiles. Il arrive souvent que ce soit l'optique qui pose un problème.



Figure 13 : un câble AOC

Equipement réseaux : Les équipements réseaux sont des dispositifs essentiels utilisés pour créer, gérer et sécuriser les réseaux informatiques. Ils permettent la communication, le partage de données et l'accès aux ressources au sein des réseaux locaux (LAN) et sur Internet. Dans le datacenter nous sommes amenés à ne changer généralement que des switches ou des équipements de management de blade.



Figure 14 : image d'un switch

3.2 Fonctionnement en ticket

Chez Microsoft, nous avons un fonctionnement en ticket. C'est-à-dire que toutes les missions de Break-Fix sont référencés dans une application appelée GDCO. Cette application à bien d'autres utilités mais je ne vais ici me concentrer uniquement sur les tickets.

La majorité des tickets sont générés de manière automatique par les serveurs, ces derniers effectuent des contrôles périodiques pour identifier toute anomalie potentielle. À la suite de cela, les tickets associés sont attribués aux techniciens qui ont pour responsabilité de les résoudre. Habituellement, les techniciens Break-Fix obtiennent leurs tickets via ce processus, bien que dans certains cas, ce sont les ingénieurs réseaux ou d'autres techniciens qui vont en émettre lorsqu'une action est requise.

Dans un ticket, on retrouve diverses informations. On trouve notamment :

- La nature du problème. C'est-à-dire s'il faut changer un composant, vérifier quelque chose en colo, investiguer sur une blade et autre. Il existe énormément de types de ticket.
- L'emplacement de la mission. On nous précise, la salle, la rangée, le racks précis dans la rangée, l'emplacement de l'équipement et même le numéro de série. Le numéro de série nous sert à être sûr que nous opérons sur le bon équipement. Si nous avons un ticket sur un câble, nous allons avoir l'emplacement du début et de la fin du câble.
- La gestion du stock. Quand nous réparons les équipements, il arrive très fréquemment que nous ayons à remplacer une pièce. Pour cela nous devons donc « check-out » la pièce, c'est-à-dire

prévenir qu'on va sortir cette pièce et l'utiliser. La gestion du stock est quelque chose de très suivi, il est donc important de bien check-out tout ce qui sort du stock.

- Faire une action. Nous avons parfois besoin de faire des demandes au système informatique gérant tous les équipements présents dans le datacenter. On peut notamment demander d'allumer ou éteindre l'équipement voir même demander les mots de passe pour se connecter au serveur pour pouvoir investiguer dessus.

En conclusion, les tickets sont les outils les plus précieux pour les techniciens Break-Fix. Ils leurs permettent de pouvoir partir réparer l'équipement désigné rapidement en ayant juste à jeter un coup d'œil sur la tâche. Cette fonctionnalité apporte énormément de productivité aux équipes.

3.3 Scrubbing

Quand on se voit assigner un ticket, la première étape est l'étape de scrubbing. Pendant cette étape, le technicien va chercher les informations importantes. Le fault code et le titre du ticket pour connaître le problème et l'action demandée. Avec ces informations là un technicien va savoir, par exemple combien de temps la tâche va lui prendre ou si elle risque d'être compliquée. Après on va avoir la sévérité c'est-à-dire l'urgence de la tâche, la sévérité va jouer sur le temps alloué à la résolution de la tâche. Puis on va chercher à connaître l'emplacement de l'appareil, la salle, la rangée, le rack précis dans la rangée, l'emplacement de l'équipement dans le rack. Sur le ticket on va aussi voir le niveau de sécurité du rack, certains racks sont protégés par des clés voire plus, il est donc toujours utile, avant de partir en salle, de savoir s'il nous faut une clé.

Certains tickets sont très guidés comme expliqué ci-dessus. Mais quelquefois il arrive que nous n'ayons que très peu d'information ailleurs que dans la description du ticket contenant les logs de l'erreur. A cet endroit-là on pourra trouver les informations comme le numéro du disque dur à changer.

Il est toujours intéressant de regarder un onglet appelé 'tâche relaté'. Cet onglet peut nous montrer si l'équipement a déjà eu des problèmes sur le composant qu'on nous demande de changer. Cela peut nous indiquer que le problème ne vient peut-être pas du composant. Par exemple un jour, nous avons comme tâche d'aller changer deux DIMMs, or la veille ces mêmes DIMMs avaient déjà été changées par un autre technicien, ce qui indique que l'équipement avait un problème plus compliqué que juste les deux DIMMs fautives. Le ticket de maintenance est donc devenu un ticket d'investigation.

3.4 Ticket de maintenance

Voyons maintenant le déroulement d'un ticket de maintenance.

1ere étape : Le scrubbing. On va chercher toutes les infos possibles qui vont nous permettre de régler le ticket le plus proprement et rapidement possible et avec le moins d'erreurs.

2e étape : Check-out des composants. On ne fait cette partie que juste avant de partir chercher le composant. Quand on veut sortir un composant, il existe parfois plusieurs composants compatibles avec lesquels on peut faire un remplacement. On prendra toujours celui qui est « Requested » c'est-à-dire demandé pour cette réparation. Parfois aucun composant n'est requested donc on prend un composant AS (Accepted Spare), ou à défaut FE (Functional Equivalent).

3e étape : Réparation en salle. Une fois en salle, on va prendre tous les outils utiles pour réaliser la maintenance. Si le serveur n'est pas sur rail, nous allons utiliser un server lift. Ces équipements nous permettent de retirer les serveurs de leur emplacement sans qu'on ne risque de les abimer et sans que nous nous blessions.



Figure 15 : Exemple d'utilisation d'un server lift

Après nous n'avons plus qu'à ouvrir le serveur et faire la réparation demandée. Une fois fini, on remet le serveur à sa place et on fait une demande via GDCO pour rallumer l'équipement. On vérifie bien que l'équipement redémarre, et si tout va bien, on peut fermer le ticket.

3.4.1 Exemple maintenance

Lors du stage, nous avons été amenés à faire beaucoup de break fix. Voici un exemple de break fix que nous avons fait plusieurs fois.

Dans le datacenter, il y a des équipements qui ne peuvent pas être arrêtés. C'est notamment le cas de blades contenant énormément de HDD. Quand nous devons en changer, nous appelons ça un « hot swap » car les disques durs sont toujours en marche quand nous venons les récupérer pour les changer.

Le scrubbing nous permet de savoir où nous allons. Pendant le stage, il y a eu des vagues de hots swap, il est alors intéressant de savoir où sont les équipements pour pouvoir s'organiser.

Une fois fait, nous pouvons check-out les composants et aller les prendre dans le stock.

Entrer en salle avec des DBD est très contrôlé, nous devons bien montrer que le composant était scellé dans son emballage.

Dans un premier temps nous devons repérer la bonne blade grâce à son numéro, numéro renseigné dans le ticket. Une fois sûr d'être devant le bon équipement, nous pouvons dévisser les vis et la sortir pour opérer le hot swap. Ces blades-là n'avaient pas besoin de server lift car elles étaient sur rails ce qui rendait notre travail plus facile. Une fois la blade sortie, il nous faut repérer le bon disque dur. Une fois le disque trouvé, nous pouvions l'enlever, et là encore nous devons regarder son numéro de série pour s'assurer que c'était bien le bon composant.

Une fois validé que tout était en ordre, nous pouvions opérer le remplacement.

Etant donné que nous remplaçons des DBD, nous ne pouvons pas sortir avec, nous avons donc dû jeter le DBD dans des poubelles prévues à cet effet en salle. Dans le ticket, nous devons renseigner la poubelle pour que la logistique sache combien de DBD sont censés se trouver dedans quand ils feront le shred.

Quand tout ça est fait, nous pouvons fermer le ticket.

3.5 Ticket d'investigation

Pour les tickets d'investigations, c'est différent.

1^{ère} étape : Tout comme les tickets de maintenance, on commence par le scrubbing.

2^e étape : Aller en salle. Là nous n'avons pas besoin de récupérer de composant, car justement on nous demande d'aller voir ce qui pose un problème. De plus, pour lancer notre logiciel nous avons besoin d'être physiquement devant le rack.

3^e étape : Demander le mot de passe. Sur le ticket, on demande les mots de passe pour pouvoir se connecter au rack manager. Le rack manager sert à accéder au blade présent dans le rack. En se connectant au rack manager, nous pouvons effectuer plusieurs choses : identifier l'équipement via une led, demander les logs d'un équipement ou encore récupérer la configuration réseau. Par la suite, il nous faut nous connecter à la blade.

4^e étape : Vérifier les composants. Certains tickets nous demandent juste d'aller vérifier via SMTK (le logiciel qui nous permet de faire nos tests sur le server), si tous les disques sont bien vu par la blade, de faire un stress test, de voir l'état des DIMMs ou autre. Dans ces cas-là, le ticket est vite résolu. Seulement parfois, la blade n'arrive pas à boot du tout. Si la blade n'arrive pas à boot, nous allons alors là passer en configuration minimale. La configuration minimale nous permet de retirer tous les éléments non essentiels qui pourraient causer des erreurs si tout fonctionne correctement, on pourra remettre les éléments un par un pour voir lequel est le fautif.

3.5.1 Exemple investigation

Cette fois-ci je vais donner un exemple de ticket d'investigation auquel j'ai pu assister.

Le ticket pour lequel nous étions appelés était un ticket pour changer une DIMM. Lors du scrubbing, on ne voit pas de tâche relatée récente donc pas de problème de ce côté-là. Le ticket ressemblait en tout point à un ticket de maintenance classique.

Donc tout comme un ticket de maintenance classique. Nous récupérons le composant, partons en salle et changeons le composant. Alors que l'on cherchait l'emplacement de la DIMM fautive, nous remarquons qu'une des DIMMs était mal clipsé à la carte mère. N'étant pas la DIMM dite fautive, nous la remettons correctement faisons notre changement et rallumons la blade.

Nous avons alors rencontré un problème, la led qui indique si la blade boot correctement s'allume en rouge. En nous connectant au rack manager, nous nous rendons compte qu'en effet, le server ne boot pas et reste bloqué dans le processus.

Nous décidons donc de passer le server en configuration minimale. Le server boot correctement. Nous pouvons donc ajouter une à une les DIMMs et tester si le server boot. Finalement, le server n'a plus eu de problème à boot. Il devait certainement y avoir un problème de connectique avec les DIMMs, ce problème étant réglé nous pouvions fermer le ticket.

4 Déploiement

Un déploiement se découpe en plusieurs étapes. Il y a d'abord la préparation. Les jours de déploiements sont très chargés et les équipements sont censés être opérationnels le plus vite possible après. Alors on se doit de préparer la zone pour que tout soit prêt le jour du déploiement.

4.1 Préparation pré-déploiement

Etant donné que nous sommes en colocation, nous recevons des salles vides juste avec l'emplacement des MoR (Middle of Row) marqué. Les MoRs sont des racks dans lesquels, nous allons mettre tous les équipements de réseaux, de management et la gestion de la console. Selon les besoins de la rangée que nous déployons, le nombre d'équipements peut varier dans les MoR, généralement ce sont les switches qui varient. C'est donc à nous d'installer les équipements qui nous intéressent.



Figure 16 : Salle d'un datacenter avant déploiement

Ensuite, nous avons besoin de la « cable map », ce sont les ingénieurs qui s'occupent de ça. De leur côté, ils vont s'occuper de matérialiser les connections entre les racks et le MoR. Une fois la cable map de fait et de reçue, nous pouvons alors faire nos étiquettes. La cable map que nous recevons ne prend pas en compte les spécificités de notre infrastructure, nous devons donc faire quelques modifications avant d'imprimer les étiquettes. Les étiquettes nous permettent de nous y retrouver plus facilement, s'il y a un problème sur un câble, nous pouvons alors savoir le début et la fin et donc savoir par où il passe et sur quel équipement il va.

Etiqueter les câbles est une tâche plutôt facile alors nous en avons beaucoup fait au début du stage, la seule difficulté est de pouvoir visualiser l'équipement sur lequel le câble va aller, et donc de savoir comment placer l'étiquette pour que le travail des techniciens ensuite soit plus facile.

Une fois les câbles étiquetés, nous devons les tirer. C'est une activité physique assez éprouvante car nous faisons ça dans les allées chaudes et nous devons tirer des bundles de câble parfois très lourds en étant en hauteur sur des échelles. Un coté des câbles tombe là où se trouve son futur rack et l'autre dans le MoR.



Figure 17 : Technicien tirant des câbles

Une fois les câbles tirés, vient le moment du dressage de câble dans le MoR. Il est très important d'avoir un câblage propre dès le début. Ça va nous permettre de mieux nous repérer et d'avoir un espace de travail dégagé pour le futur.



Figure 18 : Exemple de « cable management »

4.2 Déploiement

Quand vient le jour du déploiement, en moyenne il y a cinq techniciens réquisitionnés. A l'extérieur des salles, les logisticiens préparent les racks pour nous les faire parvenir à l'intérieur. Une fois le rack à l'intérieur, nous allons le mettre à sa place, on va le « Bolt Down », c'est-à-dire fixer à sa place. Pour assurer l'étanchéité entre les racks et s'assurer que les allées froides et chaudes soient bien isolées, nous mettons une sorte de mousse qui se colle sur le bord du rack, de façon à ce que quand le prochain arrivera, l'espace entre les deux racks sera étanche. Dès que le deuxième est en place, nous allons les fixer ensemble, et ainsi de suite.

La deuxième étape est de s'occuper de tout ce qui est lié au power. Comme nous sommes en colocation, nous ne pouvons pas nous en occuper nous-même. C'est donc un technicien du landlord qui va venir. La première étape est de mettre tous les racks à la terre. C'est primordial pour la sécurité des techniciens et des équipements. Ensuite on va brancher les PDU (Power Distribute Unit) à l'arrivée de courant. Il y a deux PDU par rack pour assurer la redondance et la plupart des équipements sont eux aussi équipés de deux arrivées de courant. Une fois tous les racks branchés, on va vérifier sur tous les racks nouvellement déployés que les arrivées de courant fonctionnent bien. On commence par la voie A, puis on allume la voie B, on va éteindre la A pour voir si la B arrive bien à prendre le relais puis on rallume la A.

Parallèlement au power, d'autres techniciens du landlord vont venir poser les dalles de ventilation dans la zone froide pour éviter toute surchauffe du côté des serveurs et autres équipements.

La troisième étape est l'étape des coppers. Il est primordial de faire cette étape avant de brancher les serveurs au réseau. Les coppers vont nous permettre de faire les mises à jour sur les serveurs, sans ça, les serveurs risqueraient d'être vulnérable à différents types d'attaque. Il faut alors attendre que tous les serveurs soient bien à jours avant de les connecter aux switchs du MoR.

La quatrième étape consiste donc à brancher les AOCs pour permettre à chaque rack de se connecter au réseau. Dans les jours qui suivent, les connexions vont être auditées pour vérifier qu'il n'y a pas de problème et si problème il y a, nous devons aller le régler.



Figure 19 : Salle complètement déployée

5 Conclusion

Le but de ce stage était pour nous de découvrir le monde de l'entreprise et ses nombreuses caractéristiques. Mes dix semaines de stage au sein des datacenters de Microsoft ont été très enrichissantes. J'ai appris beaucoup de choses sur énormément de points, qu'ils soient techniques ou humains.

J'ai eu la chance de découvrir le fonctionnement d'une grande entreprise, avec ces valeurs, ces codes et son vocabulaire spécifique.

Ces dernières semaines m'ont permis d'en apprendre plus sur le monde des datacenters et ont attisé mon attrait pour ce dernier. C'est un domaine en constant développement et plein de défis. Dans lequel j'ai pu développer mes compétences et mettre en œuvre ce que j'ai appris lors de ma formation. Pouvoir voir comment un datacenter est géré de l'intérieur et participer aux différentes missions des techniciens a été une expérience très enrichissante.

Durant le stage, j'ai eu l'opportunité de toucher à énormément de domaines, que ce soit de la fibre, du réseau, du câblage ou le fonctionnement d'une infrastructure informatique. Ainsi j'ai pu mobiliser plusieurs aspects de ma formation et développer de nombreuses compétences.

Sur le plan humain, j'ai appris ce qu'était le vrai travail d'équipe, pouvoir compter sur l'expérience de mes collègues et découvrir un milieu multiculturel dans lequel j'ai eu la chance d'échanger majoritairement en anglais.

Ce stage m'a éclairé sur le fait que dans mon futur métier je souhaiterais être la plus polyvalente possible.

Remerciements

Je tiens tout d'abord à remercier Jacques ROSIN qui a été mon manager et mon tuteur lors de ce stage pour m'avoir fait confiance, pour son écoute, sa compréhension, son aide et ses conseils. Grâce à lui, j'ai pu passer un stage riche en apprentissage et découverte.

Je souhaite également adresser mes remerciements sincères à mon directeur de formation, M. Jean-Luc DAMOISEAUX, ainsi qu'à toute l'équipe pédagogique de l'IUT R&T, grâce à qui j'ai pu avoir ce stage et qui m'ont fourni les outils nécessaires à la réussite de celui-ci.

Je remercie aussi M. Damien MANOUKIAN mon tuteur académique qui a su m'aider et me guider durant mon stage.

Enfin je souhaite remercier tout particulièrement l'équipe de Microsoft avec qui j'ai travaillé pendant ces 10 semaines. Merci pour leur accueil et merci d'avoir pris le temps de me former. J'en suis très reconnaissante.

BUT, Bachelor Universitaire de Technologie

Break Fix : Le terme "Break Fix" fait référence à un modèle de support technique où l'intervention est déclenchée par une panne ou un problème avec un système ou un équipement.

Cloud : Le cloud, ou "cloud computing" en anglais, désigne la fourniture de services informatiques (serveurs, stockage, bases de données, réseaux, logiciels, etc.) via Internet, souvent appelée "le nuage" en français. Au lieu de posséder des infrastructures informatiques physiques ou des centres de données, les entreprises et les particuliers peuvent louer ces ressources à des fournisseurs de cloud, comme Amazon Web Services (AWS), Microsoft Azure ou Google Cloud.

UPS, Uninterruptible power supply (Alimentation Sans Interruption)

LAN, Local Area Network (réseau local)

WAN, Wide Area Network (réseau étendu)

VPN, Virtual Private Network (réseau privé virtuel)

IoT, Internet of Things (l'Internet des objets)

CRM, Client Relationship Management (gestion de la relation client)

ERP, Enterprise Resource Planning (planification des ressources d'entreprise)

DBD, Data Bearing Device (dispositif porteur de données)

SSD, Solid-state Storage Device (disque de stockage à semi-conducteurs)

EPI, équipement de protection individuel

CPU, Central Processing Unit (unité centrale de traitement)

DIMM, Dual In-line Memory Module (module de mémoire à double rangée de broches)

RAM, Random Access Memory (mémoire à accès aléatoire)

NIC, Network Interface Card (Carte réseau)

HDD, Hard Disk Drive (Disque dur)

AOC, Active Optical Cable (Câble optique actif)

Blade : Une blade est une unité de traitement compacte qui s'insère dans un châssis de serveur spécifique. Chaque blade est un serveur autonome avec son propre processeur, sa mémoire, ses disques durs et ses interfaces réseau.

Fault Code : C'est le numéro de l'erreur, chaque problème sur les serveurs a un numéro précis par exemple, les câbles à remplacer ont tous le même fault code.

AS, Accepted Spare (Pièce de rechange acceptée)

FE, Functional Equivalent (Équivalent fonctionnel)

Boot : Le boot en informatique est le processus de démarrage d'un ordinateur, initié soit par un bouton matériel (comme le bouton d'alimentation), soit par une commande logicielle.

MoR, Middle of Row (Milieu de Rangée)

Bundle : un bundle signifie un paquet, un ensemble.

PDU, Power Distribute Unit (Unité de Distribution d'Énergie)

6 Sitographie

Fortinet [en ligne], [consulté le 5 juin 2024], adresse du site : [Qu'est-ce qu'un Datacenter ? Comment fonctionne un datacenter | Fortinet](#)

RedHat [en ligne], Mise à jour le 16 février 2024 [consulté le 7 juin 2024], adresse du site : <https://www.redhat.com/fr/topics/cloud-computing/public-cloud-vs-private-cloud-and-hybrid-cloud>