

Université de Gafsa
Institut Supérieur des Sciences Appliquées et de Technologie de GAFSA
Département d'automatiques des systèmes industriels



**Etude et mise en place d'une solution DCIM Open-Source
pour le centre des données du CERT**

Présenté et soutenu par :

Chahlaoui Aziz

En vue de l'obtention de

Licence Appliquée en Technologie de l'information et de la communication

Sous la Direction de :

M. Wajdi Saadaoui

Soutenu le 08/06/2023

Devant le jury composé de :

Président : **Mme. Wided AMARA**

Rapporteur : **M. Mounir TELLI**

Membres : **M. Wajdi SAADAOUI**

2022/2023

Dédicace

Je souhaite dédier ce travail à :

A mes parents, ELaich et Habiba

Pour leur amour inconditionnel, leurs sacrifices incessants et l'enseignement précieux qu'ils m'ont transmis. Leur dévouement éternel mérite toute ma reconnaissance.

Je souhaite également dédier ce travail

A mon frère Louay , pour son amour, son soutien et ces sacrifices.

Je n'oublie pas mes amies, Naim, Iskander, Khaled et Naoui, qui ont toujours été présentes, avec leur amour et leur soutien inconditionnels.

Enfin, je tiens à exprimer ma gratitude envers tous ceux qui m'ont soutenu par le passé et qui continuent de le faire aujourd'hui. J'aimerais également dédier cette reconnaissance aux membres du jury de soutenance, aux professeurs et à tous les employés de l'ISSAT qui ont contribué à mon parcours académique.

Remerciements

Je tiens à exprimer ma profonde gratitude et mes sincères remerciements à mon encadreur :

le Dr. Wajdi Saadaoui.

Je suis extrêmement reconnaissant envers lui pour avoir accepté de me superviser, pour le temps précieux qu'il m'a accordé et pour les conseils précieux qu'il m'a prodigués. Je voudrais également remercier mon encadreur au sein de la société,

M. Adel Hlilou

Pour ses directives précieuses et la qualité de ses suivis tout au long de la période de mon projet. Je suis très reconnaissant envers lui pour son soutien inestimable.

Table de matière

INTRODUCTION GENERALE	1
CHAPITRE 1 : GENERALITE	2
Introduction.....	3
I. Présentation de l'organisme d'accueil « le centre d'Études et de recherche des télécommunications »	3
I.1. Architecture de centre d'Étude et de recherche des télécommunications.....	3
I.2. Les services de centre d'Étude et de recherche des télécommunications [1]	4
I.3. Les Projets de cert.....	5
I.3.1.Principaux projets achieves	5
I.3.2. Pursuing ROadmaps and BEnchmarks for the Internet of Things (PORBE-IT)	5
I.3.3. Cadre de projet	6
I.4. Problématique	6
I.5. Cahier de charge	6
I.5.1. Objective de projet	6
I.5.2.Solution proposée	6
II. Généralité sur les Data-Centers	6
II.1. Définition d'un Data-Center	7
II.2. Avantages d'un Data-Center.....	7
II.3.Composants d'un Data-Center.....	7
II.3.1. Salle d'alimentations	7
a. UPS ou Onduleurs	7
b. Un transformateur électrique	8
c. Tableau de distributions.....	8
II.3.2. Salle d'informatique.....	9
a. Les Serveurs	9
b. Les Baies de stockage.....	11
c. Les Switches	12
II.3.3. Salle d'opération	12
II.3.4. Salle de réunion.....	13
II.4. Caractéristiques d'un Data-Center.....	13
II.4.1. Température et l'environnement.....	13
a. Les normes et spécifications.....	13

b. Les différents types de climatisation	14
c. Les différentes techniques de refroidissement.....	15
II.4.2. Alimentation électrique.....	18
a. Les tiers et niveau de classification	18
b. Disponibilité du data center.....	20
II.5. Topologie et redondance des Data-Center.....	20
II.5.1. Systèmes	22
III. Le Clouding	23
III.1. Modèles de déploiement du cloud computing.....	23
III.2. Les types de Cloud	23
a. Software as a services (SaaS)	23
b. Platform as a Service (PaaS).....	24
c. Infrastructure as a Service (IaaS).....	24
Conclusion	24
CHAPITRE 2 CONCEPTIONS	25
Introduction.....	26
I. Création de la Machine Virtuelle.....	26
I.1. Définition de Machine Virtuelle	26
I.2. Installation de VirtualBox.....	27
I.3. Téléchargement de l'image disque CentOS 7	27
I.4. Configuration de la machine virtuelle.....	28
I.4.1. Indiquer le nom et système d'exploitation	28
I.4.2. Configurer la quantité de RAM à allouer à la machine virtuelle	28
I.4.3. Création d'un disque dur.....	29
I.4.4. Stockage sur disque dur physique	31
II. Installation de CentOS 7.....	32
II.1. Définition de CentOS 7	32
II.2. Configuration les paramètres	32
II.2.1. Insertion Image ISO	32
II.2.2. Démarrer l'installation	33
II.2.3. Configurer le paramètre de localisation	34
II.2.4. Sélection de logiciels	34
II.2.5. Destination de l'installation	35
II.2.6. Nom de d'hôte et réseau	36

II.2.7. Mot de passe d'administrateur	37
II.2.8. Création d'utilisateur	37
II.2.9. Redémarrer le système	38
II.2.10. Licence information	39
III. Installation d'OpenDCIM.....	39
III.1. Installation Apache, PHP, MySQL	39
III.1.1. Installation Apache	39
III.1.2. Installation PHP	40
III.1.3. Installation serveur MySQL	41
III.1.4. Installation du module SSL d'Apache.....	42
III.2. Activer les services de serveur web	43
III.2.1. Activer et démarrer service Apache	43
III.2.2. Activer et démarrer le service de la base de données Maria DB	43
III.3. Ouvrir l'accès Web sur le pare-feu	44
III.4. Configurer le serveur MySQL.....	45
III.5. Créez une base de données pour openDCIM.....	46
III.6. Générez les clés nécessaires et copiez-les dans les répertoires appropriés	47
III.7. Créer un hôte virtuel.....	49
III.8. Téléchargez et installez openDCIM	50
III.8.1 Téléchargez la dernière version d'openDCIM sur opendcim.com	50
III.8.2. Extrader l'archive et créer un lien symbolique	51
III.8.3. Préparez le fichier de configuration pour accéder à la base de données	51
III.8.4. Redémarrer le service Apache	53
Conclusion	53
CHAPITRE 3	54
REALISATION	54
Introduction.....	55
I. Configuration les composant de data centre.....	55
I.1. Edition de Data centre.....	55
I.2. Edition des salles.....	56
I.3. Edition de travée	57
I.4. Edition de baies.....	58
I.4.1. Configuration des équipements	60
I.5. Configuration d'alimentation.....	66

II. Les rapports d'openDCIM.....	67
Conclusion	70
CONCLUSION GENERALE.....	71

Liste de figure

Figure 1: Architecture de CERT	4
Figure 2: Les salles d'un data center	7
Figure 3: UPS ou Onduleur.....	8
Figure 4: Les transformateurs HT/BT Green T.HE	8
Figure 5:Tableau de distributions	9
Figure 6: Serveurs au format tour	10
Figure 7: Serveurs au format tour	10
Figure 8: Serveurs lames encastrés dans un châssis	11
Figure 9: Baie de stockage	11
Figure 10: Eau glacée.....	14
Figure 11:Détente direct	15
Figure 12: Free Cooling	15
Figure 13: Down Flow Cooling	16
Figure 14: Hot Asile Containment.....	16
Figure 15: Cold Aisle Containment	17
Figure 16: In-Row Cooling	18
Figure 17: Tier1TIER 2	18
Figure 18:Tier2	19
Figure 19: Tier3	19
Figure 20:Tier4	20
Figure 21: Topologie et redondance des Data-Center	22
Figure 22: Représentation du Cloud	23
Figure 23: Image ISO.....	27
Figure 24: Nom et système d'exploitation	28
Figure 25 : Taille de la mémoire.....	29
Figure 26: Disque dur	30
Figure 27: Stockage sur disque dur physique	31
Figure 28: Emplacement du fichier et taille.....	32
Figure 29: Configuration de stockage et Insertion Image ISO	33
Figure 30: Installer Centos 7.....	33
Figure 31: Configuration de CentOS 7	34
Figure 32: Sèlection de logiciels "Serveur avec GUI"	35

Figure 33: Choix de participation	36
Figure 34: Configuration réseau et nom d'hôte	36
Figure 35: création de mot de passe.....	37
Figure 36: Création d'utilisateur	38
Figure 37: Redémarrer le système	38
Figure 38: Configuration initiale	39
Figure 39: Interface Principale d'openDCIM.....	55
Figure 40: Détail du centre de données	56
Figure 41: Infrastructure édition Salles d'informatique	57
Figure 42 : Infrastructure édition Travée	58
Figure 43: Infrastructure édition de baies	59
Figure 44: Inventaire des baies du centre de données	60
Figure 45: opérations du centre de données	61
Figure 46 : édition des modèles d'équipements	62
Figure 47: configuration des équipements	63
Figure 48: les connexions de réseau	66
Figure 49: configuration de tableau électrique	66
Figure 50: Rapport d'inventaire	68

Introduction générale

Ces vingt dernières années, le trafic réseau a connu une croissance exponentielle, avec des milliards de données transitant chaque jour. Des simples transferts de fichiers aux opérations bancaires complexes, nos activités quotidiennes sont de plus en plus dépendantes de ces échanges de données. Cette évolution des systèmes informatiques a généré une demande croissante en termes de stockage, convivialité, sécurité et simplicité dans le travail. Cependant, l'accès à d'importantes capacités de stockage et de calcul est souvent limité pour de nombreuses entreprises, en raison des contraintes matérielles et logicielles.

Afin de répondre à ces défis, de nombreuses entreprises choisissent de confier la gestion de leurs données, qu'il s'agisse du stockage, du traitement ou des protocoles de transfert, à un centre de données externe, également connu sous le nom de Data-Center. Cette approche permet de mutualiser les coûts et de bénéficier des dernières avancées technologiques en matière de gestion des données et des infrastructures.

Dans ce contexte, le projet vise à mettre en place une solution DCIM open-source pour le centre de données du CERT et pour mener à bien ce travail nous allons opter pour la démarche qui s'étale sur trois chapitres :

- Le premier chapitre a pour but l'évaluation des différentes solutions disponibles pour la gestion de centres de données et les fonctionnalités nécessaires (gestion des racks, du câblage, de la capacité, etc.)
- Le second chapitre est consacré à l'installation et configuration de la solution DCIM pour le Cas du CERT
- Dans dernières chapitre on va intégration avec les systèmes existants.
- On terminerons ce projet par une conclusion générale.

Chapitre 1 : Etat de l'art

Introduction

Pour contextualiser le sujet de manière adéquate, il est essentiel de commencer par présenter l'organisme d'accueil, le Centre d'Études et de Recherche des Télécommunications, et ensuite identifier le projet ainsi que les objectifs qu'il vise à atteindre.

I. Présentation de l'organisme d'accueil « le centre d'Études et de recherche des télécommunications »

Le CERT, ou Centre d'Études et de Recherche des Télécommunications, est un fournisseur de services sous la tutelle du Ministère des Technologies de l'information et de la Communication en Tunisie [1].

- ✓ Création : février 1991
- ✓ Forme juridique : Crée par la loi N° 88-145 du 31 décembre 1988
- ✓ Siège social : Parc Technologique EL GHAZALA ARIANA 2088 Tunisie
- ✓ Site web: <http://www.cert.tn>



Centre d'études et de recherches des télécommunications [1]

Les informations générales de notre entreprise d'accueil se présentent comme suit :

- ✓ Adresse : Parc Technologique EL GHAZALA ARIANA 2088 Tunisie
- ✓ Téléphone : (+216) 70 835 000
- ✓ Fax: (+216) 70 835 835

I.1. Architecture de centre d'Étude et de recherche des télécommunications

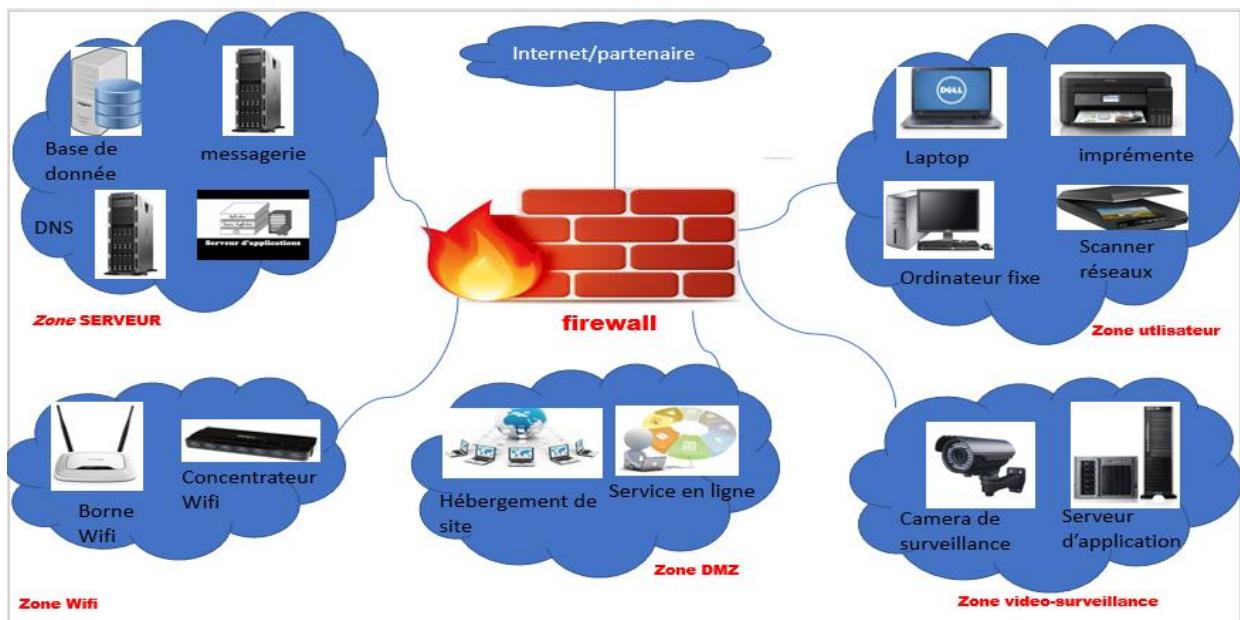


Figure 1: Architecture de CERT

I.2. Les services de centre d'Étude et de recherche des télécommunications [1]

Le rôle principal du CERT consiste à répondre aux besoins du secteur des communications en offrant un support efficace pour des études spécifiques, une assistance pour les maîtres d'ouvrage, une expertise technique, des services de veille technologique, de recherche et développement et une formation spécialisée.

Les activités du CERT s'articulent autour des principaux axes suivants :

- ✓ **Les études spécifiques** Le CERT est impliqué dans le développement des réseaux de télécommunications et de télédiffusion, en fournissant des services tels que l'ingénierie et la planification des réseaux et des services, l'établissement des cahiers des charges, les études technico-économiques, l'élaboration des schémas directeurs, ainsi que l'étude et le pilotage des projets stratégiques [1].
- ✓ **L'expertise, l'audit, l'assistance et le conseil technique** Le CERT intervient également dans le domaine des technologies de l'information en offrant des services tels que l'optimisation et le redimensionnement des réseaux (mobiles, fixes, informatiques), l'analyse des performances et l'évaluation de la qualité de service, ainsi que la sécurisation des réseaux informatiques [1].
- ✓ **L'homologation des terminaux de télécommunications** Le but de cette activité est de garantir la conformité des équipements à connecter aux réseaux nationaux de

télécommunications avec les exigences réglementaires et les normes nationales en vigueur.

[1]

- ✓ **Le contrôle et l'acceptance** L'activité consiste à vérifier la conformité des équipements et des nouvelles installations liées aux réseaux de télécommunications. Dans le cadre de projets d'installation, de mise à niveau ou d'extension d'une infrastructure de télécommunications ou d'un système d'information, le CERT vérifie la conformité des travaux par rapport aux cahiers des charges, aux réglementations et aux normes en vigueur, assurant ainsi la qualité des équipements et la conformité des prestations de services. Le CERT intervient dans l'acceptation technique des systèmes et équipements de commutation, de transmission et d'accès, des réseaux fixes et mobiles, publics et privés, ainsi que des équipements d'environnement et d'énergie pour différentes technologies et générations. [1]
- ✓ Le CERT fournit ses prestations pour le compte des opérateurs des télécommunications, des régulateurs des postes et des télécommunications, et aussi pour le compte de divers autres clients (ministères, entreprises privées...) [1]

I.3. Les Projets de cert

I.3.1.Principaux projets achieves

Parmi les projets de recherche réalisés par les ingénieurs chercheurs du CERT :

- ✓ Ingénierie des Réseaux de Nouvelle Génération (IRNG)
- ✓ Ingénierie des réseaux Wimax mobiles
- ✓ Modélisation et Compensation des Perturbations Électromagnétiques sur les Lignes ADSL
- ✓ Représentation, Analyse et Communication d'Images Numériques (RACINES)
- ✓ Ingénierie des Réseaux Cellulaires de 3ème Génération (IRC3G) ... [1]

I.3.2. Pursuing ROadmaps and BEncmarks for the Internet of Things (PORBE-IT)

PORBE-IT est un projet européen de deux années qui vise à soutenir l'exploitation des avancées de la recherche européenne dans les déploiements de l'Internet des Objets. Il est en effet nécessaire pour assurer l'interopérabilité et l'acceptation de solutions de l'Internet des Objets validés dans un contexte global d'éviter les compétitions et les chevauchements inutiles. Pour cela, PROBE-IT se concentre sur l'analyse des déploiements existants ou en cours à travers le monde et dans différentes perspectives et vise combler les besoins des décideurs, des chargés du déploiement, des fournisseurs et des utilisateurs de technologies.[1]

I.3.3. Cadre de projet

Dans le cadre de la réalisation du projet de fin d'étude pour l'obtention de la License fondamentale en Technologie de l'information et des communications à l'Institut Supérieur des Sciences Appliquées et Technologie de Gafsa, j'ai effectué un stage de fin d'études au sein de le centre d'études et de recherches des télécommunications

I.4. Problématique

Lors de l'étude qui j'ai fait, j'ai relevé les problèmes suivants :

- Un taux de temps gaspillé lors du diagnostic des pannes ce qui influe sur la qualité du service
- Plus le nombre des équipements et des services augmente plus les tâches de convenablement
- Vu l'absence d'un outil de supervision, l'administrateur n'est pas alerté en cas de problèmes de fonctionnements anormaux

I.5. Cahier de charge

I.5.1. Objectif de projet

Le but principal du projet consiste à installer une solution open-source DCIM pour le centre de données du CERT

I.5.2. Solution proposée

Le processus implique plusieurs étapes, notamment l'évaluation des diverses options disponibles pour la gestion des centres de données. Une évaluation des fonctionnalités essentielles pour le centre de données, telles que la gestion des racks, du câblage, de la capacité, etc., sera également effectuée. Ensuite, la solution DCIM appropriée sera installée et configurée pour répondre aux besoins spécifiques du CERT. Enfin, la solution DCIM sera intégrée aux systèmes existants pour assurer une transition fluide.

II. Généralité sur les *Data-Centers*

Les Data-Centers occupent une place centrale dans le système d'information en hébergeant et en traitant les données informatiques. Généralement, ces centres sont multiples et répartis sur plusieurs sites pour assurer une meilleure disponibilité et une sécurité accrue des données. Ils sont aménagés et sécurisés pour offrir un espace protégé et dédié à l'hébergement, au traitement et à la protection des données.

II.1. Définition d'un Data-Center

Le Data-Center, également appelé centre de données, est un lieu où les données sont stockées et traitées. Il est constitué de trois éléments principaux, à savoir le centre de calcul (contenant les serveurs), le centre de stockage (avec les baies de stockage) et le centre de transport (incluant les réseaux).

II.2. Avantages d'un Data-Center

Les Data-Centers sont hautement sécurisés pour garantir la protection des données stockées contre divers risques tels que les incendies, les inondations, les vols, les intrusions, les pannes et les coupures électriques. De plus, les données sont dupliquées pour prévenir les pertes de données en cas de problèmes majeurs.

II.3. Composants d'un Data-Center

Un Data-Center est constitué de trois modules distincts, et chaque module est à son tour composé de plusieurs équipements.[2]

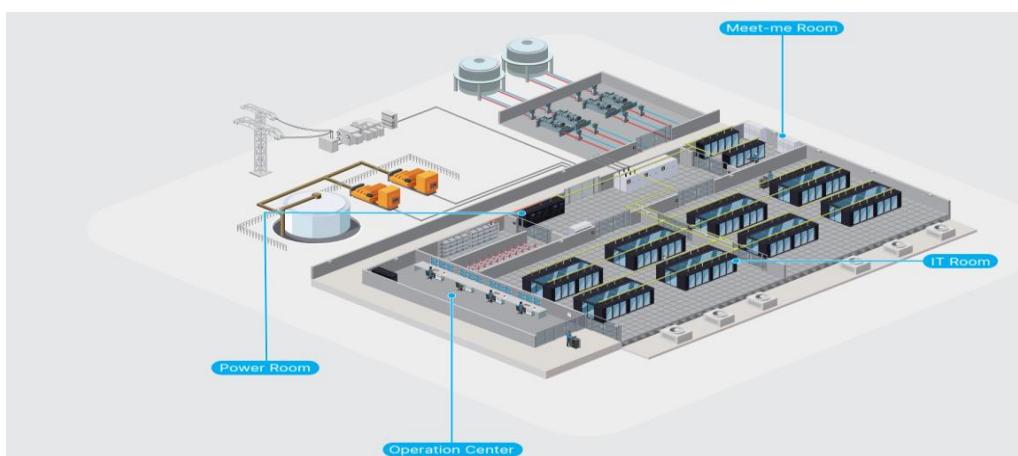


Figure 2: Les salles d'un data center

II.3.1. Salle d'alimentations

Une salle d'alimentation (ou salle électrique) est l'espace dédié à la distribution de l'alimentation électrique nécessaire pour alimenter tous les équipements du centre de données. La salle d'alimentation est composé par plusieurs équipements qui assurer le fonctionnement de data center[2]

a. UPS ou Onduleurs

Un onduleur (ou UPS pour Uninterruptible Power Supply) est un équipement essentiel dans un centre de données. Il fournit une alimentation électrique de secours en cas de panne de courant ou de baisse de tension pour garantir une disponibilité continue des équipements du

centre de données



Figure 3: UPS ou Onduleur.

b. Un transformateur électrique

Un transformateur électrique est un équipement qui permet de modifier la tension de l'alimentation électrique reçue du réseau électrique public afin de la rendre compatible avec les besoins des équipements du centre de données.[2]



Figure 4: Les transformateurs HT/BT Green T.HE

(pour High Tension/Low Tension Green Transformer with High Efficiency)

c. Tableau de distributions

Le tableau de distribution est un élément important de l'infrastructure électrique d'un centre de données.

Il s'agit d'un panneau de contrôle qui distribue l'alimentation électrique à partir des sources d'alimentation électrique, comme les transformateurs, les batteries et les groupes électrogènes, vers les équipements et les systèmes du Data-Center



Figure 5:Tableau de distributions

II.3.2. Salle d'informatique

Une salle d'informatique (également appelée IT room) dans un centre de données est un espace dédié à l'installation et au fonctionnement des équipements informatiques et de télécommunication tels que les serveurs, les équipements de stockage, les équipements de réseau et les systèmes de climatisation

a. Les Serveurs

Un Data-Center se compose d'un ensemble de serveurs qui exécutent différents systèmes d'exploitation tels que Windows, Linux, Oracle, etc. Ce sont des dispositifs matériels informatiques qui fournissent des services de calcul de données. Les nouveaux serveurs peuvent contenir jusqu'à 4 processeurs de 15 cœurs chacun et 6 Téra Octets de RAM.

Il existe trois formats de serveurs : les serveurs tour, les serveurs rack et les serveurs blade (en lame).

- **Serveurs tour**

Les serveurs de type tour ressemblent beaucoup à l'unité centrale d'un ordinateur de bureau, et conviennent particulièrement aux petites entreprises car ils peuvent être installés facilement dans n'importe quelle pièce et ne nécessitent pas un niveau de maintenance très élevé. Ces serveurs peuvent accueillir jusqu'à six disques durs et deux processeurs.[2]



Figure 6: Serveurs au format tour

- **Serveurs Rack**

Les serveurs au format rack sont conçus pour être installés dans des armoires, contrairement aux serveurs en tour qui ressemblent à des unités centrales d'ordinateurs de bureau. Ils sont dotés d'une carte mère puissante et de quatre processeurs, et sont utilisés dans les entreprises de taille moyenne ou grande qui nécessitent plus de capacités de traitement. Ces serveurs sont souvent utilisés pour exécuter des systèmes d'exploitation ou des applications qui ne peuvent pas être virtualisés.



Figure 7: Serveurs au format tour

- **Serveurs blade (en lames)**

Les serveurs lames, contrairement aux serveurs tour et rack, ne peuvent pas fonctionner seuls car plusieurs composants sont partagés avec d'autres serveurs lames qui peuvent être encastrés dans un châssis.

Ce dernier fournit l'alimentation électrique et les connexions réseau nécessaires, et les châssis sont regroupés dans des armoires comme les racks.

Ce type de serveur présente plusieurs avantages, notamment une puissance équivalente à moindre coût que les serveurs classiques, car ils ne possèdent pas d'alimentation ni de connexion réseau. De plus, ils permettent un temps de mise en marche plus rapide car ils ne nécessitent pas de câblage comme les racks, et ils permettent l'augmentation de la puissance du système sans provoquer son arrêt. [2]



Figure 8: Serveurs lames encastrés dans un châssis

b. Les Baies de stockage

Les baies de stockage (disk arrays), leur activité principale est le stockage de données, sont utilisées pour dénommer un boîtier informatique contenant des emplacements pour accueillir des disques dur. Elles sont composées de :

- Disques qui sont chargés d'emmagasiner les données,
- Un bus qui permet d'interconnecter l'ensemble des éléments de la baie, toutes les données circulent via ce dernier,
- Un ou plusieurs contrôleurs de disques,
- Un processeur qui représente l'unité de calcul qui traitera toutes les informations.

Les baies de stockage peuvent être vues comme des serveurs spécialisés dont la fonction principale est d'offrir des espaces de stockage sécurisés.



Figure 9: Baie de stockage

c. Les Switches

Il existe plusieurs types de switches qui peuvent être utilisés dans une baie de data center, selon les besoins spécifiques de l'infrastructure de réseau et les exigences de performances :

1. Switches d'accès : Ce sont les switches les plus courants utilisés dans les baies de data center. Ils sont conçus pour connecter les serveurs et les périphériques de stockage à haute vitesse dans la baie de données. Ils peuvent offrir des fonctionnalités telles que la qualité de service (QoS), la virtualisation de réseau et le contrôle de la bande passante pour garantir des performances optimales.
2. Switches de distribution : Ces switches sont utilisés pour connecter plusieurs switches d'accès dans une baie de données, afin de créer un réseau de niveau supérieur. Les switches de distribution sont conçus pour gérer le trafic à haut débit et pour fournir des fonctions de sécurité telles que l'authentification, l'autorisation et la comptabilité (AAC).
3. Switches de cœur : Ces switches sont utilisés pour connecter les switches de distribution et fournir une connectivité à haute vitesse pour les charges de travail les plus critiques du data center. Les switches de cœur sont conçus pour fournir des performances et une disponibilité maximales, ainsi que des fonctionnalités de redondance pour garantir la continuité des opérations.
4. Switches de stockage : Ces switches sont spécialement conçus pour connecter les systèmes de stockage SAN (Storage Area Network) et fournir des performances élevées, une faible latence et une haute disponibilité pour les données stockées dans le data center.

II.3.3. Salle d'opération

La salle d'opération (operation room) est une pièce qui abrite les équipements de gestion, de surveillance et de maintenance de l'infrastructure informatique. Elle est généralement considérée comme le cœur du data center car elle héberge les serveurs, les systèmes de stockage, les équipements réseau, les commutateurs, les routeurs et les autres composants critiques qui assurent le fonctionnement continu de l'ensemble du centre de données.

La salle d'opération (operation room) est une pièce qui abrite les équipements de gestion, de surveillance et de maintenance de l'infrastructure informatique. Elle est généralement considérée comme le cœur du data center car elle héberge les serveurs, les systèmes de stockage, les équipements réseau, les commutateurs, les routeurs et les autres composants critiques qui assurent le fonctionnement continu de l'ensemble du centre de données.

II.3.4. Salle de réunion

Une salle de rencontre (Meet-Me Room) dans un data centre est un espace physique neutre où les fournisseurs de services de télécommunications, les opérateurs de réseau et les clients peuvent se connecter les uns aux autres afin d'échanger des données. Cette salle est souvent située au centre du data centre et permet aux différents opérateurs de se connecter à des câbles de fibres optiques, des routeurs, des commutateurs et d'autres équipements de réseau pour faciliter les échanges de données entre eux.

La salle de rencontre est conçue pour être un espace neutre et indépendant où les clients peuvent se connecter à différents fournisseurs de services de télécommunications sans être liés à un fournisseur spécifique. Cela permet aux clients de choisir parmi une variété de fournisseurs pour trouver celui qui offre les meilleures performances et les tarifs les plus avantageux.

II.4. Caractéristiques d'un *Data-Center*

II.4.1. Température et l'environnement

Afin d'assurer le bon fonctionnement des équipements informatiques, il est important de contrôler la température, car ces derniers génèrent une grande quantité de chaleur et risquent de dysfonctionner si elle dépasse un certain seuil. Pour éviter la surchauffe, la climatisation est essentielle et doit maintenir une température proche de 20°C. Dans les villes les plus chaudes, il est possible d'utiliser un refroidissement à eau directement, ce qui est plus efficace que la climatisation classique. En revanche, dans les villes où la température moyenne est proche de 20°C, un système de récupération de l'air froid extérieur peut être utilisé.[3]

a. Les normes et spécifications

- Class 1: Salle informatique.
- Class 2: Bureaux.
- Class 3: Domicile.
- Class 4: Extérieur. Industrie

Table 1 :Les normes et spécifications

	Température		Humidité	
	Autorisée	Recommandée	Autorisée	Recommandée
Classe 1	15 – 32°	20 – 25°	20 – 80%	35 – 55%
Classe 2	10 – 35°	20 – 25°	20 – 80%	35 – 55%
Classe 3	5 - 35°	NA	8 – 80%	NA
Classe 4	5 – 40°	NA	8 – 80%	NA

b. Les différents types de climatisation

- Eau glacée

L'eau glacée est un moyen communément utilisé pour refroidir les data centers. Elle est généralement produite par des groupes frigorifiques à l'extérieur du data center, puis transportée à l'intérieur du data center via des tuyaux isolés.

Le processus de refroidissement par eau glacée fonctionne en utilisant un fluide réfrigérant qui absorbe la chaleur de l'air chaud à l'intérieur du data center et transporte cette chaleur vers l'extérieur. L'eau glacée est ensuite utilisée pour refroidir le fluide réfrigérant, avant qu'il ne soit réinjecté dans le data center pour continuer à absorber la chaleur.[3]



Figure 10: Eau glacée

- Détente direct

La détente directe est une méthode de climatisation qui est utilisée dans certains types de systèmes de climatisation de data center. Dans ce type de système, l'air est refroidi directement à partir de l'unité de traitement de l'air (UTA) en utilisant des serpentins de refroidissement.

Dans un système de climatisation à détente directe, le fluide réfrigérant est pompé directement

à travers les serpentins de refroidissement de l'UTA, où il absorbe la chaleur de l'air ambiant. L'air froid est ensuite soufflé dans la pièce pour maintenir une température optimale.[3]

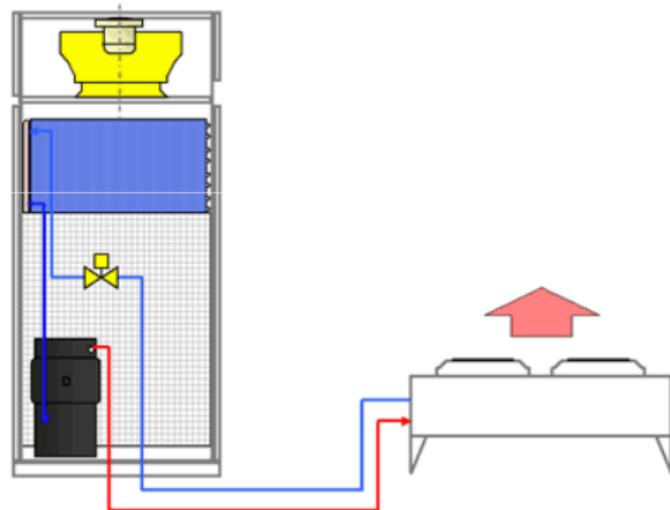


Figure 11:Détente direct

- Refroidissement gratuit (Free Cooling)

Le free cooling, également connu sous le nom de refroidissement gratuit, est une méthode de refroidissement pour les data centers qui utilise l'air extérieur pour refroidir les équipements informatiques sans avoir besoin d'utiliser un système de climatisation mécanique.

Lorsque les conditions météorologiques sont favorables, c'est-à-dire lorsque la température extérieure est plus basse que la température intérieure souhaitée du data center, le free cooling peut être utilisé pour réduire la consommation d'énergie en éliminant la nécessité d'utiliser un système de climatisation mécanique. [3]

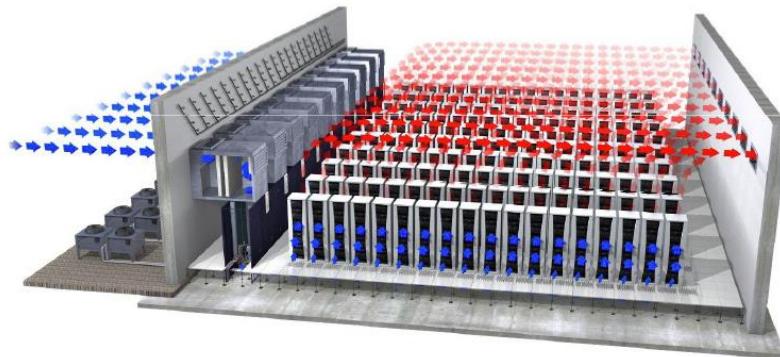


Figure 12: Free Cooling

c. Les différentes techniques de refroidissement

- Down Flow Cooling

Le Down Flow Cooling est une technique de refroidissement utilisée dans les data centers pour améliorer l'efficacité énergétique en fournissant de l'air frais directement aux

équipements informatiques. Dans cette configuration, les unités de refroidissement sont situées sur le toit du data center et l'air froid est acheminé vers les équipements à travers des grilles ou des diffuseurs situés au plafond.

Lorsque l'air frais est envoyé directement sur les équipements informatiques, il permet de maintenir une température constante et uniforme dans le data center, ce qui peut réduire la consommation d'énergie nécessaire pour refroidir les équipements. Cette technique est particulièrement utile pour les data centers qui hébergent des équipements à haute densité de puissance, tels que les serveurs de calcul haute performance. [3]

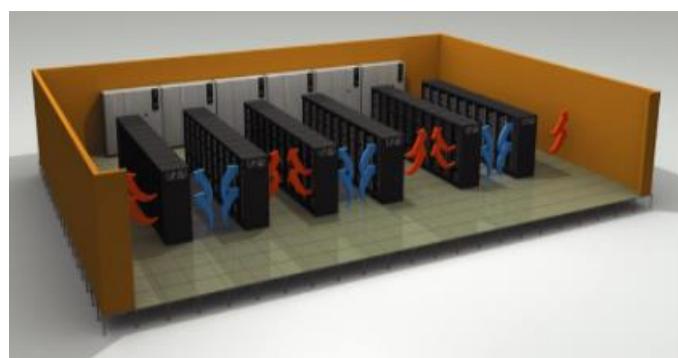


Figure 13: Down Flow Cooling

- Hot Aisle Containment

Hot aisle containment est une méthode de refroidissement des centres de données qui consiste à contenir l'air chaud généré par les équipements informatiques à l'intérieur des racks de serveurs du centre de données. Cela est réalisé en enclosant l'allée où les ventilateurs d'évacuation des serveurs expulsent l'air chaud, généralement avec un plafond ou une canalisation, pour créer une allée chaude séparée.

L'idée derrière le hot aisle containment est d'améliorer l'efficacité énergétique en réduisant la quantité d'air chaud se mélangeant avec l'air froid. Cela réduit la charge de travail sur le système de refroidissement, permettant ainsi un fonctionnement plus efficace et une réduction de la consommation énergétique.[3]

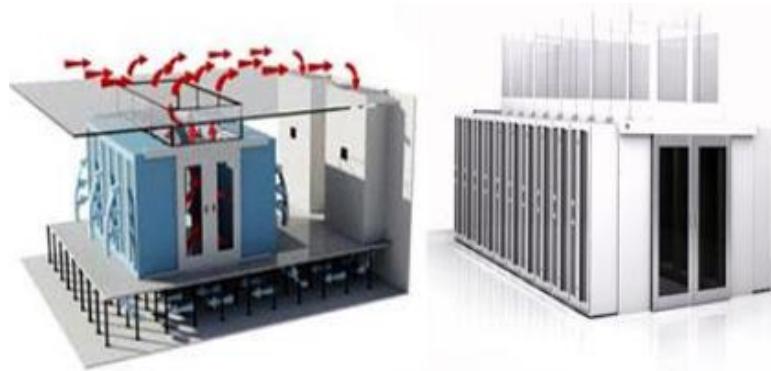


Figure 14: Hot Asile Containment

- Cold Aisle Containment

Cold aisle containment (CAC) est une méthode de refroidissement pour les centres de données qui consiste à confiner l'air frais dans l'allée froide du centre de données où les serveurs prennent leur air d'admission. L'objectif est de séparer l'air frais de l'air chaud pour améliorer l'efficacité du refroidissement et réduire la consommation d'énergie.

Dans un système de Cold Aisle Containment, les allées froides sont fermées avec des portes, des plaques de toit, ou des panneaux de confinement pour créer un environnement hermétique. L'air frais est fourni à l'intérieur de l'allée froide et est aspiré par les serveurs, qui expulsent ensuite l'air chaud dans l'allée chaude opposée. Le flux d'air est contrôlé et optimisé pour minimiser le mélange d'air chaud et froid, réduisant ainsi la consommation d'énergie pour refroidir les équipements du centre de données.[3]

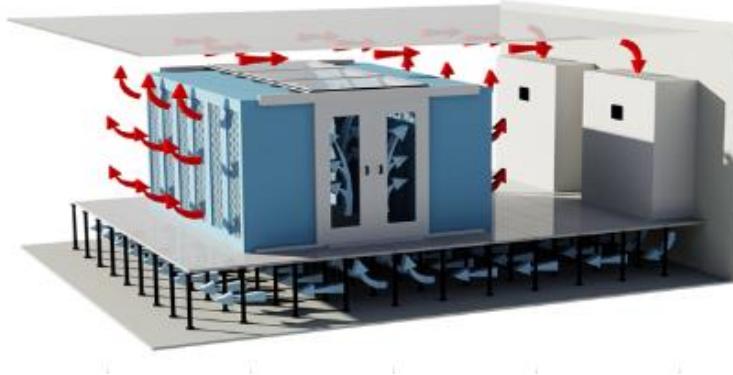


Figure 15: Cold Aisle Containment

- Caractéristiques d'un Data-Center

L'In-Row Cooling (ou HAC/CAC) est une technologie de refroidissement utilisée dans les centres de données pour maintenir une température optimale pour les équipements informatiques. Cette technologie implique l'installation de refroidisseurs directement dans les rangées de racks de serveurs.

Le HAC (ou Hot Aisle Containment) est une méthode de refroidissement qui sépare les allées chaudes et froides du centre de données. Les équipements informatiques libèrent de la chaleur dans l'allée chaude, tandis que l'allée froide est utilisée pour introduire de l'air frais. Cette méthode permet de minimiser la quantité d'air chaud qui est réintroduit dans le système de refroidissement, ce qui réduit la consommation d'énergie nécessaire pour maintenir une température stable.

Le CAC (ou Cold Aisle Containment) est une méthode similaire, mais qui utilise des équipements de refroidissement pour maintenir une température stable dans l'allée froide.

Cette méthode est plus efficace dans les environnements où la température ambiante est élevée.[3]



Figure 16: In-Row Cooling

II.4.2. Alimentation électrique

a. Les tiers et niveau de classification

- TIER 1

Tous les équipements sont alimentés directement par le réseau STEG, aucune protection n'est prévue en cas de coupure ou de perturbation du réseau

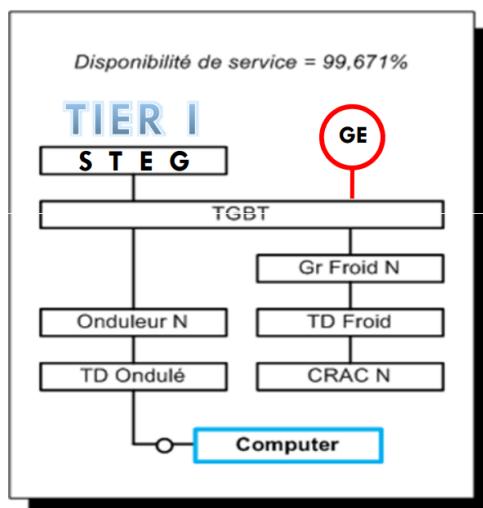


Figure 17: Tier1

Les équipements sont protégés par onduleur (non redondant), les batteries assurent la continuité en cas de coupure du réseau STEG, typiquement 5 à 15 mn

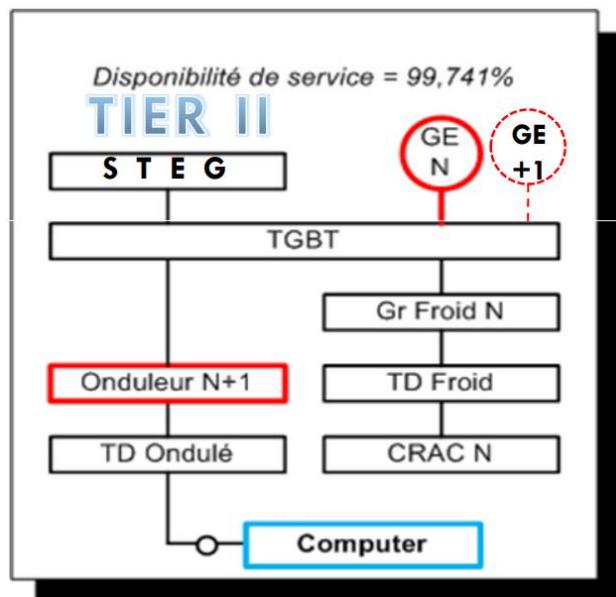


Figure 18:Tier2

- **TIER 3**

la redondance des infrastructures électriques et climatisation est prévue sur un principe 7 N+1, en cas de coupure du réseau STEG l'alimentation est assurée par les groupes électrogènes

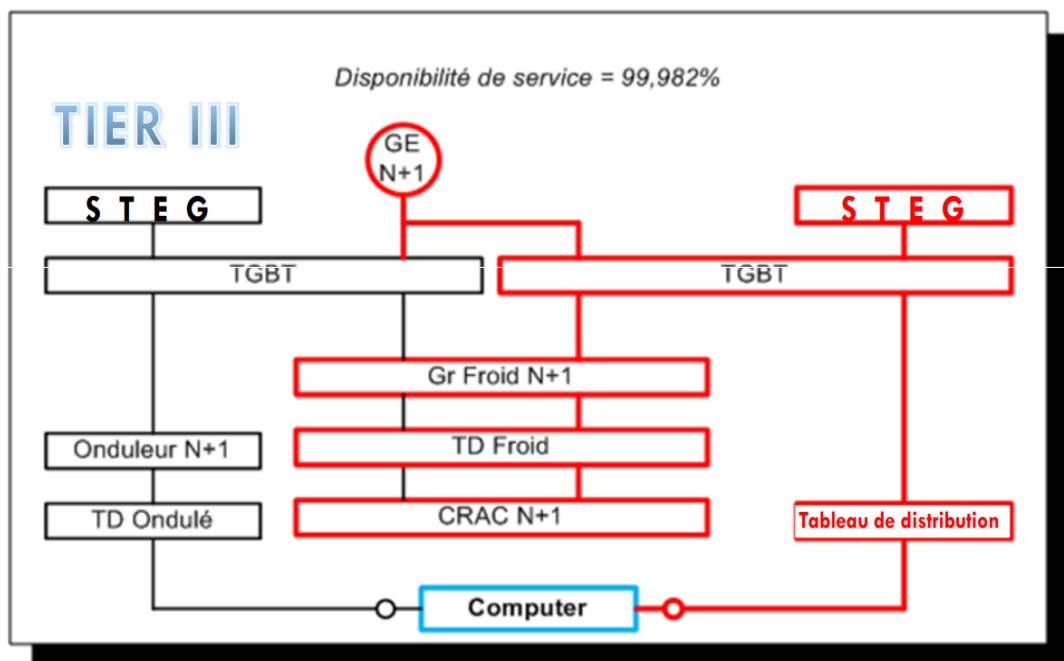


Figure 19: Tier3

- **TIER 4**

la redondance des infrastructures électriques et climatisation est assurée sur un principe 2N, les points uniques de défaillance sont supprimés.

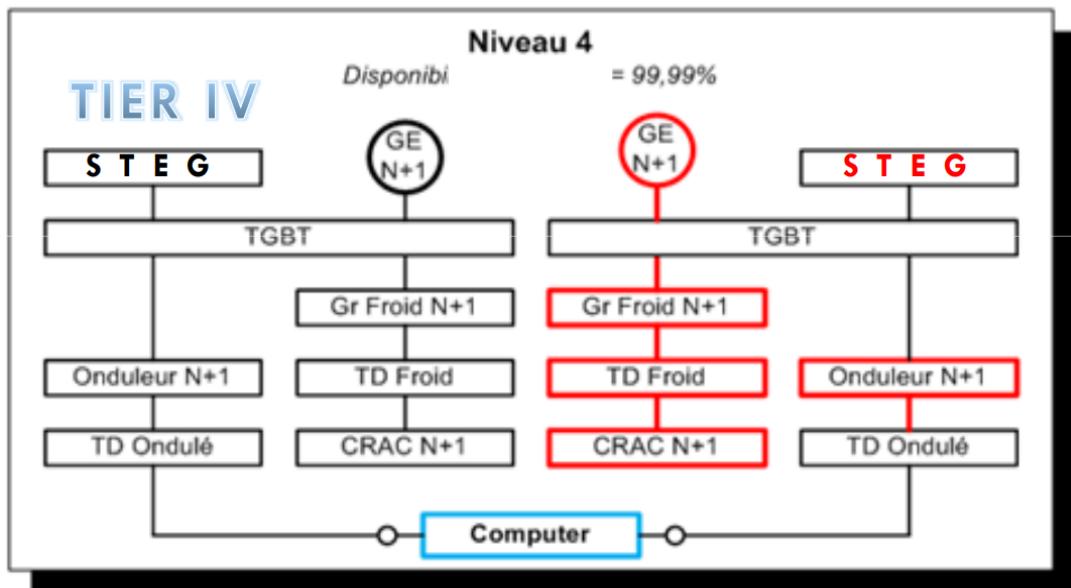


Figure 20: Tier4

b. Disponibilité du data center

Table 2 : Disponibilité du data centre

OBJECTIFS	TIER I	TIER II	TIER III	TIER IV
Maintenance Arrêt site	Oui	Oui	Non	Non
Panne d'un élément unique peut entraîner l'arrêt complet du centre	Oui	Oui	Oui	Non
Temps de coupure annuel du site	28.8 hrs	22 hrs	1.6 hrs	0.8 hrs
Disponibilité du site	99.67%	99.75%	99.98%	99.99%
ELEMENTS STRUCTURANTS				
Source alimentation électrique et refroidissement	Système	Système	Système	Système + système
Nombre de voies d'alimentation	1 unique	1 unique	1 Active 1 Passive	2 actives
Composants de système redondants (N= besoin)	N	N	N+1	2 N

Le tableau fournit une comparaison des différents niveaux de maintenance et de disponibilité des centres de données, classés en quatre niveaux : Tier I, Tier II, Tier III et Tier IV. Ces niveaux sont utilisés pour évaluer la fiabilité et la résilience des centres de données en fonction de leurs capacités de maintien en activité et de leur tolérance aux pannes.

Au niveau Tier I, la maintenance nécessite un arrêt complet du site, ce qui signifie que toutes les opérations doivent être interrompues pour effectuer des travaux de maintenance. De plus, une panne

d'un élément unique peut entraîner l'arrêt complet du centre de données. La disponibilité du site est de 99,67%, ce qui équivaut à environ 28,8 heures de temps de coupure annuel.

Le niveau Tier II présente une amélioration par rapport au Tier I en termes de maintenance. Bien qu'un arrêt complet du site soit encore nécessaire, la panne d'un élément unique ne provoque pas l'arrêt complet du centre de données. La disponibilité du site est légèrement supérieure, atteignant 99,75%, avec un temps de coupure annuel réduit à environ 22 heures.

Au niveau Tier III, des améliorations significatives sont apportées en termes de maintenance et de disponibilité. La maintenance n'implique plus un arrêt complet du site, ce qui permet d'effectuer des travaux de maintenance sans interruption des opérations. De plus, une panne d'un élément unique n'entraîne pas l'arrêt complet du centre de données. La disponibilité du site atteint 99,98%, avec un temps de coupure annuel réduit à seulement 1,6 heure.

Le niveau Tier IV représente le niveau de fiabilité et de résilience le plus élevé. La maintenance est effectuée sans arrêt du site, permettant une continuité des opérations même pendant les travaux de maintenance. De plus, le centre de données est conçu pour résister à la panne d'un élément unique grâce à des systèmes redondants. La disponibilité du site atteint 99,99%, avec un temps de coupure annuel extrêmement faible de seulement 0,8 heure.

II.5. Topologie et redondance des Data-Center

La redondance fait référence à la duplication de composants critiques, tels que les alimentations électriques, les unités de refroidissement, les connexions réseau et les serveurs, afin d'assurer la continuité des opérations en cas de défaillance d'un composant. En d'autres termes, la redondance vise à garantir que si un composant important tombe en panne, un autre composant peut prendre sa place et continuer à assurer le fonctionnement normal de la salle de télécommunications. Les différentes stratégies de redondance comprennent la redondance N+1, la redondance 2N et la redondance 2N+1.

Le tier, quant à lui, est une norme de classification définie par l'Uptime Institute qui définit les niveaux de disponibilité et de redondance pour les data centers. Le tier peut aller de tier 1 (bas niveau de disponibilité et de redondance) à tier 4 (le plus haut niveau de disponibilité et de redondance). Les niveaux de disponibilité et de redondance sont définis en fonction des composants critiques tels que l'alimentation électrique, le refroidissement, le réseau et le stockage, ainsi que de la tolérance aux pannes. [4]

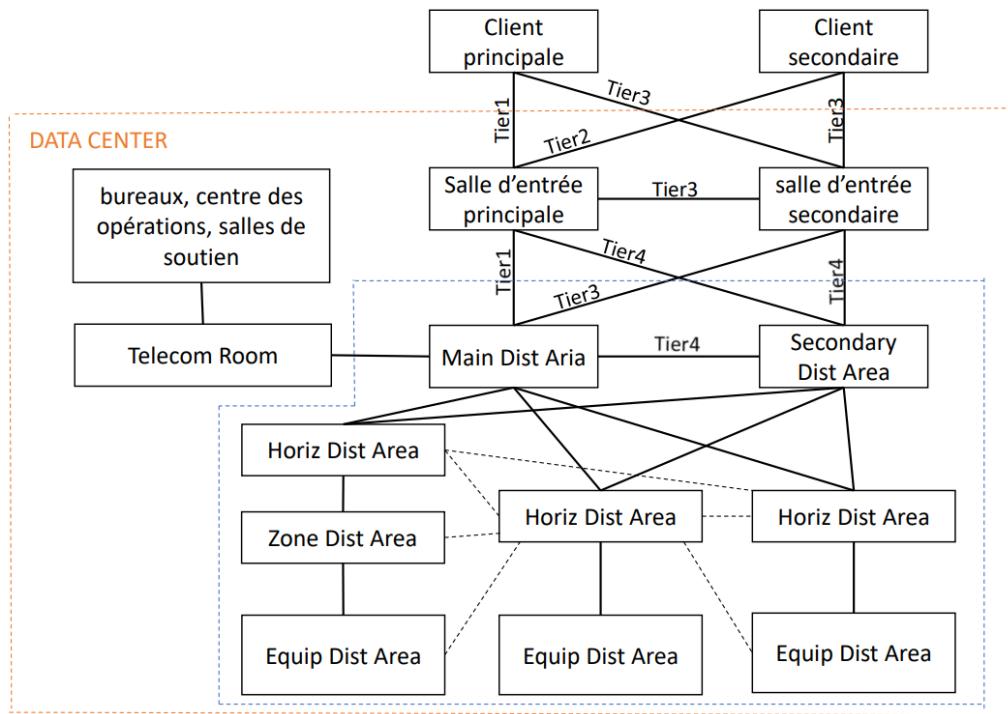


Figure 21: Topologie et redondance des Data-Center

II.5.1. Systèmes

Dans les *Data-Center* nous avons recours à plusieurs systèmes d'exploitation tel que Windows, Linux, Oracle..., ceci représente un inconvénient pour ces derniers, car chaque système d'exploitation requiert des serveurs avec des caractéristiques particulières, mais grâce à la virtualisation nous pouvons émuler la plate-forme spécifique pour chaque système.

Pour produire un service de qualité, les *Data-Centers* doivent respecter quelques mesures de sécurité essentielles, parce qu'il y a plusieurs types de menaces qui peuvent les toucher, l'une d'entre elles est d'ordre physique cette dernière se compose de quatre facteurs : menaces sur les matériels, menaces environnementales, menaces électriques et de maintenances.

- Un contrôle régulier voire constant de l'environnement doit être fait.
- La surveillance de la climatisation est essentielle au bon fonctionnement du matériel électrique.
- Un système d'alimentation d'urgence (groupe électrogène, Un générateur électrique ...) est nécessaire en cas de panne.
- Dans le but de prévenir une perte d'alimentation électrique, tous le matériel électrique (Serveur, routeurs...) doit posséder une double alimentation indépendante à l'intérieur du centre.
- La sécurité contre les incendies grâce à des systèmes de détection d'incendie par

l'analyse de particules (**VESDA** pour Very Early Smoke Detection Alarm) et des systèmes d'extinction d'incendie par gaz (l'azote, l'argonite...).

- La sécurité de l'accès physique est importante au sein de ces centres grâce à un contrôle d'accès (badge, carte magnétique, éventuellement biométrie) et un système de vidéo-surveillance relié à un service permanent de gardiennage pour éviter toute intrusion ou pour agir rapidement en cas de problèmes majeurs.
- Les données doivent être dupliquées afin de prévenir les risques de perte en cas de gros problèmes

III. Le Clouding

Il s'agit de déporter toutes les opérations effectuées sur un ordinateur, telles que le calcul et le stockage, sur des serveurs informatiques distants et pouvoir y accéder par l'intermédiaire d'un réseau qui est généralement internet. Ces serveurs sont loués à la demande, cette infrastructure constitue le *Cloud* (le nuage). [5]



Figure 22: Représentation du Cloud

III.1. Modèles de déploiement du cloud computing

Il existe trois formes de déploiement du Cloud :

- **Le Cloud privé** : c'est un Cloud qui permet de délivrer des services uniquement au sein d'une entreprise.
- **Le Cloud publique** : c'est un Cloud appartenant aux prestataires qui louent leurs services à de nombreuses entreprises et au public.
- **Le Cloud hybride** : c'est une composition des deux types précédents amené à utiliser les ressources du cloud public par le cloud privé.

III.2. Les types de Cloud

a. Software as a services (SaaS)

Le modèle **SaaS** met à la disposition du client des applications sous forme de services, la maintenance de ces applications est gérée par le fournisseur. Plus d'installation, plus de mise à jour à gérer. Ce qui signifie pour l'entreprise client une réduction du budget informatique avec le même niveau de service ou plus. [5]

b. Platform as a Service (PaaS)

Grâce à ce service les entreprises n'ont pas besoin de gérer l'infrastructure (le matériel et les systèmes d'exploitation), elles peuvent juste se concentrer sur le déploiement et la gestion de leurs applications métiers. [5]

c. Infrastructure as a Service (IaaS)

Dans le modèle **IaaS**, c'est la location d'une infrastructure informatique complète chez le provider, c'est au département informatique de l'entreprise de faire toutes les installations systèmes et la configuration des applications métiers.[5]

Conclusion

A travers ce chapitre nous avons vu ce qu'est un *Data-Center*, ses composants, ses caractéristiques, les différentes architectures qui existent, ainsi son développement, puis nous avons présenté le Cloud.

.

CHAPITRE 2 : Conception , Considérations et mise en œuvre

Introduction

OpenDCIM est un outil open source de gestion de centre de données. Il permet de gérer les équipements informatiques, les connexions réseaux, les alimentations électriques et les unités de refroidissement dans un centre de données. OpenDCIM peut également fournir des rapports détaillés sur l'état et l'utilisation des équipements ainsi que des fonctionnalités pour la planification de l'espace, la gestion des câbles et la gestion des alertes. OpenDCIM est écrit en PHP et utilise une base de données MySQL.

Avant d'installer OpenDCIM, vous devez vous assurer que votre système répond aux prérequis suivants :

- Système d'exploitation : OpenDCIM peut être installé sur un système d'exploitation basé sur Linux ou Unix. Dans ce chapitre, nous allons utiliser CentOS 7.
- Serveur web : OpenDCIM nécessite un serveur web compatible avec PHP. Apache est le serveur web recommandé.
- PHP : OpenDCIM nécessite PHP version 5.6 ou ultérieure, avec les extensions mbstring, pdo, pdo_mysql, openssl, xml et gd activées.
- Base de données : OpenDCIM nécessite une base de données MySQL version 5.5 ou ultérieure.
- Accès root : Vous devez avoir les priviléges root sur le système pour installer et configurer OpenDCIM.

I. Création de la Machine Virtuelle

I.1. Définition de Machine Virtuelle

Une machine virtuelle est un environnement informatique isolé et autonome créé à partir d'un ordinateur physique (appelé hôte) à l'aide d'un logiciel spécialisé (hyperviseur ou virtualiseur). Cette technologie permet d'exécuter plusieurs systèmes d'exploitation et applications sur une même machine physique, en créant des environnements virtuels qui simulent les caractéristiques du matériel informatique (processeur, mémoire, stockage, réseau, etc.).

Les machines virtuelles offrent de nombreux avantages, notamment la possibilité de tester des logiciels dans un environnement isolé, de développer des applications pour différentes plateformes sans avoir à posséder plusieurs ordinateurs physiques, ou encore de consolider plusieurs serveurs sur un seul ordinateur hôte pour économiser de l'espace et de l'énergie.

Les hyperviseurs les plus courants sont VirtualBox, VMware, Hyper-V, KVM/QEMU, et ils permettent de créer des machines virtuelles pour différents systèmes d'exploitation tels que Windows, Linux, macOS, etc.

I.2. Installation de VirtualBox

On peut télécharger le programme d'installation de VirtualBox sur le site officiel (<https://www.virtualbox.org/wiki/Downloads>) et exécutez-le.



I.3. Téléchargement de l'image disque CentOS 7

L'image disque CentOS 7 est un fichier binaire qui contient une image complète du système d'exploitation CentOS 7, prête à être utilisée pour créer une machine virtuelle. Elle est distribuée gratuitement et est basée sur le code source de Red Hat Enterprise Linux. CentOS 7 est une version stable et populaire de Linux utilisée pour les serveurs, les postes de travail et les environnements de développement.

L'utilisation de cette image disque simplifie et accélère le processus de création de machines virtuelles CentOS 7 pour une utilisation avec des logiciels de virtualisation tels que VirtualBox.

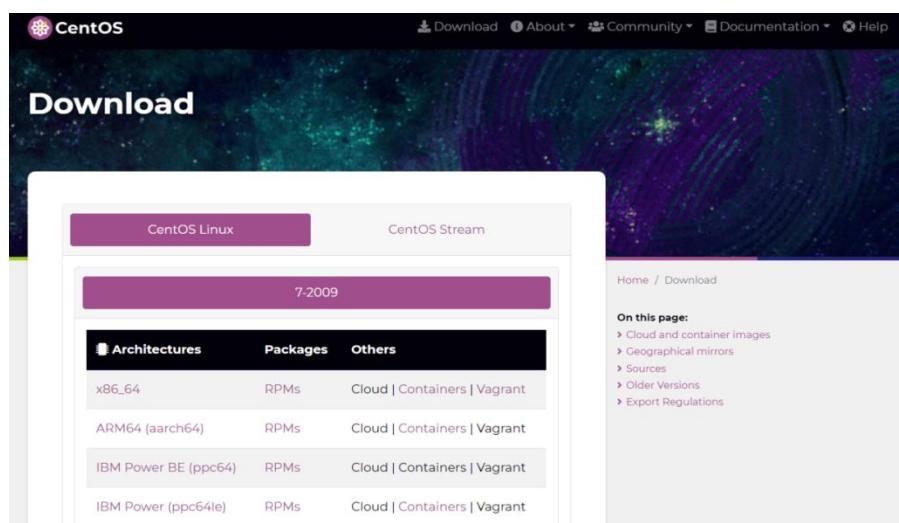


Figure 23: Image ISO

I.4. Configuration de la machine virtuelle

I.4.1. Indiquer le nom et système d'exploitation

- 1) Lancez VirtualBox et cliquez sur le bouton "Nouvelle" pour créer une nouvelle machine virtuelle.
- 2) Donnez un nom à la machine virtuelle et sélectionnez "Linux" comme type d'OS et "Red Hat (64 bits)" comme version.

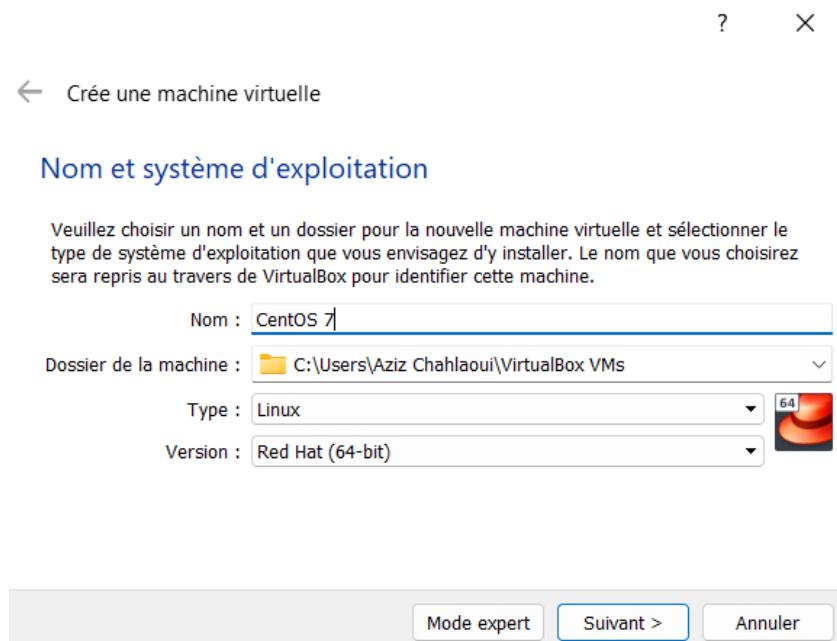


Figure 24: Nom et système d'exploitation

I.4.2. Configurer la quantité de RAM à allouer à la machine virtuelle

On choisit la taille de mémoire vive allouer à la machine virtuelle dépend de plusieurs facteurs, tels que le système d'exploitation invité, les applications que on va exécuter et la quantité de RAM disponible sur l'hôte.

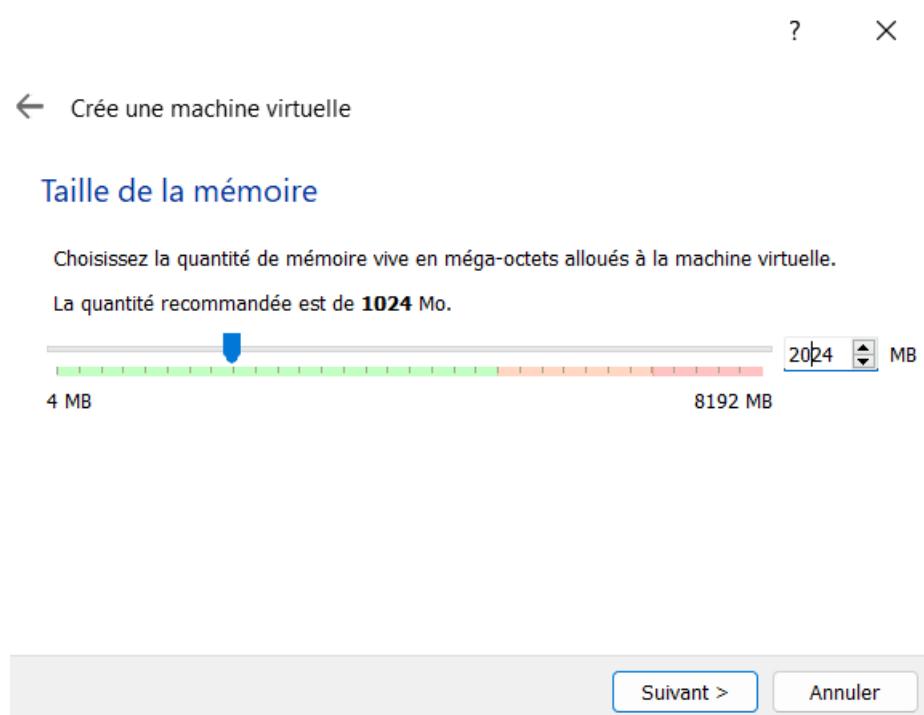


Figure 25 : Taille de la mémoire

I.4.3. Crédation d'un disque dur

La création d'un disque dur virtuel est une étape importante dans la création d'une machine virtuelle, car c'est ce disque dur virtuel qui contiendra le système d'exploitation et les applications que vous souhaitez exécuter dans la machine virtuelle. Il existe plusieurs raisons pour lesquelles vous voudriez créer un disque dur virtuel :

- Séparation de l'environnement virtuel : En créant un disque dur virtuel, vous pouvez séparer complètement l'environnement de la machine virtuelle de l'environnement de votre système d'exploitation hôte. Cela vous permet de tester des logiciels, des configurations système ou des mises à jour sans risquer de perturber votre système d'exploitation principal.
- Facilité de migration : En créant un disque dur virtuel, vous pouvez facilement migrer votre machine virtuelle vers un autre ordinateur ou une autre plate-forme de virtualisation. Vous pouvez simplement transférer le fichier de disque dur virtuel sur un autre ordinateur et l'ouvrir dans un autre logiciel de virtualisation compatible.
- Gestion de l'espace de stockage : La création d'un disque dur virtuel vous permet de gérer plus facilement l'espace de stockage utilisé par la machine virtuelle. Vous

pouvez allouer une quantité spécifique d'espace disque pour la machine virtuelle, ce qui peut vous aider à éviter d'épuiser l'espace disque disponible sur votre système hôte.

- Sauvegarde et restauration : En créant un disque dur virtuel, vous pouvez facilement sauvegarder et restaurer le contenu de votre machine virtuelle. Vous pouvez sauvegarder le fichier de disque dur virtuel sur un support de stockage externe et le restaurer en cas de perte de données ou de défaillance de la machine virtuelle.

VDI, VHD et VMDK sont tous des types de fichiers de disque dur virtuel utilisés par les logiciels de virtualisation pour stocker les données des machines virtuelles. Voici une brève description de chaque format :

- VDI (VirtualBox Disk Image) : c'est le format de fichier de disque dur virtuel utilisé par VirtualBox. Les fichiers VDI sont généralement plus petits que les autres formats de disque dur virtuel, ce qui les rend plus rapides et plus faciles à sauvegarder.
- VHD (Virtual Hard Disk) : c'est le format de fichier de disque dur virtuel utilisé par Microsoft Hyper-V. Les fichiers VHD sont également utilisés par d'autres logiciels de virtualisation tels que VirtualBox et VMware. Les fichiers VHD sont généralement plus grands que les fichiers VDI.
- VMDK (Virtual Machine Disk) : c'est le format de fichier de disque dur virtuel utilisé par VMware. Les fichiers VMDK sont généralement plus grands que les fichiers VDI et sont souvent utilisés pour les machines virtuelles nécessitant beaucoup d'espace de stockage, tels que les serveurs de fichiers et les bases de données.

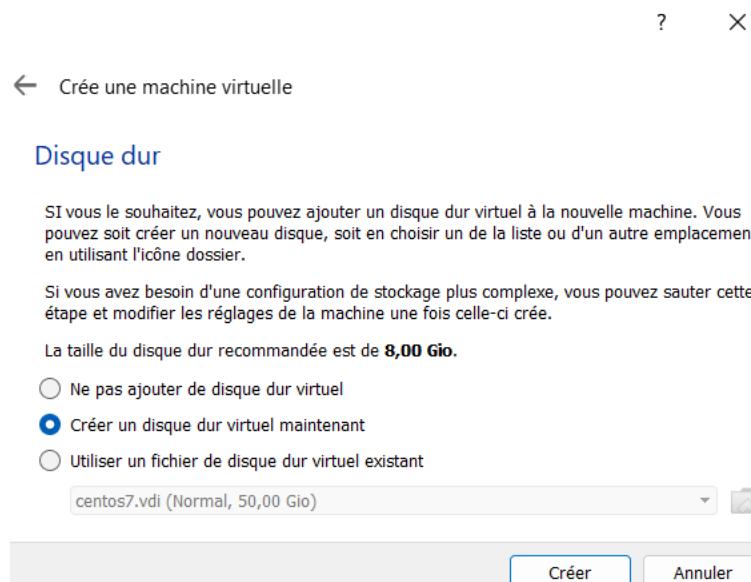


Figure 26: Disque dur

I.4.4. Stockage sur disque dur physique

Un disque dur virtuel dynamiquement alloué est un type de stockage où l'espace disque n'est pas alloué au moment de la création du disque dur virtuel. Au lieu de cela, l'espace disque est alloué dynamiquement à mesure que les données sont ajoutées à la machine virtuelle. Cela signifie que le disque dur virtuel ne prendra que l'espace disque réellement utilisé par la machine virtuelle, ce qui peut vous aider à économiser de l'espace disque sur votre système hôte. Cependant, cela peut également entraîner une fragmentation de fichiers et une légère perte de performance lorsque la machine virtuelle doit étendre le disque dur virtuel.

Un disque dur virtuel de taille fixe est un type de stockage où l'espace disque est alloué en totalité lors de la création du disque dur virtuel. Cela signifie que la taille du fichier de disque dur virtuel est fixe, quelle que soit la quantité d'espace disque réellement utilisée par la machine virtuelle. Bien que cela garantisse une performance optimale et évite la fragmentation des fichiers, cela peut également entraîner une perte d'espace disque si la machine virtuelle n'utilise pas toute la capacité du disque dur virtuel.

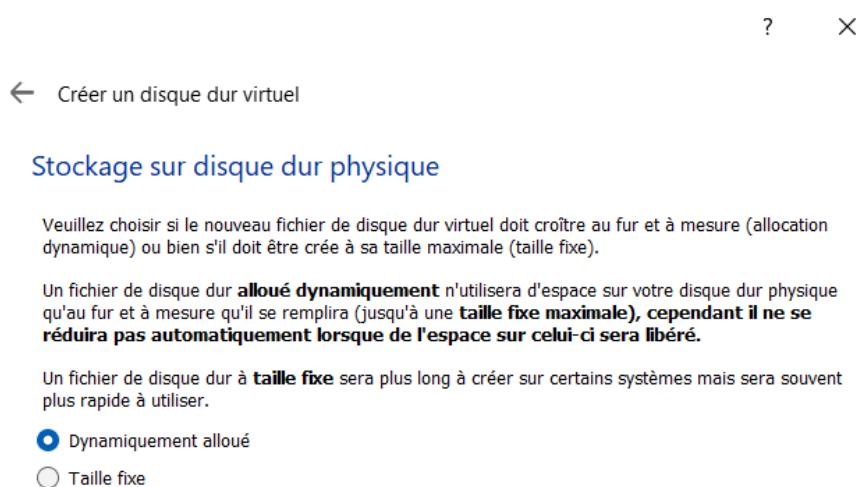


Figure 27: Stockage sur disque dur physique

L'emplacement du fichier de disque dur virtuel est l'endroit où le fichier sera stocké sur le système hôte. Vous pouvez choisir de stocker le fichier de disque dur virtuel dans un dossier spécifique sur le disque dur local ou sur un disque dur externe. L'emplacement du fichier de disque dur virtuel doit être accessible en lecture et en écriture pour la machine virtuelle.

La taille du fichier de disque dur virtuel dépend des besoins de la machine virtuelle. La taille doit être suffisante pour stocker tous les fichiers système, les applications et les données de la machine virtuelle. Si la taille du disque dur virtuel est trop petite, cela peut entraîner des problèmes d'espace disque et de performance dans la machine virtuelle. Si la taille du disque dur virtuel est trop grande, cela peut entraîner une perte d'espace disque sur le système hôte.

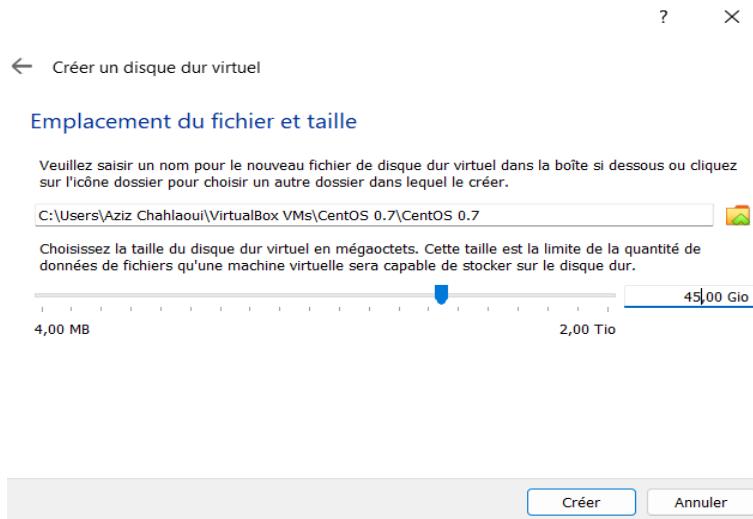


Figure 28: Emplacement du fichier et taille

II. Installation de CentOS 7

II.1. Définition de CentOS 7

CentOS 7 est un système d'exploitation open source de type Linux, basé sur les sources de Red Hat Enterprise Linux (RHEL) 7. Il est compatible avec la plupart des applications et des services utilisés dans les environnements d'entreprise.

CentOS 7 est une distribution Linux stable et robuste qui est souvent utilisée pour des tâches de serveur. Il est réputé pour sa fiabilité, sa sécurité, sa facilité d'utilisation et sa grande flexibilité. CentOS 7 utilise le noyau Linux version 3.10 et fournit des fonctionnalités de virtualisation, de stockage, de sécurité, de réseau et de gestion de système avancées.

CentOS 7 est disponible gratuitement et est soutenu par une communauté de développeurs et de contributeurs. Il est régulièrement mis à jour avec les dernières mises à jour de sécurité et de correctifs de bogues. CentOS 7 est une option populaire pour les serveurs web, les bases de données, les applications d'entreprise et les systèmes de stockage de données.

II.2. Configuration les paramètres

II.2.1. Insertion Image ISO

On ajoute l'image ISO de CentOS 7 dans le disque dur de la machine virtuelle pour pouvoir lancer le programme d'installation de CentOS 7 à partir de la machine virtuelle.

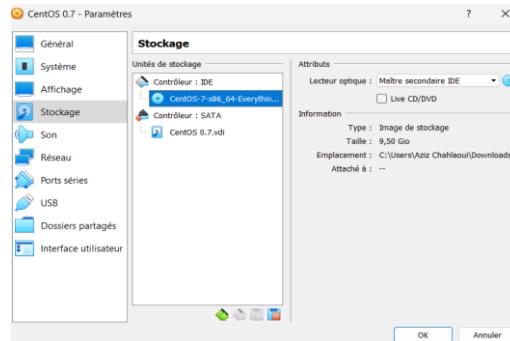


Figure 29: Configuration de stockage et Insertion Image ISO

II.2.2. Démarrer l'installation

Une fois que la machine virtuelle a été configurée, il faut démarrer la machine virtuelle et sélectionner l'option d'installation de CentOS 7

Installer CentOS 7 permet de créer une plateforme de travail stable et performante pour effectuer des tâches variées telles que le développement, l'hébergement de sites web, la virtualisation et bien d'autres.

Avant d'installer CentOS 7, il est recommandé de tester le support d'installation (le média d'installation) pour s'assurer qu'il est exempt d'erreurs ou de défauts. La plupart des images ISO de CentOS 7 fournissent une option de test du support d'installation au démarrage. Cette étape peut aider à éviter les erreurs pendant l'installation.

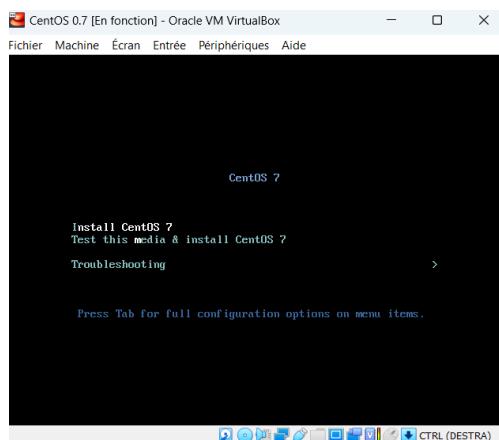


Figure 30: Installer Centos 7

II.2.3. Configurer le paramètre de localisation

Lors de l'installation, il est important de sélectionner la langue et les paramètres d'heure appropriés pour la machine virtuelle.

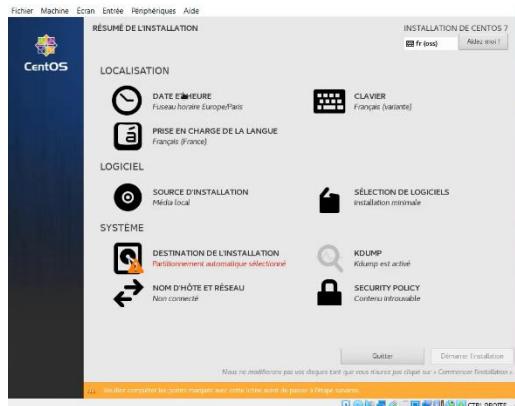


Figure 31: Configuration de CentOS 7

II.2.4. Sélection de logiciels

Dans la sélection de logiciels lors de l'installation de CentOS 7, "Serveur avec GUI" fait référence à une option d'installation qui inclut une interface graphique utilisateur (GUI) dans l'installation du serveur. Cela signifie que la version installée de CentOS 7 disposera d'un environnement de bureau complet, y compris des outils graphiques pour gérer les tâches du serveur.

Cette option est utile pour les utilisateurs qui préfèrent une interface graphique pour administrer leur serveur plutôt que de travailler en ligne de commande. La présence de la GUI permet d'effectuer certaines tâches plus facilement, telles que la configuration du réseau ou l'installation de logiciels.

Cependant, il est important de noter que l'inclusion de l'interface graphique peut augmenter l'utilisation des ressources du serveur, tels que la mémoire RAM ou le processeur, et peut rendre le système plus vulnérable aux attaques de sécurité. Par conséquent, il est recommandé de n'inclure l'interface graphique que si elle est réellement nécessaire.

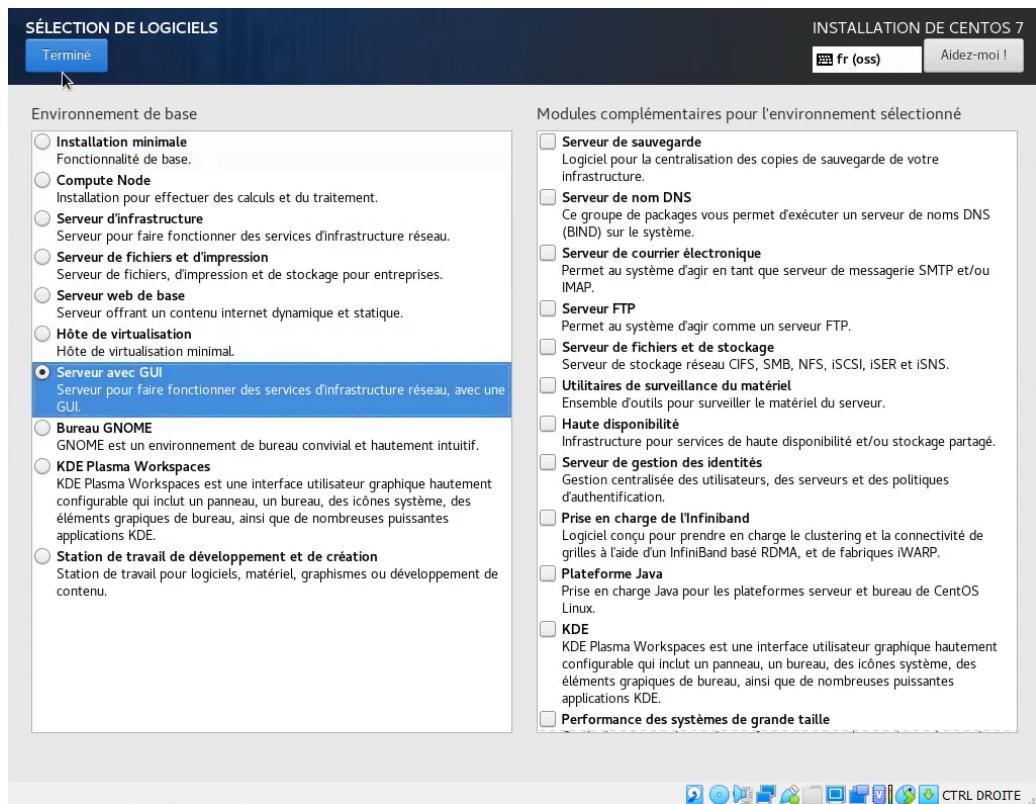


Figure 32: Sélection de logiciels "Serveur avec GUI"

II.2.5. Destination de l'installation

Lors de l'installation de CentOS 7, il est possible de choisir le partitionnement automatique pour définir la destination de l'installation. Dans ce cas, le programme d'installation utilise tout l'espace disponible sur le disque dur pour créer automatiquement les partitions nécessaires pour l'installation du système d'exploitation.

Le partitionnement automatique sélectionne généralement l'option la plus simple et la plus courante pour partitionner le disque dur, qui consiste à créer une partition racine (root) et une partition de swap. La partition racine contient les fichiers système et les applications, tandis que la partition de swap est utilisée pour le stockage temporaire des données.

Cependant, il est important de noter que l'utilisation de la partitionnement automatique peut ne pas être adaptée à tous les cas d'utilisation. Si vous avez des exigences spécifiques pour la configuration du système de fichiers, telles que la création de partitions séparées pour les données ou les journaux, il est préférable de sélectionner le partitionnement manuel pour personnaliser la configuration de la partition.

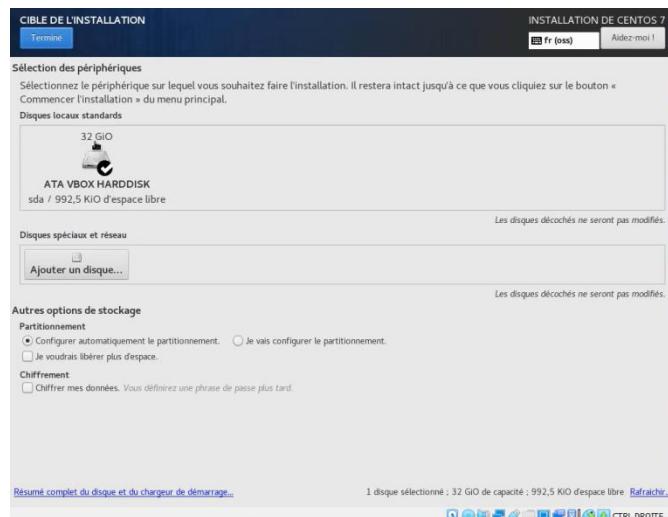


Figure 33: Choix de participation

II.2.6. Nom de d'hôte et réseau

Lors de l'installation de CentOS 7, il est nécessaire de configurer le nom d'hôte et le réseau pour que le système puisse être connecté à un réseau et communiquer avec d'autres ordinateurs.

Le nom d'hôte est le nom unique qui est utilisé pour identifier le système sur le réseau. Il est recommandé de choisir un nom d'hôte qui est facile à retenir et à identifier pour les administrateurs système et les utilisateurs du réseau. Le nom d'hôte doit être composé de lettres minuscules, de chiffres et de traits d'union ("-"), sans espaces ni caractères spéciaux.

Le réseau, quant à lui, se réfère à la configuration des paramètres de réseau pour le système, tels que l'adresse IP, le masque de sous-réseau, la passerelle par défaut et les serveurs DNS. Il est important de configurer correctement les paramètres de réseau pour que le système puisse se connecter à Internet et aux autres ordinateurs sur le réseau.

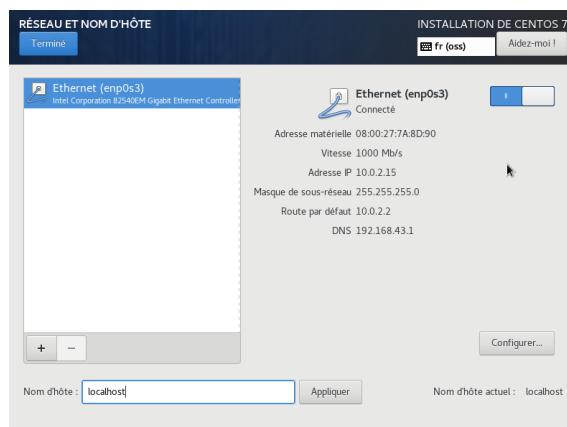


Figure 34: Configuration réseau et nom d'hôte

II.2.7. Mot de passe d'administrateur

Lors de l'installation de ²CentOS 7, il est nécessaire de définir un mot de passe administrateur (root) pour accéder à toutes les fonctionnalités du système en tant qu'utilisateur administrateur. Le mot de passe root est utilisé pour effectuer des tâches qui nécessitent des priviléges d'administrateur, telles que l'installation de logiciels, la configuration de paramètres système et la gestion des utilisateurs.

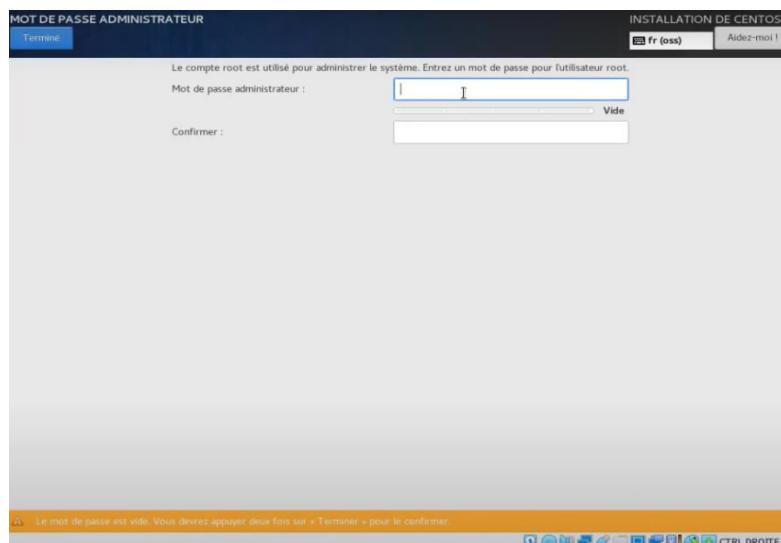


Figure 35: création de mot de passe

II.2.8. Crédation d'utilisateur

Lors de l'installation de CentOS 7, il est possible de créer un ou plusieurs comptes utilisateur supplémentaires pour permettre à plusieurs utilisateurs d'accéder au système. Les comptes utilisateur sont utilisés pour effectuer des tâches quotidiennes telles que la navigation sur Internet, la messagerie électronique, la bureautique, etc. Ces comptes utilisateurs ne disposent pas de priviléges d'administrateur.

Pour créer un nouvel utilisateur, il est généralement nécessaire de fournir des informations telles que le nom d'utilisateur, le mot de passe, le répertoire de base (le répertoire principal de l'utilisateur), le groupe principal et les groupes supplémentaires. Il est important de choisir un nom d'utilisateur qui est facile à retenir et à identifier pour les administrateurs système et les utilisateurs du système.

Une fois que le compte utilisateur a été créé, l'utilisateur peut se connecter au système en utilisant son nom d'utilisateur et son mot de passe pour accéder aux fonctionnalités du système qui lui sont autorisées.

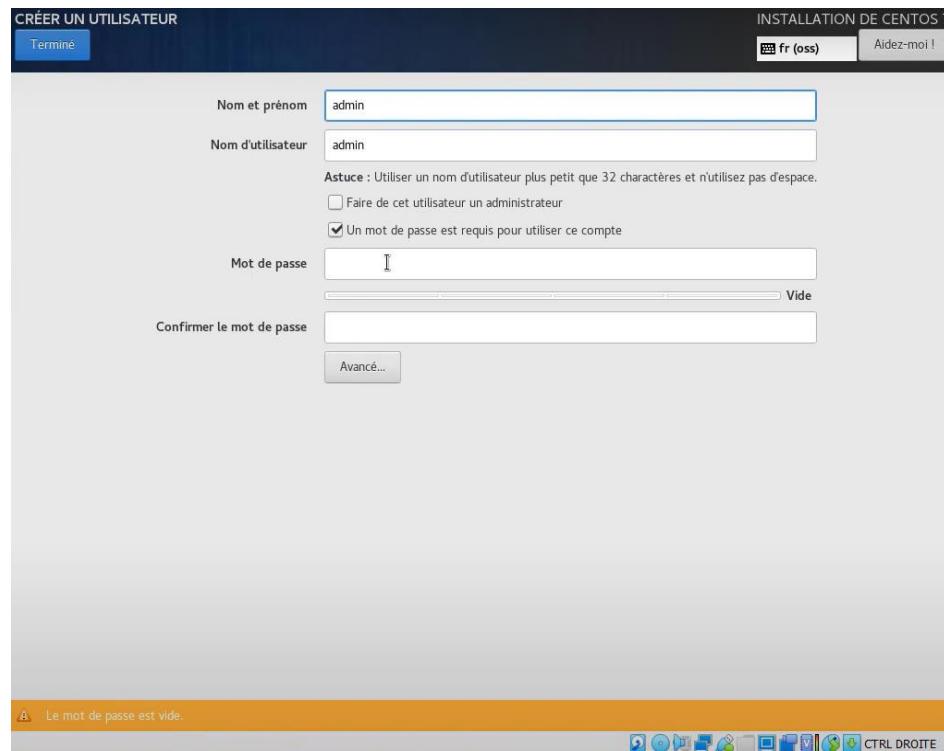


Figure 36: Création d'utilisateur

II.2.9. Redémarrer le système

On fait redémarrer pour assurer que toutes les mises à jour et les modifications effectuées pendant l'installation sont correctement appliquées au système. Il peut être nécessaire de redémarrer plusieurs fois pour terminer l'installation de certains packages et modules supplémentaires.

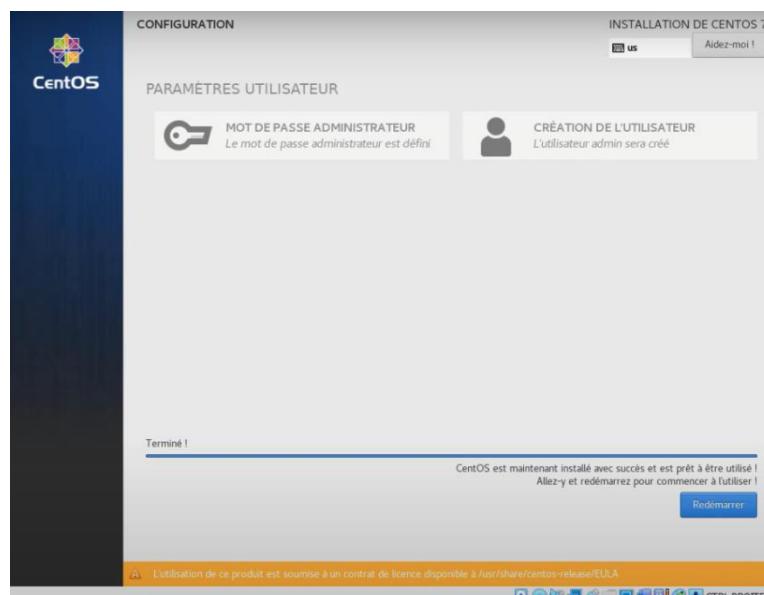


Figure 37: Redémarrer le système

II.2.10. Licence information

La licence d'utilisation est un contrat légal qui définit les termes et les conditions de l'utilisation du logiciel CentOS 7. Lorsque vous installez CentOS 7, vous êtes tenu d'accepter les termes de la licence d'utilisation avant de pouvoir continuer l'installation.

La licence d'utilisation de CentOS 7 est basée sur la licence GNU General Public License (GPL), qui est une licence libre et ouverte qui permet à quiconque de copier, modifier et distribuer le logiciel. Cela signifie que vous pouvez installer, utiliser et distribuer CentOS 7 gratuitement, à condition de respecter les termes de la licence.

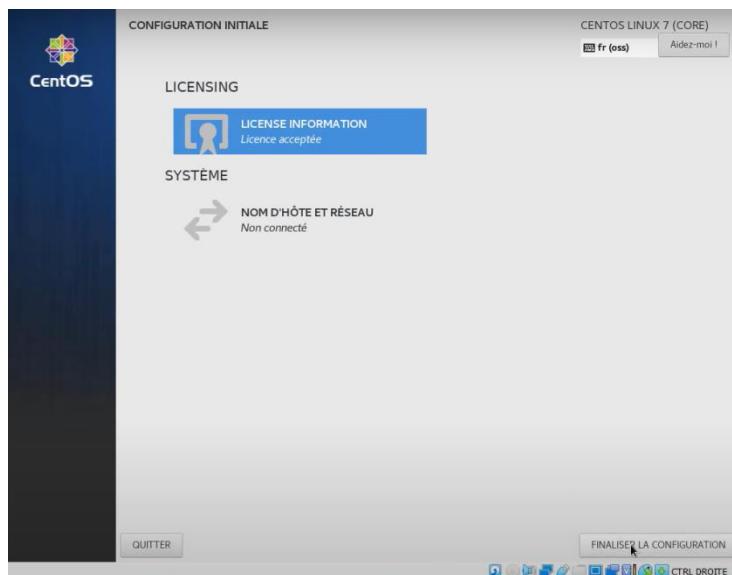


Figure 38: Configuration initiale

III. Installation d'OpenDCIM

III.1. Installation Apache, PHP, MySQL

III.1.1. Installation Apache

Apache est l'un des serveurs web les plus populaires et les plus utilisés au monde, et est largement utilisé pour héberger des sites web. Lorsqu'il est installé sur le système, le serveur web Apache fournit une plate-forme pour héberger des pages web statiques et dynamiques, ainsi que des applications web telles que des CMS (systèmes de gestion de contenu) et des applications d'e-commerce. L'installation d'Apache est une étape clé dans la mise en place d'un environnement web complet pour héberger des applications web.

```
[azizch@localhost ~]$ sudo yum -y install httpd
```

Cette commande permet d'installer le serveur web Apache sur le système

III.1.2. Installation PHP

PHP est utilisé pour créer des pages web dynamiques et interagir avec des bases de données et d'autres applications côté serveur.

L'installation de PHP est une étape clé dans la mise en place d'un environnement web complet pour héberger des applications web. Avec PHP installé, les développeurs peuvent créer des pages web générées à la volée qui se connectent à des bases de données et effectuent d'autres opérations côté serveur, ce qui permet de créer des sites web dynamiques et des applications web sophistiquées.

```
[azizch@localhost ~]$ sudo yum -y install php
```

Cette commande permet d'installer le langage de script côté serveur PHP sur le système CentOS 7

```
[azizch@localhost ~]$ sudo yum -y install php-mysql
```

Cette commande permet d'installer le module PHP pour l'extension MySQL sur un système CentOS 7

Ce module est nécessaire si vous souhaitez utiliser PHP pour se connecter à une base de données MySQL et récupérer des données pour un site web ou une application web. En installant ce module, PHP est capable de communiquer avec la base de données MySQL et d'exécuter des requêtes pour récupérer ou modifier les données stockées dans la base de données. L'installation de ce module est donc importante si vous souhaitez utiliser PHP pour développer des applications web qui interagissent avec une base de données MySQL.

```
[azizch@localhost ~]$ sudo yum -y install php-mbstring
```

Cette commande permet d'installer le module PHP pour la prise en charge des chaînes de caractères multibyte (MB).

Les chaînes de caractères multibyte sont utilisées dans de nombreuses langues autres que l'anglais, telles que le chinois, le japonais et le coréen. Ce module est important pour garantir que les applications web qui utilisent PHP sont capables de traiter correctement les caractères

MB et de les afficher correctement sur la page web. Sans ce module, les caractères MB peuvent être affichés de manière incorrecte ou ne pas être pris en charge du tout. La commande "yum -y install php-mbstring" est donc essentielle pour garantir la compatibilité des applications web avec des langues autres que l'anglais et pour s'assurer que les sites web s'affichent correctement pour les utilisateurs de différentes langues.

```
[azizch@localhost ~]$ sudo yum -y install php-snmp
```

Cette commande permet d'installer le module PHP pour la prise en charge du protocole SNMP (Simple Network Management Protocol).

SNMP est un protocole utilisé pour gérer et surveiller les réseaux informatiques. Le module PHP SNMP fournit une interface permettant de communiquer avec des périphériques réseau et de récupérer des informations sur les performances, les erreurs et d'autres paramètres liés au réseau.

En installant ce module, les développeurs peuvent utiliser PHP pour créer des applications de surveillance réseau et récupérer des informations sur les périphériques réseau tels que les routeurs, les commutateurs, les imprimantes et les serveurs. Ils peuvent également utiliser ce module pour effectuer des diagnostics sur les performances du réseau, résoudre les problèmes liés aux erreurs de communication et optimiser la performance du réseau. En somme, la commande "yum -y install php-snmp" est donc importante pour ceux qui travaillent dans le domaine de la gestion de réseau et qui souhaitent développer des applications PHP pour la surveillance et la gestion des réseaux informatiques.

III.1.3. Installation serveur MySQL

```
[azizch@localhost ~]$ sudo yum -y install mariadb-server
```

Cette commande est utilisée lors de l'installation d'OpenDCIM pour installer et configurer le serveur de base de données MariaDB, qui est une composante essentielle pour le fonctionnement de l'application OpenDCIM. Voici quelques raisons pour lesquelles cette commande est nécessaire :

- Stockage des données : OpenDCIM est une application de gestion d'inventaire de data center qui stocke toutes les informations sur les équipements, les racks, les connexions, etc. Pour stocker ces données, l'application nécessite une base de données. MariaDB est une solution de base de données open source qui est largement utilisée dans le monde de l'entreprise et qui est compatible avec les applications web, telles que OpenDCIM.
- Sécurité : MariaDB fournit des fonctionnalités de sécurité avancées, telles que la prise en charge de SSL/TLS, la gestion des utilisateurs et des autorisations, le chiffrement des données, etc. Ces fonctionnalités permettent de sécuriser les données stockées dans la base de données, ce qui est essentiel pour les environnements de data center.
- Fiabilité et performance : MariaDB est une base de données robuste et performante qui est conçue pour traiter des charges de travail élevées. Elle offre des fonctionnalités telles que la réplication, la gestion des transactions, l'optimisation des requêtes, etc. Ces fonctionnalités garantissent que la base de données est fiable et performante, même dans des environnements de data center complexes.

III.1.4. Installation du module SSL d'Apache

```
[azizch@localhost ~]$ sudo yum -y install mod_ssl
```

La commande "yum -y install mod_ssl" est utilisée dans l'installation d'OpenDCIM pour installer le module SSL (Secure Sockets Layer) pour le serveur web Apache. Ce module permet de configurer le serveur Apache pour prendre en charge le protocole HTTPS, qui est utilisé pour sécuriser les communications entre le serveur web et les clients.

Voici quelques raisons pour lesquelles cette commande est nécessaire :

- Sécurité : L'utilisation du protocole HTTPS est essentielle pour sécuriser les communications entre le serveur web et les clients. Il permet de chiffrer les données échangées, ce qui protège les informations sensibles, telles que les noms d'utilisateur, les mots de passe et les données d'inventaire.

- Conformité : De nombreuses normes de sécurité et de conformité, telles que PCI DSS, exigent l'utilisation du protocole HTTPS pour sécuriser les données des clients.
- Fiabilité : Le module SSL d'Apache est un composant fiable et éprouvé qui est largement utilisé dans le monde de l'entreprise. Il offre des fonctionnalités telles que la gestion des certificats, la prise en charge de SSL/TLS, etc. Ces fonctionnalités garantissent que le serveur Apache est fiable et sécurisé.

III.2. Activer les services de serveur web

III.2.1. Activer et démarrer service Apache

```
[azizch@localhost ~]$ sudo systemctl enable httpd.service
[sudo] Mot de passe de azizch :
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service to /usr/
lib/systemd/system/httpd.service.
[azizch@localhost ~]$ sudo systemctl start httpd.service
```

Les commandes "systemctl enable httpd.service" et "systemctl start httpd.service" sont utilisées dans l'installation d'OpenDCIM pour démarrer et activer le service du serveur web Apache.

Voici une explication détaillée de ces commandes :

- "systemctl enable httpd.service" : Cette commande permet de configurer le service httpd (le serveur web Apache) pour qu'il démarre automatiquement au démarrage du système. En exécutant cette commande, on s'assure que le serveur web est disponible et fonctionnel à chaque démarrage du système.
- "systemctl start httpd.service" : Cette commande permet de démarrer le service httpd immédiatement. Une fois le service démarré, le serveur web est disponible pour répondre aux requêtes des clients.

III.2.2. Activer et démarrer le service de la base de données Maria DB

```
[azizch@localhost ~]$ sudo systemctl enable mariadb.service
[azizch@localhost ~]$ sudo systemctl start mariadb.service
```

Les commandes "systemctl enable mariadb.service" et "systemctl start mariadb.service" sont utilisées dans l'installation d'OpenDCIM pour activer et démarrer le service de la base de données MariaDB.

Voici une explication détaillée de ces commandes :

- "systemctl enable mariadb.service" : Cette commande permet de configurer le service de la base de données MariaDB pour qu'il démarre automatiquement au démarrage du système. En exécutant cette commande, on s'assure que le service de la base de données est disponible et fonctionnel à chaque démarrage du système.
- "systemctl start mariadb.service" : Cette commande permet de démarrer le service de la base de données MariaDB immédiatement. Une fois le service démarré, la base de données est disponible pour les connexions entrantes.

III.3. Ouvrir l'accès Web sur le pare-feu

```
[azizch@localhost ~]$ firewall-cmd --zone=public --add-port=443/tcp --permanent  
success
```

La commande "firewall-cmd --zone=public --add-port=443/tcp --permanent" est utilisée dans l'installation d'OpenDCIM pour ouvrir le port 443 sur le pare-feu (firewall) du système CentOS. Ce port est utilisé pour permettre l'accès à l'interface web sécurisée (HTTPS) d'OpenDCIM.

Voici une explication détaillée de cette commande :

- "firewall-cmd" est l'utilitaire de gestion du pare-feu dans CentOS 7.
- "--zone=public" spécifie la zone du pare-feu dans laquelle la règle doit être ajoutée. Dans ce cas, la zone publique est spécifiée.
- "--add-port=443/tcp" ajoute une règle qui autorise le trafic entrant sur le port 443 en utilisant le protocole TCP. Le port 443 est utilisé pour les connexions HTTPS.
- "--permanent" indique que la règle doit être ajoutée de manière permanente au pare-feu.

Voici quelques raisons pour lesquelles cette commande est nécessaire :

- Sécurité : Le pare-feu est un composant essentiel de la sécurité du système. En ouvrant uniquement les ports nécessaires, on réduit les risques d'attaques et on améliore la sécurité globale du système.
- Fonctionnalité : Le port 443 est utilisé pour les connexions HTTPS, qui sont nécessaires pour sécuriser les communications entre le serveur web et les clients.
- Conformité : De nombreuses normes de sécurité et de conformité, telles que PCI DSS, exigent la mise en place d'un pare-feu configuré pour bloquer tous les ports non nécessaires.

```
[azizch@localhost ~]$ sudo firewall-cmd --reload
[sudo] Mot de passe de azizch :
success
```

La commande "firewall-cmd --reload" est utilisée dans l'installation d'OpenDCIM pour recharger la configuration du pare-feu du système. Cette commande est nécessaire après avoir effectué des modifications à la configuration du pare-feu, telles que l'ajout ou la suppression de règles.

Voici quelques raisons pour lesquelles cette commande est nécessaire :

- Appliquer les modifications : Lorsque des règles sont ajoutées, modifiées ou supprimées, le pare-feu doit être recharge pour appliquer ces changements. La commande "firewall-cmd --reload" permet de recharger la configuration du pare-feu sans avoir à redémarrer le pare-feu ou le système.
- Éviter les erreurs : Si la configuration du pare-feu n'est pas rechargée après des modifications, les règles ajoutées ou modifiées peuvent ne pas être appliquées, ce qui peut entraîner des erreurs ou des problèmes de sécurité.

III.4. Configurer le serveur MySQL

```
[azizch@localhost ~]$ sudo mysql_secure_installation
```

La commande "mysql_secure_installation" est utilisée dans l'installation d'OpenDCIM pour effectuer une configuration de sécurité de base pour le serveur de base de données MariaDB.

Voici les actions effectuées par la commande "mysql_secure_installation" :

- Définition d'un mot de passe pour l'utilisateur root : Cette étape consiste à définir un mot de passe sécurisé pour l'utilisateur root de la base de données MariaDB.

- Suppression des utilisateurs anonymes : Les utilisateurs anonymes sont des utilisateurs qui peuvent se connecter à la base de données sans fournir de nom d'utilisateur ou de mot de passe. La suppression de ces utilisateurs améliore la sécurité en réduisant les points d'accès potentiels.
- Interdiction de la connexion à distance en tant que root : La connexion en tant que root à la base de données depuis un ordinateur distant peut être dangereuse. Cette étape interdit la connexion à distance en tant que root, en limitant les attaques potentielles.
- Suppression de la base de données de test : La base de données de test est une base de données fournie avec MariaDB qui n'est pas nécessaire pour le fonctionnement d'OpenDCIM. Sa suppression améliore la sécurité en réduisant les points d'accès potentiels.
- Rechargement des privilèges : Cette étape recharge les privilèges de la base de données pour prendre en compte les modifications apportées par les étapes précédentes.

III.5. Créez une base de données pour openDCIM

```
[azizch@localhost ~]$ sudo mysql -u root -p
[sudo] Mot de passe de azizch :
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 10
Server version: 5.5.68-MariaDB MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> create database dcim;
Query OK, 1 row affected (0.01 sec)

MariaDB [(none)]> grant all privileges on dcim.* to 'dcim' identified by 'dcimpassword'
;
Query OK, 0 rows affected (0.01 sec)

MariaDB [(none)]> exit■
```

Ces commandes sont utilisées dans l'installation d'OpenDCIM pour créer une base de données nommée "dcim", accorder des privilèges à un utilisateur nommé "dcim" et définir un mot de passe pour cet utilisateur. Voici ce que chacune de ces commandes fait :

- "mysql -u root -p" : Cette commande permet de se connecter au serveur de base de données MariaDB en tant qu'utilisateur root. L'option "-p" demande à l'utilisateur de fournir son mot de passe.

- "create database dcim;" : Cette commande crée une base de données nommée "dcim" dans le serveur de base de données.
- "grant all privileges on dcim.* to 'dcim' identified by 'dcimpassword';" : Cette commande accorde tous les privilèges sur la base de données "dcim" à un utilisateur nommé "dcim" et définit le mot de passe de cet utilisateur comme "dcimpassword". Les privilèges incluent la création, la modification et la suppression de tables et d'enregistrements.
- "quit" : Cette commande permet de se déconnecter du serveur de base de données.

III.6. Générez les clés nécessaires et copiez-les dans les répertoires appropriés

```
[azizch@localhost ~]$ sudo openssl req -new -key ca.key -out ca.csr
[sudo] Mot de passe de azizch :
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:TN
State or Province Name (full name) []:Ariana
Locality Name (eg, city) [Default City]:La petite Ariana
Organization Name (eg, company) [Default Company Ltd]:Centre d'étude et de recherche
[D^[[A^[[D^[[B
Organizational Unit Name (eg, section) []:CERT
Common Name (eg, your name or your server's hostname) []:localhost
Email Address []:azizchahlaoui7@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:40237834aziz
An optional company name []:CERT
```

```
[azizch@localhost ~]$ sudo cp ca.crt /etc/pki/tls/certs
[azizch@localhost ~]$ sudo cp ca.key /etc/pki/tls/private/ca.key
[azizch@localhost ~]$ sudo cp ca.csr /etc/pki/tls/private/ca.csr
```

Ces commandes permettent de générer une autorité de certification (CA) auto-signée et de copier les fichiers nécessaires dans les répertoires appropriés pour une utilisation ultérieure. Chacune des commandes a une fonction spécifique, comme expliqué ci-dessous :

- La commande "openssl genrsa -out ca.key 1024" génère une clé privée RSA de 1024 bits pour la CA et la stocke dans le fichier ca.key dans le répertoire /root.
- La commande "openssl req -new -key ca.key -out ca.csr" crée une requête de signature de certificat (CSR) pour la CA en utilisant la clé privée générée précédemment et

stocke le fichier de sortie ca.csr dans le répertoire /root. Cette requête contient les informations nécessaires pour que la CA puisse être identifiée lors de l'émission de certificats.

- La commande "openssl x509 -req -days 365 -in ca.csr -signkey ca.key -out ca.crt" crée un certificat auto-signé pour la CA à partir de la CSR précédemment générée. Ce certificat est valable pendant 365 jours et le fichier de sortie ca.crt contient le certificat de la CA.
- Les trois dernières commandes copient les fichiers générés précédemment dans les répertoires /etc/pki/tls/certs et /etc/pki/tls/private, qui sont des emplacements couramment utilisés pour stocker les certificats et clés privées sur les systèmes Linux. Cela permet de rendre les certificats et les clés privées accessibles aux services qui en ont besoin pour leur utilisation.

```
[azizch@localhost ~]$ sudo gedit +/ServerName /etc/httpd/conf/httpd.conf &>/dev/null
```

Ce commande permettre l'ouverture du fichier de configuration d'Apache (httpd.conf) dans l'éditeur de texte gedit, en se positionnant directement sur la ligne contenant le nom de serveur (NomServeur).

```
Ouvrir ▾  httpd.conf  
/etc/httpd/conf  
# In which case these default settings will be overridden for the  
# virtual host being defined.  
#  
# ServerAdmin: Your address, where problems with the server should be  
# e-mailed. This address appears on some server-generated pages, such  
# as error documents. e.g. admin@your-domain.com  
#  
ServerAdmin root@localhost  
  
#  
# ServerName gives the name and port that the server uses to identify itself.  
# This can often be determined automatically, but we recommend you specify  
# it explicitly to prevent problems during startup.  
#  
# If your host doesn't have a registered DNS name, enter its IP address here.  
#  
#ServerName www.example.com:80  
ServerName opendcim.example.net:443  
#  
# Deny access to the entirety of your server's filesystem. You must  
# explicitly permit access to web content directories in other  
# <Directory> blocks below.  
#  
<Directory />  
    AllowOverride none  
    Require all denied  
</Directory>  
  
#  
# Note that from this point forward you must specifically allow  
# particular features to be enabled - so if something's not working as  
# you might expect, make sure that you have specifically enabled it  
# below.  
#  
# DocumentRoot: The directory out of which you will serve your  
# documents. By default, all requests are taken from this directory, but  
# symbolic links and aliases may be used to point to other locations.  
#  
DocumentRoot "/var/www/html"  
#
```

La ligne "ServerName opendcim.example.net:443" est ajoutée au fichier httpd.conf pour spécifier le nom de domaine du serveur et le port utilisé pour le serveur web Apache. Cette information est utilisée par Apache pour identifier le serveur lorsqu'il répond aux requêtes des clients.

Dans cet exemple, "opendcim.example.net" est le nom de domaine du serveur et ":443" est le port utilisé pour les connexions HTTPS (qui sont cryptées). Cette ligne est importante car elle permet de s'assurer que les certificats SSL/TLS du serveur web sont correctement émis pour le nom de domaine spécifié.

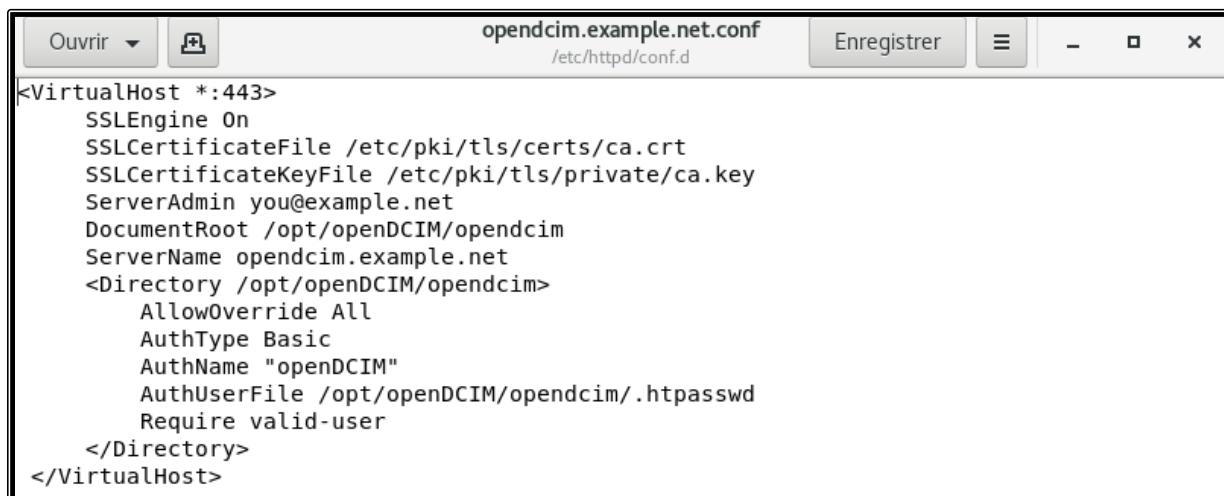
```
[azizjlll@localhost ~]$ systemctl redémarre httpd.service
```

Ce commande utilisée pour redémarrer un service système donné.

III.7. Créer un hôte virtuel

```
[azizjlll@10 ~]$ sudo gedit /etc/httpd/conf.d/opendcim.example.net.conf &>/dev/null
```

Ce commande permettre d'ouvrir le fichier de configuration « /etc/httpd/conf.d/opendcim.example.net.conf » avec l'éditeur de texte "gedit" en utilisant les privilèges de superutilisateur.



The screenshot shows a Gedit text editor window with the title bar "opendcim.example.net.conf /etc/httpd/conf.d". The main content area contains the following configuration code:

```
<VirtualHost *:443>
    SSLEngine On
    SSLCertificateFile /etc/pki/tls/certs/ca.crt
    SSLCertificateKeyFile /etc/pki/tls/private/ca.key
    ServerAdmin you@example.net
    DocumentRoot /opt/openDCIM/opendcim
    ServerName opendcim.example.net
    <Directory /opt/openDCIM/opendcim>
        AllowOverride All
        AuthType Basic
        AuthName "openDCIM"
        AuthUserFile /opt/openDCIM/opendcim/.htpasswd
        Require valid-user
    </Directory>
</VirtualHost>
```

Le bloc de configuration que vous avez fourni est une configuration typique d'un hôte virtuel (VirtualHost) utilisant le protocole SSL/TLS pour le serveur opendcim.example.net.

Voici le rôle de chaque directive dans ce bloc de configuration :

- <VirtualHost *:443> : Cette directive indique que cet hôte virtuel répondra aux requêtes HTTPS sur tous les interfaces (*), sur le port 443 (le port par défaut pour HTTPS).
- SSLEngine On : Cette directive active le moteur SSL/TLS pour ce hôte virtuel, ce qui permet de gérer les connexions sécurisées.
- SSLCertificateFile : Spécifie le chemin du fichier contenant le certificat SSL/TLS du serveur. Dans cet exemple, le fichier est "/etc/pki/tls/certs/ca.crt".
- SSLCertificateKeyFile : Spécifie le chemin du fichier contenant la clé privée correspondant au certificat SSL/TLS. Dans cet exemple, le fichier est "/etc/pki/tls/private/ca.key".
- ServerAdmin : Indique l'adresse e-mail de l'administrateur du serveur, dans cet exemple "you@example.net".
- DocumentRoot : Définit le répertoire racine des fichiers du site web pour cet hôte virtuel. Dans cet exemple, le répertoire est "/opt/openDCIM/opendcim".
- ServerName : Spécifie le nom du serveur pour cet hôte virtuel. Dans cet exemple, le nom est "opendcim.example.net".
- <Directory /opt/openDCIM/opendcim> : Cela définit les directives spécifiques à appliquer au répertoire "/opt/openDCIM/opendcim".
- AllowOverride All : Permet la surcharge des directives de configuration via des fichiers .htaccess dans le répertoire "/opt/openDCIM/opendcim".
- AuthType Basic : Indique que l'authentification basique HTTP sera utilisée.
- AuthName "openDCIM" : Définit le nom d'identification affiché lors de la demande d'authentification.
- AuthUserFile : Spécifie le chemin du fichier contenant les informations d'authentification (nom d'utilisateur et mot de passe). Dans cet exemple, le fichier est "/opt/openDCIM/opendcim/.htpasswd".
- Require valid-user : Indique que seule une identification valide est autorisée pour accéder au répertoire "/opt/openDCIM/opendcim".

III.8. Téléchargez et installez openDCIM

III.8.1 Téléchargez la dernière version d'openDCIM sur opendcim.com

```
[azizch@localhost ~]$ sudo mkdir /opt/openDCIM
[azizch@localhost ~]$ sudo cd /opt/openDCIM
[azizch@localhost ~]$ cd /opt/openDCIM
[azizch@localhost openDCIM]$ sudo curl -O https://opendcim.org/packages/openDCIM-21.01.tar.gz
```

- mkdir /opt/openDCIM : Cette commande crée un répertoire appelé "openDCIM" dans le répertoire "/opt". Ce répertoire sera utilisé pour installer le logiciel openDCIM.
- cd /opt/openDCIM : Cette commande permet de changer le répertoire de travail courant vers "/opt/openDCIM". Cela signifie que toutes les commandes suivantes seront exécutées dans ce répertoire.
- curl -O http://www.opendcim.org/packages/openDCIM-4.0.1.tar.gz : Cette commande utilise l'outil cURL pour télécharger le fichier "openDCIM-4.0.1.tar.gz" depuis l'URL spécifiée (<http://www.opendcim.org/packages/openDCIM-4.0.1.tar.gz>) et le place dans le répertoire courant (" /opt/openDCIM" dans ce cas).

III.8.2. Extrader l'archive et créer un lien symbolique

```
[azizjlll@10 ~]$ tar zxvf openDCIM-21.01.tar.gz
```

- tar zxvf openDCIM-4.0.1.tar.gz : Cette commande extrait les fichiers d'une archive compressée appelée "openDCIM-21.01.tar.gz". Elle les décomprime et les place dans un répertoire nommé "openDCIM-21.01".

```
[azizjlll@10 ~]$ ln -s openDCIM-21.01 opendcim
```

- ln -s openDCIM-4.0.1 opendcim : Cette commande crée un lien spécial qui agit comme un raccourci vers le répertoire "openDCIM-4.0.1". Le lien symbolique porte le nom "opendcim". Ainsi, vous pouvez accéder au répertoire "openDCIM-4.0.1" en utilisant simplement le nom "opendcim".

III.8.3. Préparez le fichier de configuration pour accéder à la base de données

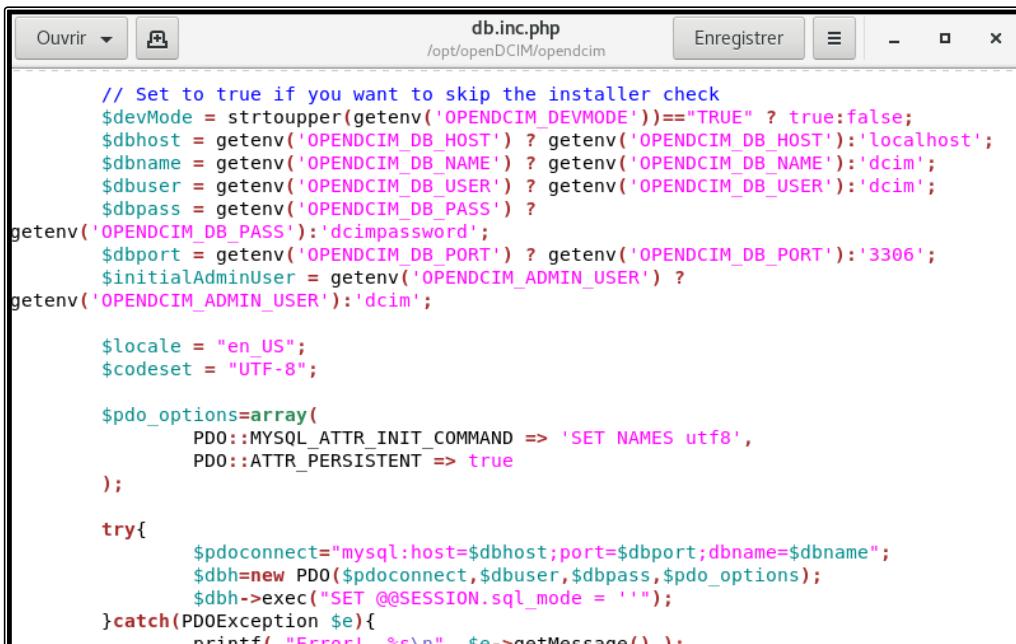
```
[azizjlll@10 ~]$ cd /opt/openDCIM/opendcim
```

- cd /opt/openDCIM/opendcim : Cette commande change le répertoire de travail courant pour "/opt/openDCIM/opendcim". Cela signifie que les commandes suivantes seront exécutées dans ce répertoire.

```
[azizjlll@10 ~]$ cd qp.tuc.bpb-qtsf.qtuc.bpb
```

- cp db.inc.php-dist db.inc.php : Cette commande effectue une copie du fichier "db.inc.php-dist" et crée un nouveau fichier appelé "db.inc.php". La nouvelle copie "db.inc.php" sera utilisée pour la configuration de la base de données dans openDCIM.

```
[azizjlll@10 ~]$ sudo gedit db.inc.php &>/dev/null
```



The screenshot shows a gedit text editor window with the file "db.inc.php" open. The file contains PHP code for database configuration. It uses environment variables to set host, name, user, and password. It also defines PDO options and attempts to connect to MySQL using PDO.

```
// Set to true if you want to skip the installer check
$devMode = strtoupper(getenv('OPENDCIM_DEVMODE'))=="TRUE" ? true:false;
$dbhost = getenv('OPENDCIM_DB_HOST') ? getenv('OPENDCIM_DB_HOST'):'localhost';
$dbname = getenv('OPENDCIM_DB_NAME') ? getenv('OPENDCIM_DB_NAME'):'dcim';
$dbuser = getenv('OPENDCIM_DB_USER') ? getenv('OPENDCIM_DB_USER'):'dcim';
$dbpass = getenv('OPENDCIM_DB_PASS') ? getenv('OPENDCIM_DB_PASS'):'dcimpassword';
$dbport = getenv('OPENDCIM_DB_PORT') ? getenv('OPENDCIM_DB_PORT'):'3306';
$initialAdminUser = getenv('OPENDCIM_ADMIN_USER') ? getenv('OPENDCIM_ADMIN_USER'):'dcim';
getenv('OPENDCIM_ADMIN_USER'):'dcim';

$locale = "en_US";
$codeset = "UTF-8";

$pdo_options=array(
    PDO::MYSQL_ATTR_INIT_COMMAND => 'SET NAMES utf8',
    PDO::ATTR_PERSISTENT => true
);

try{
    $pdoconnect="mysql:host=$dbhost;port=$dbport;dbname=$dbname";
    $dbh=new PDO($pdoconnect,$dbuser,$dbpass,$pdo_options);
    $dbh->exec("SET @SESSION.sql_mode = ''");
} catch(PDOException $e){
    printf( "Error! %s\n", $e->getMessage() );
}
```

On va Modifier les lignes suivantes pour refléter vos paramètres d'hôte de base de données (dans cet exemple localhost), le nom de la base de données (dcim) et les informations d'identification que vous avez attribuées lors de la création de la base de données :

```
$dbhost = 'localhost';
```

```
$dbname = 'dcim';
```

```
$dbuser = 'dcim';
```

```
$dbpass = 'dcimpassword';
```

III.8.4. Redémarrer le service Apache

```
[azizjlll@localhost ~]$ systemctl redémarre httpd.service
```

Conclusion

Dans ce chapitre, la création de la machine virtuelle, l'installation de CentOS 7 et l'installation d'OpenDCIM sont des étapes essentielles pour mettre en place un environnement efficace de gestion des données et des infrastructures, offrant ainsi une solution complète et optimisée pour les entreprises.

CHAPITRE 3 : **Réalisation et validation**

Introduction

L'objectif de cette partie est de mettre en place une solution DCIM open-source pour le centre des données du CERT

I. Configuration les composant de data centre

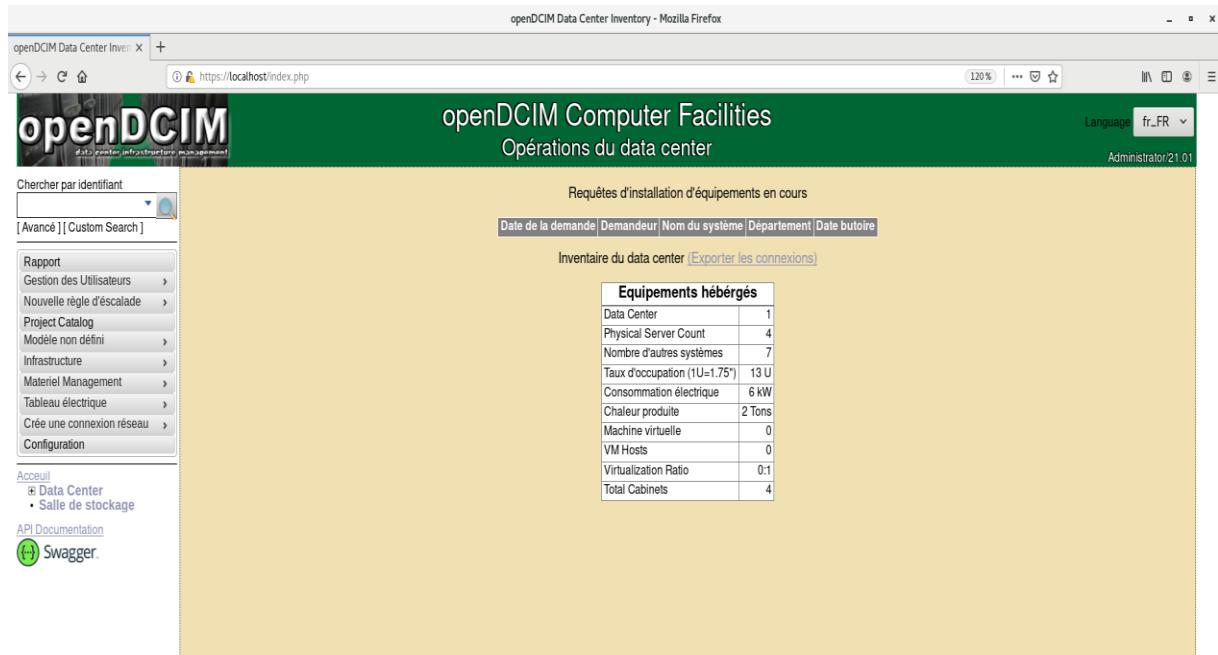


Figure 39: Interface Principale d'openDCIM

I.1. Edition de Data centre

On ajoute un centre de données dans OpenDCIM pour gérer l'inventaire physique de tous les équipements et ressources informatiques présents dans le centre de données. Cela permet de garder une trace de tous les actifs physiques, tels que les serveurs, les commutateurs, les routeurs, les câbles, les panneaux électriques, etc.

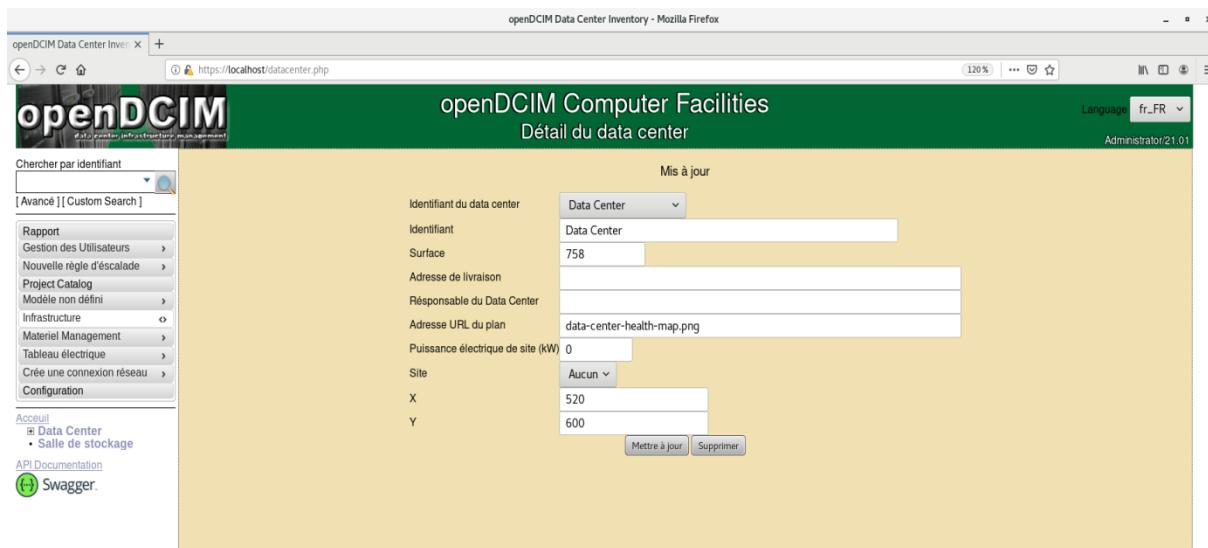


Figure 40: Détaille du centre de donnée

- Identifiant du data center: C'est un identifiant unique attribué à un centre de données spécifique pour faciliter son suivi et son identification.
- Identifiant: C'est un identifiant unique attribué à une ressource spécifique dans OpenDCIM pour faciliter son suivi et son identification.
- Surface: Il s'agit de la surface totale du centre de données en mètres carrés.
- Adresse de livraison: C'est l'adresse à laquelle le matériel doit être livré pour être installé dans le centre de données.
- Responsable du Data Center: Il s'agit de la personne qui est chargée de la gestion et de l'exploitation du centre de données.
- Adresse URL du plan: C'est l'adresse URL où les plans détaillés du centre de données sont stockés pour référence future.
- Puissance électrique de site (kW): Il s'agit de la capacité électrique totale du centre de données en kilowatts (kW).
- Site: C'est le nom du site où le centre de données est situé.
- X: Il s'agit de la coordonnée horizontale du centre de données sur un plan ou une carte.
- Y: Il s'agit de la coordonnée verticale du centre de données sur un plan ou une carte.

I.2. Edition des salles

On ajoute des salles dans OpenDCIM pour pouvoir gérer de manière efficace l'emplacement physique de l'équipement informatique ou de réseau dans un centre de données

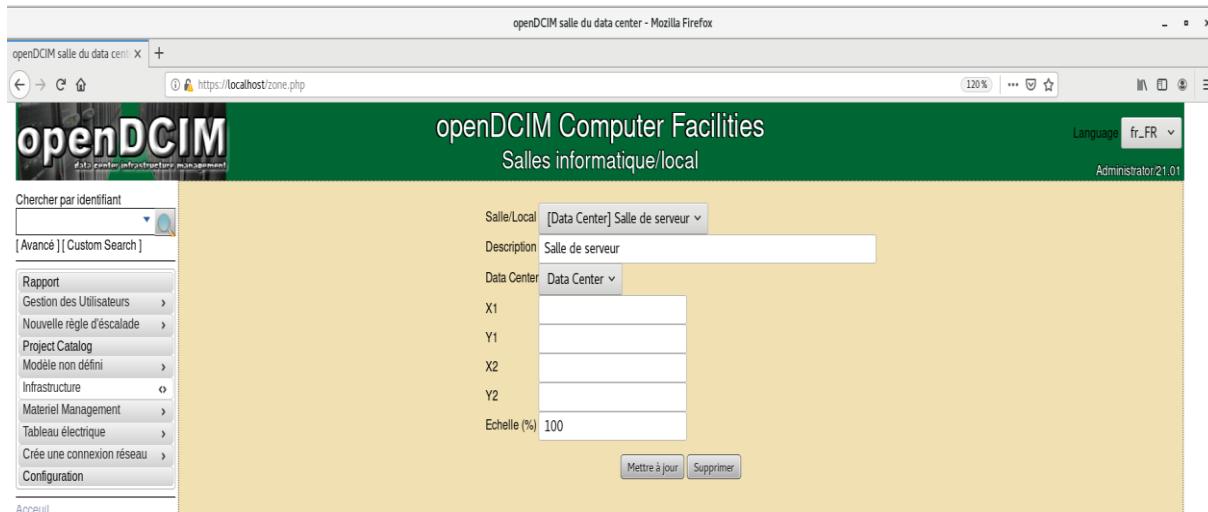


Figure 41: Infrastructure édition Salles d'informatique

- Salle/Local: Il s'agit du nom de la salle ou du local dans lequel se trouve l'équipement informatique ou de réseau.
- Description: C'est une description textuelle de la salle ou du local, qui peut inclure des informations sur sa fonction ou son usage.
- Data Center: C'est le nom du centre de données dans lequel se trouve la salle ou le local.
- X1: Il s'agit de la coordonnée horizontale du coin supérieur gauche de la salle ou du local sur un plan ou une carte.
- Y1: Il s'agit de la coordonnée verticale du coin supérieur gauche de la salle ou du local sur un plan ou une carte.
- X2: Il s'agit de la coordonnée horizontale du coin inférieur droit de la salle ou du local sur un plan ou une carte.
- Y2: Il s'agit de la coordonnée verticale du coin inférieur droit de la salle ou du local sur un plan ou une carte.
- Échelle (%): C'est la proportion de la taille réelle de la salle ou du local par rapport à sa représentation sur le plan ou la carte, exprimée en pourcentage.

I.3. Edition de travée

On ajoute des travées dans OpenDCIM pour pouvoir organiser de manière logique et efficace les armoires et le matériel informatique dans une salle de centre de données.

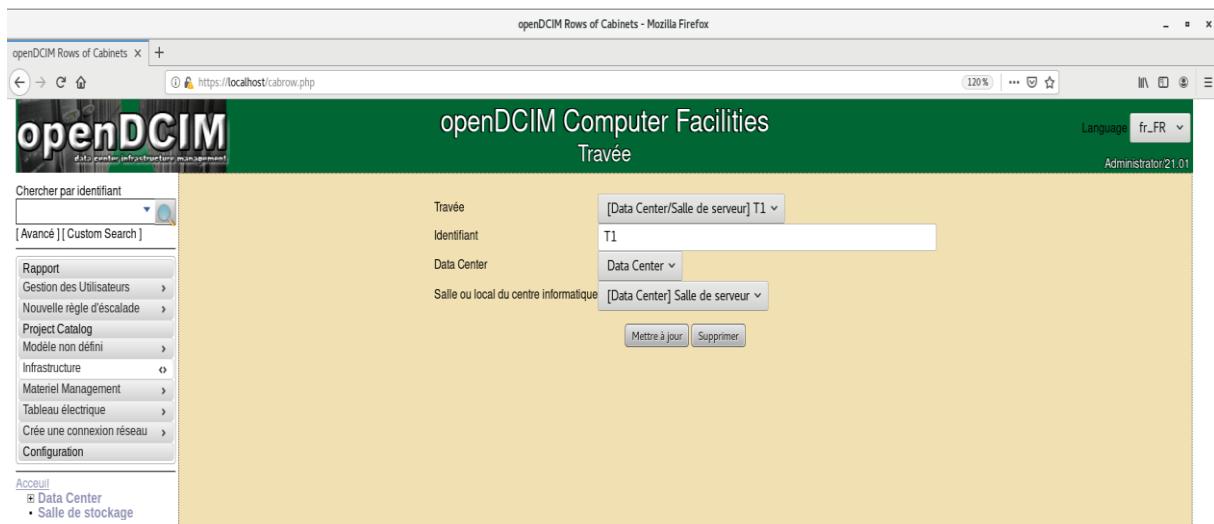


Figure 42 : Infrastructure édition Travée

- Travée : une rangée d'armoires adjacentes dans une salle de centre de données.
- Identifiant : un numéro unique utilisé pour identifier de manière univoque une travée dans OpenDCIM.
- Data Center : un site qui héberge des équipements informatiques et de stockage de données. Il s'agit généralement d'une installation spécialement conçue pour fournir un environnement contrôlé et sécurisé pour ces équipements.
- Salle ou local du centre informatique : une pièce spécifique dans un centre de données qui abrite des armoires et de l'équipement informatique. Les salles de centre informatique sont généralement équipées de systèmes de refroidissement, d'alimentation électrique et de sécurité pour assurer le bon fonctionnement de l'équipement et la sécurité des données qu'il contient.

I.4. Edition de baies

On ajoute les baies dans OpenDCIM pour gérer efficacement l'emplacement et l'utilisation des équipements dans le centre de données.

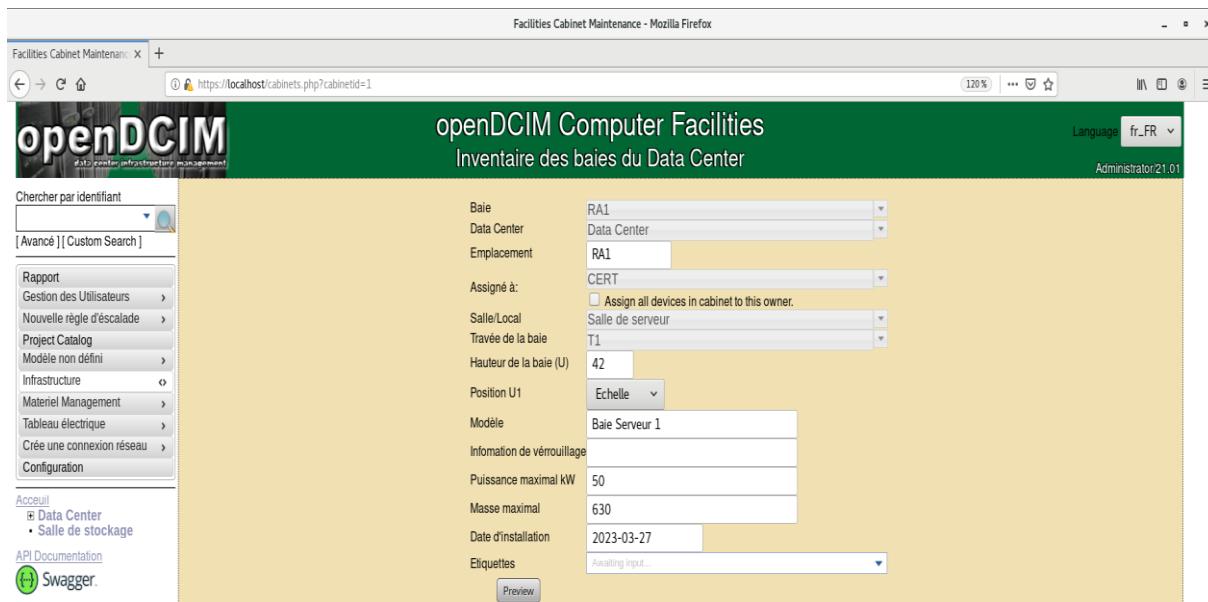


Figure 43: Infrastructure édition de baies

- Baie : une armoire de centre de données dans laquelle les équipements informatiques et de stockage de données sont installés.
- Data Center : un centre de données où se trouve la baie.
- Emplacement : l'emplacement physique de la baie dans le centre de données.
- Assigné à : le nom ou le groupe d'utilisateurs auquel la baie est assignée.
- Assign all devices in cabinet to this owner : une option pour assigner tous les équipements dans la baie au même propriétaire que la baie elle-même.
- Salle/Local : la salle ou le local du centre informatique où se trouve la baie.
- Travée de la baie : l'emplacement de la baie dans la travée.
- Hauteur de la baie (U) : la hauteur de la baie en unités (U), où une U équivaut à 1,75 pouce (4,445 cm).
- Position U1 : la position de départ de la baie en unités (U).
- Modèle : le modèle ou le type de la baie.
- Information de verrouillage : des détails sur la manière dont la baie est verrouillée et sécurisée.
- Puissance maximale en kW : la quantité maximale de puissance électrique que la baie peut consommer en kW.
- Masse maximale : la masse maximale que la baie peut supporter.
- Date d'installation : la date à laquelle la baie a été installée.

- Etiquettes : des étiquettes ou des mots-clés qui peuvent être ajoutés à la baie pour faciliter la recherche et l'organisation.

Dans le data centre de CERT il y a 4 baies

- RA1
- RA2
- RA3
- RA4

The screenshot shows the 'Inventaire des baies du Data Center' (Inventory of Data Center Racks) page. The top navigation bar includes links for 'Travée T1 :: 4 Baies :: Data Center', 'openDCIM Computer Facilities', 'Language: fr_FR', and 'Administrator(2.0.0)'. On the left, there's a sidebar with a search bar, a 'Rapport' section listing various management tasks like 'Gestion des Utilisateurs', and a navigation tree for 'Data Center' (Salle de serveur, T1, Storage Room, Salle de stockage). The main content area displays four tables representing racks RA1, RA2, RA3, and RA4. Each table has columns for 'Pos' (Position) and 'Device'. The positions range from 17 at the bottom to 42 at the top. Green diamond icons are overlaid on specific slots: slot 17 in all four racks, slot 27 in RA2, slot 37 in RA3, and slot 41 in RA1.

Figure 44: Inventaire des baies du centre de donnée

I.4.1. Configuration des équipements

- Edition de constructeur

Les constructeurs dans OpenDCIM sont utilisés pour spécifier les différentes marques et modèles d'équipements présents dans le centre de données, tels que les serveurs, les commutateurs, les routeurs, les onduleurs, les armoires, les capteurs et les câbles.

The screenshot shows the openDCIM Data Center Inventory interface in Mozilla Firefox. The title bar reads "openDCIM Data Center Inventory - Mozilla Firefox". The main content area is titled "openDCIM Computer Facilities" and "Opérations du data center". On the left, there is a sidebar with various navigation links such as "Rapport", "Gestion des Utilisateurs", "Nouvelle règle d'escalade", "Project Catalog", "Modèle non défini", "Infrastructure", "Matériel Management", "Tableau électrique", "Crée une connexion réseau", and "Configuration". Below these are links for "Accueil", "Data Center", "Salle de stockage", "API Documentation", and "Swagger". A search bar at the top says "Chercher par identifiant" with options for "Avancé" and "Custom Search". In the center, there is a table with columns "id", "name", and "grid". The table lists various manufacturers and their grid IDs. A context menu is open over the table, showing options like "Edition des modèles d'équipements", "Device Image Management", "Edition des constructeurs", and "Repository Sync". The bottom right corner of the interface shows "Administrator 21.01".

id	name	grid
3	3M	110
1	ADTRAN	80
9	APC	2
7	Cisco	11
4	Corning	68
5	Dell	18
8	Eaton	19
11	Generic	1
2	HP	26
10	Huawei	70
6	Legrand	50
12	QNAP	37
0	3COM	3
0	3PAR	106
0	Acer	111
0	ADC	112
0	ADIC	81
0	Alcatel	41
0	Allied Telesync	150
0	AlliedTelesis	82
0	AMP	113
0	AMP Netconnect	153
0	APEX	83
0	Apple	4
0	Archer Networks	114

Figure 45: opérations du centre de donnée

- **Edition des modèles d'équipements**

Les modèles dans OpenDCIM sont préconfigurés qui permettent aux utilisateurs de définir rapidement et facilement des propriétés communes pour les équipements de centre de données. Les templates sont utilisés pour définir des configurations d'équipements standard pour différents types d'équipements, tels que les serveurs, les commutateurs, les routeurs et les onduleurs. Les utilisateurs peuvent créer leurs propres templates pour différents types d'équipements ou utiliser les templates fournis par OpenDCIM.

Model	Height	Weight	Wattage	DeviceType	PSCount	NumPorts	FrontPictureFile	RearPictureFile	ChassisSlots	RearChassisSlots	LastModified
ARUBA 2530 24G POE+ 2SFP+ SWITCH (J9854A)	1	4	222	Switch	1	26			0	0	2016-08-02 10:22:50
ARUBA 2530-48G-POE+ 2SFP+ SWITCH (J9853A)	1	5	439	Switch	1	50			0	0	2016-08-02 10:22:53
ARUBA 3800 24SFP 2SFP+ SWITCH (J9584A)	1	7	127	Switch	1	26			0	0	2016-08-02 10:22:59
BL460C Gen 8	1	8	200	Server	0	0			0	0	2015-06-25 08:03:43
C7000 Blade Enclosure	10	110	200	Chassis	6	0			16	8	2015-06-25 08:03:27
DL370 G6	4	100	8001	Server	2	5			0	0	2015-12-16 14:05:33
J8697A 5406ZL	4	12	150	Chassis	2	0			7	0	2017-01-07 01:37:03
J9091A 8212ZL CHASSIS	9	22	150	Chassis	4	1			17	1	2017-01-07 01:40:22
J9092A ZL MGT MDL	1	10	75	Switch	0	1			0	0	2017-01-07 01:40:51
J9093A ZL FAB MDL	1	1	0	Physical Infrastructure	0	0			0	0	2017-01-07 01:41:21
J9095A ZL SUPT MDL	1	10	75	Switch	0	0			0	0	2017-01-07 01:41:47
J9534A ZL 24P GIG-T POE+	1	15	225	Switch	0	24			0	0	2017-01-07 01:44:39
J9536A ZL 20P GT POE+/2P SFP	1	15	225	Switch	0	22			0	0	2017-01-07 01:45:52
KVM8A-SM-02-I2C	1	25	440	Accessory	0	0			0	0	2017-01-07 01:46:55

Figure 46 : édition des modèles d'équipements

Dans le cas de CERT on utilise les équipements suivant :

- AP7721 ATS: Il s'agit d'un commutateur de transfert automatique (ATS) produit par la marque APC. L'ATS permet de connecter deux sources d'alimentation distinctes à un équipement, et de basculer automatiquement d'une source à l'autre en cas de panne de courant.
- PROCURVE 2610-24 SWITCH (J9085A): Il s'agit d'un commutateur réseau produit par la marque HP (maintenant connue sous le nom de HPE). Le ProCurve 2610-24 est un commutateur Ethernet géré qui offre des fonctionnalités de base telles que la gestion de la qualité de service (QoS), la sécurité des ports, la configuration VLAN et la prise en charge du protocole Spanning Tree.
- POWEREDGE R630: Il s'agit d'un serveur en rack produit par la marque Dell. Le PowerEdge R630 est un serveur hautes performances qui peut être configuré pour prendre en charge une variété de charges de travail, telles que les bases de données, la virtualisation et l'analyse de données.
- PROLIANT DL360 GEN8: Il s'agit d'un serveur en rack produit par la marque HP (maintenant connue sous le nom de HPE). Le ProLiant DL360 Gen8 est un serveur hautes performances conçu pour les environnements d'entreprise qui exigent des performances et une fiabilité élevées.

- **16P LC DUPLEX FIBER:** Il s'agit d'un panneau de brassage en fibre optique qui offre 16 ports LC duplex pour la connectivité des câbles à fibre optique. Les ports LC sont des connecteurs de fibre optique couramment utilisés pour les applications Ethernet à haute vitesse.
- **Ajouter les équipements**

Figure 47: configuration des équipements

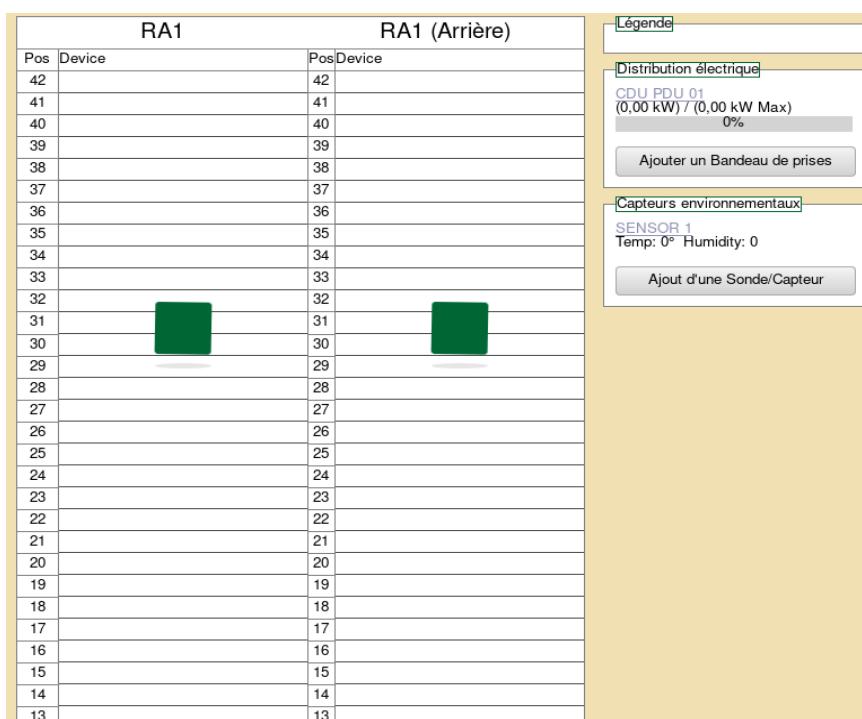
- **N° d'identification logiciel :** Il s'agit d'un numéro d'identification unique attribué au logiciel OpenDCIM.
- **Statut :** Cela indique l'état actuel de l'équipement dans le centre de données. Par exemple, si l'équipement est en ligne ou hors ligne.
- **Identifiant :** Il s'agit d'un numéro d'identification unique attribué à chaque équipement dans le centre de données.
- **Numéro de série :** C'est le numéro de série unique attribué à l'équipement par le fabricant.
- **Numéro d'inventaire :** Il s'agit d'un numéro d'identification unique attribué à l'équipement dans le système d'inventaire du centre de données.
- **IP principal :** Il s'agit de l'adresse IP principale associée à l'équipement.

- Date de fabrication : C'est la date à laquelle l'équipement a été fabriqué.
- Date d'installation : C'est la date à laquelle l'équipement a été installé dans le centre de données.
- Entreprise effectuant la garantie : Il s'agit de l'entreprise qui fournit la garantie pour l'équipement.
- Date d'expiration de la garantie : C'est la date à laquelle la garantie de l'équipement expire.
- Infrastructure physique : Cela décrit la configuration physique de l'équipement dans le centre de données, y compris son emplacement et sa hauteur.
- Baie : Il s'agit de l'emplacement physique de l'équipement dans la baie du centre de données.
- Référence de l'équipement : C'est la référence unique attribuée à l'équipement par le fabricant.
- Hauteur : C'est la hauteur physique de l'équipement dans la baie du centre de données.
- Position : C'est la position physique de l'équipement dans la baie du centre de données.
- Demie profondeur : Il s'agit de la demi-profondeur physique de l'équipement dans la baie du centre de données.
- Face arrière : C'est le côté arrière de l'équipement.
- Nombre de ports réseaux : Il s'agit du nombre de ports réseau disponibles sur l'équipement.
- Puissance nominale : C'est la puissance nominale de l'équipement.
- Charge : C'est la charge actuelle de l'équipement.
- Connexions électriques : Il s'agit des connexions électriques de l'équipement.
- Type d'équipement : Cela décrit le type d'équipement, tel que serveur, commutateur réseau, etc.
- SNMP Configuration : Simple Network Management Protocol (SNMP) est un protocole de gestion de réseau qui permet de collecter des informations sur les équipements du réseau. La configuration SNMP permet de configurer le protocole SNMP sur l'équipement.
- Version SNMP : Il s'agit de la version de SNMP utilisée pour la configuration.
- Communauté SNMP (Lecture seul) : C'est un mot de passe utilisé pour accéder aux informations de l'équipement via SNMP en mode lecture
-

- **Ajouter bandeau de prises CDU**

On ajoute des bandeaux de prise et des sondes/capteurs dans OpenDCIM pour surveiller

l'utilisation de l'alimentation électrique et la température de l'environnement dans le centre de données. Les bandeaux de prise sont des dispositifs qui sont connectés à des équipements électroniques tels que des serveurs, des commutateurs et des routeurs, et qui mesurent la consommation d'énergie de ces équipements. Les sondes/capteurs mesurent quant à eux la température, l'humidité et d'autres paramètres environnementaux dans le centre de données.



- **Connexions de réseau**

Les connexions réseau dans OpenDCIM est important car cela permet de collecter des informations sur les équipements réseau tels que les serveurs, les commutateurs et les routeurs. Ces informations peuvent être utilisées pour surveiller l'état des équipements et pour aider à diagnostiquer les problèmes qui peuvent survenir.

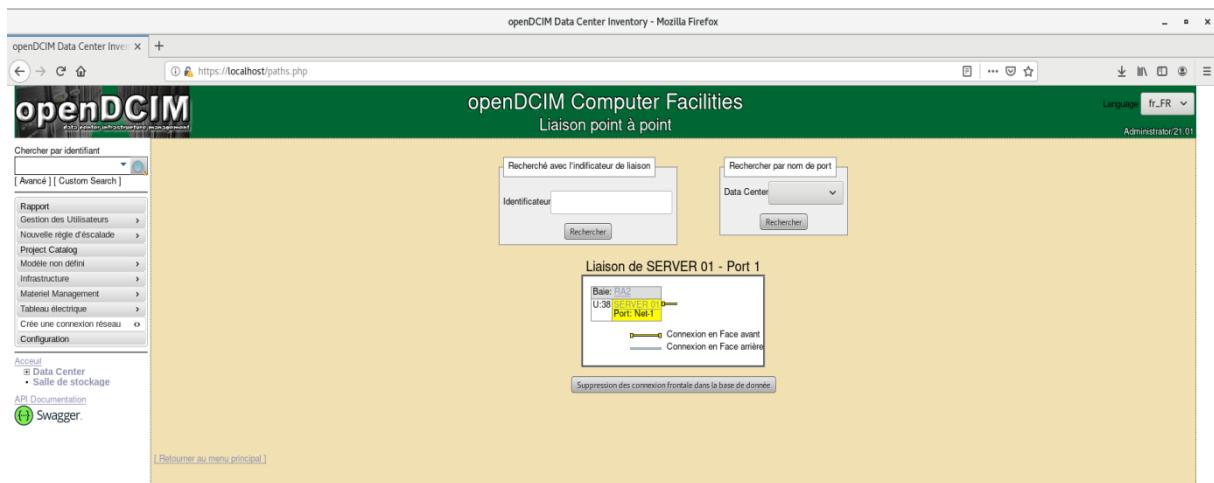


Figure 48: les connexions de réseau

I.5. Configuration d'alimentation

On ajoute tableau électrique d'un data centre dans openDCIM pour fournir une source d'alimentation électrique fiable, contrôlée et sécurisée pour les équipements informatiques qui y sont installés. Le tableau électrique permet de distribuer l'alimentation électrique provenant de l'alimentation principale du bâtiment ou de l'installation vers les équipements du centre de données.

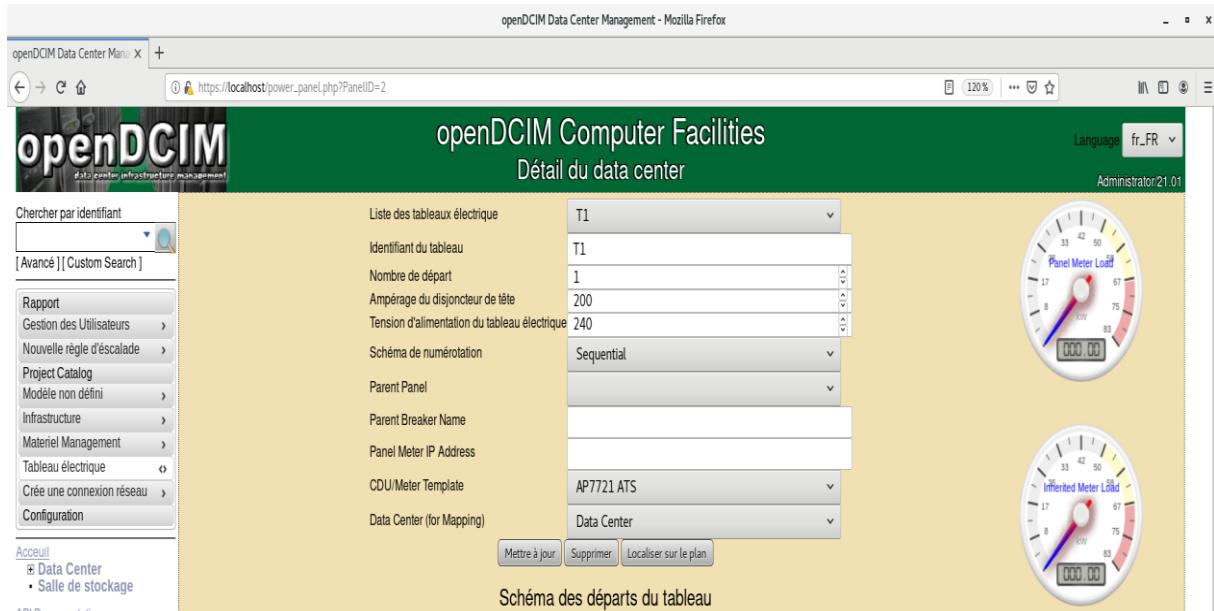


Figure 49: configuration de tableau électrique

- Liste des tableaux électriques: une liste de tous les tableaux électriques présents dans un centre de données.

- Identifiant du tableau: un numéro ou un nom unique attribué à un tableau électrique pour l'identifier de manière univoque dans le centre de données.
- Nombre de départ: le nombre total de départs électriques, c'est-à-dire le nombre d'équipements informatiques ou d'autres appareils connectés au tableau électrique.
- Ampérage du disjoncteur de tête: l'ampérage maximal du disjoncteur principal du tableau électrique, qui détermine la quantité d'énergie électrique que le tableau électrique peut fournir.
- Tension d'alimentation du tableau électrique: la tension électrique d'alimentation fournie au tableau électrique, généralement en volts (V).
- Schéma de numérotation: le schéma de numérotation utilisé pour identifier les départs électriques individuels dans le tableau électrique, qui peut inclure des numéros, des lettres ou d'autres symboles.
- Parent Panel: le tableau électrique parent auquel le tableau électrique est connecté, s'il y en a un. Cela peut être important pour suivre la source d'alimentation électrique dans le centre de données.
- Parent Breaker Name: le nom du disjoncteur parent ou du fusible connecté au tableau électrique, s'il y en a un.
- Panel Meter IP Address: l'adresse IP du compteur électrique ou du dispositif de surveillance connecté au tableau électrique pour surveiller la consommation d'énergie électrique.
- CDU/Meter Template: le modèle de distribution de courant ou le modèle de compteur utilisé dans le tableau électrique pour surveiller et contrôler la distribution de l'énergie électrique.
- Data Center (for Mapping): le nom ou l'identifiant du centre de données dans lequel le tableau électrique est situé, utilisé pour cartographier les équipements électriques dans le centre de données.

II. Les rapports d'openDCIM

Les rapports dans OpenDCIM sont utiles pour fournir des informations détaillées sur les ressources du centre de données. Ils permettent de générer des rapports sur les données de l'inventaire, les allocations des ressources, les connexions de réseau et les consommations d'énergie.

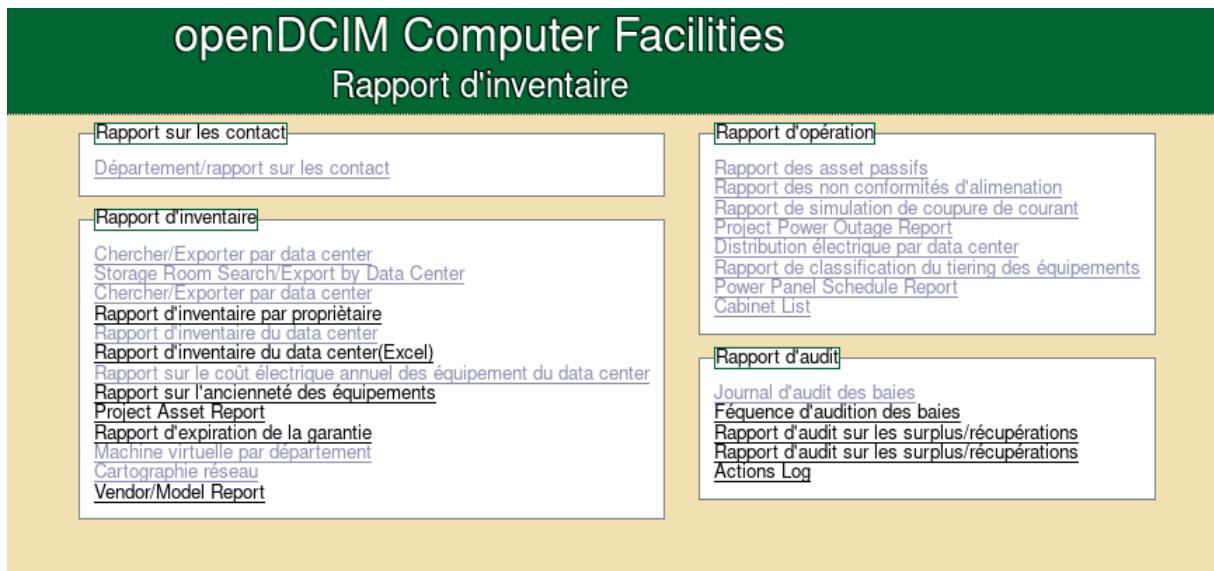


Figure 50: Rapport d'inventaire

- Rapport sur les contact :
- Département/rapport sur les contacts : un rapport qui répertorie les contacts pour chaque département du centre de données.
- Rapport d'inventaire :
- Chercher/Exporter par data center : une fonctionnalité qui permet de filtrer les équipements par centre de données et d'exporter les résultats de la recherche.
- Storage Room Search/Export by Data Center : une fonctionnalité qui permet de chercher et d'exporter les équipements stockés dans une salle de stockage spécifique pour un centre de données donné.
- Rapport d'inventaire par propriétaire : un rapport qui répertorie les équipements par propriétaire.
- Rapport d'inventaire du data center : un rapport qui répertorie tous les équipements d'un centre de données donné.
- Rapport d'inventaire du data center (Excel) : un rapport d'inventaire du centre de données qui peut être exporté au format Excel.
- Rapport sur le coût électrique annuel des équipements du data center : un rapport qui calcule le coût annuel de l'électricité pour les équipements du centre de données.
- Rapport sur l'ancienneté des équipements : un rapport qui répertorie l'âge de chaque équipement du centre de données.
- Project Asset Report : un rapport qui répertorie tous les équipements liés à un projet donné.

- Rapport d'expiration de la garantie : un rapport qui répertorie les équipements dont la garantie va bientôt expirer ou qui a expiré.
- Machine virtuelle par département : un rapport qui répertorie toutes les machines virtuelles par département.
- Cartographie réseau : une carte qui montre la topologie du réseau du centre de données.
- Vendor/Model Report : un rapport qui répertorie tous les équipements par fournisseur/modèle.
- Rapport d'opération :
- Rapport des asset passifs : un rapport qui répertorie tous les équipements passifs d'un centre de données, tels que les câbles, les connecteurs, les panneaux de brassage, les étagères, etc.
- Rapport des non conformités d'alimentation : un rapport qui répertorie tous les équipements du centre de données qui ne sont pas conformes aux normes de puissance ou de voltage.
- Rapport de simulation de coupure de courant : un rapport qui simule les conséquences d'une panne d'alimentation sur le centre de données, en fournissant des informations sur les équipements affectés, le temps de récupération, etc.
- Project Power Outage Report : un rapport qui répertorie tous les équipements affectés par une panne d'alimentation sur un projet spécifique.
- Distribution électrique par data center : un rapport qui montre la façon dont l'alimentation électrique est distribuée dans un centre de données, y compris les circuits électriques, les panneaux de distribution, les disjoncteurs, les prises, etc.
- Rapport de classification du tiering des équipements : un rapport qui classe les équipements en fonction de leur importance pour le fonctionnement du centre de données, selon les normes de classification tier (Tier 1 à Tier 4).
- Power Panel Schedule Report : un rapport qui répertorie tous les équipements connectés à chaque panneau électrique dans le centre de données, ainsi que leur emplacement.
- Cabinet List : une liste de tous les cabinets de serveurs dans le centre de données, avec des informations sur leur emplacement, leur capacité, leur utilisation, etc.

Data Center	Emplacement	Position	Hauteur	Identifiant	Numéro de série	IP principal	Type d'équipements	Modèle	Etiquettes	Propriétaire	Contact principal	Date d'expiration de la garantie	Date d'installation	Device Status	Demie profondeur	Face arrière	Hyperviseur
Data Center	RA1	0	0	SENSOR_1			Sensor	AP9312TH - PROBE		CERT	Non assigné	1970-01-01	2023-05-02	Reserved	0	0	None
Data Center	RA1	1	1	BANDE DE BRESSIONAGE			Physical Infrastructure	16P LC DUPLEX FIBER		CERT	Non assigné	1970-01-01	2023-04-19	Reserved	1	1	None
Data Center	RA1	39	1	SERVER			Server	PROLIANT DL380 GEN8		CERT	Non assigné	1970-01-01	2023-04-27	Reserved	0	0	None
Data Center	RA1	40	1	PDU_01			CDU	AP7721 ATS		CERT	Non assigné	1970-01-01	2023-04-24	Reserved	0	0	None
Data Center	RA2	0	1	SERVER_03			Server	POWEREDGE R630		CERT	Non assigné	1970-01-01	2023-04-25	Reserved	0	0	None
Data Center	RA2	0	0	SENSOR_2			Sensor	AP9312TH - PROBE			Non assigné	1970-01-01	2023-05-02	Reserved	0	0	None
Data Center	RA2	36	1	SERVER_02			Server	POWEREDGE R630			Non assigné	1970-01-01	2023-04-25	Reserved	0	0	None
Data Center	RA2	38	1	SERVER_01			Server	POWEREDGE R630			Non assigné	1970-01-01	2023-04-25	Reserved	0	0	None
Data Center	RA2	42	1	PDU			CDU	AP7721 ATS			Non assigné	1970-01-01	2023-04-27	Reserved	0	0	None
Data Center	RA3	0	1	SWITCH_2			Switch	PROCURVE 2610-24 SWITCH [JS065A]			Non assigné	1970-01-01	2023-04-27	Reserved	0	0	None

Figure 51 : Gestion de centre de donnée

Conclusion

Dans ce chapitre nous avons abordé la configuration des composants d'un centre de données, y compris l'édition du data centre, des salles, des travées et des baies. Nous avons également examiné la configuration des équipements et de l'alimentation, ainsi que les rapports générés par openDCIM.

Conclusion générale

L'installation d'une solution open-source DCIM (Data Center Infrastructure Management) pour le centre de données du CERT (Computer Emergency Response Team) présente de nombreux avantages et opportunités. Tout d'abord, cette solution permet une gestion efficace de l'infrastructure du centre de données, en fournissant une visibilité complète sur les équipements, les connexions et les ressources disponibles.

En utilisant une solution open-source, le CERT peut bénéficier de la flexibilité et de l'évolutivité offertes par une communauté active de développeurs et d'utilisateurs. Cela permet d'adapter et de personnaliser la solution en fonction des besoins spécifiques du CERT, sans dépendre d'un fournisseur propriétaire.

De plus, la mise en place d'un DCIM open-source peut contribuer à réduire les coûts liés à l'acquisition de licences logicielles. Les solutions open-source sont généralement disponibles gratuitement ou à un coût moindre, ce qui permet au CERT d'allouer ses ressources financières à d'autres domaines critiques.

L'utilisation d'une solution DCIM dans un centre de données est essentielle pour optimiser les performances, améliorer l'efficacité énergétique, prévenir les pannes et assurer la continuité des opérations. Grâce à la gestion centralisée de l'infrastructure, le CERT peut surveiller et contrôler tous les aspects du centre de données, garantissant ainsi un environnement fiable et sécurisé pour ses opérations.

En conclusion, l'installation d'une solution open-source DCIM est une décision stratégique pour le CERT, offrant une gestion efficace, une personnalisation flexible et une réduction des coûts. Cela renforce la capacité du CERT à répondre rapidement et efficacement aux incidents de sécurité informatique, tout en optimisant les performances de son centre de données.

Références bibliographiques et webographies

- [1] <http://www.cert.tn/>, consulté le 27/05/2023
- [2] <https://www.deltaww.com/en-US/products/Data-Center-Infrastructure/ALL/>
consulté le 22/02/2023
- [3] <http://www.tiaonline.org/> consulté le 150/03/2023
- [4] 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public
Information consulté le 28/04/2023
- [5] <https://kinsta.com/fr/blog/types-de-cloud-computing/> consulté le 19/04/2023

Résumé

Le présent travail s'inscrit dans le cadre de projet de fin d'études pour l'obtention du diplôme en licence de technologies de l'information et de la communication. Le rapport présente une étude sur la conception et la réalisation d'un data center à l'aide d'OpenDCIM. Il commence par une introduction générale qui présente l'organisme d'accueil, le Centre d'Études et de Recherche des Télécommunications, ainsi que les objectifs du projet. Ensuite, il explore les concepts de base des data centers, y compris leurs composants, leurs caractéristiques et leur topologie. Le chapitre suivant se concentre sur la création d'une machine virtuelle, l'installation de CentOS 7 et l'installation d'OpenDCIM. Enfin, le chapitre de réalisation aborde la configuration des composants du data center et la génération de rapports à l'aide d'OpenDCIM.

Mots clés : Centre de données/Gestion/Virtualisation/Cloud/Réseaux/Data-Center InfrastructureManagement(DCIM)/Racks/Câblage/Capacité/Conception/Installation/Configuration/Intégration

Abstract

This project report presents a study on the design and implementation of a data center using OpenDCIM as part of a final year project to obtain a degree in Information and Communication Technology. The report begins with a general introduction, introducing the hosting organization, the Center for Telecommunications Studies and Research, and outlining the project objectives. It then explores the fundamental concepts of data centers, including their components, characteristics, and topology. The subsequent chapter focuses on creating a virtual machine, installing CentOS 7, and deploying OpenDCIM. Lastly, the implementation chapter covers the configuration of the data center components and the generation of reports using OpenDCIM.

Keywords: Datacenter, Management, Virtualization,, Cloud, Networks,, DataCenter InfrastructureManagement(DCIM), Racks, Cabling, Capacity, Design, Installation, Configuration, Integration.